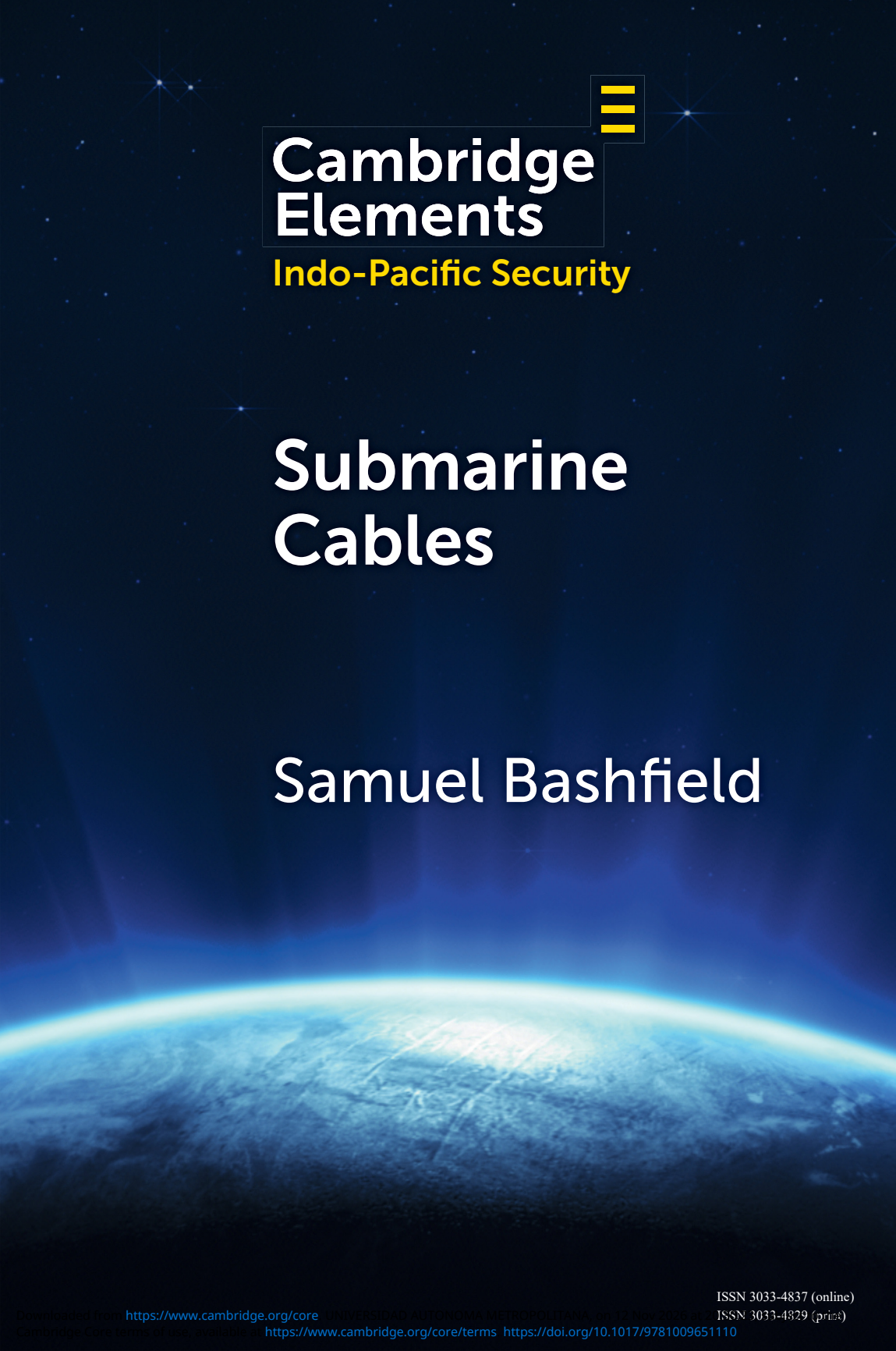


ISSN 3033-4837 (online)
ISSN 3033-4829 (print)

Downloaded from https://www.cambridge.org/core UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2025 at
Cambridge Core terms of use, available at https://www.cambridge.org/core/terms https://doi.org/10.1017/9781009651110

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Cambridge Elements

Elements in Indo-Pacific Security

edited by

Kai He

Griffith University

Steve Chan

University of Colorado Boulder

Rumi Aoyama

Waseda University

SUBMARINE CABLES

Samuel Bashfield

La Trobe University

CAMBRIDGE UNIVERSITY PRESS

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110



Shaftesbury Road, Cambridge CB2 8EA, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

Cambridge University Press is part of Cambridge University Press & Assessment,
a department of the University of Cambridge.

We share the University's mission to contribute to society through the pursuit of
education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781009651127
DOI: 10.1017/9781009651110

© Samuel Bashfield 2026

This publication is in copyright. Subject to statutory exception and to the provisions of
relevant collective licensing agreements, with the exception of the Creative Commons
version the link for which is provided below, no reproduction of any part may take
place without the written permission of Cambridge University Press & Assessment.

An online version of this work is published at doi.org/10.1017/9781009651110
under a Creative Commons Open Access license CC-BY-NC-ND 4.0 which
permits re-use, distribution and reproduction in any medium for non-commercial
purposes providing appropriate credit to the original work is given. You may not
distribute derivative works without permission. To view a copy of this license, visit
https://creativecommons.org/licenses/by-nc-nd/4.0

When citing this work, please include a reference to the DOI 10.1017/9781009651110

First published 2026

A catalogue record for this publication is available from the British Library

*A Cataloging-in-Publication data record for this Element is available from the
Library of Congress*

ISBN 978-1-009-65112-7 Hardback
ISBN 978-1-009-65109-7 Paperback
ISSN 3033-4837 (online)
ISSN 3033-4829 (print)

Cambridge University Press & Assessment has no responsibility for the persistence
or accuracy of URLs for external or third-party internet websites referred to in this
publication and does not guarantee that any content on such websites is, or will
remain, accurate or appropriate.

For EU product safety concerns, contact us at Calle de José Abascal, 56, 1°, 28003
Madrid, Spain, or email eugpsr@cambridge.org.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the
Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Submarine Cables

Elements in Indo-Pacific Security

DOI: 10.1017/9781009651110
First published online: July 2026

Samuel Bashfield
La Trobe University

Author for correspondence: Samuel Bashfield, s.bashfield@latrobe.edu.au

Abstract: How and why are key Indo-Pacific states adapting respective foreign and defence policies to secure submarine cable networks amid heightened Sino-US network-based competition? States are driven to control submarine cable networks as these infrastructures transmit information between continents and islands, traverse vulnerable maritime zones and constrict data through limited chokepoints. China's Digital Silk Road has challenged Western submarine cable dominance, prompting a suite of countermeasures by Western states individually and in coalition. This Element posits a nodes-flows-production typology to illustrate how states are attempting to control connectivity nodes, secure transmission flows and dominate production. The analysis highlights how states are pursuing central network positions to mitigate vulnerability – but this structural competition risks enabling weaponisation. This microcosm of network-based competition reveals how the contest to control submarine cable infrastructure is defining contemporary great power rivalry and rewiring the Indo-Pacific's arteries. This title is also available as Open Access on Cambridge Core.

Keywords: submarine cables, Sino-US competition, digital infrastructure, network-based competition, weaponised interdependence

© Samuel Bashfield 2026

ISBNs: 9781009651127 (HB), 9781009651097 (PB), 9781009651110 (OC)
ISSNs: 3033-4837 (online), 3033-4829 (print)

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Contents

1 Introduction: Seabed Lines of Communication 1

2 Submarine Cable Competition in Context 19

3 Cable Breaks Abound: Accidental, Negligent or Malicious? 30

4 The Indo-Pacific Adapts 47

5 The Nodes-Flows-Production Contest 70

6 Conclusion: The Seabed and Indo-Pacific Security 80

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

1 Introduction: Seabed Lines of Communication

> We know every single day that what's connecting us around the world, physically and visually, are these cables and the systems that run on them. And we want to make sure that these systems are trusted, that they're secure, and that people can be connected all around the world.
>
> Former US Secretary of State Antony Blinken speaking at the headquarters of Japanese technology firm NEC in 2024.[1]

Sino-US competition is defining Indo-Pacific international security as both poles (and respective allies) compete for relative power. Due to entrenched strategic competition, both powers are attempting to reduce reliance on adversary supply chains and lessen perceived vulnerabilities across critical sectors and services. International data flows – integral to the functioning of modern digital societies – are under renewed scrutiny by both China and the United States. Approximately 98 per cent of international data flows are transmitted via optical fibre submarine telecommunications cables which transit the seabed (see Figure 1). Since the Crimean War in the mid-1850s, submarine cables have a rich history of cutting, censorship and military communication enablement in many conflicts. In recent years, concerning episodes of suspected cable sabotage and resulting increased media attention have raised the public profile of submarine cable networks and corresponding vulnerabilities – resulting in heightened scrutiny amongst politicians, military and government leaders, academics, the cable industry and the general polity. In the modern era, these critical infrastructures are perceived as vulnerable due to risks associated with breaks, espionage, sabotage and data integrity. While these networks have been fought over in consecutive conflicts since the 1850s, after a period of relative stability in the post–Cold War era, intensified network-based Sino-US competition in the Indo-Pacific is now once again playing out on the seabed.

In the last fifteen years, as China's relative global power has matured, the rising power is attempting to displace Western (primarily US, French and Japanese) historical domination of the submarine cable industry via its Digital Silk Road Initiative. Simultaneously, in Europe and the Indo-Pacific, various instances of seabed warfare (e.g. Nord Stream) and suspicious seabed incidents (e.g. Taiwan Matsu Islands) have occurred, contributing to a reinvigorated political focus on seabed critical

[1] Antony Blinken, 'Secretary Antony J. Blinken Remarks to the Press', United States Department of State, 29 July 2024, https://2021-2025.state.gov/secretary-antony-j-blinken-remarks-to-the-press-26/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

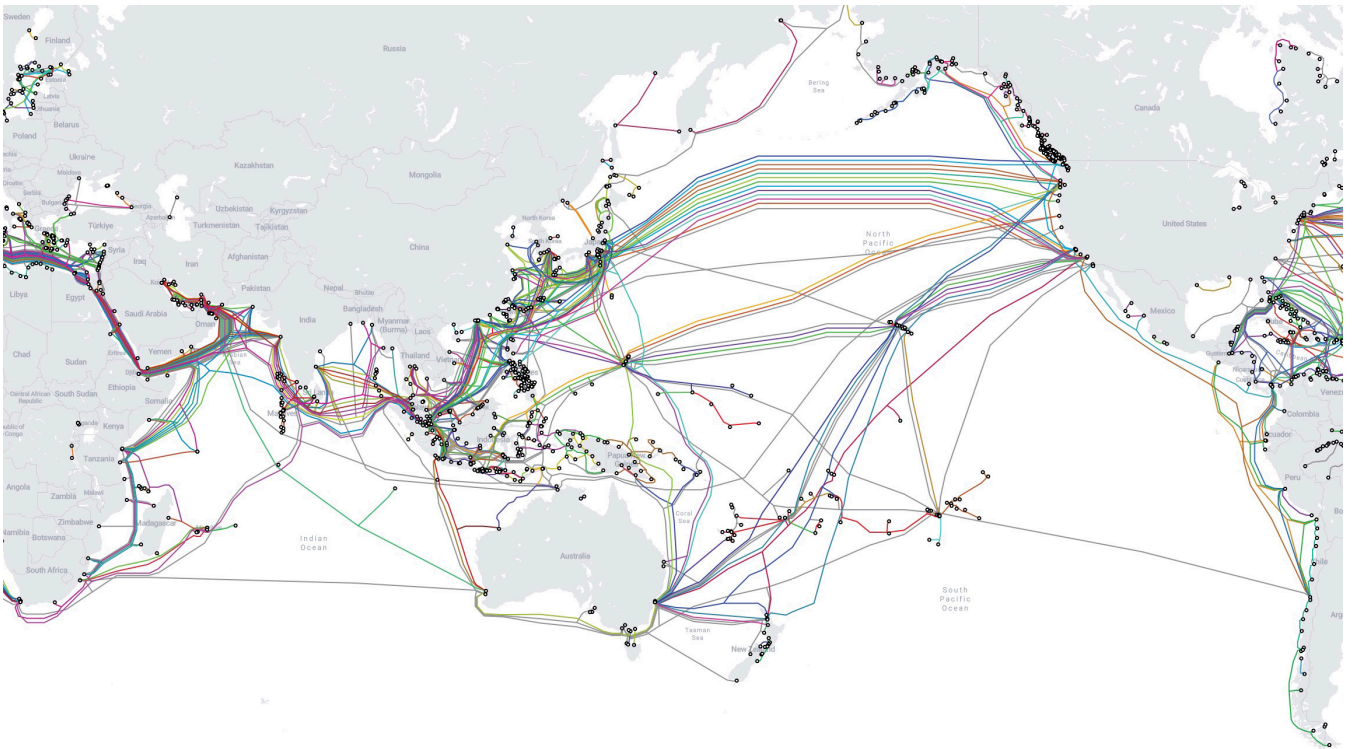


Figure 1 Indo-Pacific existing and planned submarine cable networks as at April 2026, CC BY-SA 4.0.

Indo-Pacific Submarine Cable Map, TeleGeography, April 2026, CC BY-SA 4.0, www.submarinecablemap.com/#/.

infrastructure security amongst many Indo-Pacific states. As a result, submarine cable network resilience and connectivity have become a key area of action and cooperation by Indo-Pacific nations, and through multilateral institutions including the Quadrilateral Security Dialogue. In sum, as Sino-US geopolitical competition intensifies throughout the Indo-Pacific, control over optical fibre cables which transit the seabed has become a high-stakes battleground with profound implications for the functioning of our modern digital society.

At the nation-state level, severe cable outages can pose grave national security risks. In the most extreme cases, submarine cable outages can cut entire nations from data connectivity, forcing reliance on satellite connectivity which transmits reduced capacity and is slow and expensive. Cable outages reduce data transmission capacities and require the telecommunications cable owners and operators to reprioritise data flows, potentially disrupting emergency communications and military command and control functions. Too, cable outages may require data be re-routed through vulnerable or less secure cable networks – built and operated by adversaries – thus introducing interception and espionage risks. Prolonged outages also have the potential to economically and politically destabilise states which could be leveraged for geopolitical purposes. Importantly, cable faults have regional consequences and rarely affect just one state. A cable fault will usually affect the myriad landing states, as well as users located regionally or indeed globally. Thus, states have a responsibility to secure these seabed lines of communication within their respective jurisdictions (and in the high seas) not only for their respective social, economic and security well-being, but also for the collective regional and global benefit. According to scholar Ash Rossiter, states are recognising 'the need to play an increasingly active role in the security of the undersea cables'.[2]

In the subsequent sections, I illustrate (empirically and theoretically) how and why key Indo-Pacific states are adapting respective foreign and defence policies to secure submarine cable networks amid intensifying US–China competition and perceived seabed instability. I am compelled to examine the global and regional dynamics which have driven Indo-Pacific states to once again scrutinise submarine cable security with increased alarm and the corresponding policy responses. I posit that states compete for cable centrality as these infrastructures rapidly

[2] Ash Rossiter, 'Cable Risk and Resilience in the Age of Uncrewed Undersea Vehicles (UUVs)', *Marine Policy* 171 (January 2025): 2, https://doi.org/10.1016/j.marpol.2024.106434.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

transmit information between continents and islands, geographically *traverse* maritime and coastal zones, and physically *constrict* and aggregate information flows through limited chokepoints. This competition manifests in new forms of state intervention and policies to monopolise infrastructural *nodes*, control data *flows* and dominate network *production*. Competition over submarine cable networks in the Indo-Pacific demonstrates the broader concept of network-based competition, first posited by academic Seth Schindler and colleagues, which frames contemporary Sino-US competition as a contest for centrality in digital, infrastructure, production and financial networks.[3]

Within this network-based competition framework, scholars Henry Farrell and Abraham Newman's 'weaponised interdependence' approach illustrates how states can operationalise control over network nodes through the 'panopticon effect' and the 'chokepoint effect', referring to the ability to intercept information flows and restrict network hub use, respectively.[4] While Farrell and Newman provide a 'structural explanation of interdependence in which network topography generates enduring power imbalances among states',[5] this Element applies the framework to submarine cable networks, examining how states are attempting to gain and maintain respective central positions. I detail how Indo-Pacific states compete to attain network positions with an eye to reducing their respective vulnerability, though such structural positioning creates conditions that could enable weaponisation – whether or not states intend to exploit these positions.

To substantiate these arguments, this Element proceeds as follows. This introductory section provides a brief historical analysis of submarine cable technical development and geopolitics, before overviewing the network components and why these infrastructures are perceived as both vulnerable and strategic. The second section, 'Submarine Cable Competition in Context', evaluates the growing scholarly literature and outlines key considerations pertaining to modern Sino-US competition, with a focus on technology. The Element's theoretical grounding – network-based competition and weaponised interdependence – is then posited, followed by

[3] Seth Schindler et al., 'The Second Cold War: US-China Competition for Centrality in Infrastructure, Digital, Production, and Finance Networks', *Geopolitics* 29, no. 4 (2024): 1085, https://doi.org/10.1080/14650045.2023.2253432.

[4] Henry Farrell and Abraham L. Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion', *International Security* 44, no. 1 (2019): 55–56, https://doi.org/10.1162/isec_a_00351.

