Connecting the Indo-Pacific:

The future of subsea cables and opportunities for Australia

JOCELINN KANG
DR JESSIE JACOB

SEPTEMBER 2024

Policy Brief

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

About the authors

Jocelinn Kang is a technical specialist with Cyber, Technology and Security at ASPI.

Dr Jessie Jacob is a senior analyst with Cyber, Technology and Security at ASPI on secondment from the Australian government.

Acknowledgements

ASPI acknowledges the Ngunnawal and Ngambri peoples, who are the traditional owners of the land upon which this work was prepared. We pay our respects to Elders past and present.

We would like to thank all those who contributed to the development and completion of this report. We'd like to extend our deepest appreciation to the cable owner-operators and suppliers, telecom carriers, representatives from the International Cable Protection Committee, policymakers and government representatives, security experts and academics from Australia, Canada, France, Japan, the Philippines, Taiwan, the Kingdom of the Netherlands, the United States and the Pacific for their expert insights and knowledge of the industry, which directly informed much of the analysis presented here. We're also grateful to Danielle Cave, Bart Hogeveen, Alex Caples, Mike Bareja, Daria Impiombato, Chris Taylor and reviewers from the Australian Government and industry as well as anonymous reviewers for their invaluable feedback and help to refine this report's content and focus. Finally, we'd like to thank Justin Bassi and Byron Illyes, for their expertise and enthusiasm on the matter.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality and innovation, quality and excellence, and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the authors and should not be seen as representing the formal position of ASPI on any particular issue.

ASPI Cyber, Technology and Security

ASPI's Cyber, Technology and Security (CTS) analysts inform policy debates in the Indo-Pacific through original, rigorous and data-driven research. CTS is a leading voice in global debates on cyber, emerging and critical technologies, foreign interference and issues related to information operations and disinformation. CTS has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building and internet safety, satellite analysis, surveillance and China-related issues. To develop capability in Australia and across the Indo-Pacific region, CTS has a capacity-building team that conducts workshops, training programs and large-scale exercises for the public, private and civil-society sectors.

CTS enriches regional debate by collaborating with civil-society groups from around the world and by bringing leading global experts to Australia through our international fellowship program. We thank all of those who support and contribute to CTS with their time, intellect and passion for the topics we work on.

If you would like to support the work of the CTS, contact: ctspartnerships@aspi.org.au.

Funding

No specific funding was received to produce this report.

Cover image: iStockphoto/da-kuk.

Connecting the Indo-Pacific:

The future of subsea cables and opportunities for Australia

JOCELINN KANG
DR JESSIE JACOB

SEPTEMBER 2024

Policy Brief

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

First published September 2024

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel Canberra + 61 2 6270 5100
Tel Washington DC +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

 Facebook.com/ASPI.org

 @ASPI_org

Contents

Key insights

- The submarine cable landscape has entered a new era and is now shaped by the rising participation of hyperscalers —hyperscale cloud and content providers— as well as the strategic actions of major powers and minilateral groups. This new environment in the Indo-Pacific presents new risks that need to be managed, but also new opportunities, particularly for nations like Australia.
- The proliferation of submarine data cables (subcables) traversing the Indo-Pacific is opening up unparalleled information access, communication and technological opportunities. They're the fastest, most cost-efficient and highest capacity means to transport data globally and are essential to support the growth of cloud-based services and critical technologies such as artificial intelligence (AI).
- US-based hyperscalers—in particular Google, Meta, Microsoft and Amazon—have an increasing influence on the subcable industry that hasn't yet been fully recognised or seriously considered. These hyperscalers account for the majority of total submarine cable capacity usage, with that share continuing to grow. This means that an increasing portion of the world's data is under the stewardship of only a few entities, making the availability of that data highly dependent on their seamless operation. Such a concentration creates a digital supply-chain dependency risk, where potential disruptions could lead to widespread consequences. Additionally, as their bandwidth needs increase, hyperscalers are transitioning from being primary customers of network capacity to owning and operating subcable systems. As a result, they are managing even more of the 'internet services stack'—content services, data centres and now network transport. This further compounds the dependency risk and the consolidation of control raises concerns about the principle of an open internet.
- The increasing presence of hyperscalers is occurring at a time of heightened political tension between major powers the US and China, and that tension is most acute in the Indo-Pacific. The control of data, in this case manifested in the routing, laying, landing and repair of subcables, has been used as one of many stages for political signalling. The geopolitical competition surrounding submarine cables poses challenges to national security, subcables supply-chain resilience, connectivity, and data infrastructure, particularly in regions like the Indo-Pacific, where countries must carefully navigate the evolving digital landscape.
- Australia is well positioned to secure its emerging role as a regional digital hub for subcables, and AI and cloud-data centres in the Indo-Pacific. With more strategic focus, it could capitalise on this new environment of increased subcable connectivity and digital investments by leveraging its digital infrastructure to offer alternative routes for global data traffic, helping to foster better regional connectivity.
- Australia's potential can be maximised through decisive action and decisions that would help improve regional subcable resilience and digital connectivity, including its own. This report makes five key recommendations, including that the Australian Government supports and strengthens regional repair and maintenance capabilities, ensuring that the management and protection of cables remains best practice, while continuing to work with regional partners to shape the regulatory norms and standards of the region.
- To manage risks to Australia's data security and digital economy ambitions, this report also recommends that the Australian Government engages more closely with industry, makes potential regulatory adjustments, and maintains strategic oversight and vigilance to digital supply-chain dependency risks and anticompetitive behaviour. Not only will those measures build connectivity and resilience domestically and regionally, but they align with Australia's foreign-policy, development, security and cyber objectives, and will also support Australia's growth and attractiveness as a subcables hub.

Introduction

Amid the ongoing global digital transformation, the submarine telecommunications cable network has grown from 130 cables in 2010 to more than 550 cables today,[1] reflecting subcables' critical and leading role in global communications. Submarine cables are the fastest and most cost-efficient means to transport data internationally, with a capacity that far surpasses satellites.[2] They carry 99% of transoceanic public internet and private network data traffic,[3] facilitating global economic and financial activity as well as government and military communications and operations.

The exponential increase in demand for data transmission bandwidth is the primary driver behind the proliferation of subcables. The following factors cumulatively contribute to that demand:

1. the widespread adoption of cloud-based services, accelerated by the Covid-19 pandemic, along with increased use of AI, which has increased the need for data centres and, consequently, created greater demand for international connectivity
2. the development of data-heavy applications and demand from digital streaming media
3. the proliferation of smart devices and access through high-capacity access networks such as 4G and 5G.

This demand for data will grow with advances such as 6G, which is expected to enter pre-commercial trial from 2028, and the uptake of emerging technologies such as holographic communications. Business analysts estimate that the global subcable system market will grow at a compound annual rate of 10.3% out to 2029.[4]

The globe's relentless demand for data has transformed the subcable landscape. Previously the domain of telecommunications carriers, today the industry is increasingly being shaped by a small group of US-based 'hyperscalers'. Hyperscale cloud and content providers bring unprecedented capital investments and control a significant portion of the internet services supply chain: content, data, storage, processing and transport.

The other contributing factor is the ongoing geopolitical competition, primarily between the US and China. That competition, and the rise of minilateral groupings, is shaping the subcable industry in the Indo-Pacific, where strategic control over data flows and infrastructure has become a critical element of national-security and economic agendas.

More fundamentally safe, secure and reliable subcable systems are the linchpin for the development, adoption and application of critical technologies. That's even more so for nations surrounded by oceans, where such infrastructure is essential to increase technological prowess and economic prosperity. Since subcables have become so integral to global connectivity and economic development, any disruptions to them can have widespread repercussions, impacting businesses, government services and public access to critical communication infrastructure. For example, in 2022, Tasmania experienced a small taste of that vulnerability, as damage to the state's two main communications subcables in two separate incidents forced businesses to close for the day.[5] That same year, the Pacific island of Tonga lost access to all communications for about five weeks when its single international subcable was severed in a volcanic eruption.[6] Similarly, Vietnam experienced major outages and network degradation due to disruptions of multiple cables in 2022; in 2023, all of its five cables were down, forcing reliance on terrestrial links for international connectivity.[7]

Outside of natural disasters, subcables are susceptible to a range of other disruptions as well. For a long time, states have expressed concerns about the potential for cables to be used for foreign interference and interception, as evidenced by the US-led Operation Ivy Bells against the Soviets in the 1970s, and more recently suspicions over the activities of the Russian intelligence ship, *Yantar*, and allegations involving India's access to a Mauritian landing station.[8] The ownership of cables can offer control that can be used for political and economic coercion; subcables concentrated in maritime choke-points, such as the Luzon Strait and Malacca Strait, and in contested waters, such as the South China Sea, are particularly vulnerable.[9]

Given those risks, subcable infrastructure is recognised as both critical infrastructure and critical information infrastructure. Ownership and control of the cables are now seen as matters of strategic, economic and intelligence interest, making them a key part of the region's geostrategic competition. Amid all of these developments, Australia is emerging as a reliable and relatively secure subcable hub for the region, attracting more hyperscale data centre and submarine cable investment. Australia is also ramping up regional cooperation and development assistance to Pacific partners to help foster a consistent and efficient subcable ecosystem for the wider region.

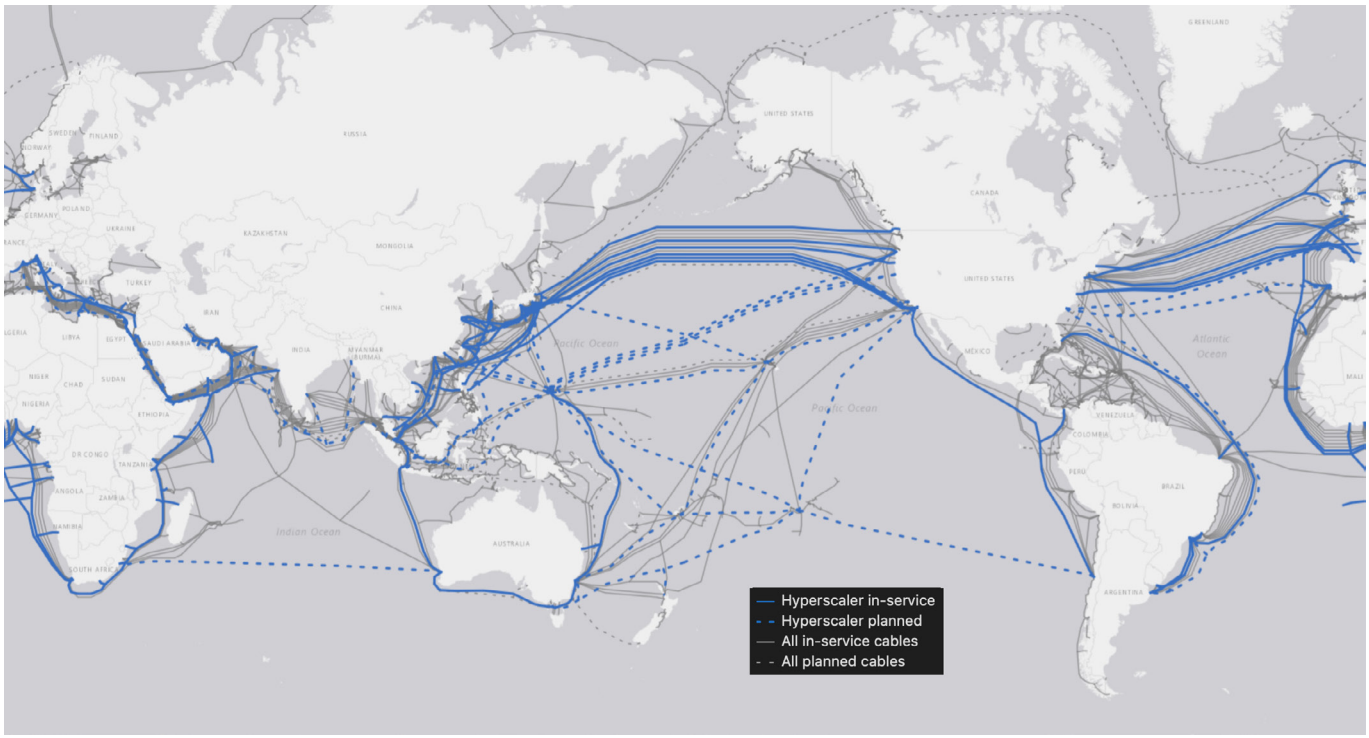
This report examines the role of hyperscalers as drivers of the subcable market and the geostrategic context of subcable systems. It highlights the significance of these developments for Australia, exploring both the potential benefits and challenges. It discusses how Australia can capitalise on those evolving dynamics to solidify its position as a regional digital hub in the Indo-Pacific and provides five key recommendations for the Australian Government to consider actioning to achieve those ends.