[5] Farrell and Newman, 'Weaponized Interdependence', 45.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

the Element's novel typology of *nodes*, *flows* and *production*. Section 3, 'Cable Breaks Abound: Accidental, Negligent or Malicious?' documents the spate of cable breaks in both the Indo-Pacific and Europe, which heightened awareness of cable vulnerability and validated security concerns that have shaped state interventions, as mapped in Section 4, 'The Indo-Pacific Adapts'. Section 5, 'The Nodes-Flows-Production Contest', analyses these responses and overlays a network-based competition lens to characterise Indo-Pacific policy intervention under three broad categories – nodes, flows and production. This typology reveals how states compete for network centrality to reduce vulnerability, though such structural competition creates conditions that risk weaponisation. This Element's concluding section, 'The Seabed and Indo-Pacific Security', analyses the implications for Internet bifurcation, assesses notions of victory amid intensifying Sino-US competition and examines various constraints limiting state control over submarine cable networks.

This Element makes three distinct contributions to the scholarly understanding of Indo-Pacific submarine cable infrastructure contestation and network-based competition. First, it provides a new empirical analysis of how key Indo-Pacific states are adapting foreign and defence policies to perceived seabed insecurity, including the establishment of China's Digital Silk Road, the Australian Infrastructure Financing Facility for the Pacific and the Quad Partnership for Cable Connectivity and Resilience, amongst other initiatives. Second, this Element posits a novel nodes-flows-production typology to understand how network-based competition is operationalised in the Indo-Pacific, detailing how states are attempting to control submarine cable regional connectivity (nodes), secure and exploit data transmission (flows) and defend supply chains including repair capacity (production). Third, the subsequent sections establish how states compete for network centrality to reduce vulnerability – though such structural competition creates conditions that risk weaponisation, reflecting Farrell and Newman's warning against increasing systemic weaponisation risk.

1.1 From the Telegraph to Optical Fibre

Transmitting information efficiently has been a perennial challenge for human society. Submarine cable networks are now the connective tissue between terrestrial fibre networks and play an indispensable role in enabling the modern Internet and data transfer. Since the first networks were laid, these infrastructures have been primarily privately owned by myriad telegraph companies, telecommunication firms, and now big tech firms (known in the industry as 'hyperscalers'), often through consortia arrangements.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

These infrastructures have evolved since the mid-1800s, technologically, commercially and strategically – issues this brief history examines.

Until the optical telegraph was operationalised in the eighteenth century, information transmission was limited to the speed of a horse or ship. Early telegraphy was enabled by optical telegraphs, which conveyed text via visual signals. To convey messages, signal towers were constructed at regular intervals (within sight distance) and affixed with semaphore rigs which were manipulated to pass messages. However, electrical telegraphy quickly replaced optical telegraphy. Electrical telegraphy used wires to transmit electrical signals between points. The first commercial electrical telegraph was operational by the mid-1800s, and efforts were made to insulate cables for subsea use. By 1852 London and Paris were connected by a submarine telegraph link, and Ireland was connected to London by 1853.[6] In 1866 the first transatlantic telegraph was completed, and lines were rapidly laid to India in 1870 and Australia in 1872. By 1902, with the completion of a network across the Pacific Ocean, Britain's submarine cable industry had laid a truly global network – dubbed the 'All Red Line'.[7] While cables were usually laid by telegraph companies for commercial gain, the British Admiralty, Colonial Office, War Office and Foreign Office's 'political reasons' helped to justify these networks.[8] Indeed, according to academic Jill Hills, 'the submarine telegraph cable extended the "space" of empire to facilitate the unification of territory into nation-states and to allow long-distance control of alien territories'.[9] Hills adds that despite the telegraph system being privately owned, the British elite perceived the network as a 'strategic resource to be used for the defense of empire'.[10]

Submarine telegraphy played a key role in various international conflicts. Global network expansion through British subsidies was instigated by conflict, including the Indian Mutiny, the Crimean War, the American Civil War, the Boer War and the First World War.[11] At the outset of the First World War, Britain swiftly severed Germany's submarine telegraph cables, and attacking/defending these infrastructures

[6] Tom Standage, *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's Online Pioneers* (Phoenix, 1998), 70–71.
[7] The British Empire was commonly coloured red on political maps.
[8] Daniel R. Headrick, *The Tools of Empire: Technology and European Imperialism in the Nineteenth Century*, 1st ed. (Oxford University Press, 1981), 162.
[9] Jill Hills, *The Struggle for Control of Global Communication: The Formative Century* (University of Illinois Press, 2002), 4.
[10] Hills, *The Struggle for Control of Global Communication: The Formative Century*, 5.
[11] Hills, *The Struggle for Control of Global Communication: The Formative Century*, 278.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

remained a key battleground throughout the conflict at a global scale. Cable laying and repair became a perilous task, requiring naval escorts due to the risk of attack. According to historian Jonathan Reed Winkler, 'although most of the fighting between Germany and Britain occurred on the Western Front, it was the struggle for control over worldwide communications that made the war global'.[12] In one prominent Indo-Pacific example in 1914, the German light cruiser SMS *Emden* was sunk by the Australian light cruiser HMAS *Sydney* in the Indian Ocean's Cocos Islands, which the SMS *Emden* visited to destroy British telegraphy infrastructure. However, cable networks were not simply cut and severed but also comprehensively censored throughout the First World War, as part of a broader effort to disrupt and intercept enemy communications. The British implemented a vast system of censorship across its cable network, with an emphasis on restricting enemy naval or military information transmission, preventing false report circulation, collecting actionable military intelligence and denying the enemy commercial benefit.[13] British cable censors were located across the globe, from Egypt to Fiji and from Mauritius to New Zealand.[14]

During the Second World War, submarine telegraph cables were again a key target as Britain both severed Germany's subsea connections in the Atlantic and also censored other messages and deliberately slowed cable traffic.[15] In the Indo-Pacific, Japan took aim at submarine cable infrastructure, cutting or seizing most British, Dutch, French and American cables in East Asia following the Pearl Harbour attack and shelling Cocos Islands' landing station in 1942.[16] By severing or seizing submarine cables, governments and militaries were forced to instead transmit messages via radio, which was more easily intercepted. For example, during the Second World War, two cables were severed off Vietnam's coast near Saigon which connected Japan and which the Allies struggled to intercept.[17] By severing

[12] *Nexus: Strategic Communications and American Security in World War I* (Harvard University Press, 2008), 22.
[13] 'Report on Cable Censorship During the Great War (1914–1919)', War Office, 1919, DEFE 1/402, p. 394, National Archives, United Kingdom.
[14] 'Report on Cable Censorship During the Great War (1914–1919)', 397–399.
[15] Daniel R. Headrick, 'Strategic and Military Aspects of Submarine Telegraph Cables, 1851–1945', in *Communications Under the Seas: The Evolving Cable Network and Its Implications*, ed. Bernard Finn and Daqing Yang, Dibner Institute Studies in the History of Science and Technology (MIT Press, 2009), 200.
[16] Headrick, 'Strategic and Military Aspects of Submarine Telegraph Cables, 1851–1945', 200.
[17] Richard Dunley, 'Undersea Cable Control: The Information Dimension', *The Interpreter, The Lowy Institute*, 5 May 2025, www.lowyinstitute.org/the-interpreter/undersea-cable-control-information-dimension.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

these Japan-operated cable networks, Japanese military communications instead transmitted wirelessly, which could more readily be intercepted and decrypted. Indeed, according to scholars Motohiro Tsuchiya and Kristi Govella, 'as the construction of these cable networks is influenced by geopolitics so too is their destruction'.[18]

During the early Cold War period, coaxial cables began to be laid on the seabed, enabling a far greater data-carrying capacity including multiple voice channels. Coaxial cables were able to transmit high-frequency signals at higher speeds which enabled radio, television and early Internet transmission. While few details exist about submarine cable sabotage during the Cold War period, several notable examples have been detailed. First, in 1959, after a high number of cable breaks occurred off Newfoundland, the Soviet fishing vessel *Novorossiysk* was boarded by the USS *Roy O. Hale*.[19] The Americans suspected the *Novorossiysk* of purposefully sabotaging cables and boarded the fishing vessel after complaints from cable operators AT&T and Western Union to examine the ship's logs. Although the US Navy concluded publicly that it found no incriminating proof of intentional sabotage, this incident was the first ever enforcement action justified by the 1884 Convention for the Protection of Submarine Telegraph Cables.[20] Second, through the 1970s the United States tapped Soviet military cables in the Sea of Okhotsk, north of Japan. Codenamed Operation Ivy Bells, this joint US Navy, US Central Intelligence Agency and US National Security Agency action targeted Soviet communications pertaining to nuclear intercontinental ballistic missile tests and capabilities. In order to tap the cable networks, US submarines installed recording devices, which were then retrieved and processed.[21] While Operation Ivy Bells was compromised in the early 1980s, as scholar Caitlin Morris notes, these taps 'are credited as some of the most daring and successful intelligence operations of the Cold War'.[22]

[18] Motohiro Tsuchiya and Kristi Govella, 'Undersea Cables and the Extension of Empire: The Rise of Britain, Japan, and the United States and the Competition to Connect Hawai'i', *Marine Policy* 181 (November 2025): 7, https://doi.org/10.1016/j.marpol.2025.106844.

[19] David F. Winkler, *Incidents at Sea: American Confrontation and Cooperation with Russia and China, 1945–2016* (Naval Institute Press, 2017), 72.

[20] Winkler, *Incidents at Sea: American Confrontation and Cooperation with Russia and China, 1945–2016*, 72. The second enforcement action justified by the 1884 Convention for the Protection of Submarine Telegraph Cables took place in the Baltic Sea in 2024, detailed below.

[21] Caitlin Morris, 'Operation IVY BELLS: Lessons Learned from an "Intelligence Success"', *Journal of the Australian Institute of Professional Intelligence Officers* (Woden, ACT) 20, no. 3 (2012): 18, https://search.informit.org/doi/10.3316/informit.296641032846275.

[22] Morris, 'Operation IVY BELLS: Lessons Learned from an "Intelligence Success"', 17.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

During the 1980s, fibre optic cables were developed and replaced coaxial cables – which used light (rather than electricity) to transmit signals through thin glass threads. Fibre optic cables had a much greater carrying capacity, and the first transatlantic fibre optic cables operational in 1988 – TAT-8 – could carry 280 megabits per second, which equated to 40,000 telephone circuits. The first fibre optic cable to traverse the Pacific – Trans-Pacific Cable 3 (TPC-3) – was laid a year subsequent in 1989. Fibre optic cables were largely laid on the same routes as retiring coaxial cables, and as technology rapidly improved, cable carrying capacity sharply increased, meaning many optical fibre cables reached 'economic obsolescence before technological obsolescence'.[23] Optical fibre submarine cables rapidly replaced coaxial cables during the 1990s, dramatically increasing the flow of bits, enabling the Internet's global commercialisation and its embedding into many facets of society.

Importantly too, the telecommunications industry underwent a dramatic transformation during the 1980s and 1990s as large state-owned telecommunications firms were broken up and privatised. During the 1980s American AT&T was broken up as Japan's Nippon Telegraph and Telephone Corporation and Britain's British Telecom were privatised, with France Telecom following in the 1990s.[24] As a result, submarine cable network development was increasingly driven by profit, and a cable-laying boom ensued – eventually crashing in the late 1990s due to excess built capacity.[25] However, despite the cable market crash, the boom resulted in a dramatic increase in global carrying capacity – while in 1988, 1,800 voice paths crossed the Pacific and submarine cables carried 16 per cent of transmission capacity globally, by 2003, 1.87 billion voice paths crossed the Pacific and cables carried 94.4 per cent of global data transmission capacity.[26] Put simply, in the post–Cold War period, submarine cable networks became a key enabler of modern information flows and the indispensable backbone of the Internet, but not without controversy.

The role submarine cables played in Western signals intelligence collection efforts was laid bare in 2013 when former American intelligence contractor Edward Snowden leaked a large cache of highly security-classified documents to journalists. As the documents detailed, the US National Security Agency, sometimes in collaboration with Five Eyes international partner agencies and telecommunications firms, used submarine cable

[23] Nicole Starosielski, *The Undersea Network* (Duke University Press, 2015), 46.
[24] Starosielski, *The Undersea Network*, 46.
[25] Starosielski, *The Undersea Network*, 53.
[26] Starosielski, *The Undersea Network*, 53.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

infrastructure to undertake 'upstream' collection – meaning intercepting transiting data from fibre optic cables and internet backbone infrastructure.[27] As the leaked documents illustrated, upstream collection took place on a global scale including at cable network infrastructures located in non-Five Eyes countries. The Edward Snowden global surveillance disclosures – including revelations about indiscriminate Western cable interception programmes – sparked global controversy. According to American academic Jeffrey T. Richelson, the revelations 'sparked one of the most significant controversies in the history of the U.S. Intelligence Community'.[28] Importantly, and as this Element will detail, Snowden's revelations sowed distrust of Western telecommunications infrastructure amongst various Global South nations at the time, with implications for supplier choices in the years that followed.

A significant commercial shift is currently changing the economics of submarine cable network installation and operation. While most cable projects in the past several decades have been owned and financed through consortia arrangements – whereby multiple (usually) telecommunications firms collaborate to install and share a new network – American big tech firms, also known as hyperscalers or content providers, are now driving the development of many new networks. These hyperscalers, most prominently Google, Meta, Amazon and Microsoft, can justify joining consortia or owning cables outright, principally to support their respective cloud services, video/audio calling, searches, video content distribution and increasingly so for artificial intelligence (AI) production (whether training or geographically dispersed inference). According to TeleGeography, a data research firm, AI is a 'key driver of future long-haul demand',[29] and for cable networks entering service between 2024 and 2027, hyperscalers have invested in 100 per cent of trans-Atlantic routes, 80 per cent of trans-Pacific routes, and 77 per cent of routes in Oceania.[30] By investing in these networks through a consortium, or indeed as the sole owner, these hyperscalers are able to build high-capacity networks; determine

[27] Craig Timberg, 'Slide Shows NSA Surveillance of Data from Undersea Cables', *Washington Post, The*, 11 July 2013, Regional Business News, https://research.ebsco.com/linkprocessor/plink?id=980da233-a37e-34ff-9978-caea8a3d0fa6.

[28] Jeffrey T. Richelson, 'The Snowden Affair: Web Resource Documents the Latest Firestorm over the National Security Agency', National Security Archive Electronic Briefing Book No. 436, The National Security Archive, 4 September 2013, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/.

[29] 'Artificial Intelligence, Transport Networks', TeleGeography, 2025, www.telegeography.com/products/transport-networks/analysis/ai/index.html.

[30] 'Content Providers, Transport Networks', TeleGeography, 2026, www.telegeography.com/products/transport-networks/analysis/content-providers/index.html.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

cable landing points which align with data centres; reduce costs; build redundancy and swap fibre pairs or partial fibre pair capacity with other hyperscalers or carriers.[31] As a result, traditional telecommunication carriers are no longer the principle users of international data capacity through submarine cables, and the ever-growing hunger for capacity from American hyperscalers is increasingly dictating new subsea network dynamics.

1.2 Submarine Cable Networks

As I stress in this Element, submarine cable networks are indeed 'networks' – consisting of many elements, materials and components which enable data to flow between the parts and the control centre. These networks are one sub-element of the Internet's enabling infrastructure, which comprises various parts including routers, modems, media and exchanges. This section overviews various core elements of a submarine cable network to illustrate the network's physicality and to highlight some technological developments.

Fundamentally, data is represented in ones and zeroes and transmitted by a network 'packet' through an optical fibre cable. Each packet consists of both control information (which directs the packet to its destination and is often referred to as a header) and the user data (commonly referred to as a payload). Importantly, modern optical fibre networks often distribute packets across multiple networks, which are re-assembled at the destination. When stored, data is generally kept within a semiconductor memory chip as electrons. To transmit packets rapidly between landmasses, data is generally transferred via a submarine cable or via satellite. As satellite data transmission is relatively slow and costly, submarine cable networks transfer approximately 98 per cent of international data traffic and are the backbone of the modern Internet. To transmit packets through submarine cables, data is transmitted optically by specialised lasers via optical fibres.

While specifics vary, modern submarine cables consist of various components, and the glass optical fibres are sheathed by multiple insulating layers.[32] The thin glass optical fibres at the core are insulated by silicone gel, ultra-high strength steel wires, a copper sheath, a polyethylene insulator, nylon yarn bedding, galvanised armour wires and

[31] TeleGeography, 'Content Providers, Transport Networks'.
[32] 'Submarine Cable FAQs', TeleGeography, 2025, www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

tar-soaked nylon yarn.[33] These cables, termed the wet segment, are often armoured and buried in shallower waters and near the coast, but in deep waters are laid on the seabed and are roughly the diameter of a garden hose.[34] Long-distance cables are electrified by power repeaters, which are located at approximately 80-to-100-kilometre intervals. According to TeleGeography, as of early 2025 active and planned submarine cables total over 600, and in excess of 1.48 million kilometres of cable is currently in service.[35]

These cables are connected to terrestrial fibre networks via various shore-based infrastructures (also known as the dry segment). When a cable makes landfall, it generally passes through a beach manhole or a beach joint which connects to a cable landing station. While cable landing stations have historically been built near the beach manhole and connected via backhaul to data centres, now cable landing stations and data centres can be co-located, and numerous submarine cable networks often terminate at a single cable landing station. Cable networks are controlled by network operations centres and network management systems (which can often be operated remotely), which control and monitor network activity and performance. Finally, submarine cable networks are laid and repaired by a fleet of specialised vessels complete with highly trained crews. These cable ships, built with bow and/or stern sheaves, lay, maintain and repair the infrastructures. While some of these cable ships are owned and operated directly by the firm laying the networks, others are subcontracted to perform the task. Moreover, many cable repair vessels operate as part of a subscription-based maintenance repair agreement zone, while some are contracted directly by the cable operator in the event of a fault.