The evolving dynamics of the submarine cable industry

The rise of hyperscalers

The rise of hyperscalers—large cloud and content service providers such as Google, Meta, Microsoft and Amazon—has fundamentally transformed the global subcable landscape, altering both the market dynamics and the architecture of the internet (Figure 1). Those four companies reportedly account for 71% of all used international capacity—a staggering increase from less than 10% just a decade earlier.[10] Technology companies Apple, Netflix, Alibaba and Akamai use much of the remaining capacity.[11] The surge in demand for subcable capacity is a direct consequence of digital transformation across the globe, which has reshaped the internet from a federated network of networks into a more centralised system increasingly dominated by a handful of large technology giants.

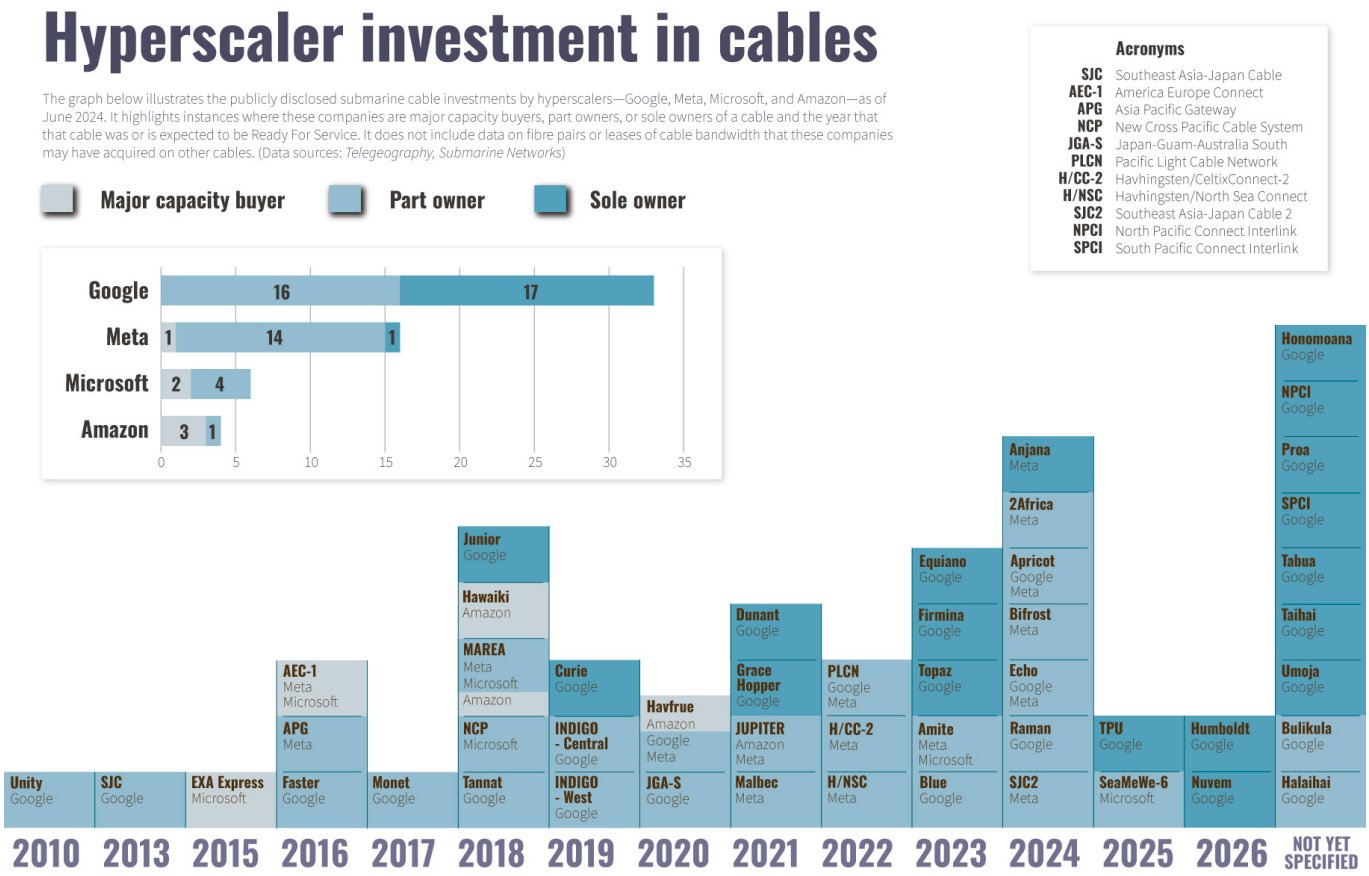
Figure 1: Hyperscaler-owned or planned cables around the world, June 2024



Source: Image created by authors using data from *TeleGeography*.

The hyperscalers have consolidated their market power by capitalising on the exponential growth in data and the pervasive 'always online' usage pattern. They're the primary drivers of the demand for hyperscale computing environments—massive, scalable infrastructures that constitute 'the cloud'. To support their expansive digital services and global networks, hyperscalers have found value in owning the network transport between their data centres. By doing so, they can exert control over the service quality and security of their networks. That's led hyperscalers to transition from being major customers of capacity to owning their own subcable systems (Figure 2). That shift reflects their broader strategy of vertical integration, which extends their control over the internet services value chain, from content creation to data storage, processing and network transport.

Figure 2: Hyperscaler submarine cable investments



Source: Image by ASPI authors, using data from *TeleGeography*, *Submarine Networks*, and ASPI research.[12]

The entry of hyperscalers into the subcable industry has disrupted traditional market structures, which were previously dominated by telecoms carriers. Hyperscalers have become key stakeholders in subcable system projects, driving 23.5% of the systems that began operation between 2019 and 2023.[13] They bring unprecedented financial resources that significantly increase the likelihood of the successful completion of projects compared to traditional ventures, in which only 52% of announced subcable systems came to completion.[14] With their financial backing as anchor investors, hyperscalers' involvement reduces financial risks for other companies that want to invest in the same cable as the hyperscalers. [15] On the other hand, as hyperscalers shift to invest in their own cables instead of being major customers of wholesale capacity, traditional wholesale telecoms carrier consortiums are facing challenges in securing anchor tenants for similar routes, threatening the viability of their projects.[16] Furthermore, suppliers of cable components are increasingly prioritising hyperscalers due to the financial certainty they bring, disadvantaging smaller players, which can struggle with more complex and fragmented funding structures.[17]

In addition to altering the competitive landscape, hyperscalers have pushed the industry to grow and evolve to meet their fast-paced, large-scale business needs. They're driving suppliers such as Japan's NEC to develop innovative ways to provide higher capacity cables.[18] Additionally, hyperscalers have introduced greater vendor competition in cable

systems equipment through their push for 'open systems', in which multiple vendors can provide equipment within a cable system, instead of a single vendor providing an end-to-end solution. They're also changing the way cables make landfall by adopting the 'open cable model' in which, instead of terminating in a cable landing station (CLS), they terminate in a data centre (or a CLS with data centre-type equipment). This is a preference for many newer cables, as they benefit from more direct interconnection with carriers, hyperscalers and enterprise customer networks.[19]

This transition to cable ownership means that hyperscalers are increasingly deciding where cables land, reshaping the architecture of the global subcable network. Whereas the subcable industry once connected population centres (cities where the interconnection points with terrestrial networks were usually located), hyperscalers are building out routes between data centres (which are located where there's sufficient space and power for their hyperscale data centre facilities). Those new and diverse routes as well as the resulting new CLS locations, introduces greater resilience to the global network, which is crucial as the demand for bandwidth continues to grow.

As hyperscalers have extended their control over subcable infrastructure, significant implications for data security have emerged. While constructing and owning a subcable doesn't inherently mean controlling all the fibre pairs within the cable (and therefore all the data that flows through it), the growing trend of extensive bandwidth use by hyperscalers of global network capacity raises critical concerns about the concentration of data, including sensitive data under the stewardship of a few entities. This digital supply-chain dependency risk, coupled with the volume of data that hyperscalers control across multiple layers of the internet services stack heightens the risk of a single point of failure. A compromise of their digital assets or networks—whether through malicious attacks or accidental failures—could lead to widespread disruptions, undermining the resilience of global communications.

This consolidation of control of the internet services stack also poses threats to the principle of an open internet, where all content and services are equally accessible without preferential treatment. Hyperscalers, which control both connectivity and content, might prioritise their own services, thereby limiting consumer choice and undermining competition. That consolidation of control also poses a broader challenge to national sovereignty, as it heightens the vulnerability of nations to the strategic interests of those powerful corporations. The balance of power is increasingly shifting towards those that can harness and leverage advanced technologies, and tech giants are at the forefront of that transformation. This shift in power dynamics means that governments must engage more directly with those entities and work together to balance commercial interests with safeguarding national interests.

Moreover, the rise of hyperscalers isn't just a commercial phenomenon; it's deeply intertwined with geopolitical considerations. These companies operate within a complex political–strategic context. On the one hand, they want to make sure they continue to comply with rules and regulations and position themselves as trusted vendors globally. On the other hand, we're seeing these US companies align with US strategic interests in the subcable industry. While not new or unique to the US (for example, the Australian Government-backed purchasing of Digicel Pacific in 2022),[20] it is important to remember that the hyperscalers are not immune to geopolitics. For example, in 2021, in a move that secured a landing for the Pacific Light Cable Network, Google and Meta were party to a national-security agreement with the US Department of Justice,[21] agreeing to shut out their China-associated partner and 'pursue diversification of interconnection points in Asia, including but not limited to Indonesia, Philippines, Thailand, Singapore and Vietnam'.[22] Since then, Google has announced the planned development of a web of cables through the Pacific between the US, Northeast Asia, Australia and South America as part of its Pacific Connect Initiative. Those cables are being leveraged by the US and allies Japan and Australia to build subcable connectivity and redundancy for Pacific island countries.[23] Government or multinational development bank funding is typical for cables in this region, as low-population countries generate little traffic demand and therefore such projects often aren't commercially viable.

As hyperscalers continue to expand their global network of data centres and subcables, their role in the industry is likely to remain prominent. They expect sustained demand for subcable investments, but the exact rate of growth remains uncertain, as they struggle to forecast beyond a two- to three-year horizon.[24] Nonetheless, the impact of hyperscalers on the global subcable ecosystem is undeniable, and their influence is reshaping both the physical and digital landscapes of global connectivity.

The effects of geostrategic competition

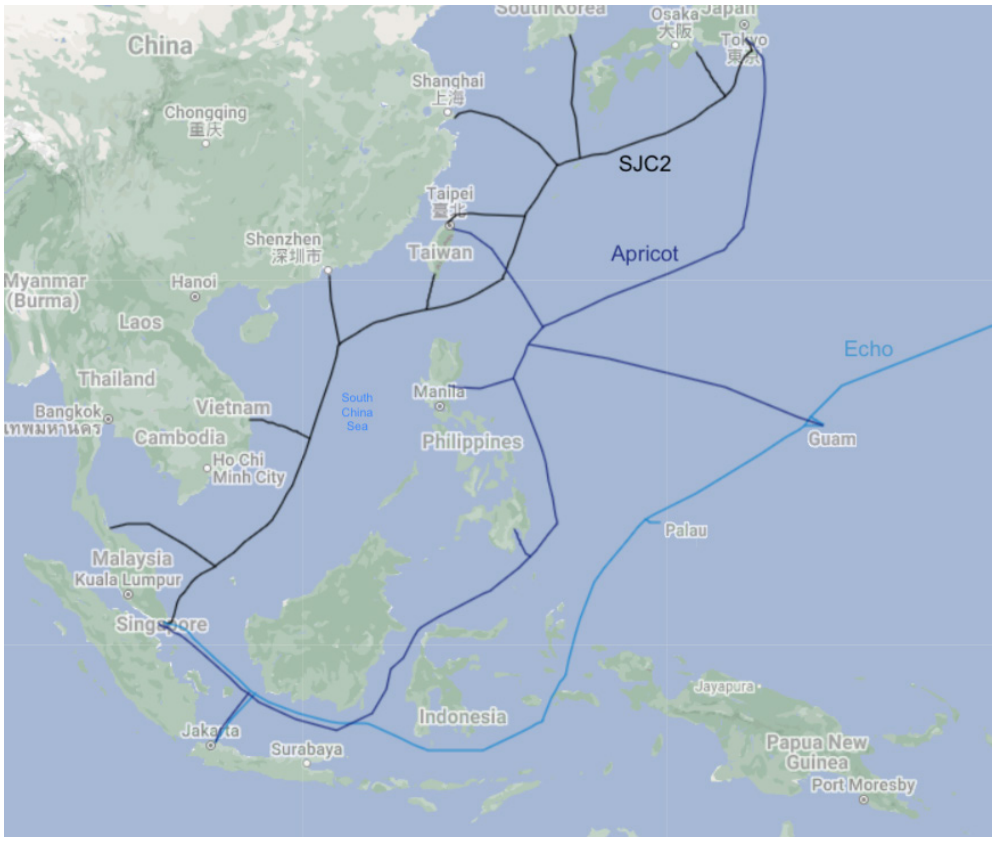
The subcable landscape is deeply affected by the actions of major powers, such as the US and China, minilateral groupings, such as the Quad, and regional infrastructure investment schemes, such as China's Belt and Road Initiative. Those factors are shaping the deployment of new subcable systems and dictating the maintenance of existing systems, with immediate repercussions for connectivity, security and digital investments in the Indo-Pacific.

In 2019, the Australian Government made a landmark contribution of two-thirds majority funding of the Coral Sea Cable project that connects Australia with Solomon Islands and Papua New Guinea.[25] Australia's involvement was initially a reactive measure to counter immediate security concerns over a proposal by the Chinese company Huawei to construct a cable between Sydney and Honiara.[26] Although initially driven by short-term considerations, the development served as a turning point, marking the beginning of a more deliberate effort by Australia to protect and manage its role in the Indo-Pacific's telecommunications and data landscape.

The US, concerned about potential espionage and data-security risks, has blocked new subcable projects that would directly connect the US with mainland China or Hong Kong[27] and US-connected cable projects that involve Chinese telecoms carriers. For instance, the BtoBE/CAP-1 project, initially set to link the US with Hong Kong, Singapore and Malaysia, faced intense scrutiny, leading to a rerouting to the Philippines and the exclusion of China's state-owned telecommunications company, China Mobile, from the consortium. Despite those adjustments, the remaining consortium members (Meta and Amazon) ultimately withdrew their application, leaving the project incomplete.[28] The US has also intervened to displace Chinese cable suppliers from subcable projects, such as the SeaMeWe-6 cable, for which the US leveraged diplomatic influence and economic incentives to pressure consortium members to select the US firm SubCom over China's HMN Technologies.[29]

China, in addressing its own espionage concerns[30] and probably fuelled by feelings of being sidelined from international projects[31] has intensified its control over subcable deployments and maintenance around the South China Sea. Lengthy permit-approval processes and stringent requirements have adversely affected cable projects. Examples include the Southeast Asia – Japan Cable (SJC2), which has been facing delays, and Apricot and Echo (Figure 3), which have been routed to avoid the route through the disputed territories in the South China Sea.[32] Before even being able to apply to lay a cable, China's permit system reportedly requires that project developers obtain a non-objection letter from the People's Liberation Army.[33] China's permit requirements for subcables traversing its claimed territorial waters and exclusive economic zone, an area marked by territorial disputes, allow Chinese authorities to influence the management of those cables and to secure the involvement of Chinese companies.[34] Additionally, companies' compliance with China's permit demands advances China's campaign to demonstrate sovereignty over contested waters. Other Asian nations (Taiwan, the Philippines and Indonesia) have also tightened the regulations that must be met when operating in their waters.[35] The resulting regulatory complexity has caused delays and altered plans, raising the costs and logistical challenges for subcable projects.[36] Furthermore, as overlapping territorial claims means that jurisdiction is unclear, cable owner-operators will go through permit processes for all claimant countries when conducting repairs, further increasing delays.

Figure 3: Cable projects affected by the disputed territories in the South China Sea; SJC2 is facing delays, and Apricot and Echo have been routed through less efficient routes to avoid the area



Source: Image created by the authors, using cable data from *TeleGeography*.

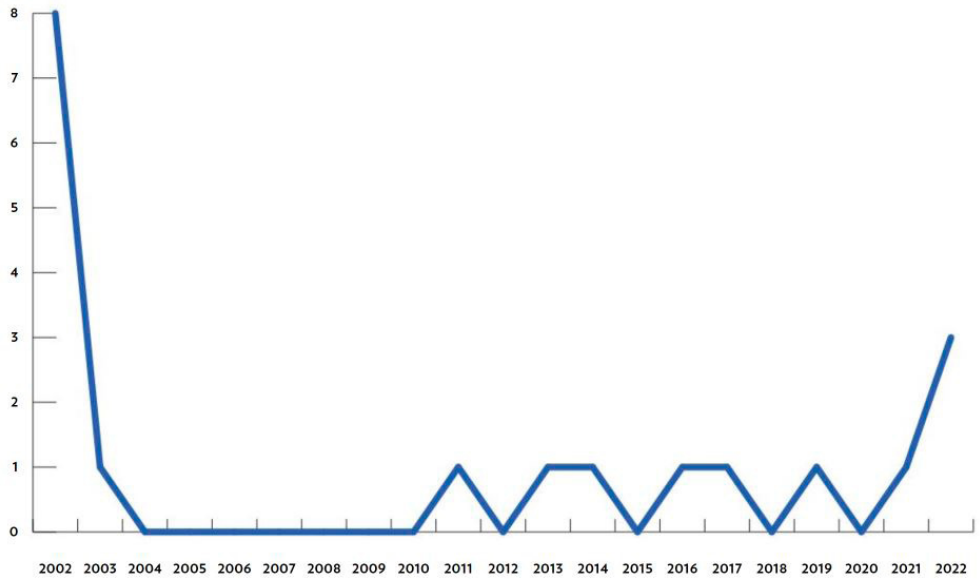
As China strives to exert greater control over the cable connections across the South China Sea, the US and its allies, Australia and Japan, are strategically investing in building out subcable networks in the Pacific.[37] Through this minilateral partnership, these three countries are jointly funding the East Micronesia cable system and building redundancy to Palau by building a branch off the existing Echo cable system (Figure 3). Additionally, they're working bilaterally in partnership with commercial cable owners such as Google, and with independent infrastructure provider, Hawaiki, to enhance connectivity to Pacific island countries. The cable effort as part of the US–Australia 'Innovation Alliance', announced in October 2023, is one such example. Australia has committed US$50 million through the Australian Infrastructure Financing Facility for the Pacific (AIFFP), and the US has pledged US$15 million, to the benefit of the Federated States of Micronesia, Kiribati, the Marshall Islands, Nauru, Papua New Guinea, Solomon Islands, Timor-Leste, Tuvalu and Vanuatu.[38] This project aims to enhance regional connectivity and access to global markets, and provide alternatives to Chinese telecommunication and data infrastructure. Similar efforts are underway between the US and Japan to build 'trusted and resilient networks' in the Pacific, including US$16 million allocated to cables systems for the Federated States of Micronesia and Tuvalu.[39] Australia and New Zealand are also partnering to jointly fund a branch off BW Digital's Hawaiki cable to bring redundancy to Tonga.[40]

A fragile supply chain

One significant factor affecting the entire subcable network is the small size of the global industry of specialised cable ships and cable manufacturers, which are stretched trying to meet the demand for their services. The rapid expansion of subcables has outpaced the growth of the fleet responsible for laying and maintaining this critical infrastructure; the scarcity of specialised cable-repair ships is a longstanding issue.[41] As of 2023, there were 69 cable ships worldwide, and a mere 22 were designated specifically for repair duties.[42] While the addition of three new vessels in 2022 marked a notable increase—given that only six ships have been added since the early 2000s (Figure 4)—these expensive resources are still stretched thinly.[43] If repair ships are engaged elsewhere, significant delays can occur, as was seen with

Tonga's protracted periods of no or little connectivity following natural disasters over the past few years. Furthermore, cable laying is more lucrative than cable repair—it is unsurprising that, for ships that can do both, they will not prioritise repair contracts (particularly for small customers) if cable laying is on offer. The scarcity of cable laying capability has arisen partly due to a historical lack of demand, but the recent surge in cable installations has led to delays in new projects, even for the cashed-up hyperscalers.