A variety of new sensor technologies are being integrated into submarine cable networks, which can be used to monitor network cable operations as well as the underwater environment. Various technologies, including but not limited to distributed acoustic sensing, state of polarisation sensing and distributed fibre sensing, are being deployed on networks to better observe network performance and to identify risks to networks in real time – enabling proactive repairs and even interdiction of ships or individuals which pose risks to cables. Additionally, some cables (described as SMART Cables – Science Monitoring And Reliable Telecommunication) are being fitted with oceanographic sensors which can be used to monitor

[33] TeleGeography, 'Submarine Cable FAQs'.
[34] TeleGeography, 'Submarine Cable FAQs'.
[35] TeleGeography, 'Submarine Cable FAQs'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

environmental indices, including sea levels, climate and earth changes, tsunamis and earthquakes.[36] These sensing and monitoring technologies have profound environmental and network security implications but also raise important questions about how intelligent commercial submarine cable networks could be utilised by militaries and security agencies to better monitor the underwater domain and, correspondingly, whether these infrastructures thus become legitimate military targets during a conflict.

When submarine cables are damaged, the cables are not always entirely severed. A 'shunt fault' occurs when the cable's insulation is compromised, thereby disrupting the electricity flow to repeaters. Even though many cables are buried in relatively shallow water initially, damage is still possible, often due to seabed movements and subsequent cable exposure. Cable faults can occur due to a variety of issues, including component failure, dredging, geological incidents and abrasion. Many faults cannot be formally attributed, and the cause can remain unknown. As cable monitoring and sensing become more widely implemented, it is easier for cable operators to pinpoint fault locations and disrupt an external threat before damage occurs.

To safeguard and protect submarine telegraph networks from damage, various international legal and diplomatic initiatives have been undertaken. In May 1865 the International Telegraph Union was established with a mandate to coordinate international telegraph networks and to set standards and frameworks. In 1932 the International Telegraph Union was combined with the International Radiotelegraph Union to become the International Telecommunication Union – still operating in the modern era. Moreover, in 1884 key states signed the Convention for the Protection of Submarine Telegraph Cables which aimed to protect cable networks and set rules pertaining to submarine cable networks laying and installation. According to the Convention, outside of territorial waters:

> The breaking or injury of a submarine cable, done wilfully or through culpable negligence, and resulting in the total or partial interruption or embarrassment of telegraphic communication, shall be a punishable offense, but the punishment inflicted shall be no bar to a civil action for damages.[37]

[36] Bruce M. Howe et al., 'SMART Subsea Cables for Observing the Earth and Ocean, Mitigating Environmental Hazards, and Supporting the Blue Economy', *Frontiers in Earth Science* 9 (2022), www.frontiersin.org/articles/10.3389/feart.2021.775544.

[37] 'Convention for the Protection of Submarine Telegraph Cables (1884 Cable Convention)', Library of Congress, 14 March 1884, 92, National Security Archive, https://nsarchive.gwu.edu/document/18529-national-security-archive-convention.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

However, according to Article 15 of the Convention, 'it is understood that the stipulations of this Convention shall in no wise [sic] affect the liberty of actions of belligerents'.[38] Article 26 of the 1958 Geneva Convention on the High Seas outlined how 'all States shall be entitled to lay submarine cables and pipelines on the bed of the high seas', adding that laying and maintenance should not be impeded, and due regard should be made to existing seabed infrastructure.[39] Article 27 required states legislate measures to punish individuals who wilfully or through culpable negligence damage submarine cables within respective jurisdictions.[40] The 1958 Geneva Convention on the Continental Shelf further outlined in Article 4 that continental shelf exploration and natural resource exploitation must not impede submarine cable laying or maintenance.[41] In the same year the International Cable Protection Committee (ICPC) was founded – comprising governments and submarine cable industry players – which aimed to improve cable security by providing a forum for technical, legal and environmental exchanges at a global level.[42]

The 1982 United Nations Law of the Seas Convention (UNCLOS) is considered the primarily legal regime for submarine cable protection in the modern era. According to Article 58, states are free to lay submarine cables within exclusive economic zones provided due regard is given to the rights and duties of the coastal state and comply with relevant local laws and regulations.[43] Likewise, Article 79 outlines that all states can lay cables on continental shelfs.[44] Importantly, Article 87 notes that all states are free to lay submarine cables in the high seas, and Article 113 requires states adopt legislation which establishes that conduct which interrupts or obstructs, or is liable to interrupt or obstruct, submarine cable networks – whether through culpable negligence or wilfully – a punishable offence.[45] Many states do not fulfil this UNCLOS obligation to criminalise conduct which damages, or could damage, these seabed networks.

[38] 'Convention for the Protection of Submarine Telegraph Cables (1884 Cable Convention)', 94.
[39] Convention on the High Seas, § United Nations, Treaty Series, vol. 450, p. 11, p. 82 (1958), www.legal-tools.org/doc/7b4abc-1/pdf/.
[40] Convention on the High Seas.
[41] Convention on the Continental Shelf, § United Nations, Treaty Series, vol. 499, p. 311 (1958), https://legal.un.org/ilc/texts/instruments/english/conventions/8_1_1958_continental_shelf.pdf.
[42] 'About the ICPC', International Cable Protection Committee, 2025, www.iscpc.org/about-the-icpc/.
[43] United Nations Convention on the Law of the Sea (1982), 44, www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.
[44] United Nations Convention on the Law of the Sea, 55.
[45] United Nations Convention on the Law of the Sea, 57, 64.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

1.3 Perceived Infrastructural Vulnerability

As I argue throughout this Element, submarine cable networks are sites of acute geopolitical competition as these infrastructures first, rapidly *transmit* information between continents and islands; second, geographically *traverse* vulnerable maritime and coastal zones; and third, physically *constrict* data to limited static conduits, see Figure 2. I engage and expand each of these unique network characteristics in turn – to illustrate why submarine cable networks have historically been, and continue to be, a site of geopolitical contention and state control.

Submarine cable networks transcend spatial boundaries and *transmit* information as bits at the speed of light. Importantly, the packets of data which flow through cable networks do not only cross international borders – but should be considered in a more holistic and comprehensive manner. Many submarine cable networks transmit information domestically within states – whether connecting an archipelago, connecting the mainland to islands, or across harbours or lakes. These cable networks may transmit information between states and dependent territories, within

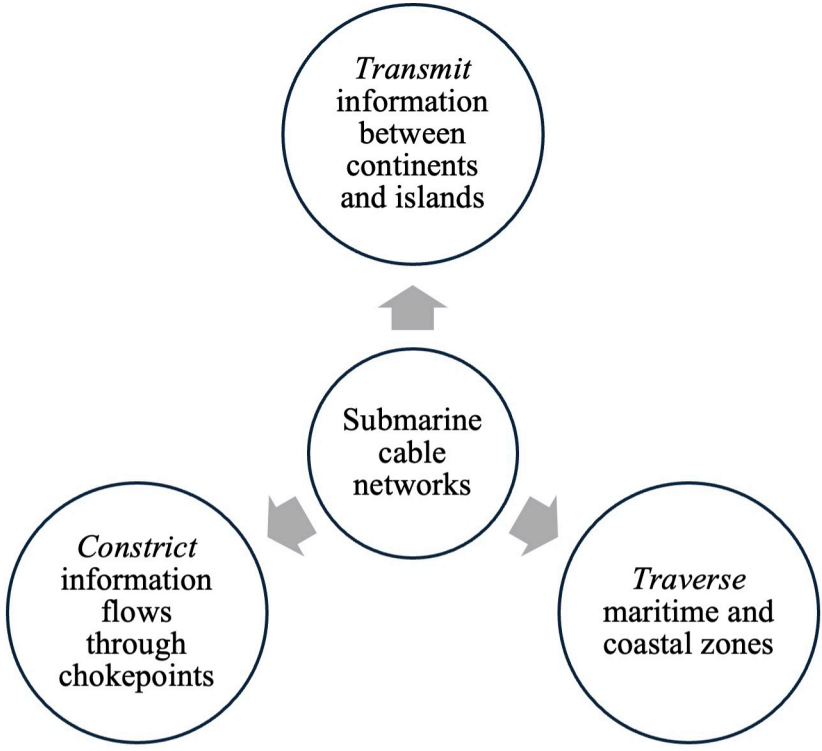


Figure 2 Submarine cable network characteristics driving state control.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

empires, to allies, to conflict zones, to multilateral diplomatic networks, to international organisations and between scientific bodies. The bits which these networks transmit enable critical infrastructure operations and our modern digital society relies on data flows for basic functioning – including financial systems, medical infrastructure, personal communications and government services. Put simply, a submarine cable network's critical role in information transmission – which underpins the functioning of our modern society – drives state control and influence.

The second factor driving states to intervene in submarine cable networks in the way these networks *traverse* vulnerable maritime and coastal zones. According to scholars Christian Bueger and Timothy Edmunds, maritime spaces are subjected to unique vulnerabilities, including a greater propensity for interstate conflicts, extremism and terrorism, and blue crime.[46] These networks are laid through the high seas, contested seas, maritime choke points, conflict zones and congested seabed areas. These networks routinely operate beyond state jurisdictions or within overlapping jurisdictions. As effective maritime domain awareness is unachievable by most states – especially underwater – the maritime environment in which these networks are laid is little understood and under-monitored. States' ability to monitor or protect these static seabed infrastructures is limited by the unique challenges of operating in the maritime domain, often beyond respective jurisdictions or beyond the geographically imposed capacities of navies or coast guards.

Third, submarine cable networks *constrict* and aggregate data flows through limited and often geographically congregated conduits. Due to the considerable costs required to lay, maintain and operate submarine cable networks – which require a robust business case or considerable state subsidies – cable networks are limited in number and limited in geographic distribution. By virtue of this relative network scarcity (when compared with terrestrial fibre), submarine cable networks necessarily constrict data flows through limited conduits, resulting in perceived vulnerability. Specifically, these limited conduits enable states to censor network traffic and to otherwise control the data flows. The limitation on network conduits also simplifies signals intelligence collection, which can be concentrated in landing stations. By constricting data flows in this manner, states correspondingly place a high priority on both ensuring cable network suppliers are 'trusted' and ensuring repair capacity is sufficient to safeguard network uptime.

[46] Christian Bueger and Timothy Edmunds, *Understanding Maritime Security* (Oxford University Press, 2024), 3.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

As a colleague and I have argued elsewhere,[47] this current era of submarine cable competition differs from previous eras in four fundamental ways. First, the basic functioning of our modern societies relies on the connectivity provided by submarine cable networks (and indeed digital infrastructure more broadly) to a higher degree than in previous eras. Global annual bandwidth demand is rapidly growing,[48] and according to one report, approximately US$10 trillion in financial transactions is facilitated daily through cables.[49] While satellite data transfer is improving, space-based communications cannot match the speed and capacity modern submarine cables provide – making these seabed conduits an indispensable enabler of our modern digital society. Second, in the post–Cold War era, state sovereignty and direct control of these seabed networks have eroded due to privatisation. Scholar Brendon Cannon notes that 'cables are not sovereign property as such. They are instead a mix of public and private and often involve consortium'.[50] Third, and as I elaborate in Section 2, modern submarine cable competition in the Indo-Pacific is fuelled by Sino-US competition. Fourth, states in the modern era are taking a regional approach to cable security rather than being concerned with just the networks which connect it or its territories directly. As a result, foreign assistance budgets and other tools of statecraft are being mobilised to influence third-country networks. These four aspects – our unprecedented modern reliance on submarine cable networks, the post–Cold War decline of state cable industry control, modern Sino-US competition centred around technology and the regional state approach to cable security – distinguish this modern era of cable competition from those which preceded it.

1.4 Research Approach and Scope

At the outset, it must be noted that this Element primarily analyses civilian seabed critical infrastructure rather than military seabed cables and sensors. Indeed, the seabed hosts an array of military seabed infrastructures, including cables, sensors and hydrophones. The location and

[47] Samuel Bashfield and Rebecca Strating, '"Friendshoring" the Seabed: Securing Submarine Cables through Network Centrality', *European Journal of International Security* First View (2025): 1–20, https://doi.org/10.1017/eis.2026.10042.

[48] 'Transport Networks: Findings', TeleGeography, 2025, www.telegeography.com/products/transport-networks/analysis/findings/findings.pdf.

[49] 'Factsheet: Submarine Cables – Maritime Awareness Project', National Bureau of Asian Research, accessed 14 December 2025, https://map.nbr.org/2018/07/submarine-cables/.

[50] Brendon J. Cannon, 'Undersea Cable Security in the Indo-Pacific: Enhancing the Quad's Collaborative Approach', *Marine Policy* 171 (January 2025): 3, https://doi.org/10.1016/j.marpol.2024.106415.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

details of these infrastructures are generally security-classified and closely guarded military secrets. While this Element does engage with military postures, due to the limited availability of data with respect to military seabed infrastructure, this work is primarily focussed on civilian critical seabed infrastructure. In addition, while the seabed is increasingly congested due to seabed electricity cables, seabed gas pipelines, conduits associated with offshore energy extraction (renewable and fossil) and the prospect of seabed mining, this Element will focus its analysis on submarine telecommunication cables.

Moreover, while submarine cable networks are routinely severed and damaged by anchors, fishing equipment and natural incidents, this Element will focus primarily on state-based and malicious risks – risks which are more prominent in an era of heightened strategic competition. Data from the International Cable Protection Committee shows that of the 100–150 submarine cable faults which occur annually, none are verified to have been severed maliciously,[51] with the possible exception of the June 2025 conviction of a Chinese vessel captain for damaging a cable network off Taiwan.[52] However, these routine threats to submarine cable networks are generally well-managed by industry and usually do not result in state intervention. As I will establish in this Element, states in the Indo-Pacific are devising foreign and defence policies to secure cable networks in this era of heightened geopolitical competition and increased regional conflicts – an era in which cable interference and sabotage are re-emerging as a concern amongst Indo-Pacific leaders and officials. Another challenge in drafting this Element is the rapidly evolving nature of submarine cable policy, as cable incidents continue to occur and state responses mature. As such, the proceeding sections are an attempt to catalogue and analyse this developing policy domain, which will consolidate as the months and years progress. Lastly, this Element provided but a brief analysis of the international legal dimensions of submarine cable security, which has been analysed extensively elsewhere,[53] to instead focus on Indo-Pacific security considerations.

[51] Lionel Carter et al., *Submarine Cables and the Oceans: Connecting the World*, UNEP-WCMC Biodiversity Series no. 31 (UNEP World Conservation Monitoring Centre & International Cable Protection Committee Ltd, 2009), 45, www.iscpc.org/publications/.

[52] Koh Ewe and I-ting Chiang, 'Taiwan Jails China Captain for Undersea Cable Sabotage', *BBC News* (London), 12 June 2025, www.bbc.com/news/articles/cwy3zy9jvd4o.

[53] Rob McLaughlin et al., 'Submarine Communication Cables and the Law of Armed Conflict: Some Enduring Uncertainties, and Some Proposals, as to Characterization', *Journal of Conflict and Security Law* 27, no. 3 (2022): 297–338, https://doi.org/10.1093/jcsl/krac014; Douglas Guilfoyle et al., 'The Final Frontier of Cyberspace: The Seabed Beyond National Jurisdiction and the Protection of Submarine Cables', *International*

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

2 Submarine Cable Competition in Context

To understand submarine cable contestation in the Indo-Pacific, three contexts require illumination. First, a growing body of scholarly literature proves that cables have historically been sites of geopolitical contestation, but that contemporary competition highlights distinct dynamics of digital dependence and privatisation. Second, submarine cables occupy a perilous position at the intersection of intensifying Sino-US competition, which spans 5G telecommunications technology, Internet governance and semiconductors. Third, network-based competition and weaponised interdependence frameworks provide apt analytical tools to examine Indo-Pacific cable competition. This section evaluates cable scholarship, situates cables in Sino-US competition and posits a theoretical framework before introducing the nodes-flows-production typology which illustrates network-based competition.

2.1 Growing Submarine Cable Scholarly Literature

Various scholars have analysed how geopolitics and conflict have played out on the seabed and affected submarine cable networks. According to historian Daniel H. Headrick's 1981 book *The Tools of Empire: Technology and European Imperialism in the Nineteenth Century*, cables were 'an essential part of the new imperialism'.[54] Specifically, in peacetime, cables were the lifeline for imperial business communications; in a crisis, cables were 'valuable tools of diplomacy' and in war, cables were 'security itself'.[55] Fellow historian Jonathan Reed Winkler's 2008 monograph *Nexus: Strategic Communications and American Security in World War I* finds that the First World War demonstrated how 'the imposition of censorship over the cables touching U.S. territory, the coordination of this with other forms of Allied censorship, and the creation of a wartime traffic monitoring group gave U.S. officials a taste of the great power to be gained from control of the cables'.[56] Historian Paul Kennedy, writing in a 1979 edited volume chapter titled 'Imperial Cable Communications and Strategy' finds that between 1870 and 1914, Britain's efforts to both build a comprehensive cable system and to effectively plan offensive and

and Comparative Law Quarterly 71, no. 3 (2022): 657–696, Cambridge Core, https://doi.org/10.1017/S0020589322000227.

[54] *The Tools of Empire: Technology and European Imperialism in the Nineteenth Century*, 163–164.

[55] *The Tools of Empire: Technology and European Imperialism in the Nineteenth Century*, 163–164.

[56] *Nexus: Strategic Communications and American Security in World War I*, 268.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

defensive seabed operations 'strengthened the military bonds of empire in peacetime', while also enabling Britain to 'meet the hazards and shocks which a worldwide war could present'.[57]

While the above academic literature examines submarine cable security from the mid-1850s until the end of the First World War, less analysis has been dedicated to the Second World War or Cold War era. Despite this, as Sino-US geopolitical tensions intensify, and as conflict returns to the European continent, some scholars are positing analysis. Scholar Nicole Starosielski's 2015 monograph *The Undersea Network* argues for a 'counterintuitive' understanding of global cable infrastructure which is 'wired rather than wireless; semicentralized rather than distributed; territorially entrenched rather than deterritorialized; precarious rather than resilient; and rural and aquatic rather than urban'.[58] Moreover, academic Peter J. Hugill finds that submarine cables are an 'explicitly geopolitical construct, integral to the process of hegemonic maintenance, challenge, and response that has been ongoing among the polities at the core of the capitalist world economy'.[59]

Concurrently, a growing body of literature is emerging which assesses submarine cable security and international relations. Scholars Christian Bueger and Tobias Liebetrau's 2021 article 'Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network' warns that research 'interest in cables has increased, but remains confined to a narrow technical debate, which does not pay attention to the politics of technology and the governance challenges that cables raise'.[60] Scholar and diplomat Hilary McGeachy's 2022 analysis titled 'The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns' argues that 'submarine cables have "always" had strategic value' and that 'submarine cables provide a means to understand more about the concept of strategic technology competition'.[61] McGeachy finds

[57] 'Imperial Cable Communications and Strategy, 1870–1914', in *War Plans of the Great Powers 1880–1914*, ed. Paul Kennedy (George Allen & Unwin, 1979), 94.

[58] Starosielski, *The Undersea Network*, 10.

[59] 'The Geopolitical Implications of Communication under the Seas', in *Communications Under the Seas: The Evolving Cable Network and Its Implications*, ed. Bernard Finn and Daqing Yang (The MIT Press, 2009), 259, https://doi.org/10.7551/mitpress/9780262012867.003.0122.

[60] 'Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network', *Contemporary Security Policy* 42, no. 3 (2021): 392, https://doi.org/10.1080/13523260.2021.1907129.

[61] 'The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns', *Australian Journal of International Affairs* 76, no. 2 (2022): 162, https://doi.org/10.1080/10357718.2022.2051427.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

that since 2015, both China's efforts to establish Chinese firms in the cable supply chain and renewed government attention on 'information-related companies and infrastructure' have altered Western strategic assessments on submarine cable networks.[62] Also, legal scholars Douglas Guilfoyle, Tamsin Phillipa Paige and Rob McLaughlin's 2022 paper contends that cables' 'increased utility, and the radically increased reliance of States upon submarine data cables for data transfer, serves to emphasise the potential consequences of their vulnerability to damage by malicious acts, accidents, or natural phenomena'.[63]

Some scholars have given specific attention to submarine cable policy in the Indo-Pacific. Scholar Kristi Govella argues that maritime and economic securitisation has altered the prevailing cable policy discourse, that in the Indo-Pacific specifically this new discourse is 'already reshaping the physical layout of regional cable architecture' due to investment decisions and that cable network resilience should be driven by a 'whole life cycle' strategy.[64] Academic Brendon J. Cannon finds that the Quad can further work to strengthen cable security through developing 'interagency coordination' and 'global governance', as well as by 'developing regional connectivity strategies'.[65] Despite some Indo-Pacific nations – especially in the Pacific Ocean[66] – not accepting the securitisation discourse, scholar Tara Maria Davenport argues that the physical protection of these subsea networks is 'an inherent component of "resilience"'.[67] On Southeast Asia, analyst Elina Noor finds that ASEAN nations are increasingly being forced to choose between Chinese or American subsea networks, which is consequently fragmenting subsea digital connectivity.[68] These

[62] 'The Changing Strategic Significance of Submarine Cables: Old Technology, New Concerns', 162.

[63] 'The Final Frontier of Cyberspace: The Seabed Beyond National Jurisdiction and the Protection of Submarine Cables', 658.

[64] Kristi Govella, 'Undersea Cables, Geoeconomics, and Security in the Indo-Pacific: Risks and Resilience', *Marine Policy* 180 (October 2025): 1, https://doi.org/10.1016/j.marpol.2025.106809.

[65] Cannon, 'Undersea Cable Security in the Indo-Pacific: Enhancing the Quad's Collaborative Approach', 5.

[66] According to scholar Amanda H. A. Watson, various leaders of states in the Pacific Ocean – while aware of submarine cable network geopolitics – focus policy efforts instead on providing robust and affordable digital connectivity to respective jurisdictions. Amanda H. A. Watson, 'Undersea Cables: The Official Perspectives Expressed in the Pacific Region', *Marine Policy* 178 (August 2025): 5, https://doi.org/10.1016/j.marpol.2025.106735.

[67] Tara Maria Davenport, 'The Protection of Submarine Cables in Southeast Asia: The Security Gap and Challenges and Opportunities for Regional Cooperation', *Marine Policy* 171 (January 2025): 2, https://doi.org/10.1016/j.marpol.2024.106435.

[68] Elina Noor, 'Entangled: Southeast Asia and the Geopolitics of Undersea Cables', *Indo-Pacific Outlook* 1, no. 5 (2024): 2.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

scholars collectively echo that submarine cable security cannot be considered in isolation and indeed should be situated at the intersection of the prevailing geopolitical rivalry.

2.2 Sino-US Tech and Internet Competition

China and the United States are engaged in an intense battle for supremacy in the Indo-Pacific. Both states are competing for military, cultural, institutional, economic and technological superiority. According to Eric Schmidt, former Google CEO, Sino-US technology and innovation competition is the 'century defining contest'.[69] China has rapidly risen as a great power and is attempting to dislodge the United States in various domains, especially in networks. According to scholars Kai He and Mingjiang Li's writing in 2020, 'US–China strategic competition has just begun.'[70]

Various scholars agree that technology and innovation is a key contributor to great power status. According to historian Paul Kennedy, military power relies on a strong economy, which in turn requires superior technology.[71] Kennedy asserts that the relative power of states and empires is determined by the effect that economic and technological change has on social structures, governance arrangements and military power.[72] Political scientist Robert Gilpin finds that superior military and industrial technologies allow states to 'seize the opportunities or overcome the constraints provided by the external environment in order to advance its economic, security, or other interests'.[73] Put simply, cutting-edge technology and robust innovation are key drivers of power in the international system of states.

In recent years, China has invested heavily in high-tech innovation and rapidly climbed the economic value chain. Chinese tech firm Huawei[74] has led the charge in many of these technologies, especially in the

[69] Eric Schmidt, 'Innovation Power: Why Technology Will Define the Future of Geopolitics', *Foreign Affairs*, 28 February 2023, www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics.

[70] Kai He and Mingjiang Li, 'Understanding the Dynamics of the Indo-Pacific: US–China Strategic Competition, Regional Actors, and Beyond', *International Affairs* 96, no. 1 (2020): 1, https://doi.org/10.1093/ia/iiz242.

[71] Paul Kennedy, *The Rise and Fall of Great Powers: Economic Change and Military Conflict from 1500 to 2000*, 2nd ed. (Unwin Hyman Limited, 1989), 439.

[72] Kennedy, *The Rise and Fall of Great Powers: Economic Change and Military Conflict from 1500 to 2000*, 439.

[73] Robert Gilpin, *War and Change in World Politics* (Cambridge University Press, 1981), 54.

[74] Huawei formerly owned submarine cable firm Huawei Marine Networks, which was sold in 2020 and rebranded as HMN Technologies (HMN Tech) – see Section 4.2.2.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

telecommunications domain. According to scholars Andrew B. Kennedy and Darren J. Lim, innovating information and communication technologies have been a focus for China, underpinned by considerable increases in R&D expenditure.[75] As technological prowess relates to international relations, Kennedy and Lim argue that 'under certain conditions the rising state's [technological innovation] activities will generate negative order externalities for the dominant state, particularly by undermining its preferred rules, practices and institutional arrangements'.[76] Despite these negative order externalities, political scientist Daniel Drezner highlights that 'technological latercomers' often struggle to gain global market share as 'the ingredients for motivating technological catch-up are ill-suited for technological leadership'.[77] In any case, in the eyes of many first Trump Administration officials, Huawei was a strategic rather than a commercial challenge, as 'Huawei was a national champion of America's primary geopolitical rival'.[78]

Sino-US technology competition takes a variety of forms and extends into competition for Internet-related technologies. From AI, 5G telecommunications, e-commerce and digital payments, to social media, quantum computing and semiconductor manufacture, American and Chinese firms are competing for supremacy. Indeed, in Internet standards and governance, the two nations advocate for differing governance conceptions (multistakeholder vs state-centred), and China is advocating to replace the long-established TCP/IP (Transmission Control Protocol/Internet Protocol) with a 'New IP', which would incorporate greater controls at the network level.[79] Furthermore, Sino-US technological competition extends beyond just the two superpowers and extends to respective partners and allies. Scholar Xinghua Liu finds that the United States does not further its technological leadership unilaterally but employs a 'digital coalition' model, in coordination with like-minded allies and

[75] Andrew B. Kennedy and Darren J. Lim, 'The Innovation Imperative: Technology and US–China Rivalry in the Twenty-First Century', *International Affairs* 94, no. 3 (2018): 561, https://doi.org/10.1093/ia/iiy044.

[76] Kennedy and Lim, 'The Innovation Imperative: Technology and US–China Rivalry in the Twenty-First Century', 571.

[77] Daniel Drezner, 'State Structure, Technological Leadership and the Maintenance of Hegemony', *Review of International Studies* 27, no. 1 (2001): 25, Cambridge Core, https://doi.org/10.1017/S0260210501000031.

[78] Chris Miller, *Chip War: The Fight for the World's Most Critical Technology* (Simon & Schuster, 2022), 314.

[79] Edoardo Campanella and John Haigh, 'The Battle for the Internet', *Survival* 66, no. 1 (2024): 76, https://doi.org/10.1080/00396338.2024.2309076.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

states, to compete technologically with China.[80] In this sense, allies and partners play key roles in operationalising the superpowers' technological and innovation agendas and in enabling technological supremacy.

As this analysis illuminates, the United States and China are locked in entrenched competition across a variety of domains, crucially, including technology innovation generally and Internet leadership specifically. This rivalry, in the context of Sino-US network-based competition and physical infrastructure characteristics I outline below, aids in understanding why submarine cable networks have become a key battleground, especially when compounded against the European seabed warfare harbinger, as the next section outlines.

2.3 Network-Based Competition and Weaponised Interdependence

The contemporary Sino-US rivalry can be understood as 'network-based competition' – meaning a contest for centrality in digital, infrastructure, production and financial networks.[81] In this framework, posited by academic Seth Schindler and colleagues, the dominant components of networks are interconnectivity, interdependence and control of non-linear often non-hierarchical nodes.[82] This framework builds on international relations scholarship which illuminates the role of infrastructure in international relations,[83] and the importance of political, economic and social linkages and networks.[84] Furthermore, this framework builds on existing theorising concerning connectivity geopolitics,[85]

[80] Xinghua Liu, 'Coalition Building and Sino–US Competition in the Digital Era', *The Chinese Journal of International Politics* 17, no. 4 (2024): 447, https://doi.org/10.1093/cjip/poae022.

[81] Schindler et al., 'The Second Cold War', 1085.

[82] Schindler et al., 'The Second Cold War', 1094; Bob Jessop et al., 'Theorizing Sociospatial Relations', *Environment and Planning D: Society and Space* 26, no. 3 (2008): 393, https://doi.org/10.1068/d9107.

[83] Jutta Bakonyi and May Darwich, 'Infrastructures and International Relations: A Critical Reflection on Materials and Mobilities', *International Studies Review* 26, no. 4 (2024), https://doi.org/10.1093/isr/viae046; Daniel McCarthy, ed., *Technology and World Politics: An Introduction*, 1st ed. (Routledge, 2018); Seth Schindler et al., 'The New Cold War and the Rise of the 21st-Century Infrastructure State', *Transactions of the Institute of British Geographers* 47, no. 2 (2022): 331–346, https://doi.org/10.1111/tran.12480.

[84] Miles Kahler and David A. Lake, 'Globalization and Governance', in *Governance in a Global Economy*, ed. Miles Kahler and David A. Lake (Princeton University Press, 2004), 3, https://doi.org/10.1515/9780691234687-003.

[85] Colin Flint and Cuiping Zhu, 'The Geopolitics of Connectivity, Cooperation, and Hegemonic Competition: The Belt and Road Initiative', *Geoforum* 99 (February 2019): 97, https://doi.org/10.1016/j.geoforum.2018.12.008.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

and the ways in which power in the international system is not 'uniform or continuous over space' but is dependent on a combination of 'proximity and reach'.[86]

Through this lens, state control of data, knowledge, technical standards, capital and production capacity affords network leverage, which in turn is a source of hegemony in the international system.[87] Hegemony under this approach affords the ability of a state to 'order relations among actors'.[88] This approach is based on both critical geopolitical economy scholarship and contemporary Cold War historiography.[89] Rather than relying on a realist approach which emphasises structural conditions and the anarchic global system, this network-centric approach highlights the interconnected nature of modern international relations in which 'network centrality' is a key state goal.[90] According to Schindler and colleagues:

> Rather than a zero-sum contest to control territory, the US and China seek to establish centrality in networks through which they can project geopolitical and geoeconomic power. In practice, this is done through a range of strategies, such as (1) establishing rules of the game that determine how networks are integrated, who can participate in them and enforcing compliance, (2) restructuring networks, or, in limited cases, (3) building alternative competing networks.[91]

Scholar William Kindred Winecoff highlights that under this 'network approach', the United States will maintain predominance if other states continue to integrate into US-led networks, but that interdependence can result in other states feeling threatened by such 'hierarchical patterns of interdependence [resulting in these states] seek[ing] to resist exposure by forming alternative clubs'.[92] Moreover, scholars Robert O. Keohane and Joseph S. Nye, Jr describe a '"policy-networks" model of governance', through which 'interdependence' results in 'continuing

[86] John Allen, *Lost Geographies of Power*, RGS-IBG Book Series (Blackwell Publishing, 2003), 3.
[87] Schindler et al., 'The Second Cold War', 1094–1095.
[88] G. John Ikenberry and Daniel H. Nexon, 'Hegemony Studies 3.0: The Dynamics of Hegemonic Orders', *Security Studies* 28, no. 3 (2019): 411, https://doi.org/10.1080/09636412.2019.1604981.
[89] Schindler et al., 'The Second Cold War', 1085.
[90] Schindler et al., 'The Second Cold War', 1087.
[91] Schindler et al., 'The Second Cold War', 1094.
[92] William Kindred Winecoff, '"The Persistent Myth of Lost Hegemony," Revisited: Structural Power as a Complex Network Phenomenon', *European Journal of International Relations* 26, no. 1_suppl (2020): 243, https://doi.org/10.1177/1354066120952876.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

interactions' amongst players.[93] They also argue that within limits, 'asymmetrical interdependencies' can be considered 'sources of power among actors'.[94]

Connected to network-based competition, the concept of 'weaponised interdependence' was first articulated by academics Henry Farrell and Abraham Newman in 2019 to describe how network interconnectedness can afford exploitable benefits to states with jurisdictional (whether physical or legal) control over network nodes and vulnerabilities for those without.[95] Importantly, networks are often structured asymmetrically, meaning some nodes are more comprehensively connected than others, meaning interdependencies can be leveraged.[96] According to Farrell and Newman:

> states with political authority over the central nodes in the international networked structures through which money, goods, and information travel are uniquely positioned to impose costs on others. If they have appropriate domestic institutions, they can weaponize networks to gather information or choke off economic and information flows, discover and exploit vulnerabilities, compel policy change, and deter unwanted actions.[97]

Under the weaponised interdependence framework, two forms of weaponisation are described – the 'panopticon effect' and the 'chokepoint effect'. The panopticon effect refers to the way in which states with jurisdictional or physical access to network hub nodes can use their position of network centrality to intercept and glean information which is otherwise transiting the hub – offering a 'key window into the activity of adversaries'.[98] The 'chokepoint effect' refers to the 'coercive power' network centrality provides states, allowing hub access by other states (or indeed firms) to be limited or penalised for strategic reasons.[99] Importantly, Farrell and Newman find that to harness both the panopticon and chokepoint effects, states need both network hub jurisdictional control and ample legal and regulatory 'institutional capacity'.[100]

[93] Robert O. Keohane and Joseph S. Nye Jr, 'Redefining Accountability for Global Governance', in *Governance in a Global Economy*, ed. Miles Kahler and David A. Lake (Princeton University Press, 2004), 395, https://doi.org/10.1515/9780691234687-017.
[94] Robert O. Keohane and Joseph S. Nye, *Power and Interdependence*, 4th ed. (Pearson, 2011), 15.
[95] Farrell and Newman, 'Weaponized Interdependence', 56.
[96] Farrell and Newman, 'Weaponized Interdependence', 45.
[97] Farrell and Newman, 'Weaponized Interdependence', 45.
[98] Farrell and Newman, 'Weaponized Interdependence', 55.
[99] Farrell and Newman, 'Weaponized Interdependence', 56.
[100] Farrell and Newman, 'Weaponized Interdependence', 58.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

The weaponised interdependence idea was first articulated as a warning to government officials against the unintended effects of leveraging network access and network choke points. By exploiting interdependence, fellow states may likewise attempt to leverage networks, to disengage from networks or to reduce vulnerability by revising networks.[101] As Farrell and Newman write, 'the more that privileged states look to take advantage of their privilege, the more that other states and nonstate actors will take action that might potentially weaken or even undermine the interdependent features of the preexisting system'.[102] Therefore, states would be wise to resist weaponising interdependence, so centralised exchanges can continue to deliver universal benefits. However, it seems some US officials adopted the idea as a strategy. Writing several years after first positing the weaponised interdependence concept in 2019, Farrell and Newman noted that at least one Trump Administration officials had read their academic article and concluded that weaponising choke points was sound policy.[103] According to academic Chris Miller in his book *Chip War*, while discussing Huawei with a former senior US official, the source commented: 'weaponized interdependence … it's a beautiful thing'.[104]

However, the degree to which states could indeed weaponise interdependence in submarine cable network dynamics has been questioned. Scholar Lars Gjesvik argues that, while 'seemingly ripe for state exploitation as digital infrastructures become more critical, the second incarnation [2010 onwards] of the [submarine cable] network has instead empowered private corporations and given them greater ability to resist state attempts at weaponization'.[105] Gjesvik's analysis centred on trans-Atlantic cable networks. Indeed, the private ownership of these seabed networks will limit the degree to which states can intervene and interfere. Rather, through this present Element I seek to articulate how and why states are *attempting* to control these networks, rather than the success or otherwise of the resulting interventions (which is engaged with in Section 5), vis-à-vis private actors.