Figure 4: Number of cable ships added, 2002 to 2022, by year

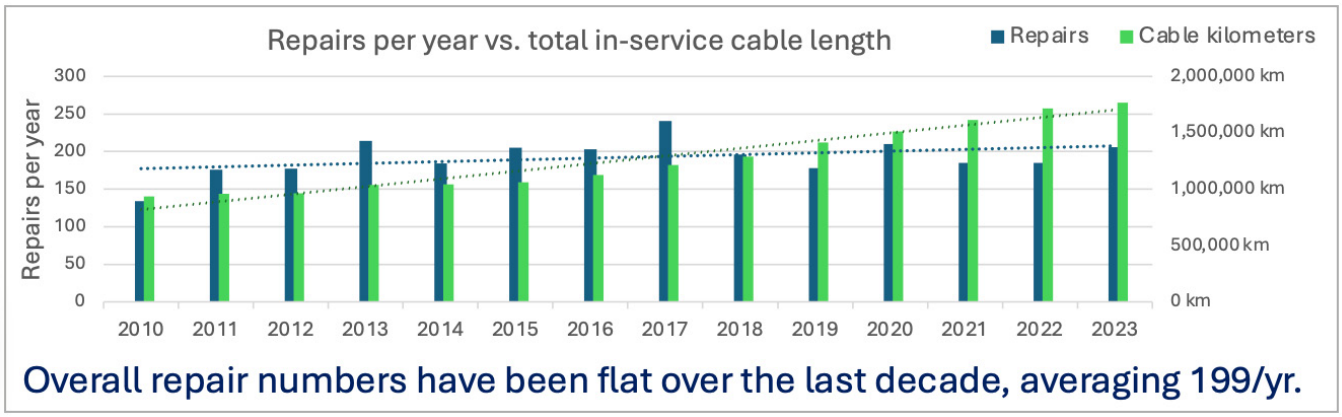


Source: *Submarine Telecoms Forum*.[44]

Despite the growing risks, the industry operates with a limited and ageing fleet. Most ships are over three decades old, are less energy efficient compared to modern vessels, and require frequent maintenance.[45] Yet the financial justification to replace traditional cable ships isn't compelling—small profit margins, particularly for repairs, increase the business risk. Uncertainty about the rate of growth of subcables has a ripple effect throughout the supply chain, particularly in the planning of new cable-laying vessels, which are decades-long projects.[46] Shipowners remain cautious about expanding their fleets due to the high costs associated with idle ships, which can reach tens of thousands of dollars per day,[47] and the painful lessons learned from oversupply following the dot-com crash in 2000. Additionally, workforce constraints, characterised by an ageing workforce and a low profile for recruitment, exacerbate the challenge.[48]

On the repair front, some in the industry calculate that it's more cost-effective to try to extend the lives of the current vessels instead of building new ones. Fortunately, mostly cable incidents occur in shallow water less than 100 metres deep, which allows smaller ships to be appropriately retrofitted to meet short-term needs.[49] However, rising national-security concerns have led nations to become more selective about who's trusted to repair their submarine cables, further narrowing the pool of available ships.[50] The issue is further complicated by delays caused through the need to obtain (potentially several) repair permits.[51]

Figure 5: Number of cable repair incidents per year against total in-service cable length 2010-2023



Source: International Cable Protection Committee.[52]

Interestingly, data provided by the International Cable Protection Committee shows that, over the last decade, there has only been a slight increase in the number of cable repair incidents, averaging just under 200 per year (Figure 5). That reported stability may be due to the significant financial incentives for cable owners to minimise cable downtime, as no data across a cable means no revenue, repairs are costly and there may be further costs to send data over a competitor's network. As a result, the industry has developed preventative measures, such as active monitoring systems that alert cable owners to ships nearing cable positions, helping to avoid accidental cuts.

The challenges extend beyond the fleet—the supply of cable itself is constrained. Most of the global supply of subcables is provided by four major cable manufacturers that have the capability to reliably produce a high volume of cables: SubCom (US), NEC (Japan), Alcatel Submarine Networks (ASN) (Finland/France) and Huawei Marine Networks (now HMN Tech) (China). Smaller cable investors or consortiums with more complex funding arrangements may encounter delays in securing cable suppliers' services, as they must fully demonstrate project funding while competing with hyperscalers who can more easily secure contracts. Additionally, the ongoing tech rivalry between the US and China is leading to a bifurcation of supply chains, effectively limiting US-based companies, including the hyperscalers, to just three of those suppliers.

In response to US policies limiting its international subcable connectivity, China is actively developing its own cable industry to achieve self-sufficiency (Table 1), gaining experience and slowly building credibility in the global market.[53]

Table 1: Chinese self-sufficiency in the subcable supply chain

(Key Chinese players in critical sectors of the subsea cable market)

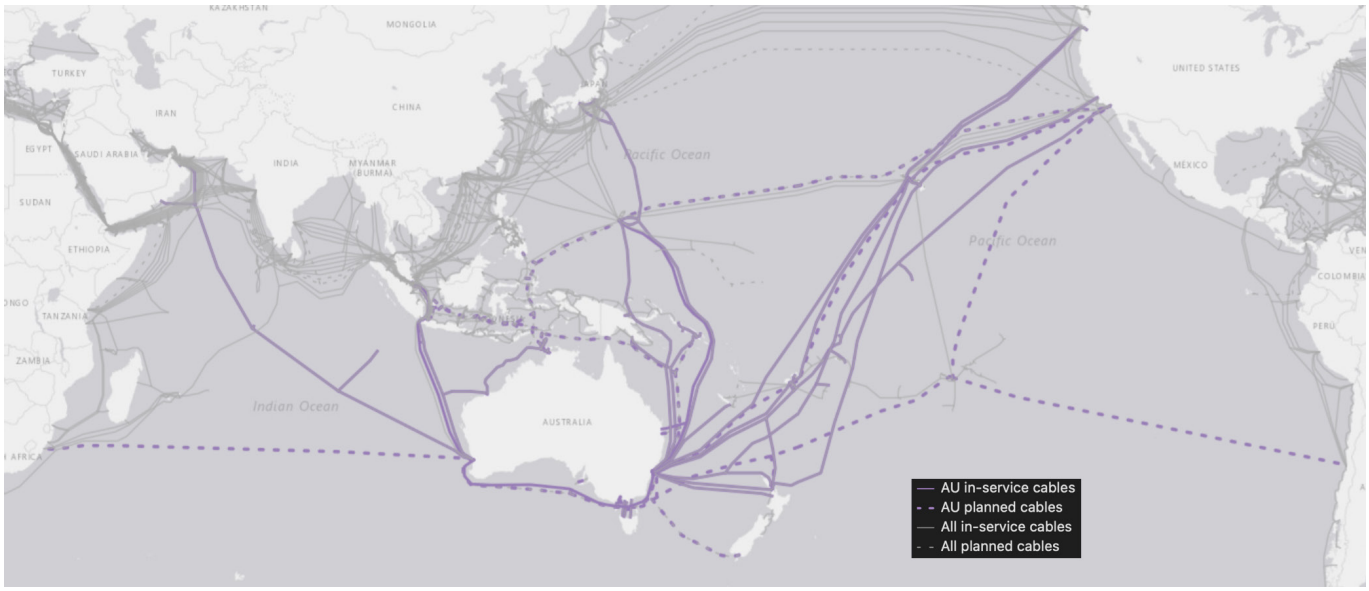
	Chinese companies	Global rivals
Main investors	China Telecom, China Mobile, China Unicom	Google (US), Amazon (US), Meta (US)
Cable builders, equipment suppliers	HMN Technologies, FiberHome	SubCom (US), Alcatel Submarine Networks (France), NEC (Japan)
Fibre-optic cables	Hengtong, FiberHome, Yangtze Optical Fibre and Cable, Jiangsu Zhongtian Technology	Corning (US), Nexans (France), NEC (Japan), Furukawa Electric (Japan)
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)
Cable ship operators	FiberHome Marine, China Submarine Cable Construction[a], S.B. Submarine Systems	TE SubCom (US), Global Marine Group (UK), LDA Group (France)
Data centre, server makers	Huawei, Inspur, Lenovo	Google (US), Meta (US), Amazon (US)

[a] Subsidiary of China Telecom.
Source: *Nikkei Asia*, 26 June 2024.[54]

Significance for Australia

The evolving landscape of subcables holds, surprisingly perhaps, great potential for Australia. Amid intensifying geopolitical rivalries between the US and China and the rapid expansion of digital infrastructure by hyperscalers across the Pacific Ocean, Australia is emerging as a hub in the region's digital ecosystem (Figure 6).

Figure 6: Australia as a digital corridor to the US and a new gateway to Asia

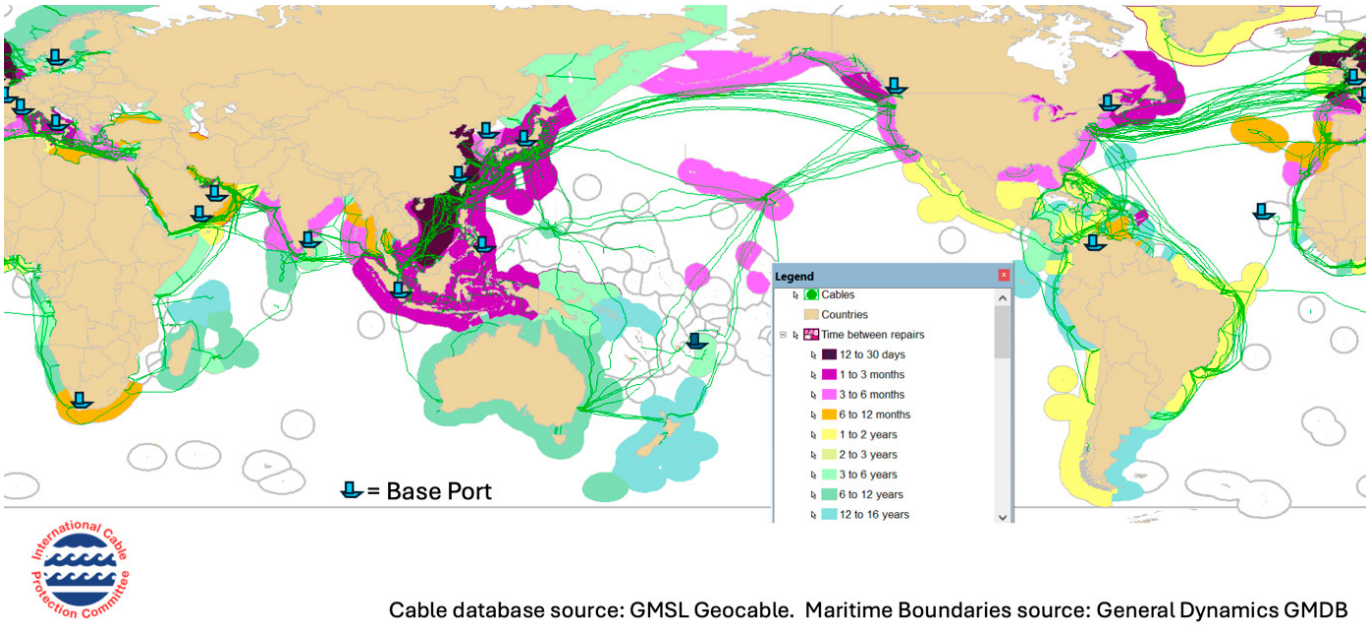


Source: Image created by the authors, using cable data from *TeleGeography*.[55]

Australia's strategic position and its ability to provide safe and secure routes for global data traffic is becoming increasingly important. Australia's position near the centre of the Indo-Pacific Tectonic Plate, for example, means it faces low seismic activity, further reinforcing its reliability as a global data transit point.[56]Australia also provides alternative routes for global traffic that bypass traditionally risky pathways, enhancing the resilience and reliability of international data flows. As a digital corridor for the Middle East and Europe, for example, Australia provides an alternative route to the US via the Pacific. Frequent cable disruptions, regional unrest and high cost of thoroughfare around the geographical cable choke-point through the Red Sea and Suez Canal underscore the value of this alternative route.[57] Additionally, Australia has infrequently required cable repair (Figure 7). Industry sources attribute this to a combination of factors: fewer cables, wide distances between landmasses, and having a relatively short continental shelf (where most cuts occur).