Moreover, scholars Dwayne Woods and Junda Li apply the weaponised interdependence framework to submarine cable networks in their 2024

[101] Farrell and Newman, 'Weaponized Interdependence', 76.
[102] Farrell and Newman, 'Weaponized Interdependence', 76.
[103] Henry Farrell and Abraham Newman, *Underground Empire: How America Weaponized the World Economy* (Penguin Press, 2024), 102.
[104] Miller, *Chip War: The Fight for the World's Most Critical Technology*, 307.
[105] Lars Gjesvik, 'Private Infrastructure in Weaponized Interdependence', *Review of International Political Economy* 30, no. 2 (2023): 724, https://doi.org/10.1080/09692290.2022.2069145.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

article 'Dangerous Depths of Bifurcation: The Rise of "Inter-National Security Narcissists" and Undersea Cable (Dis)Connections', arguing that the framework 'falls short in accounting for the proactive reshaping of network topologies by states seeking to mitigate these very vulnerabilities'.[106] When it comes to submarine cable networks, using a sequential game model, Woods and Li find that in response to perceived cable network vulnerability, both China and the United States have respectively attempted to construct parallel (or bifurcated) networks, which has resulted in the 'fragmentation' of the global cable system – a phenomenon the weaponised interdependence framework had not previously accounted for.[107] While Woods and Li model bifurcation as a response to vulnerability, this Element identifies the mechanisms through which key Indo-Pacific states reshape network topologies, utilising a novel nodes-flows-production typology to understand how states seek centrality – not just how centrality is mitigated.

Building on this growing astute scholarship, this Element is unique due to the way it catalogues both the global dynamics pertaining to submarine cable vulnerability and how key Indo-Pacific states have adapted foreign and defence policy. Moreover, this present treatment's novel categorisation of state responses to perceived cable insecurity is a defining feature, in addition to the network-based competition lens which guides analysis and illustrates how Sino-US competition over submarine cable networks can inform competition in other network domains – including digital, infrastructure, production or capital.

2.4 Infrastructural Control Imperatives

I now turn to identify three imperatives which are driving new foreign and defence policies associated with submarine cables in the Indo-Pacific. These imperatives are *nodes*, *flows* and *production* (see Figure 3). Each of these factors is illustrated in turn and used as a typology in Section 5 to illustrate how states are attempting to attain and maintain centrality in submarine cable networks.

Nodes refers to the submarine cable network's physical geography and chokepoint positioning. Specifically, nodes consist of the physical network, including landing station locations, cable routes and interconnection

[106] Dwayne Woods and Junda Li, 'Dangerous Depths of Bifurcation: The Rise of "Inter-National Security Narcissists" and Undersea Cable (Dis)Connections', *Asian Security* 20, no. 2 (2024): 107, https://doi.org/10.1080/14799855.2024.2425296.

[107] Woods and Li, 'Dangerous Depths of Bifurcation: The Rise of "Inter-National Security Narcissists" and Undersea Cable (Dis)Connections', 107.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

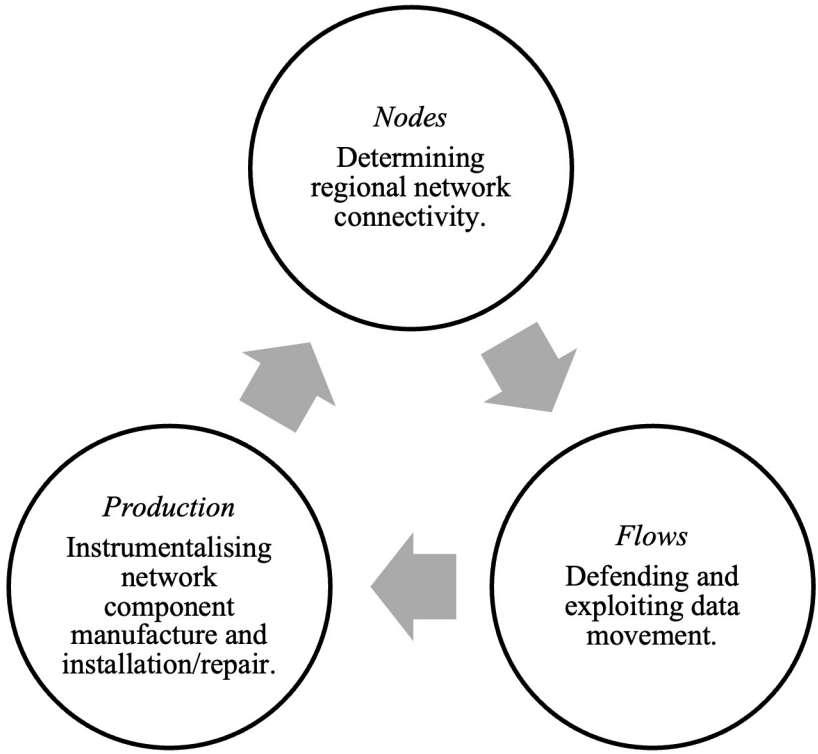


Figure 3 State Submarine Cable Control Imperatives.

(branching) points. By influencing and controlling network nodes, states can determine the contours of data flows and include or exclude fellow states in global data flows. States can attain forms of network centrality by controlling network nodes – creating privileged positions for themselves and/or allies/partners in data flows and through excluding others. Importantly, nodes denote the physical architecture of data connectivity, and centrality or control can be leveraged for strategic or economic gain.

Flows denote the data stream which transits submarine cable networks, such as Internet traffic, AI inference, cloud data or government communications, transferred across international boundaries. Controlling data movement is significant for states, whether defending flows from interruption or sabotage or exploiting for espionage or signals intelligence purposes. In this sense, flows create both a vulnerability and an opportunity for states – and this aspect is driving states to adopt policies which enable better control over data transmission.

Production pertains to the entire submarine cable network supply chain, from materials and components to specialised installation and repair

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

capacities. These firms and supply chains are significant as the owners, operators, builders and repairers of this infrastructure are primarily privately owned. Due to the concentrated nature of this specialised and sensitive industry, which operates at a global scale, many states are reluctant or unwilling to rely on suppliers headquartered in countries deemed politically untrustworthy. By developing sovereign or allied supply chain capacity, states reduce dependence on adversary suppliers for cable installation and repair, thereby avoiding vulnerabilities that could enable network exploitation.

These state imperatives are interconnected and are mutually reinforcing. For example, controlling nodes can better enable defence and exploitation of flows, and state influence over production can afford power over nodes. Section 5 employs this novel framework to analyse how various key Indo-Pacific states are attempting to attain positions of network centrality in submarine cable nodes, flows and production.

2.5 Conclusion

This section posited the analytical framework employed throughout this Element. Network-based competition illustrates how states compete for centrality in infrastructure networks, and weaponised interdependence demonstrates how these infrastructures can be exploited through the panopticon and chokepoint effects. My novel nodes-flows-production typology is a useful lens to understand how states in the Indo-Pacific are intervening in submarine cable networks, securing central network positions that reduce vulnerability but can create the structural conditions that risk weaponisation. The next section shifts focus to examine various suspicious cable incidents in Europe and the Indo-Pacific, which in combination have driven increased state intervention in this strategic communications domain.

3 Cable Breaks Abound: Accidental, Negligent or Malicious?

A spate of recent submarine cable incidents in Europe and the Indo-Pacific has revealed seabed insecurity as a renewed public policy concern. Whether in the Baltic Sea, the Red Sea or in the waters off Taiwan, these contemporary incidents share commonalities, including dragged anchors, plausible deniability or constrained and/or underwhelming responses from affected states. Although geographically dispersed, these incidents show how political instability or conflict on land can result in seabed insecurity. This section documents these important cases,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

demonstrating how these collectively foster conditions which are driving systematic state intervention in cable networks.

3.1 European Waters

While the European incidents occurred in the context of Russia's hybrid warfare campaign against NATO states during the Ukraine conflict, rather than driven by Sino-US competition, these nonetheless illustrate how geopolitical rivalry can manifest as seabed insecurity, thereby generating the climate of uncertainty and fear that is driving new cable policies. Instances of suspected[108] seabed warfare, which hadn't taken place since the Second World War, emerged as a key security concern in many European capitals as acts of suspected cable sabotage abounded. While these cases occurred in European rather than Indo-Pacific waters – the subject of this Element – these cases are nonetheless relevant for several reasons. First, while occurring in Europe, these incidents made headlines globally, meaning relevant government and military officials across the Indo-Pacific would have been (at minimum) aware of the incidents. Second and relatedly, these incidents demonstrated to officials outside Europe how possible modern grey-zone seabed warfare tactics can play out and how submarine cables can be targeted, in the context of a major continental war, in this case between Russia and Ukraine. Third, these cases demonstrate the strategic and commercial impacts of multiple simultaneous cable breaks under suspicious circumstances. Fourth, Europe's policy, legal and military responses illustrated to non-European states the options available to secure submarine cable networks, which could be adapted to local (in this case Indo-Pacific) contexts. Ultimately, I understand these European cases as a 'harbinger' for Indo-Pacific states, which have prompted new policy responses, as detailed in Section 4.

3.1.1 Svalbard: January 2022

In the lead-up to Russia's full-scale invasion of Ukraine, the first seabed incident to rattle European capitals occurred. On 7 January 2022, the Svalbard Undersea Cable System, which connects Norway's Svalbard Satellite Station and the Norwegian mainland, was partly severed. The Svalbard Satellite Station, the world's largest satellite ground station and located in the Arctic Circle, enables various critical functions for NASA and the European Organisation for the Exploitation of Meteorological

[108] Of the European cases outlined here, only the Nord Stream incident has been confirmed as sabotage.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Satellites, as well as facilitating European Space Agency Earth observation and Galileo and Copernicus satellite operations. Norway's Svalbard Archipelago is strategically located near Russia's Northern Fleet (tasked with nuclear deterrence patrols) based at Severomorsk in the Kola Peninsula and could play a role in maritime anti-access/area denial operations in the Barents Sea and the North Atlantic in the event of conflict.[109] The incident severed one of the two 1,300 kilometre fibres connecting the satellite station, owned by Space Norway, forcing the cable operators to rely on the backup link.[110] Heavy trawling was occurring in the vicinity of the cable network at the time of incident.[111] In the incident's aftermath, various analysts and journalists speculated about the possibility of foul play.[112] While police opened an investigation, no individual was charged, and the incident was never formally attributed. Despite Norwegian authorities' failure to pin a culprit, this incident was the first of several suspicious incidents to occur in Europe since 2022.

3.1.2 Nord Stream: September 2022

On 26 September 2022, three explosions ruptured the Nord Stream 1 and 2 natural gas pipeline network which connected Russia to Germany through the Baltic Sea. While not a submarine telecommunications cable network, this incident is nevertheless relevant and detailed here as it was a prominent example of seabed warfare against seabed critical infrastructure in the Baltic Sea. This incident occurred in the context of Russia's invasion of Ukraine involving tactics relevant to submarine cable protection. Moreover, the incident contributed to the perceived insecurity of seabed critical infrastructure globally – whether telecommunication cables or gas pipelines. Nord Stream 1 was opened in 2011 at a

[109] Andreas Østhagen et al., *Arctic Geopolitics: The Svalbard Archipelago*, CSIS Briefs (Center for Strategic and International Studies, 2023), 7, www.csis.org/analysis/arctic-geopolitics-svalbard-archipelago.

[110] Jacob Gronholt-Pedersen and Gwladys Fouche, 'Dark Arctic: NATO Allies Wake up to Russian Supremacy in the Region', *Reuters*, 16 November 2022, www.reuters.com/graphics/ARCTIC-SECURITY/zgvobmblrpd/.

[111] Håvard Gulldahl and Inghild Eriksen, 'This Is What the Damaged Svalbard Cable Looked like When It Came up from the Depths', Dk, *NRK*, 26 May 2024, www.nrk.no/tromsogfinnmark/this-is-what-the-damaged-svalbard-cable-looked-like-when-it-came-up-from-the-depths-1.16895904.

[112] Thomas Newdick, 'Undersea Cable Connecting Norway with Arctic Satellite Station Has Been Mysteriously Severed', *The War Zone*, 10 January 2022, www.twz.com/43828/undersea-cable-connecting-norway-with-arctic-satellite-station-has-been-mysteriously-severed; Atle Staalesen, '"Human Activity" behind Svalbard Cable Disruption', *The Independent Barents Observer* (Norway), 11 February 2022, https://thebarentsobserver.com/en/security/2022/02/unknown-human-activity-behind-svalbard-cable-disruption.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

cost of US$8 billion, and Nord Stream 2 was completed in September 2021 (but never operated) at a cost of US$11 billion.[113] While the network was majority owned by Russia's state-owned Gazprom, Western European energy firms had partnered and invested substantial sums in the gas network. News of the pipeline attack drew strong statements from European and world leaders. European Commission president Ursula Von der Leyen blamed the leaks as 'sabotage' and threatened that any attacks on Europe's energy infrastructure would be met with the 'strongest possible response'.[114] Then, US Secretary of State Antony Blinken called the incident 'apparent sabotage' and Mateusz Morawiecki, prime minister of Poland, added that the attack 'probably marks the next step of escalation of the situation in Ukraine'.[115] Kremlin spokesman Dmitry Peskov dismissed any Russian involvement in the attack as 'predictable, stupid and absurd'.[116]

According to reporting in the *Washington Post* in June 2023, classified documents allegedly released by former Air National Guardsman Jack Teixeira as part of 'The Discord Leaks' show that the CIA and European intelligence agencies were aware of a Ukrainian plot to attack the gas pipeline network as early as mid-2022.[117] This revelation prompted Russia's Deputy Head of the Security Council Dmitry Medvedev to state that 'we [Russia] have no constraints – even moral – left to prevent us from destroying the ocean floor cable communications of our enemies'.[118] In early February 2024 Sweden concluded its investigation, citing a lack of jurisdiction, and Danish police concluded its case later that month, citing that while sabotage did occur, there existed no

[113] 'Russia May Demand Compensation for Nord Stream Pipeline Blasts – Diplomat', Energy, *Reuters*, 27 March 2023, www.reuters.com/business/energy/russia-may-demand-compensation-over-nord-stream-explosions-diplomat-2023-03-27/.

[114] Philip Oltermann et al., 'European Leaders Blame Sabotage as Gas Pours into Baltic from Nord Stream Pipelines', Business, *The Guardian*, 27 September 2022, www.theguardian.com/business/2022/sep/27/nord-stream-1-2-pipelines-leak-baltic-sabotage-fears.

[115] Oltermann et al., 'European Leaders Blame Sabotage as Gas Pours into Baltic from Nord Stream Pipelines'.

[116] Merlyn Thomas and Elsa Maishman, 'Nord Stream Leaks: Sabotage to Blame, Says EU', *BBC News* (London), 28 September 2022, www.bbc.com/news/world-europe-63057966.

[117] Shane Harris et al., 'U.S. Had Intelligence of Detailed Ukrainian Plan to Attack Nord Stream Pipeline', *Washington Post* (Washington, DC), 6 June 2023, www.washingtonpost.com/national-security/2023/06/06/nord-stream-pipeline-explosion-ukraine-russia/.

[118] Guy Faulconbridge, 'Russia Now Has Free Hand to Destroy Undersea Communications Cables, Putin Ally Says', Europe, *Reuters*, 14 June 2023, www.reuters.com/world/europe/russias-medvedev-says-moscow-now-has-free-hand-destroy-enemies-undersea-2023-06-14/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

basis for a criminal case.[119] However, in mid-2024 Germany issued an arrest warrant for a Ukrainian diving instructor, whom it alleges sabotaged the pipeline with two fellow Ukrainian accomplices, although the Ukrainian government was not implicated.[120] While a gas pipeline and not a submarine telecommunications cable, the Nord Stream sabotage highlighted the vulnerabilities associated with Europe's seabed critical infrastructure during conflict. Neither pipeline has been repaired.

3.1.3 NewNew Polar Bear: October 2023

Another European gas pipeline, as well as various submarine telecommunication cables, was damaged in another suspicious incident in October 2023. This time, on 8 October 2023 the Hong Kong-flagged and Chinese-owned *NewNew Polar Bear* cargo ship dragged its anchor in the Baltic Sea and severed the €300 million European Union-financed Balticconnector bidirectional natural gas pipeline, which traverses 77 kilometres of sea between Inkoo in Finland and Paldiski in Estonia. Simultaneously, the anchor severed various submarine cable networks, including the Kingisepp-Kaliningrad System (Baltika), owned by Russia's Rostelecom and connecting St Petersburg through the Baltic Sea to the Russian exclave of Kaliningrad.[121] Also damaged was the Sweden-Estonia (EE-S1) cable network, owned by Arelion, GN Great Nordic and Telia Eesti, which connects Stavsnäs, Sweden with Kärdla and Tallinn in Estonia, and was operational in 1995.[122] Finally, one cable connecting Estonia and Finland owned by Internet service provider Elisa was also damaged on 8 October, although the exact cable was not disclosed.[123]

In the incident's aftermath, NATO Secretary General Jens Stoltenberg stated that if indeed the act was 'proven to be an attack on NATO

[119] Laura Gozzi, 'Nord Stream: Denmark Closes Investigation into Pipeline Blast', *BBC News* (London), 26 February 2024, www.bbc.com/news/world-europe-68401870.