In contrast, locations in the South China Sea frequently require cable repair (Figure 7) and places such as Hong Kong, which once served as a favoured entry point into Asia, are seeing their appeal as a subcable hub quickly diminish.[58] This is largely due to developments such as the People's Republic of China's National Security Law and Hong Kong's subsequent regulatory alignment with mainland China. It is also affected by difficulties faced by non-Chinese vendors in laying new cables through the South China Sea.[59] Those regulatory shifts in Hong Kong have driven investors to seek more dependable and streamlined routes for their subcable projects.[60]

Figure 7: Global repair frequency map—time between repairs



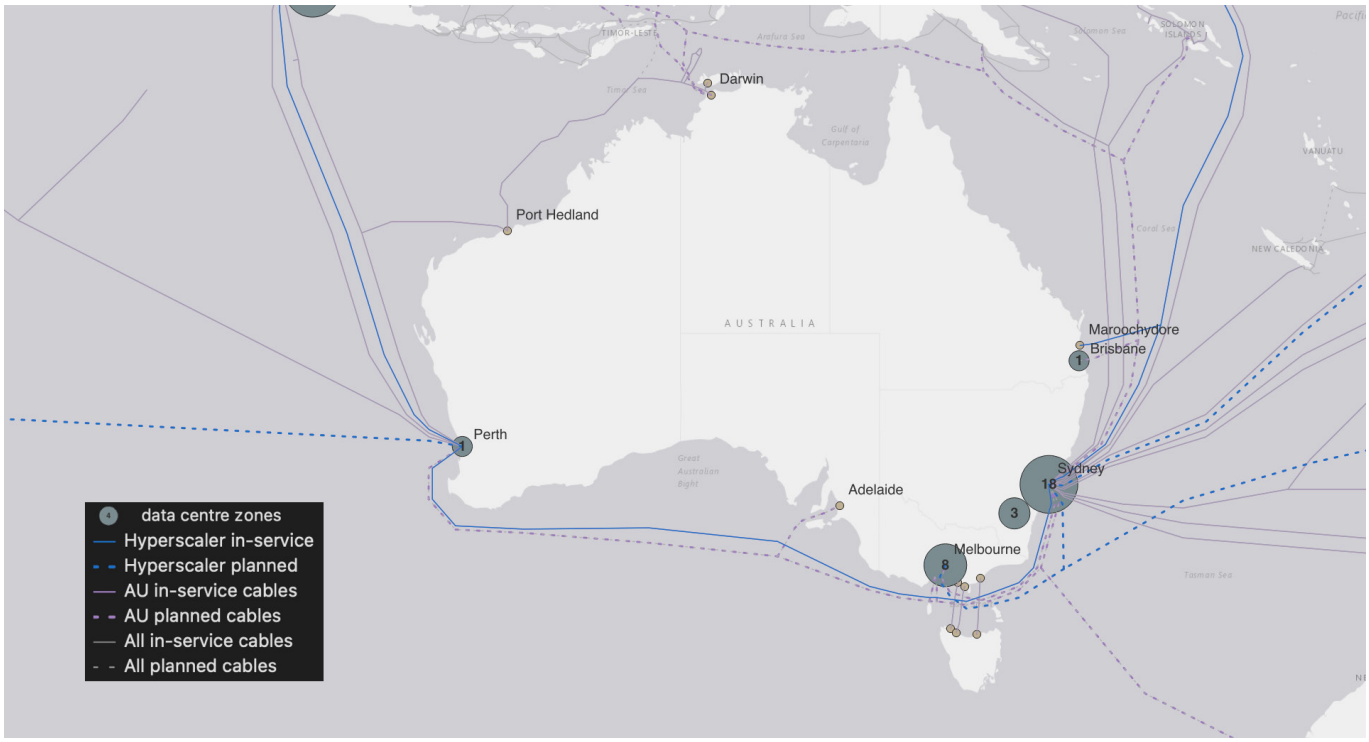
Source: International Cable Protection Committee.[61] Image enhanced for readability by authors.

Australia, with five operational and two planned subcables connecting to Asia, its subcable equipment free from high-risk vendors,[62] supported by strong domestic backhaul and access networks, with a stable political, social and geological environment, is a reliable alternative pathway and resilient route for international data traffic. That potential is further enhanced by the planned expansion of the subcable systems on the east and west coasts of Australia.[63]

It is qualities such as these that characterise Australia's strategic appeal to regions such as South America. In 2020, the Chilean Government decided to develop the first fibre-optic subcable connection between South America and the Asia–Pacific region, creating a cable link between Chile with Australia. This project was chosen over a Chinese proposal involving Chinese cable supplier, Huawei, that would have connected Chile to Shanghai. Key factors in this decision reportedly included Australia's lack of high-risk vendor equipment in its network and its new connection to Asia via the Japan-Guam-Australia (JGA) submarine cable.[64] This development is forming as the Humboldt cable, owned by Google, which is expected to be completed in 2026.[65]

Australia's growing connectivity also bolsters its data centre industry. Coupled with its renewable-energy potential, Australia is drawing investment in data centres, particularly for resource-hungry AI workloads (Figure 8).[66] Major investments are flowing in from hyperscalers, including $5 billion over two years from Microsoft to expand its cloud computing and AI infrastructure in Canberra, Melbourne and Sydney,[67] along with $13.2 billion over five years from Amazon for data centres in Sydney and Melbourne.[68] Australia now ranks second only to India in projected hyperscaler data centre expansions in the Asia–Pacific.[69] Additionally, state and territory governments in Australia are actively courting digital investments in the Northern Territory and Western Australia.[70] Given that submarine cables and data centres are interdependent, strengthening one will naturally reinforce the other.

Figure 8: Australia's submarine cables and cloud data centre zones



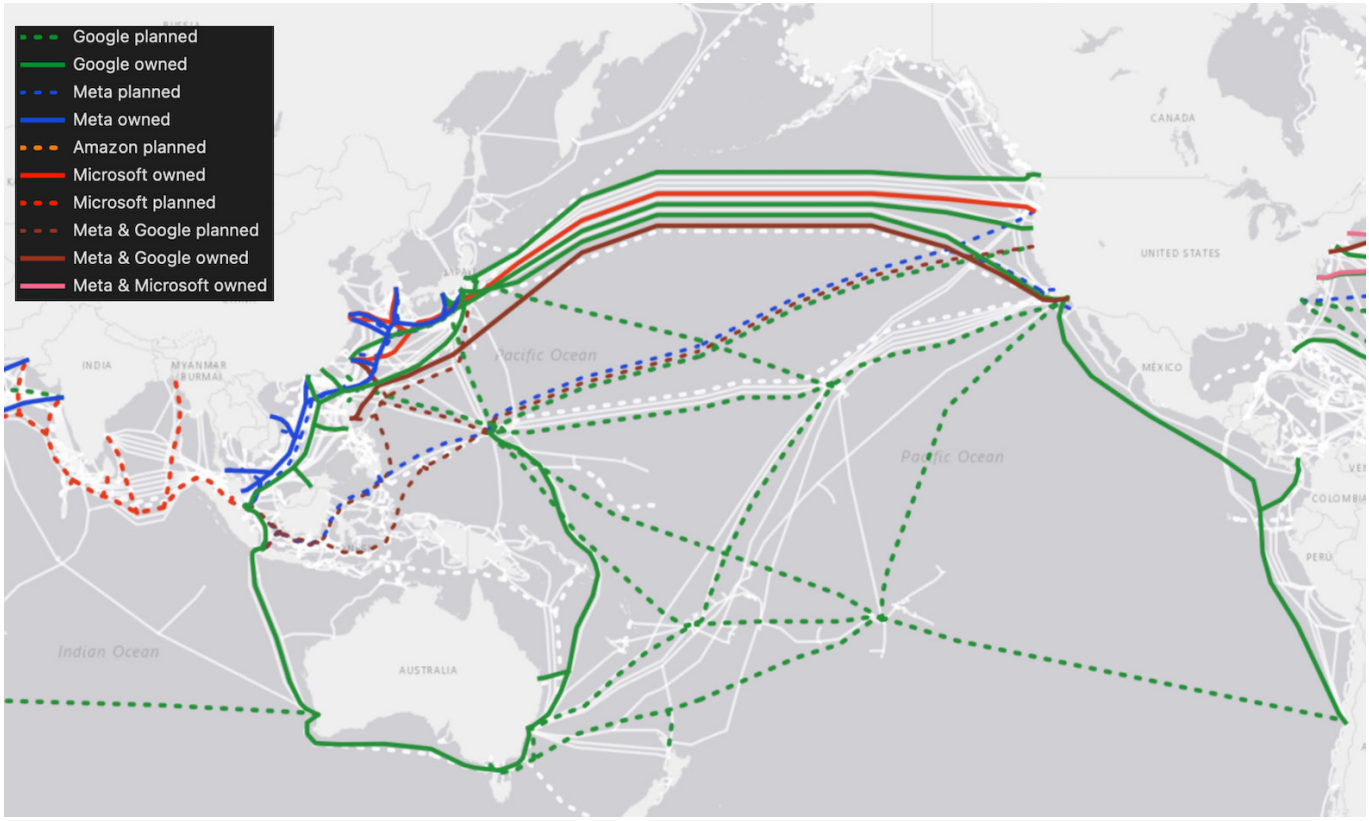
Source: Image created by authors, using data from *TeleGeography*.

Australia is also exerting its influence beyond its own borders, investing in subcable projects across the region, particularly in the South Pacific. Those investments aren't just about enhancing connectivity but also about securing Australia's relationships in the region and providing alternatives to infrastructure provided by China. By funding and facilitating such projects, Australia is better positioning itself as a key player in the region's digital future, offering secure and reliable connectivity to Pacific neighbours.

Despite those opportunities, the evolving landscape isn't without its challenges for Australia and the region. As previously noted, one such challenge is the growing trend of hyperscaler dominance in the subcables ecosystem and, more broadly, in global digital communications. This concentration of power has far-reaching implications for the risk management of a substantial portion of the world's data. Those technology giants now exert considerable control over the entire internet services stack and the massive amounts of data flowing through their extensive and complex networks, from content to network infrastructure. While there are clear benefits that hyperscalers bring to the subcable industry and to global connectivity, including the Indo-Pacific (Figure 9), there are long-term implications of this shift in power dynamics that must be carefully considered by governments, especially given the strategic and economic value of data.

In response to those risks, governments have legally challenged the way hyperscalers conduct business, particularly when it comes to content or software and hardware monopolies.[71] In Australia, current legislation limits the extent to which those companies can vertically integrate, and the Australian Competition and Consumer Commission (ACCC) can intervene to ensure that communication services remain competitive. For example, the ACCC is currently conducting an inquiry into the markets for the supply of digital platform services, including investigating a concentration of power, and ultimately practices that may result in future harm.[72] As technology continues to evolve, it's critical for government to be agile and make legislative amendments when it comes to technology-enabled anticompetitive behaviour.[73]

Figure 9: Hyperscalers' existing and planned submarine cables connecting Australia and the Pacific



Source: Image created by authors using cable data from *TeleGeography*.

The other significant risk for Australia is the lack of an assured cable repair capability. This is both a business risk for the commercial cable operators, as well as a national-security risk to the resilience of nationally critical and strategic submarine cable communications infrastructure. Even though Australia and the South Pacific islands fall within the maintenance zones of several current marine maintenance agreements, only the South Pacific Marine Maintenance Agreement (SPMA) exclusively covers Australian waters and the South Pacific. The others extend into the repair-intensive regions around Asia (Figure 7). Under the SPMA, cable maintenance is handled by the soon-to-be French Government owned[74] Alcatel Submarine Networks (ASN) and Malaysian OMS Group (OMSG), using a single vessel, the CS *Lodbrog*, which has access to a cable depot in Samoa.[75] This single ship is responsible for a vast region, stretching from Australia's western cables to Tahiti and as far north as Hawaii.

Although this arrangement has so far proven adequate, it is increasingly vulnerable due to a combination of factors. A major challenge is the limited availability globally of specialised cable vessels. The growing demand for cable-laying services, which are more lucrative than repairs, further reduces the pool of available ships for maintenance. This combination of factors increases the difficulty of finding a ship at a competitive rate to service the region. Without a sovereign or assured repair ship, Australia's subcable repair capability is wholly dependent on market forces and foreign-controlled, privately-owned vessels.

As Australia begins to position itself as a reliable and safe alternative route for the global submarine cable network, the importance of timely and reliable cable repair only increases. It is not only about the repairs of the portion of the cable closest to Australia, but also of the other end of the cable. Delays in repairs due to the ageing and insufficient fleet, or significant bureaucratic hurdles to repairing cables in contested areas, could severely disrupt connectivity, particularly in the event of simultaneous outages—a risk that's increasingly likely, given the growing number of cables, increases in adverse weather events and the high geopolitical tensions. This is an even greater risk for Pacific island partners who often have no or only very limited connectivity backup when there is cable disruption.

This problem is compounded by the emerging division of the global subcable network into distinct US and Chinese subcable ecosystems. The US concerns about the national security implications of Chinese repair ships continues, further complicating the options for repair.[76] It also presents geopolitical challenges for countries in the region, given the pressure to choose between US infrastructure and Chinese alternatives, with consequences for data security and international cooperation. A senior US State Department official has suggested that Pacific island nations that choose to connect to the partially US-funded Google cables being planned across the Pacific would need to avoid 'untrusted' Chinese equipment, including data centres, being connected to those cables, which could compromise data security and restrict digital information sharing and cooperation with the US and its allies.[77]

Currently, the bifurcation of cable routes in the Indo-Pacific region has a minimal impact on the internet experience for end users, only potentially introducing slight delays in traffic due to the more circuitous routes to and from Asia and the ongoing use of existing, ageing direct connections. This limited effect is largely because the internet is designed to dynamically reroute data, making the best effort for it to reach its destination. However, the situation could change significantly if the US or China subsequently instituted specific pathways for data transmission.

Australia's investments in the regional subcable ecosystem, its central role in regional connectivity and its strategic partnerships are key assets in this evolving landscape. However, balancing the opportunities brought by increased connectivity and investment with the diverse risks—including hyperscaler dominance and repair capabilities—will be critical in maintaining Australia's leadership and securing its digital future.

Seizing opportunities as a digital hub

To seize the opportunities as a digital hub for the region, Australia must consider improvements to its subcable resilience. This includes supporting and strengthening repair and maintenance capabilities, enhancing cable-system redundancy and security, consulting with industry on Australia's regulatory approach to ensure that its management and protection of cables remains best practice, and continuing to work with regional partners to shape the regulatory norms and standards of the region.

Enhancing these measures will achieve three things: it will support Australia's growth and attractiveness as an emerging subcables hub, it will build connectivity and resilience domestically and regionally, and it will help meet Australia's foreign-policy, development, security and cyber objectives.

Regional collaboration

One strength of Australia's subcable resilience strategy is regional collaboration. Australia is currently working to canvass and promote critical aspects of subcable resilience. Through the Cable Connectivity and Resilience Centre, established by the Department of Foreign Affairs and Trade (DFAT), Australia is positioning itself as a trusted partner for countries in the Indo-Pacific. The centre, which holds great potential if managed effectively over the years to come, has been created with the intention of supporting partner governments in policy and regulatory development and reforms, and strengthening public–private sector engagement on new cable projects.[78]

Australia's engagement extends to subcable-specific projects through other initiatives, such as through the aforementioned AIFFP. This facility is using various arrangements to enhance connectivity and redundancy for Pacific island countries, such as funding branching cable systems off the main trunk of commercial cables or the installation of branching units to assist local telecom operators to fund the cable connectivity. Announced projects include cable branches to Pacific and regional islands from Hawaiki Nui 1 and HANTRU-1 cables, on track to come online over the next few years.[79]

These new and emerging initiatives addresses key infrastructure development issues by leveraging Australia's capital and policy and regulatory expertise. However, Australia could do more to enhance maintenance and repair practices to both boost the resilience of its own international connections and to assist regional partners with theirs. Australia needs to take the lead to ensure that greater cable repair and maintenance capability is available to meet regional requirements.

Additionally, Australia's support to connectivity in the region must be comprehensive. While investing in building subcables contributes to social and economic development, Australia must simultaneously include support to build overall cybersecurity and data-security awareness and resilience. Through those initiatives, it can assist the region to develop regulations for better physical protection of the cable system and the digital protection of its data, and avoiding practices that present security risks to the region, such as using equipment from high-risk vendors.

Cable system resilience and security

CLSs are fundamental yet often overlooked components of the subcable ecosystem that connect the subcables to terrestrial networks. Given their importance and the concentration of cables at CLSs, they're prime targets for adversaries seeking to disrupt or compromise communications. To mitigate those risks, there's a growing imperative to diversify the geographical locations of CLSs and enhance both their physical and their cybersecurity measures.

The industry has begun to expand from heavily occupied landing sites in Sydney and Perth, establishing new landing locations and CLSs in areas such as the Sunshine Coast, Port Hedland and Darwin and planning for more in Adelaide, Melbourne, Brisbane and other locations in Sydney. That geographical diversification reduces the risk of a single point of mass failure and enhances overall network resilience.

However, physical diversification alone is insufficient. There's an increasing need to address the cyber vulnerabilities associated with CLSs, including those stemming from high-risk vendor equipment. That includes not only the main communication equipment, but also ancillary devices and their networks, such as site security cameras. Compromised devices could serve as entry points for adversaries to infiltrate and exploit the broader cable or physical monitoring network. Effective cybersecurity protocols must also extend to the network management software used for remotely monitoring and controlling cable operations.[80] Vulnerabilities in that software could lead to significant disruptions, akin to the high-profile SolarWinds supply-chain breach in 2020, the CrowdStrike misconfiguration in 2024, or the thwarted cyberattack on a cable operator in Hawaii in 2022.[81]

Intercontinental subcables are inherently vulnerable, with one end typically terminating in a foreign jurisdiction. Australian providers, for instance, may have limited control over the management of the CLSs in those other countries. This becomes particularly significant when those CLSs are owned, controlled or accessed by entities operating under legal frameworks that conflict with Australia's interests. In such cases, the risk of unauthorised access or insider threats is heightened, underscoring the importance of robust personnel security protocols. To address these vulnerabilities, bilateral or multilateral agreements could play a pivotal role to standardise security requirements and management practices across jurisdictions. Such agreements could streamline processes and enhance the security of global subcable infrastructure.

To address some of those challenges, the Australian Government has legislated the requirement to mitigate these kinds of threats to critical infrastructure, primarily through the *Security of Critical Infrastructure Act 2018*.[82] This necessarily includes cyber threats, for which the government is promoting greater cybersecurity awareness to industry through technical advice and guidance on the cybersecurity of critical infrastructure.[83]

Building greater resilience can be achieved by establishing a diverse array of data-transmission routes. That redundancy is critical for maintaining connectivity amid disruptions from physical attacks, natural disasters or cyber threats. Key strategies include deploying geographically diverse landing sites, diversifying global connections,

reinforcing a robust domestic backbone network capable of rerouting traffic, and leveraging alternative transport mediums, on land, through the air and in space.

One such alternative is low Earth orbit (LEO) satellite communications. Although those satellites can't yet replace subcables due to the satellites' smaller bandwidth, they provide valuable backup and redundancy during subcable disruptions. Recent advances in the speed and capacity through megaconstellation LEO satellites, such as those deployed by Starlink and Amazon Kuiper, have demonstrated their value in critical situations such as the Ukraine conflict and the Tonga volcano disaster. However, current reliance on foreign providers such as Starlink for these services has raised questions in Pacific island countries about how governments navigate the complexities of regulating and managing the presence of international satellite operators within their jurisdictions, including how to retain the economic benefits locally.

Strengthening repair and maintenance capabilities

As Australia solidifies its status as a regional digital hub, there's a pressing need to enhance its access to subcable maintenance and repair capabilities, not only for its growing number of cables but also to support broader regional connectivity and resilience.

After the volcano eruption in Tonga in 2022, it took a repair ship 10 days to travel 4,700 kilometres to reach the affected area.[84] The high cost of these vessels, combined with the vast expanse of the ocean, means that the rapid deployment of repair ships isn't always possible.

While the responsibility and commercial incentive for maintaining submarine cables lie with cable operators, the strategic and national-security significance of the cables now demands that the matter also come under government consideration.

For Australia, Japan, the US and New Zealand, which are investing in expanding connectivity and redundancy in the Pacific, there's additional consideration beyond their own repair needs. It would be irresponsible and short-sighted to help develop subcable infrastructure in the region and not strategically support its repair and maintenance, especially in a region marked by geopolitical tensions and natural environmental vulnerabilities. Submarine cables require maintenance, and cable damage isn't wholly preventable. Strengthening cable-repair capabilities, therefore, presents an opportunity for Australia and its allies to bolster regional resilience, and where further support and investment can make a significant impact. Public–private partnerships with cable operators could play a role, including with Google, which is building a strong presence in the Pacific

While subcable resilience can be enhanced through redundancy (more cables) or alternative modes of transport (from terrestrial cables to space-based communications), it would be worth assessing whether increased repair capability, such as greater availability of ships, is a more economic and beneficial option than increased redundancy of cables in terms of infrastructure development aid to an individual country. This is particularly relevant considering the substantial initial and ongoing costs associated with deploying redundant cables, which might not be offset by potential revenues.[85] Additionally, satellite alternatives might not be appropriate in certain circumstances for various reasons, including that they could pose a commercial threat to existing subcable providers by diverting customer traffic.[86]

Domestic legislation, regulation and infrastructure support

Australia's domestic legislative framework for subcable protection zones presents opportunities for improvement and modernisation. While the country's commitment to physical resilience in this sector is evident in its legislation and regulation, the framework—particularly for establishing protection zones—hasn't been updated since 2010, despite developments in the industry and the growing importance of subcables. As Australia's role as a digital hub expands,

with more cables connecting the nation and greater engagement with regional partners on best practices, there's a pressing need to reassess the framework to ensure that it remains fit for purpose.

Australia is one of the few countries with subcable resilience legislation. Schedule 3A was added to the *Telecommunications Act 1997* in 2005 to establish a scheme for creating protection zones for subcables of national significance. Those zones prohibit particular activities that would be likely to result in damage to the subcables, such as fishing using gear that rests on or near the seabed.

However, no new cable protection zones (CPZs) have been established since 2007, even though CLSs have expanded across the country. Although the industry recognises the value of the zones, it's reluctant to initiate new ones, preferring to encourage the Australian Communications and Media Authority (ACMA) to create new CPZs, and claiming that companies don't want to pay for something that their competitors could freely benefit from. While not insignificant, the fee of $161,251 to apply to initiate the regulatory process for a CPZ is relatively small compared to the hundreds of thousands or more it costs to restore a cable.

That hesitance highlights a gap between the intended protection offered by the zones and the willingness of industry to invest in them. To address this, Australia should obtain and analyse data on cable disruptions within and outside of CPZs to assess the zones' effectiveness and inform decisions on whether more zones should be declared. Given that domestic data may be limited, it would be worthwhile to also collect data from countries with similarly designated zones and more sea traffic. That data would help to justify the declaration of additional CPZs if they're proven to be significantly safer for subcables. Following Singapore's lead, Australia could mandate the reporting of all cable outages to its telecoms regulator to facilitate this data collection.[87] Additionally, ACMA and the Cable Connectivity and Resilience Centre could actively engage with cable-system developers or their representatives to determine whether the CPZ application requirements conflict with project-financing timelines or system-development milestones, making the application for a CPZ more costly for the applicant beyond the application fee.