[120] 'Nord Stream Sabotage: Germany Issues Arrest Warrant – DW – 08/14/2024', *Dw.Com*, 14 August 2024, www.dw.com/en/nord-stream-explosions-germany-issues-arrest-warrant/a-69933920.

[121] Mark Trevelyan, 'Russian Firm Says Baltic Telecoms Cable Was Severed as Chinese Ship Passed Over', Europe, *Reuters*, 7 November 2023, www.reuters.com/world/europe/russia-says-telecoms-cable-damaged-last-month-just-before-nearby-baltic-gas-2023-11-07/.

[122] John Granlund and Aris Velizelos, 'Finländsk Polis Pekar Ut "intressant" Ryskt Fartyg – Färdades Över Förstörd Svensk Kabel', *SVT Nyheter*, 18 October 2023, www.svt.se/nyheter/inrikes/misstankt-ryskt-fartyg-over-trasiga-undervattenskabeln.

[123] Jari Tanner, 'Damage to Gas Pipeline, Telecom Cable Connecting Finland and Estonia Caused by "External Activity"', World News, *AP News*, 10 October 2023, https://apnews.com/article/finland-estonia-pipeline-24d6623cf2778464fdb4ef1d85c70d91.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

critical infrastructure … it will be met by a united and determined response from NATO'.[124] Finland's Minister of European Affairs Anders Adlercreutz questioned how the *NewNew Polar Bear*'s captain could fail to realise he was dragging an anchor for hundreds of kilometres, adding that despite a lack of admissions, 'I think everything indicates that it was intentional'.[125] Finnish authorities declared that the damage 'could not have occurred by accident' and appeared to be a 'deliberate … external act'.[126] In August 2024, Chinese authorities in Beijing concluded a probe which found that indeed the *NewNew Polar Bear* did damage the gap pipeline and submarine telecommunication cables, but that the incident was accidental due to a 'strong storm'.[127] While the submarine cables were rapidly repaired, the Balticconnector repairs took six months, and gas was again flowing in April 2024.

3.1.4 Yi Peng 3: *November 2024*

The subsequent incident to rattle Europe occurred on 17 and 18 November 2024, when two submarine telecommunication cables were severed under suspicious circumstances. During the incident, the Chinese-flagged bulk carrier *Yi Peng 3* dragged its anchor while traversing the Baltic Sea, severing two submarine cable networks. The severed cables included the BCS East-West Interlink submarine cable which connects Sventoji, Lithuania with Sweden's Gotland Island. The 218 kilometre cable was commissioned in 1997 and is owned by Sweden's Arelion.[128] Also severed was the C-Lion1, owned by Finnish firm Cinia Oy and commissioned in 2016; this 1,172 kilometre cable connects Hanko and Helsinki

[124] Jon Henley, 'NATO Vows to Respond If Finland-Estonia Gas Pipeline Damage Is Deliberate', World News, *The Guardian*, 11 October 2023, www.theguardian.com/world/2023/oct/11/nato-vows-to-respond-if-finland-estonia-gas-pipeline-damage-is-deliberate.

[125] Claudia Chiappa and Pierre Emmanuel Ngendakumana, '"Everything Indicates" Chinese Ship Damaged Baltic Pipeline on Purpose, Finland Says', *POLITICO*, 1 December 2023, www.politico.eu/article/balticconnector-damage-likely-to-be-intentional-finnish-minister-says-china-estonia/.

[126] Jon Henley and Jillian Ambrose, 'Undersea Pipeline Damage Appears to Be Deliberate, Says Finland', World News, *The Guardian*, 10 October 2023, www.theguardian.com/world/2023/oct/10/undersea-pipeline-damage-appears-to-be-deliberate-says-finland.

[127] Finbarr Bermingham, 'Beijing Admits Hong Kong-Flagged Ship Destroyed Key Baltic Gas Pipeline "by Accident"', *South China Morning Post* (Hong Kong), 12 August 2024, www.scmp.com/news/china/diplomacy/article/3274120/china-admits-hong-hong-flagged-ship-destroyed-key-baltic-gas-pipeline-accident?module=perpetual_scroll_0&pgtype=article.

[128] 'Submarine Cable Map: BCS East-West Interlink', TeleGeography, 2025, www.submarinecablemap.com/submarine-cable/bcs-east-west-interlink.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

in Finland to Rostock in Germany.[129] Following the incident, Germany's Defence Minister Boris Pistorius told reporters that 'we have to say, without knowing exactly who it came from, that this is a hybrid action. We also have to assume, without knowing it yet, that it was sabotage'.[130] According to the Swedish Prosecution Authority, 'the offence is currently being investigated as sabotage'.[131]

Rather than allow *Yi Peng 3* to depart the Baltic Sea (as did *NewNew Polar Bear* in 2023), a Danish Navy ship pursued and intercepted the *Yi Peng 3*, and European warships surrounded the bulk carrier while investigations ensured. Investigators believed the *Yi Peng 3* severed both cables by intentionally dragging its anchor for over 160 kilometres in mild sea and weather conditions.[132] While the Kremlin press office stated that allegations of its involvement in the incident are 'absurd, unsubstantiated accusations', the *Wall Street Journal* reported that various Western law-enforcement and intelligence officials understand a link exists – indeed the vessel was carrying Russian fertiliser and had just departed Russia's Ust-Luga port prior to the incident.[133]

Following a month-long diplomatic delay, on 21 December 2024 China allowed German, Swedish, Finnish and Danish investigators to board the *Yi Peng 3*,[134] which had anchored in the Kattegat strait between Sweden and Denmark. Later that day, *Yi Peng 3* departed westward to resume commercial activity.[135]

[129] 'Submarine Cable Map: C-Lion1', TeleGeography, 2025, www.submarinecablemap.com/submarine-cable/c-lion1.

[130] 'Germany Says "Sabotage" Presumed in Damaged Baltic Sea Telecom Cables', *Al Jazeera*, 19 November 2024, www.aljazeera.com/news/2024/11/19/germany-says-sabotage-presumed-in-damaged-baltic-sea-telecom-cables.

[131] *Al Jazeera*, 'Germany Says "Sabotage" Presumed in Damaged Baltic Sea Telecom Cables'.

[132] Bojan Pancevski, 'Chinese Ship's Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables', *Wall Street Journal* (New York), 29 November 2024, www.wsj.com/world/europe/chinese-ship-suspected-of-deliberately-dragging-anchor-for-100-miles-to-cut-baltic-cables-395f65d1.

[133] Sebastian Moss, 'Investigators Suspect Baltic Sea Cable Cuts Were Deliberate, Chinese Ship to Blame', *Data Center Dynamics*, 28 November 2024, www.datacenterdynamics.com/en/news/investigators-suspect-baltic-sea-cable-cuts-were-deliberate-chinese-ship-to-blame/; Pancevski, 'Chinese Ship's Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables'.

[134] Anne Kauranen and Nerijus Adomaitis, 'Recent Suspected Underwater Sabotage Incidents in the Baltic Sea', *Reuters*, 3 January 2025, www.reuters.com/world/europe/recent-suspected-underwater-sabotage-incidents-baltic-sea-2024-12-03/.

[135] Miranda Bryant, 'Sweden Says China Denied Request for Prosecutors to Board Ship Linked to Severed Cables', World News, *The Guardian*, 23 December 2024, www.theguardian.com/world/2024/dec/23/china-refused-investigation-into-ship-linked-to-severed-baltic-cables-says-sweden.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

3.1.5 The Eagle S Incident: December 2024

While investigations into the *Yi Peng 3* were ongoing, another incident occurred on Christmas Day 2024, during which the Cook Islands flagged oil tanker *Eagle S* fouled four submarine telecommunication cables as well as one submarine electricity cable in the Baltic Sea. After departing Russia's Ust-Luga port (as did *Yi Peng 3*), *Eagle S* sailed westward through the Gulf of Finland within Finland's Exclusive Economic Zone dragging its anchor.[136] The *Eagle S*' anchor damaged several seabed infrastructures, including Estlink 2, a 650 megawatt, €320 million high-voltage power cable connecting Estonia and Finland, which was inaugurated in 2014 and connected Nordic and Baltic energy markets. Damaged also was the Finland–Estonia Connection 1 (FEC-1) and Finland–Estonia Connection 2 (FEC-2), both inaugurated in 2000 and owned by Finnish telecom Elisa, which connects Tallinn in Estonia and Helsinki in Finland. Both cable networks fouled by *Eagle S* were repaired by 7 January 2025.[137] Hong Kong-based CITIC Telecom International's Baltic Sea Submarine Cable network was also fouled by the *Eagle S*. The Baltic Sea Submarine Cable network, inaugurated in 2000 and measuring 1,042 kilometres, connects Tallinn in Estonia, Helsinki in Finland and Stockholm in Sweden.[138] Lastly, C-Lion1, severed by *Yi Peng 3* a little over a year earlier, was also fouled.

The *Eagle S* was formally seized by Finnish authorities on 26 December 2024. Finnish police and border guards commandeered the vessel and took charge of the bridge, holding it in Finnish territorial waters.[139] A Finnish court on 3 January 2025 rejected a request by the United Arab Emirates-based owners to release the vessel.[140] According to Estonian reporting, if the *Eagle S* was not stopped, its anchor would have impacted the Estlink 1 submarine power cable within half an hour and the recently

[136] Alexander Lott, 'Christmas Day Cable Cuts in the Baltic Sea', *EJIL: Talk!*, 31 December 2024, www.ejiltalk.org/christmas-day-cable-cuts-in-the-baltic-sea/.

[137] 'Elisa's Damaged Submarine Cables in the Baltic Sea Repaired', Elisa, 7 January 2025, https://elisa.com/corporate/news-room/press-releases/elisa's-damaged-submarine-cables-in-the-baltic-sea-repaired/87594841499067/.

[138] 'Submarine Cable Map: Baltic Sea Submarine Cable', TeleGeography, 2025, www.submarinecablemap.com/submarine-cable/baltic-sea-submarine-cable.

[139] David McHugh, 'Finland Stops Russia-Linked Vessel over Damaged Undersea Power Cable in Baltic Sea', *AP News*, 27 December 2024, https://apnews.com/article/eu-finland-estonia-baltic-sea-power-cable-6741ef1ce9130602abac6214d7297717.

[140] Essi Lehto, 'Finnish Court Upholds Seizure of Oil Tanker in Undersea Cables Probe', Europe, *Reuters*, 3 January 2025, www.reuters.com/world/europe/finland-court-rejects-owners-request-release-oil-tanker-2025-01-03/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

repaired Balticconnector gas pipeline within the hour.[141] The *Eagle S* is thought to be part of Russia's fuel tanker 'Shadow Fleet', which circumvents Western sanctions imposed associated with Russia's war against Ukraine, bypasses Western insurance regimes, is usually ageing and is owned by obscure entities.[142] Finnish Prime Minister Petteri Orpo told reporters that this latest damage 'underlies the danger of the [Russia's] shadow fleet in the Baltic Sea'.[143] In June 2025, Finland's National Bureau of Investigation concluded its investigation and charged the *Eagle S*' captain, first officers and second officers with aggravated sabotage and aggravated interference with telecommunications,[144] but in October 2025 the charges were dismissed by a Helsinki District Court citing a lack of jurisdiction and questions of intent.[145]

3.1.6 Europe's Response

These cumulative incidents have dramatically heightened tensions in the seas surrounding Europe and have resulted in a variety of responses from individual European states and multilateral European organisations. Various European nations are incorporating seabed critical infrastructure protection into respective defence and national security strategies. For example, according to Ireland's 2024 Defence Policy Review, the nation will place 'an immediate focus on our maritime domain and the protection of critical undersea infrastructure'.[146] According to France's 2022 National Strategic Review, the nation aims to better monitor and assess seabed activity to support France's advanced submarine cable

[141] Alexander Kryukov, 'Soome Hoidis Ära Ka Estlink 1 Lõhkumise Ja Balticconnectori Uue Lõhkumise', Välismaa, *ERR*, 28 December 2024, www.err.ee/1609561714/soome-hoidis-ara-ka-estlink-1-lohkumise-ja-balticconnectori-uue-lohkumise.

[142] McHugh, 'Finland Stops Russia-Linked Vessel over Damaged Undersea Power Cable in Baltic Sea'.

[143] Sebastian Moss, 'Finnish Authorities Board Ship Suspected of Cutting Subsea Internet and Power Cables', *Data Center Dynamics*, 26 December 2024, www.datacenterdynamics.com/en/news/finnish-authorities-board-ship-suspected-of-cutting-subsea-internet-and-power-cables/.

[144] Miranda Bryant, 'Finland Charges Tanker Crew Members with Sabotage of Undersea Cables', World News, *The Guardian*, 11 August 2025, www.theguardian.com/world/2025/aug/11/finland-accuses-tanker-crew-sabotage-undersea-cables-anchor.

[145] Tom Ruys and Yiannis Bamnios, 'Anchoring Criminal Jurisdiction at Sea: The Helsinki District Court's Eagle S Judgement and Its Impact for the Protection of Submarine Cables and Pipelines', *EJIL: Talk!*, 7 November 2025, www.ejiltalk.org/anchoring-criminal-jurisdiction-at-sea-the-helsinki-district-courts-eagle-s-judgement-and-its-impact-for-the-protection-of-submarine-cables-and-pipelines/.

[146] *Defence Policy Review* (Government of Ireland, 2024), 3, www.gov.ie/en/publication/78a1f-defence-policy-review-2024/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

industry and indeed, in January 2025, the French government purchased Alcatel Submarine Networks (ASN) – a world-leading submarine network business – from Nokia.[147] In 2022 France also released a first-of-its-kind public Seabed Warfare Strategy.[148] The Netherlands' 2024 Defence White Paper highlights Russian attempts at mapping North Sea underwater infrastructure and notes that 'sabotage is suspected' regarding the *NewNew Polar Bear* incident and its 2023 Security Strategy admits that 'the increased dependence on the North Sea and seabed for critical infrastructure gives opponents more opportunities to disrupt our society in part or whole'.[149] According to the United Kingdom's 2023 Defence Command Paper, its procurement of multi-role ocean surveillance vessels will 'further enhance protection of the undersea and seabed infrastructure that is essential to the UK's economic and energy security'.[150] The United Kingdom launched its Atlantic Bastion programme in December 2025, which will create a 'hybrid force' of autonomous vessels, AI and crewed platforms to defend submarine cables and pipelines.[151] Finland also considered seabed critical infrastructure in its 2024 Government Defence Report, noting that 'the safeguarding of uninterrupted trade, incident-free maritime transport and undersea infrastructure is critical to ensuring the continued safety, security and functioning of society in Finland'.[152]

[147] *National Strategic Review* (Government of the French Republic, 2022), 49, 51, www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf; 'Nokia Completes Its Sale of Leading Submarine Networks Business, ASN (Alcatel Submarine Networks), to the French State', Nokia, 3 January 2025, www.nokia.com/about-us/news/releases/2025/01/03/nokia-completes-its-sale-of-leading-submarine-networks-business-asn-alcatel-submarine-networks-to-the-french-state/.

[148] *Seabed Warfare Strategy: Report by the Working Group* (Ministère des Armées, 2022), www.archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf.

[149] *The Security Strategy for the Kingdom of the Netherlands* (Government of the Netherlands, 2023), 17, www.government.nl/topics/security-strategy-for-the-kingdom-of-the-netherlands/documents/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands; *Defence White Paper* (Government of the Netherlands, 2024), 12, https://english.defensie.nl/downloads/publications/2024/09/05/defence-white-paper-2024.

[150] *Defence Command Paper 2023: Defence's Response to a More Contested and Volatile World* (UK Ministry of Defence, 2023), www.gov.uk/government/publications/defence-command-paper-2023-defences-response-to-a-more-contested-and-volatile-world.

[151] 'UK Unveils New Undersea Warfare Technology to Counter Threat from Russia', UK Government, 8 December 2025, www.gov.uk/government/news/uk-unveils-new-undersea-warfare-technology-to-counter-threat-from-russia.

[152] *Government Defence Report* (Ministry of Defence, Finland, 2024), 32, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/166004/PLM_2024_7.pdf?sequence=4&isAllowed=y.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

At the multilateral level, NATO has launched a suite of initiatives to safeguard European seabed infrastructure. The NATO Critical Infrastructure Cell was stood up and held its first meeting in May 2024, at which NATO Secretary General Jens Stoltenberg noted that in response to Russia's hybrid campaign, 'the increasing dependency of our societies on undersea infrastructure means we need to do more to enhance their security'.[153] Also in 2024, NATO launched its Maritime Centre for the Security of Critical Undersea Infrastructure, an 'operational hub', based at NATO's Maritime Command in Northwood, United Kingdom.[154] In January 2025 NATO launched 'Baltic Sentry' – a collaborative military activity to bolster NATO's presence in the Baltic Sea to better defend seabed critical infrastructure.[155] As part of Baltic Sentry, a range of military platforms, including frigates, maritime patrol aircraft and naval drones, were deployed to improve NATO member countries' ability to deter and respond to seabed critical infrastructure incidents, and in September 2025 the mission was bolstered by further assets after 'unidentified drones' were detected near Denmark's military installations.[156] Also in January 2025, as part of Baltic Sentry, NATO announced TASK FORCE X, an initiative to better harness emerging technologies – including AI and autonomous systems – to better monitor and protect seabed critical infrastructure.[157]

In February 2025, the European Commission published its 'Joint Communication to Strengthen the Security and Resilience of Submarine Cables', which announced initiatives focussed on cable incident prevention, detection, response and deterrence, and also detailed a proposal to establish a Cable Vessel Reserve Fleet.[158] European Commission

[153] 'NATO Holds First Meeting of Critical Undersea Infrastructure Network', North Atlantic Treaty Organization, 23 May 2024, www.nato.int/cps/en/natohq/news_225582.htm.