The other potential gap is the monitoring of the protection zones. Criminal liability acts as a deterrent, but deterrence works only if there's a perception that criminals will be caught and punished.[88] There's a range of prevention measures in CPZs, including cable monitoring by industry[89] and awareness-raising activities. Zone patrolling is conducted by Maritime Border Command, as threats to subcables are one of the many types of threats to security within its remit.[90] This may be insufficient: nearly 15 years ago, ACMA recommended that further study was needed to determine whether active monitoring is necessary in the zones.[91] At that time, the government opted to rely on existing practices. Now, with the increasing strategic value of subcables, commissioning a study to determine the value and feasibility of a CPZ monitoring regime would help to identify any gaps and uplift Australia's current framework.

Australia's path to cementing its status as an attractive and effective regional digital hub relies on its ability to navigate an array of opportunities and challenges. By investing strategically in its digital infrastructure, enhancing its cybersecurity posture and fostering robust public–private partnerships, Australia can mitigate risks and promote secure, equitable connectivity. Moreover, Australia must continue to shape regional and global digital norms, ensuring that issues of data security, digital safety, privacy and sovereignty are at the forefront of discussions with its regional partners. Through those efforts, Australia not only safeguards its own interests but also strengthens its role in driving innovation and stability in an increasingly digitally-dependent world.

Recommendations

Australia has the opportunity to solidify its position as a regional digital hub, but to do so effectively it must take strategic actions that build on its existing strengths and address emerging challenges in the digital infrastructure landscape.

We offer the following five key policy recommendations.

Strengthen submarine cable infrastructure resilience

1. *Secure an assured subcable repair capability.* The Australian Government should lead efforts to secure an assured subcable-repair ship for the region. While current arrangements are sufficient for the moment, this initiative would ensure that there is a capability to reliably repair and maintain both domestic and regional cable networks into the future. This will be vital for maintaining connectivity and supporting regional allies and partners. This could be done through collaboration with Quad partners, New Zealand and regional cable operators, or an even wider selection of countries considering this capability would help to maintain a reliable alternative route in the global submarine cable network. DFAT's Cable Connectivity and Resilience Centre could commission analysis and convene a Track 1.5 forum to discover options, feasibility and costs to obtain such a capability for the repair of Australian, New Zealand and South Pacific cables.

   Besides repair ships, the forum should also look at the ability to reliably and consistently source subcable equipment, as well as a skilled and sustainable workforce with appropriate expertise.

2. *Review cable protection legislation and regulation.* The government should review Australia's current regulatory regime for the security and protection of cables. The review should consider enhancing active monitoring for CPZs, methods of obtaining cable fault data (whether this be through instituting mandatory reporting of disruptions, or through the International Cable Protection Committee's cable fault data records) and the potential expansion of CPZs based on empirical evidence. The review should be conducted by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA), as it administers the Tel Act.

Balance industry investment with the national interest and optimise government–industry collaboration

To truly realise Australia's potential as a regional digital hub, policymakers must understand the value of data along with its associated opportunities and risks. As hyperscalers become more influential within the subcable ecosystem, it's crucial for Australia to take a holistic approach to data. While it's outside the scope of this paper to consider how best to manage the broader issue of the large tech companies' dominance over communications (beyond current regulations against anticompetitive behaviour), it's critical that there's awareness that considerations incorporate the subcable ecosystem.

To that end, the Australian Government should:

3. *Evaluate the impact of hyperscaler investment on Australia's strategic data interests.* As Australia becomes a more prominent AI data centre hub, more hyperscaler submarine cables will inevitably connect. The communications component of DITRDCA should lead a comprehensive evaluation of how the concentration of subcable ownership and stewardship of data by a few key companies affects Australia's broader data goals and the national vision for data. That evaluation should address digital supply-chain risks of data confidentiality and data availability and weigh them against the economic benefits of data, ensuring that policies remain aligned with national interests. The outcomes of the ACCC's digital platform services inquiry should inform the evaluation. This initiative would complement several strategies on adjacent issues, including the 2023–2030 Australian Cyber Security Strategy, and several frameworks for the safeguarding of Australian Government data.[92]

4. The Australian Government should also deepen its engagement with hyperscalers to align commercial activities with national security priorities and seize future opportunities for collaboration and partnerships. This could be facilitated by:
   - *Establishing a domestic subcable coordination unit.* The government should consider the utility of a domestic subcable coordination unit. The unit would complement the work of the Cable Connectivity and Resilience Centre and serve as a domestic counterpart focused on national infrastructure, cybersecurity and industry relations. The Department of Home Affairs may be the most suitable to host the unit as the policy agency on critical infrastructure. Given that these issues are currently spread across several departments, this unit should have direct links to relevant government areas, including ACMA, DITRDCA and the Australian Cyber Security Centre.
   - Alternatively, or at the very least, *establishing a single point of contact for engaging with hyperscalers and other subcables industry stakeholders.* This streamlined approach would facilitate continuous dialogue and better alignment of industry practices with Australia's strategic objectives. The government should also encourage industry stakeholders to designate a similar point of contact to represent their interests and foster continuous dialogue.
5. *Review public–private partnerships.* The DITRDCA (or if more appropriate, the Department of Treasury or the ACCC) in collaboration with DFAT and ACMA, should lead a regular review of all public–private partnerships involving subcables and related digital infrastructure. The review process should be modelled on existing frameworks used for development assistance and research funding partnerships, ensuring continuous improvement and the incorporation of lessons learned. Given the increasing role of hyperscalers in those partnerships, the review process should ensure that the collaborations effectively leverage the capabilities of hyperscalers while ensuring they operate within a framework that can also accommodate the interests of smaller domestic telecommunications providers. This would serve to manage the risk of global communications relying on the operations, security and interests of a small handful of entities. The review should assess the effectiveness, transparency and alignment of the partnerships with Australia's national interests, including economic, security and strategic objectives. The outcomes should inform the development of best practices and guidelines for future public–private partnerships, ensuring that they're structured to maximise benefits while minimising risks to national security and sovereignty.

Notes

1 'Number of submarine communication cables and landing points active or under construction worldwide from 2010 to 2023', *Statista*, 2024, online; Kristin Lee, 'This is not a drill: the 2024 submarine cable map is here', *TeleGeography*, 19 February 2024, online.

2 Satellites were the faster way to transport data internationally when submarine telecommunications were copper coaxial cables. However, with the introduction of fibre-optic telecommunication cables, satellites cannot match the data capacity of these cables, not even the significantly increased speeds and capacity offered by the new generation mega-constellation low-Earth orbit (LEO) satellites.

3 Large enterprises or organisations that have high data demands, low latency requirements or dedicated data-link needs acquire dedicated capacity on submarine cables so that they can control and be assured of those network resources. Those links are for their private organisational networks.

4 'Submarine cable systems market', *Markets and Markets*, 2024, online.

5 Lydia Hales, 'Tasmania's internet outage caused by damaged Telstra cables demonstrates the state's vulnerability', *ABC News*, 2 March 2022, online.

6 Edwina Seselja, Richard Ewart, 'Tonga reconnects with outside world after data cable cut off by volcanic eruption, tsunami repaired', *ABC News*, 22 February, 2022, online

7 Elina Noor, 'Entangled: Southeast Asia and the geopolitics of undersea cables', 7 February 2024, *Indo-Pacific Outlook*, University of Hawaii Mānoa Center for Indo-Pacific Affairs, 1(5), online

8 Olga Khazan, 'The creepy, long-standing practice of undersea cable tapping', *The Atlantic*, 16 July 2013, online; Devirupa Mitra, 'Snooping storm brews in Mauritius over Indian team accessing internet landing station', 15 July 2022, *The Wire India*, online.

9 Lane Burdette, 'Leveraging submarine cables for political gain: US responses to Chinese strategy', *Journal of Public and International Affairs*, 5 May 2021, online.

10 'Submarine cable map 2023', *TeleGeography*, 2023, online.

11 Dan Swinhoe, 'Submarine cables find new impetus under hyperscalers', *Data Center Dynamics*, 23 November 2021, online.

12 Data from Alan Mauldin, 'A (refreshed) list of content providers' submarine cable holdings', *TeleGeography*, 27 June 2024, online; *Submarine Networks*, online; visualisation adapted from 'Submarine cable map 2019', *TeleGeography*, online.

13 In the period from 2019 to 2023, 24 (23.5%) of the 102 cable systems were driven by hyperscalers. 'Hyperscalers and the evolution of submarine cable ownership', in *Submarine telecoms industry report*, Submarine Telecoms Forum, issue 12, online.

14 *Submarine telecoms industry report 2023–2024*, Submarine Telecoms Forum, 14, 104, online.

15 David Abecassis, Michael Kende, Dion Teo, Nabeel Hussain, *Economic and social impact of Meta's submarine cable investments in APAC*, report for Meta, Analysys Mason, December 2021, online.

16 One such example is the Italy-to-Singapore Eagle cable that was cancelled due to a lack of an anchor tenant. Swinhoe, 'Submarine cables find new impetus under hyperscalers'.

17 Dan Swinhoe, 'The cable ship capacity crunch', *Data Center Dynamics*, 6 December 2022, online; Chris van Zinnicq, 'Perspectives on the financing of submarine cable projects', *SubTel Forum Magazine*, 29 March 2022, online.

18 Brian Quigley, Mattia Cantono, 'Boosting subsea cables with multi-core fiber technology', *Google Cloud*, 13 September 2023, online; 'NEC develops world's first next-generation optical fiber prototype high-capacity multi-core optical transmission system', NEC, 15 July 2022, online.

19 Diana Goovaerts, 'Thanks to cloud, hyperscalers are changing the way subsea cables make landfall', *Fierce Network*, 26 September 2023, online.

20 Minister for Foreign Affairs Senator the Hon Penny Wong, 'Telstra finalises acquisition of Digicel Pacific', Australian Government, 14 July 2022, online.

21 The agreement was made with 'Team Telecom', formally known as Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector. The committee assists the US Federal Communications Commission with its 'with its public-interest review of foreign participation in the telecommunications sector'. National Security Division, 'The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector', Department of Justice, US Government, no date, online.

22 Office of Public Affairs, 'Team Telecom recommends FCC grant Google and Meta licenses for undersea cable', media release, Department of Justice, US Government, 17 December 2021, online.

23 Winston Qiu, 'Google to invest $1 billion to expand Pacific Connect Initiative to Japan', Submarine Cable Networks, 11 April 2024, online.

24 'The state of the network: 2023 edition', *TeleGeography*, 2023, online.

25 'Coral Sea Cable System', Coral Sea Cable Company, online.

26 'Huawei Marine signs submarine cable contract in Solomon Islands', Huawei, 7 July 2017, online

27 Joe Brock, 'US and China wage war beneath the waves—over internet cables', *Reuters*, 24 March 2023, online; Joe Brock, 'Exclusive: China plans $500 million subsea internet cable to rival US-backed project', *Reuters*, 7 April 2023, online.

28 'Amended and restated joint application for cable landing license—streamlined processing requested', Federal Communications Commission, Washington DC, online; Brock, 'US and China wage war beneath the waves—over internet cables'.

29 Brock, 'US and China wage war beneath the waves—over internet cables'.

30 'Submarine cables become tool for certain countries to steal intelligence: China's National Security Ministry', *Global Times*, 24 May 2024, online; 国安部：海底光缆成个别国家窃取情报、谋求政治利益的工具 [Ministry of State Security: Undersea optical cables have become a tool for some countries to steal intelligence and persue political interests], *CCTV*, 24 May 2024, online.