[154] 'NATO Officially Launches New Maritime Centre for Security of Critical Undersea Infrastructure', NATO, 28 May 2024, https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui.aspx.

[155] 'NATO Launches "Baltic Sentry" to Increase Critical Infrastructure Security', NATO, 14 January 2025, www.nato.int/en/news-and-events/articles/news/2025/01/14/nato-launches-baltic-sentry-to-increase-critical-infrastructure-security.

[156] Jessie Williams, 'Nato to Step up Vigilance in Baltic Sea Region after Drones Spotted over Military Bases', World News, *The Guardian*, 27 September 2025, www.theguardian.com/world/2025/sep/27/denmark-new-drone-sightings-biggest-military-base.

[157] 'NATO TASK FORCE X: Deterring Today and Protecting Tomorrow', NATO, 31 January 2025, www.act.nato.int/article/nato-task-force-x/.

[158] *Joint Communication to Strengthen the Security and Resilience of Submarine Cables*, JOIN(2025) 9 final (European Commission, 2025), https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

executive vice president Henna Virkkunen stated that 'we want to make sure Europe is equipped not only to prevent and detect sabotage to cables but also to actively deter, repair and respond to any threat to critical infrastructure'.[159] The bloc is also making significant investments in new submarine cable networks through its Connecting Europe Facility Digital programme, which by December 2024 had invested €420 million in submarine cable projects that link the EU and its immediate region.[160] Lastly, the Joint Expeditionary Force – a UK-led multinational partnership with various European militaries which pools and coordinates high-readiness military forces – has deepened cooperation on seabed critical infrastructure protection since 2023 and has jointly monitored European critical seabed infrastructure using ships and aircraft.[161] Notably, European states have focussed primarily on the physical threat of cable cutting and sabotage, rather than espionage. This dynamic contrasts with the predominant Indo-Pacific discourse, which is shaped by concerns about data interception and signals intelligence collection through cable infrastructure.

3.2 Indo-Pacific Seabed Insecurity

In the Indo-Pacific, cable insecurity has emerged across two distinct regions: the waters off Taiwan, where repeated incidents have been linked to Chinese-flagged vessels, and the Red Sea, where Houthi attacks on merchant shipping have imperilled critical intercontinental cable routes. These regions are addressed in turn.

3.3 Taiwan

Submarine cable networks are routinely fouled in the waters off Taiwan – especially cable networks which connect Taiwan's outer islands located in the Taiwan Strait. Media reports have swirled for several years about suspicious damage to Taiwan's submarine cable networks.[162] Indeed, according to one report, between 2019 and 2023 Taiwan recorded

[159] 'EU to Spend Nearly a Billion Euros to Protect Undersea Cables', Europe, *Reuters*, 21 February 2025, www.reuters.com/world/europe/eu-will-propose-establishing-fleet-vessels-emergency-undersea-cable-repairs-2025-02-21/.

[160] *Joint Communication to Strengthen the Security and Resilience of Submarine Cables*, 4.

[161] Rosie Knighton, *What Is the Joint Expeditionary Force?*, Research Briefing no. 10074 (House of Commons Library, 2024), 4, https://researchbriefings.files.parliament.uk/documents/CBP-10074/CBP-10074.pdf.

[162] Elisabeth Braw, 'China Is Practicing How to Sever Taiwan's Internet', *Foreign Policy*, 21 February 2023, https://foreignpolicy.com/2023/02/21/matsu-islands-internet-cables-china-taiwan/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

thirty-six cable incidents associated with its submarine cable networks.[163] As a result of these incidents – and China's ongoing provocations against the state – Taipei is working actively to protect its digital seabed links.

Much of this cable insecurity is concentrated in the waters off Taiwan's Matsu Islands. The second of two networks which connect Taiwan's Matsu Islands was severed in May 2022, causing a ten-day Internet outage, relatively short due to the fact that repairs had already been arranged for the first fouled cable.[164] Then, in February 2023, two submarine cables which connect Taiwan's outlying Matsu Islands were severed in a six-day period, first by a Chinese fishing vessel and subsequently by the anchor of a Chinese cargo ship.[165] The 13,000 residents of Taiwan's Matsu Islands were effectively left without Internet access for 50 days until the first cable network was repaired, with severely limited connectivity provided by a microwave radio transmission system which prioritised critical government communications.

Further concerning incidents took place in 2025. On 3 January 2025, Taiwanese authorities briefly detained the Cameroon-registered vessel *Shun Xing 39*, suspecting it of dragging its anchor over – and as a result severing – the US-bound Trans-Pacific Express submarine cable.[166] Due to inclement weather, the vessel could not be boarded and subsequently departed Taiwanese waters. The vessel was thought to be owned by a Hong Kong firm linked to China and operating with a Chinese crew. According to Taiwan's Coast Guard with reference to the incident: 'we cannot rule out the possibility of a Chinese flag-of-convenience ship engaging in grey-zone harassment'.[167] Lloyd's List Intelligence reported that the vessel indeed had three identities – Tanzania-flagged *Xing Shun 39*, Cameroon-flagged *Shun Xing 39* and Cameroon-flagged *Xing Shun 39* – a 'deliberate deceptive practice'.[168]

[163] Kathleen Calderwood et al., 'Why Ships Lurking in Taiwan's Waters Could Be a "Prelude to a Coming War"', *ABC News*, 16 May 2025, www.abc.net.au/news/2025-05-17/is-china-cutting-taiwan-internet-cables-as-psychological-warfare/105281582.

[164] Wen Lii, 'After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience', *The Diplomat*, 15 April 2023, https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/.

[165] Lii, 'After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience'.

[166] Helen Davidson, 'Taiwan Investigating Chinese Vessel over Damage to Undersea Cable', World News, *The Guardian*, 7 January 2025, www.theguardian.com/world/2025/jan/07/taiwan-investigating-chinese-vessel-over-damage-to-undersea-cable.

[167] Davidson, 'Taiwan Investigating Chinese Vessel over Damage to Undersea Cable'.

[168] 'Taiwan Hunts Cable Cutter Disguised with 3 Digital Identities', *Lloyd's List Intelligence*, 13 January 2025, www.lloydslistintelligence.com/thought-leadership/blogs/taiwan-is-hunting-one-cable-cutting-vessel-disguised-with-three-separate-digital-identities.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Just one month subsequent, on 25 February 2025, the Taiwan-Penghu No. 3 subsea cable system was severed. According to reports, the Togolese-registered and China-linked cargo ship *Hongtai 58* (also known as *Hongtai168*) was anchored above the cable network for several days and did not respond to radio warnings to depart the cable grounds for fear of fouling the seabed networks.[169] The cable network was severed on 25 February 2025, and the Taiwanese Coast Guard swiftly intercepted the vessel, escorted it to Anping (on Taiwan's south-west coast) and boarded, detaining its crew.[170] In response, Beijing accused Taiwan of 'manipulating' China's involvement before the facts could be established.[171] Despite Beijing's protests, in June 2025 a court in Taiwan convicted the ship's captain to three years imprisonment for damaging the submarine cable network with an anchor, noting that 'the impact is enormous, and the defendant's actions should be severely condemned'.[172]

As a result of these incidents, Taiwan is attempting to alleviate its dependency on submarine cable networks by investing in alternative data transmission methods. The country is pursuing advanced satellite systems and investing in its indigenous space industry.[173] As an interim measure, Taiwan has developed communications balloons, which Wu Cheng-wen, Taiwan's science and technology minister, described as an 'intermediate solution' to restore emergency communications.[174] Improvements to Taiwan's telecommunications legislation – which would boost prison sentences and fines for cable damage – were also pursued.[175] In October 2025 Taiwan launched a new global initiative to enhance submarine cable security, dubbed the Management Initiative on International Undersea Cables, also known as 'RISK' an acronym for risk mitigation, information

[169] Cichen Shen, 'Taiwan Coastguard Detains Cargoship after Another Undersea Cable Break', Piracy and Security, *Lloyd's List*, 25 February 2025, www.lloydslist.com/LL1152686/Taiwan-coastguard-detains-cargoship-after-another-undersea-cable-break.

[170] Yimou Lee, 'Taiwan Detains China-Linked Cargo Ship after Undersea Cable Disconnected', Asia Pacific, *Reuters* (London), 25 February 2025, www.reuters.com/world/asia-pacific/taiwan-detains-china-linked-cargo-ship-after-undersea-cable-disconnected-2025-02-25/.

[171] 'China Says Taiwan "manipulating" Undersea Cable Cutting Incident before Facts Clear', Asia Pacific, *Reuters* (London), 26 February 2025, www.reuters.com/world/asia-pacific/china-says-taiwan-manipulating-undersea-cable-cutting-before-facts-clear-2025-02-26/.

[172] Ewe and Chiang, 'Taiwan Jails China Captain for Undersea Cable Sabotage'.

[173] Jane Rickards, 'Wary of Cable Sabotage, Taiwan Looks to Satellites as Back-Ups', *The Strategist*, 18 February 2025, www.aspistrategist.org.au/wary-of-cable-sabotage-taiwan-looks-to-satellites-as-back-ups/.

[174] Rickards, 'Wary of Cable Sabotage, Taiwan Looks to Satellites as Back-Ups'.

[175] Lii, 'After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve Its Communications Resilience'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

sharing, systemic reform and knowledge building.[176] According to Taiwan's Foreign Minister Lin Chia-lung, the initiative is a 'global partnership' and that Taiwan's experiences 'have taught us an important lesson – resilience cannot be taken for granted. It must be built through planning, implementation, and cooperation'.[177]

It is unclear whether these concerning incidents involving submarine cables in Taiwan's waters are accidental, negligent or malicious. Moreover, no concrete links have been made between these incidents and Beijing, or indeed the Baltic Sea incidents. Indeed, the waters off Taiwan are busy shipping routes, frequented by fishing and other commercial vessels and dredging is common. However, these incidents have been perceived by some as Chinese provocations, testing Taiwan's resolve and response or the strength of the US–Taiwan relationship,[178] possible probes ahead of a future invasion.[179] Whether or not these beliefs are valid, the relatively high number of submarine cable incidents off Taiwan's coats has contributed to a regional discourse of seabed insecurity, prompting defensive initiatives.

3.3.1 Red Sea

Another friction point for submarine cable networks on the periphery of the Indo-Pacific is the Red Sea. The Red Sea is a vital transit point for high-capacity cable networks connecting Asia, the Middle East, Africa and Europe. This narrow sea, connected to the Indian Ocean by the Bab al-Mandab choke point, is bordered by Yemen, Djibouti, Somalia and Eritrea. Soon after conflict returned to the Gaza Strip in October 2023, Yemen's Houthi rebels instigated a crisis in the Red Sea by attacking transiting vessels with links to Israel. Since November 2023, over fifty Houthi attacks against vessels have been recorded by the US Department of Transportation, including unmanned aerial vehicle attacks, unmanned surface vehicle attacks, ballistic missile and cruise missile attacks, amongst

[176] 'Taiwan Launches Undersea Cable Defense Plan', *Subsea Cables*, 28 October 2025, www.subseacables.net/industry-news/taiwan-launches-undersea-cable-defense-plan/.

[177] 'Taiwan Launches Global Initiative on Security of Undersea Cables', Government, Overseas Community Affairs Council, R.O.C. (Taiwan), 30 October 2025, www.ocac.gov.tw/OCAC/Eng/Pages/Detail.aspx?nodeid=329&pid=80857001.

[178] Hans Horan, 'Beijing's Targeting of Taiwan's Undersea Cables Previews Cross-Strait Tensions Under a Trump Presidency', *The Diplomat*, 17 January 2025, https://thediplomat.com/2025/01/%e2%80%8b%e2%80%8bbeijings-targeting-of-taiwans-undersea-cables-previews-cross-strait-tensions-under-a-trump-presidency/.

[179] Braw, 'China Is Practicing How to Sever Taiwan's Internet'; Calderwood et al., 'Why Ships Lurking in Taiwan's Waters Could Be a "Prelude to a Coming War"'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

other tactics.[180] In response, a twenty-four-nation coalition stood up Operation Prosperity Guardian in December 2023, which was tasked with ending the Houthi blockade and countering Houthi attacks against vessels transiting the Red Sea. Moreover, in January 2024 the US and UK coordinated air strikes against Houthi sites in Yemen.[181] The ongoing civil war and political instability in Yemen demonstrate how insecurity and volatility on land can deleteriously impact submarine data connectivity by delaying routine maintenance and emergency repair – with global implications.

On 24 February 2024, three major submarine cable networks reported faults in the Red Sea – the Asia Africa Europe-1 (AAE-1), Europe India Gateway (EIG) and the SEACOM/Tata TGN-Eurasia.[182] Coincidentally, just several days earlier on 18 February 2024, the Belize-flagged MV *Rubymar* was attacked by the Houthis while transiting the Red Sea. The vessel sank on 2 March 2024 – the first ship sunk by the Houthis during the crisis – and has subsequently been blamed by some for severing the submarine cable networks while drifting and dragging its anchor. According to US National Security Council spokesman John Kirby, 'those cables were cut, most likely by an anchor dragging from the Rubymar as she sank'.[183] Despite this view, the precise cause of these cable faults has not been confirmed.

Following the MV *Rubymar's* sinking, further high-capacity trunk cables were cut in 2024 and 2025. Despite being severed in February 2024 as above (and repaired by that July), the Asia Africa Europe-1 (AAE-1) cable was again severed in December 2024. Moreover, the PEACE submarine cable system was fouled in March 2025, also in the Red Sea. Then, in September 2025 four major subsea networks were severed in the vicinity of the Bab el-Mandeb Strait, including the South East Asia–Middle East–Western Europe 4 (SMW4), the India–Middle East–Western Europe

[180] 'MSCI Advisory: 2024-006-Southern Red Sea, Bab El Mandeb Strait, Gulf of Aden, Indian Ocean, Somali Basin, Arabian Sea, Gulf of Oman, Strait of Hormuz, and Persian Gulf-Threats to Commercial Vessels', US Department of Transportation, Maritime Administration, 2024, www.maritime.dot.gov/msci/2024-006-southern-red-sea-bab-el-mandeb-strait-gulf-aden-indian-ocean-somali-basin-arabian-sea.

[181] 'Conflict in Yemen and the Red Sea', Council on Foreign Relations, Global Conflict Tracker, 12 November 2025, https://cfr.org/global-conflict-tracker/conflict/war-yemen.

[182] Tim Stronge, 'What We Know (And Don't) About Multiple Cable Faults in the Red Sea', *TeleGeography*, 5 March 2024, https://blog.telegeography.com/what-we-know-and-dont-about-multiple-cable-faults-in-the-red-sea.

[183] Olivia Solon and Mohammed Hatem, 'Houthi-Sunk Ship's Anchor Likely Severed Sea Internet Cables', Politics, *Bloomberg*, 7 March 2024, www.bloomberg.com/news/articles/2024-03-06/anchor-from-houthi-sunk-ship-likely-damaged-undersea-cables.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

(IMEWE), the FALCON GCX as well as the Europe India Gateway.[184] Microsoft's widely used Azure cloud services were also disrupted by the cable outage.[185] According to one report, industry specialists attribute these outages to a commercial vessel's dragged anchor, and subsequent repairs were slow.[186]

For its part, the Houthis deny any efforts at disrupting cables, despite reports that a map of submarine cable networks in the Red Sea was posted to a Houthi-linked Telegram (messaging app) channel.[187] According to Yemeni rebel leader Abdel Malek al-Houthi, 'we have no intention of targeting sea cables providing internet to countries in the region'.[188] Rather, the chief concern in the Red Sea is the inordinately long repair time required to fix fouled cable networks due to onerous Yemeni permitting requirements and the difficulty for repair crews to operate in conflict zones. While the most economical route between Europe and Asia, owners and investors of new cable networks are now avoiding the Red Sea, perceiving it as a 'critical, high-risk single point of failure', according to an industry insider.[189] This case demonstrates how conflict and political instability can disrupt these critical infrastructures, prolonging maintenance and repair.[190] As the Red Sea is a transit point for high-capacity intercontinental subsea networks, cable breaks in this region have a disproportionately detrimental effect on global data connectivity.

3.4 Conclusion

These incidents have transformed the public perception of submarine cable infrastructures from hidden data conduits to critical liabilities and

[184] Saf Malik, 'Ship Likely Cut Subsea Cables in the Red Sea, Disrupting Connectivity across Three Continents', *Capacity Global*, 9 September 2025, https://capacityglobal.com/news/ship-likely-cut-subsea-cables-in-the-red-sea-disrupting-connectivity-across-three-continents/.

[185] Seher Asaf, 'Microsoft Azure Services Disrupted by Red Sea Cable Cuts', *BBC News* (London), 7 September 2025, www.bbc.com/news/articles/c3rvx470yg8o.

[186] Malik, 'Ship Likely Cut Subsea Cables in the Red Sea, Disrupting Connectivity across Three Continents'.

[187] Frank Gardner, 'Could the Houthis Sabotage Undersea Cables?', *BBC News* (London), 8 February 2024, www.bbc.com/news/world-middle-east-68231945.

[188] Quoted in Hanna Ziady, 'Red Sea Cables Have Been Damaged, Disrupting Internet Traffic', Business, *CNN*, 4 March 2024, www.cnn.com/2024/03/04/business/red-sea-cables-cut-internet.

[189] Loni Prinsloo et al., 'Google, Meta Delay Red Sea Cables as Security Risks Rattle Plans', *Bloomberg.Com*, 18 November 2025, www.bloomberg.com/news/articles/2025-11-17/google-meta-delay-red-sea-cables-as-security-risks-rattle-plans.