31 Sarah Rahman, 'The cable ties to China's Digital Silk Road', *The Interpreter*, 29 April 2024, online.

32 Alan Weissberger, 'China seeks to control Asian subsea cable systems; SJC2 delayed, Apricot and Echo avoid South China Sea', *Technology Blog*, 14 March 2023, online; Bill Yates, '12 of Asia's most important submarine cable projects', *Capacity*, 29 August 2023, online.

33 Alan Dupont, 'Seabed warfare evolving as internet cables the new sinews of military muscle and commerce', Lowy Institute, 29 July 2023, online.

34 'China exerts control over internet cable projects in South China Sea', *Financial Times*, 13 March 2023, online.

35 Suruga, 'Asia's internet cable projects delayed by South China Sea tensions'; 'China exerts control over internet cable projects in South China Sea'.

36 'The state of the network: 2024 edition'; Weissberger, 'China seeks to control Asian subsea cable systems; SJC2 delayed, Apricot and Echo avoid South China Sea'; Yates, '12 of Asia's most important submarine cable projects'.

37 Anthony Albanese, 'Quad leaders' joint statement', 20 May 2023, online.

38 Trevor Hunnicutt, 'Exclusive: Google to run internet cables to Pacific islands in Australia–US deal', *Reuters*, 25 October 2023, online.

39 'United States – Japan joint leaders' statement', The White House, Washington DC, 10 April 2024, online.
40 Niva Yadav, 'BW Digital to expand Hawaiki cable to connect Tonga', Submarine Telecoms Forum, 24 June 2024, online.
41 APEC Policy Support Unit, *Economic impact of submarine cable disruptions*, Asia Pacific Economic Forum (APEC), December 2012, online.
42 Josh Dzieze, 'The cloud under the sea', *The Verge*, 17 April 2024, online; *Submarine telecoms industry report*, issue 11, 2023–24.
43 'Current cable ships', in *Submarine telecoms industry report*, issue 11, 23 October 2022, online.
44 'Current cable ships'
45 'Current cable ships'; Swinhoe, 'The cable ship capacity crunch'.
46 Olivier Pinaud, 'Big Tech colonizes seabed to assert control of the internet', *Le Monde*, 2 January 2023, online.
47 Swinhoe, 'The cable ship capacity crunch'.
48 Dzieze, 'The cloud under the sea'.
49 Mike Clare, *Submarine cable protection and the environment*, International Cable Protection Committee, March 2021, online.
50 Dustin Volz, Drew FitzGerald, Peter Champelli, Emma Brown, 'US fears undersea cables are vulnerable to espionage from Chinese repair ships', *Wall Street Journal*, 19 May 2024, online.
51 Swinhoe, 'The cable ship capacity crunch'; 'More subsea cables bypass China as Sino-US tensions grow', *Nikkei Asia*, 11 May 2024, online.
52 From the document 'Global cable repair data analysis 2024', provided to the authors by the International Cable Protection Committee, online.
53 Cheng Ting-Fang, Lauly Li, Tsubasa Suruga, Shunsuke Tabeta, 'China's subsea cable drive defies US sanctions', *Nikkei Asia*, 26 June 2024, online.
54 Cheng et al., 'China's undersea cable drive defies US sanctions'.
55 The authors chose not to highlight the SeaMeWe-3 cable connected to Australia as it's due to come to the end of its 25-year engineering life in 2024.
56 C Sinadinovski, T Jones, D Stewart, N Corby, 'Earthquake history, regional seismicity and the 1989 Newcastle earthquake', Geoscience Australia, no date, online.
57 Doug Madory, 'Outage in Egypt impacted AWS, GCP and Azure interregional connectivity', Kentik, 14 June 2022, online; Eleanor Watson, 'Ship sunk by Houthis likely responsible for damaging 3 telecommunications cables under Red Sea', *CBS News*, 6 March 2024, online; Sebastian Moss, 'Egypt's submarine cable stranglehold', *DatacenterDynamics*, 15 September 2022, online.
58 A hub is a location where submarine cables interconnect with each other. They often terminate or branch out from those locations here. In the industry, Hong Kong is considered a secondary hub. Singapore is a major hub.
59 J Zhang, 'Heading in the direction of bifurcated networks: Hong Kong's evolution amidst the global submarine cable system', *ARPE*, 2024, 3(8), online.
60 Cheng et al., 'China's subsea cable drive defies US sanctions'.
61 From the document 'Global cable repair data analysis 2024', provided to the authors by the International Cable Protection Committee, online.
62 'Submarine cable map: Australia', *TeleGeography*, 2024, online; 'Submarine cable map: HMN Tech', 2024, online.
63 'The transoceanic cable project is big for Chile', *International Finance*, 21 September 2020, online; Paul Budde, 'Submarine cable network to make Australia a digital world leader', *Independent Australia*, 26 June 2024, online.
64 'How geopolitics shaped Chile's trans-Pacific cable route', *Bnamericas*, 31 July 2020, online; Yohei Hirose, Naoyuki Toyama, 'Chile picks Japan's trans-Pacific cable route in snub to China', *Nikkei Asia*, 29 July 2020, online.
65 Office of the Spokesperson, 'Welcoming the first subsea cable between South America and the Indo-Pacific region', media note, State Department, US Government, 11 January 2024, online.
66 Australian Trade and Investment Commission, 'Australia: APAC's rising regional hub for green data centres', Australian Government, no date, online.
67 'Microsoft announces A$5 billion investment in computing capacity and capability to help Australia seize the AI era', news release, Microsoft, 24 October 2023, online.
68 Brandon How, 'AWS to invest $13.2bn in Australian cloud infrastructure', *InnovationAus.com*, 4 April 2023, online.
69 Benjamin Parkin, Camilla Hodgson, 'India pulls in tech giants for its AI ambitions', *Financial Times*, 17 June 2024, online; Abecassis et al., *Economic and social impact of Meta's submarine cable investments in APAC*, 9.
70 Sophi Hamel, 'Australia's role and opportunity in the contested arena of subsea cable networks', United States Study Centre, Sydney University, 8 December 2023, online; 'Western Australia: the southern hemisphere's global hub for data centre operations', Western Australian Government, November 2022, online.
71 Andrew Lacy, Sarah Jordan, Arman Oruc, Charlotte Brunsdon, Brady PP Cummins, Anuj Ghai, Ortal Ben Aharon, 'Antitrust & competition technology 2023 year in review', *Goodwin Law*, 25 March 2024, online.
72 Australian Competition and Consumer Commission (ACCC), 'Digital platform services inquiry 2020–25', Australian Government, no date, online.
73 See, for example, ACCC, 'New competition laws needed in response to expansion of digital platforms', media release, Australian Government, 27 November 2023, online.
74 'Nokia enters into an agreement with the French State regarding the sale of leading submarine networks business ASN', Nokia, 27 June 2024, online.
75 'ASN and OMS awarded South Pacific Marine Maintenance Agreement', Southern Cross Cable Network, 1 February 2023, online.
76 Volz et al., 'US fears undersea cables are vulnerable to espionage from Chinese repair ships'; 'Chapter 532: Cable security fleet', *United States Code*, Office of the Law Revision Counsel, US House of Representatives, online.
77 Kirsty Needham, 'Pacific islands need to boost digital security to join undersea cable, says US official', *Reuters*, 31 January 2024, online.
78 Penny Wong, 'Launch of the Cable Connectivity and Resilience Centre', media release, 29 July 2024, online.
79 'Extending the Hawaiki Nui submarine cable network', Australian Infrastructure Financing Facility for the Pacific, online; 'The Project', East Micronesia Cable System, online.
80 Justin Sherman, *Cyber defense across the ocean floor: the geopolitics of submarine cable security*, Atlantic Council, 13 September 2021, online.
81 'Federal agents disrupted cyberattack targeting phone, internet infrastructure on Oahu', *Hawaii News Now*, 13 April 2022, online; Peter Boylan, 'Cyberattack on Hawaii undersea communications cable thwarted by Homeland Security', *Star Advertiser*, 12 April 2022, online; AJ Vicens, 'DHS investigators say they foiled cyberattack on undersea internet cable in Hawaii', *Cyberscoop*, 13 April 2022, online.
82 Cyber and Infrastructure Security Centre, 'Legislation, regulation and compliance', Department of Home Affairs, Australian Government, no date, online.
83 Australian Signals Directorate, Australian Cyber Security Centre, 'Critical infrastructure: technical advice and non-regulatory guidance for critical infrastructure', Australian Government, no date, online.
84 Tom Bateman, 'Tonga is finally back online. Here's why it took 5 weeks to fix its volcano-damaged internet cable', *EuroNews*, 23 February 2022, online.
85 'Commercial challenges for Pacific island cables', Submarine Telecoms Forum, July 2024, 137:40, online.
86 'Commercial challenges for Pacific island cables'.

87 Infocomm Media Development Authority, 'Guidelines on the management of submarine cable damage incidents in Singapore port limits and the Traffic Separation Scheme Zone', Singapore Government, no date, online.

88 Daniel S Nagin, 'Deterrence in the twenty-first century', *Crime and Justice in America*, vol. 42, online.

89 'ASN opens a new era in subsea intelligent sensing based on advanced DAS technology', ASN, no date, online.

90 Australian Border Force, 'Maritime Border Command', Australian Government, no date, online.

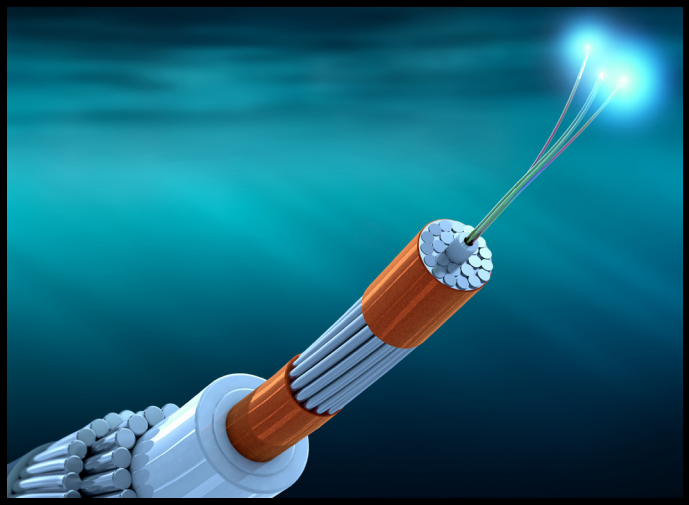
91 Australian Communications and Media Authority, *Report on the operation of the submarine cable protection regime*, Australian Government, 30 September 2010, online.

92 Digital Transformation Agency, 'Data and Digital Government Strategy', Australian Government, no date, online; Department of Home Affairs, 'Safeguarding Australian Government data', Australian Government, no date, online.

Acronyms and abbreviations

ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
AI	artificial intelligence
AIFFP	Australian Infrastructure Financing Facility for the Pacific
ASN	Alcatel Submarine Networks
CLS	cable landing station
CPZ	cable protection zone
DFAT	Department of Foreign Affairs and Trade
DITRDCA	Department of Infrastructure, Transport, Regional Development, Communications and the Arts
LEO	low Earth orbit
SJC2	Southeast Asia–Japan 2 Cable
SPMA	South Pacific Marine Maintenance Agreement
TSD	The Sydney Dialogue

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE



ISSN 2200-6648