[190] Alan Mauldin, 'The Red Sea: A Key Subsea Cable Crossroads Under Siege', *TeleGeography*, 17 January 2024, https://blog.telegeography.com/the-red-sea-a-key-subsea-cable-crossroads-under-siege.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

targets. Europe's spate of cable cuts, blamed on Russia's hybrid operations, has prompted a militarised response, evidenced through NATO's Baltic Sentry and respective national cable protection strategies. In the Indo-Pacific, repeated incidents off Taiwan indicate possible grey-zone Chinese activity, and Red Sea instability shows how conflict imperils global connectivity through repair delays. In sum, these incidents indicate that cables are vulnerable and that attributing incidents (legally or otherwise) can be challenging. While several major Indo-Pacific interventions preceded these incidents, these incidents since 2022 have validated early concerns and accelerated competitive positioning. The next section details key Indo-Pacific state policy responses that began in the mid-2010s and intensified following these incidents, showing how states compete for network centrality amid renewed recognition of cable vulnerability.

4 The Indo-Pacific Adapts

As China's Digital Silk Road and expanding cable industry challenged Western dominance from 2015 onwards, cables re-entered Indo-Pacific strategic competition after decades of relative stability. The incidents documented in Section 3 validated these concerns and intensified policy responses. This section maps both early interventions and recent accelerations. This empirical section highlights how various key Indo-Pacific states and blocks are adapting to perceived submarine cable vulnerability and reshaping regional connectivity. I commence by examining early efforts by the BRICs grouping to lay its own submarine cable network. The analysis then turns to China's various efforts at increasing its market capitalisation, including through the Digital Silk Road and state-subsidised industry. Efforts by Quad nations both collectively and individually are then examined, in addition to the Trilateral Partnership for Infrastructure Investment in the Indo-Pacific. The interventions this section analyses demonstrate network-based competition in operation, as Indo-Pacific states actively mould network topologies but create conditions that risk weaponisation as states seek to reduce respective vulnerabilities – interventions that can be understood across the nodes, flows and production dimensions (introduced in Section 2). While the nodes-flows-production typology provides analytical clarity, in practice these imperatives frequently overlap as the same initiative, or policy, can simultaneously pursue nodal control, flow security and production dominance. Section 5 untangles these dimensions.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

4.1 BRICS

One of the first attempts at challenging Western submarine cable network dominance in the post–Cold War era was undertaken by the BRICS. The grouping, which then consisted of Brazil, Russia, India, China and Saudi Arabia (but has since expanded), in 2012 sought to construct a 34,000 kilometre submarine cable network, dubbed the 'BRICS Cable'.[191] It was hoped that the BRICS Cable, expected to cost US$1.5 billion and operational by 2014, would better facilitate communications between the bloc and, in turn, promote trade and investment amongst the grouping. The BRICS Cable network would also better connect Africa (through South Africa) with BRICS member nations.[192] The proposed cable network was turbocharged in 2013 when US National Security Agency contractor Edward Snowden disclosed a cache of highly classified documents to the media, many of which overviewed how the United States and its allies monitor and intercept data flowing through submarine cable networks, a practice known as 'upstream' collection.[193] The Snowden Disclosures gave BRICS members another reason to pursue a submarine cable network – to safeguard data integrity by routing around US and Western signals intelligence collectors. According to analyst Lane Burdette, Brazil was a key proponent of the BRICS cable network, as the South American nation perceived an overreliance on US data routing.[194]

In 2015 the BRICS cable idea was shelved. While the exact reason for the project's failure is murky, some blame a lack of finances,[195] while others point to a lack of cohesion amongst the grouping.[196] According to scholar Daya Kishan Thussu, the BRICS Cable 'would have been a

[191] James Barton, 'South Africa – The Keystone in the BRICS Cable System', Optical & Fixed Networks, *Developing Telecoms*, 2 May 2012, https://developingtelecoms.com/tech/optical-fixed-networks/3885-south-africa-the-keystone-in-the-brics-cable-system.html.

[192] Gao Wanglai, 'BRICS Cybersecurity Cooperation: Achievements and Deepening Paths', *China International Studies* 68 (January 2018): 131, HeinOnline.

[193] Timberg, 'Slide Shows NSA Surveillance of Data from Undersea Cables'.

[194] Lane Burdette, 'Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy', *Journal of Public & International Affairs*, 2021, https://jpia.princeton.edu/news/leveraging-submarine-cables-political-gain-us-responses-chinese-strategy.

[195] *Submarine Telecoms Industry Report*, Issue 3 (Terabit Consulting, 2014), 11, www.terabitconsulting.com/mt-content/uploads/2018/01/2014-submarine-cable-market-industry-report_5a6f58f26e92a.pdf.

[196] Stacia Lee, 'International Reactions to U.S. Cybersecurity Policy: The BRICS Undersea Cable', *The Henry M. Jackson School of International Studies*, 8 January 2016, https://jsis.washington.edu/news/reactions-u-s-cybersecurity-policy-bric-undersea-cable/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

symbolic act of di-Americanizing the infrastructure of the Internet'.[197] Although the BRICS cable never eventuated, BRICS leaders continue to prioritise digital infrastructure. According to the 2024 Kazan Declaration, member states are encouraged to 'explore the possibility for joint activities in the field of digital infrastructure to ensure the integrity, stability of the functioning and security of national segments of the Internet'.[198] The failed BRICS Cable case demonstrates how both economic and security imperatives drove an attempt to intervene in the submarine telecommunication network ecosystem.

4.2 China

In this era of heightened international tensions, China is actively furthering regional connectivity via submarine cable networks in line with its national interest – as Beijing considers cable networks a security concern.[199] This section outlines China's political-level strategy including its Belt and Road and Digital Silk Road strategies, its growing cable industry and how its illegal claim over the South China Sea is deleteriously affecting submarine cable connectivity for neighbouring nations.

4.2.1 The Digital (Information) Silk Road

While China consolidated its submarine cable connectivity projects under its Digital Silk Road in 2015 (part of the Belt and Road Initiative), many of the projects were already being pursued as part of China's 'informatisation' efforts as well as via its 'Digital China' strategy.[200] The Belt and Road Initiative is China's signature international development programme, which, according to scholars Colin Flint and Cuiping Zhu, is an effort at simultaneous 'economic integration, regional influence, and global geopolitical competition'.[201] Informatisation refers to 'the introduction of digital

[197] Daya Kishan Thussu, 'BRICS De-Americanizing the Internet?', in *BRICS Media: Reshaping the Global Communications Order?*, 1st ed., ed. Daya Kishan Thussu and Kaarle Nordenstreng, Internationalizing Media Studies (Routledge, 2021), 281.

[198] *Kazan Declaration: Strengthening Multilateralism for Just Global Development and Security*, XVI BRICS Summit (BRICS, 2024), 20, https://cdn.brics-russia2024.ru/upload/docs/Kazan_Declaration_FINAL.pdf?1729693488349783.

[199] Jun Zhang, 'Heading in the Direction of Bifurcated Networks: Hong Kong's Evolution amidst the Global Submarine Cable System', *Asian Review of Political Economy* 3, no. 1 (2024): 20, https://doi.org/10.1007/s44216-024-00029-1.

[200] April A. Herlevi, 'China's Strategic Space in the Digital Undersea', The National Bureau of Asian Research, Essay Series, *Mapping China's Strategic Space*, 14 March 2024, https://strategicspace.nbr.org/chinas-strategic-space-in-the-digital-undersea/.

[201] Flint and Zhu, 'The Geopolitics of Connectivity, Cooperation, and Hegemonic Competition: The Belt and Road Initiative', 95.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

technologies and the leveraging of data and information to make more efficient all aspects of the economy and government',[202] while 'Digital China', a core element of the nation's 14th Five-Year Plan (published in 2021), furthered informatisation through accelerated digitised development.[203] Furthermore, the nation's 'Made in China 2025' strategy (published in 2015) prioritised 'internet infrastructure', including accelerating the construction and development of fibre-optic networks.[204]

Against this policy backdrop, China's efforts at promoting submarine cable network resilience, connectivity and production beyond its borders are now consolidated under its Digital Silk Road initiative. Part of the Belt and Road Initiative (originally announced in 2013), the Digital Silk Road (announced in 2015) focussed China's efforts on submarine cable network construction. According to its March 2015 official 'Action Plan on the Belt and Road Initiative':

> We should jointly advance the construction of cross-border optical cables and other communications trunk line networks, improve international communications connectivity, and create an Information Silk Road. We should build bilateral cross-border optical cable networks at a quicker pace, plan transcontinental submarine optical cable projects, and improve spatial (satellite) information passageways to expand information exchanges and cooperation.[205]

In 2017, China released its 'Vision for Maritime Cooperation under the Belt and Road Initiative' which emphasised promoting 'maritime connectivity' including submarine cable networks.[206] The vision highlighted the Asia Pacific Gateway (APG) cable network (NEC-laid which connects East Asia to Southeast Asia) as a completed project under the initiative. Also in 2017, China's vice-minister at the Ministry of Industry and

[202] Rogier Creemers and Paul Triolo, 'Analyzing China's 2021–2025 Informatization Plan', *DigiChina, Stanford University*, 24 January 2022, https://digichina.stanford.edu/work/analyzing-chinas-2021-2025-informatization-plan-a-digichina-forum/.

[203] 'Translation: 14th Five-Year Plan for National Informatization', *DigiChina*, 2021, https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/.

[204] *Notice of the State Council on the Publication of 'Made in China 2025'*, no. 28 (PRC State Council, 2015), 13, https://cset.georgetown.edu/publication/notice-of-the-state-council-on-the-publication-of-made-in-china-2025/.

[205] 'Action Plan on the Belt and Road Initiative', Government, The State Council, The People's Republic of China, 30 March 2015, www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm.

[206] 'Vision for Maritime Cooperation under the Belt and Road Initiative', Government, The State Council, The People's Republic of China, 20 June 2017, www.gov.cn/archive/publications/2017/06/20/content_281475691873460.htm.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Information Technology, Chen Zhaoxiong, told attendees at the Fourth World Internet Conference in Wuzhen that as part of his nation's Digital Silk Road, China's 'info-communications industry will not only pay attention to our own development, but also other countries across the world'.[207] From its inception, China's approach to submarine cable network connectivity took a distinctly international rather than domestic character.

Several years subsequent, in 2022, China's State Council Information Office published a White Paper articulating its international cyberspace agenda. According to the document, its top priority was information infrastructure construction, and the White Paper articulated how cable network projects contribute to improve connectivity amongst BRI participating countries.[208] According to the White Paper:

> Chinese enterprises have provided support for many countries in constructing information and communications infrastructure, opening up digital information expressways for other developing countries. By laying cables and building base stations, China has helped expand the coverage of optical communication in these countries, giving a powerful boost to local telecommunications.[209]

In recent years, China has declared its submarine cable network achievements as part of the BRI and the Digital Silk Road. In China's October 2023 White Paper on its Belt and Road Initiative, the nation spruiked its Digital Silk Road achievements, including progress constructing various international submarine cables, without naming networks.[210] Also, according to a report published by China's World Internet Conference in 2023, the US$290 million Asia Direct Cable (ADC) System, led by China Telecom but laid by Japan's NEC, has been labelled a Belt and Road project.[211]

[207] Andrew Moody and Cheng Yu, '"Digital Silk Road" Expected to Link World', Europe, *China Daily* (Beijing), 12 August 2017, https://europe.chinadaily.com.cn/epaper/2017-12/08/content_35256662.htm.

[208] 'Jointly Build a Community with a Shared Future in Cyberspace', Government, The State Council Information Office, The People's Republic of China, 7 November 2022, http://english.scio.gov.cn/whitepapers/2022-11/07/content_78505694_5.htm.

[209] The State Council Information Office, The People's Republic of China, 'Jointly Build a Community with a Shared Future in Cyberspace'.

[210] 'The Belt and Road Initiative: A Key Pillar of the Global Community of Shared Future', Government, The State Council Information Office, The People's Republic of China, 10 October 2023, http://english.scio.gov.cn/whitepapers/2023-10/10/content_116735061_5.htm.

[211] *Collection of Practice Cases of Jointly a Community with a Shared Future in Cyberspace* (World Internet Conference, 2023), 8, www.wicinternet.org/pdf/CollectionofPracticeCasesofJointlyBuildingaCommunitywithaSharedFutureinCyberspace2023.pdf.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Of note, while China's cable network projects have primarily been intra-Asia, efforts at digitally connecting Africa are also a feature of China's strategy. In July 2024, Jin Zhuanglong, China's Minister of Industry and Information Technology spoke about China's assistance to create a 'digital Africa' – which will include both submarine and terrestrial cable assistance.[212] In sum, although it is difficult to attribute cable networks directly to the nebulous Belt and Road Initiative or the Digital Silk Road, laying new submarine cable networks by Chinese firms is a cornerstone of China's efforts at remaking global digital information flows as part of its flagship foreign policy initiative.

4.2.2 China's Growing Cable Industry

To implement China's efforts at increased market capitalisation globally, its primary submarine cable network firm is HMN Technologies (herein HMN Tech) – formerly Huawei Marine Networks, then a division of Huawei Technologies. Of the over 600 operational cable networks in 2025, 40 were supplied by HMN Tech (including under its former guise of Huawei Marine Networks).[213] While many HMN Tech networks are small domestic networks, large projects include the 25,000-kilometre PEACE Cable network which connects Singapore to France via Maldives, Pakistan, Seychelles, Kenya, Somalia, Saudi Arabia, Egypt, Cyprus, Malta and Tunisia. The firm was slated to lay the South East Asia–Middle East–Western Europe 6 (SeaMeWe-6) cable network until the United States government intervened in 2023, resulting in the contract being awarded to US-based SubCom[214] and in response China planned a US$500 million cable network that would rival SeaMeWe-6.[215] Although HMN Tech's footprint is global, no HMN Tech-supplied cable network connects India, Australia, the United States or Japan.

The firm has faced strong geopolitical headwinds. After rapidly gaining market share in the 2010s, the United States placed Huawei Technologies and many of its affiliates on its 'Entity List', which restricted the firms'

[212] 'China, Africa Move to Strengthen Digital Cooperation', Government, The State Council, The People's Republic of China, 30 July 2024, www.gov.cn/news/202407/30/content_WS66a821e0c6d0868f4e8e990b.html.

[213] 'Submarine Cable Map – HMN Tech', TeleGeography, 2025, www.submarinecablemap.com/supplier/hmn-tech.

[214] Joe Brock, 'U.S. and China Wage War beneath the Waves – over Internet Cables', *Reuters*, 24 August 2023, www.reuters.com/investigates/special-report/us-china-tech-cables/.

[215] Joe Brock, 'China Plans $500 Million Subsea Internet Cable to Rival US-Backed Project', China, *Reuters* (Singapore), 6 April 2023, www.reuters.com/world/china/china-plans-500-mln-subsea-internet-cable-rival-us-backed-project-2023-04-06/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

purchase of US-made parts and components.[216] In 2020, after sustained pressure against the firm by the United States, Huawei technologies divested Huawei Marine Networks, and an 81 per cent stake was acquired by Suzhou-headquartered Hengtong Group – a large Chinese optical fibre and power cable manufacturer. The firm was renamed as HMN Technologies (shortened to HMN Tech) and in a statement upon rebranding, the firm noted that 'HMN Tech remains an independent joint venture entity with an independent board and management team'.[217] According to the firm, in the last 10 year it has participated in over 100 projects and constructed in excess of 60,000 kilometres of submarine cables worldwide.[218] An HMN Tech corporate video notes that 'in the past decade, we have left our mark on the world'.[219]

China is also a major regional hub for submarine cable repair capabilities. Cable repair capacity is concentrated in S.B. Submarine Systems (SBSS). Originally a joint venture between the Chinese government and UK-registered Great Eastern Telecommunications in 1995, in 2005 British-headquartered Global Marine Systems became a major stakeholder.[220] SBSS' ships contribute to a regional consortium which repairs cables (including American) in the Pacific's Yokohama Zone.[221] However, in mid-2024 SBSS was embroiled in international controversy after Wall Street Journalists accused the firm's vessels of hiding location data and reported that US officials are warning telecommunication companies that SBSS crews could tamper with cables during repairs.[222] This scandal promoted SBSS to issue a public statement, noting that it operates honestly, transparently and legally and that it opposes the 'generalization of a national security concept to suppress and discredit our company'.[223] Despite this, due to concerns over China's ability to interfere with cable networks via SBSS (parent company is now China Telecom which is part

[216] David Shepardson and Karen Freifeld, 'China's Huawei, 70 Affiliates Placed on U.S. Trade Blacklist', Business, *Reuters*, 16 May 2019, www.reuters.com/article/business/chinas-huawei-70-affiliates-placed-on-us-trade-blacklist-idUSKCN1SL2W4/.

[217] 'Huawei Marine Networks Rebrands as HMN Technologies', HMN Tech, 3 November 2020, www.hmntech.com/enPressReleases/37764.jhtml.

[218] *HMN Tech Corporate Video*, 2025, 4:16, www.hmntech.com/enCorporateVideo.jhtml.

[219] *HMN Tech Corporate Video*.

[220] 'SBSS Company History', SBSS, 2025, www.sbss.com/en/site/history.

[221] Dustin Volz et al., 'China Poses Espionage Threat To Undersea Cables, U.S. Fears', *The Wall Street Journal* (New York), 20 May 2024, www.wsj.com/public/resources/documents/J85vUfSru4fvpSlPPhtV-WSJNewsPaper-5-20-2024.pdf.

[222] Volz et al., 'China Poses Espionage Threat To Undersea Cables, U.S. Fears'.

[223] 'Statement on the Wall Street Journal Article', SBSS, 23 May 2024, www.sbss.com/en/site/news_details/268.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

of the state-owned China Telecommunications Corporation), Global Marine is reportedly divesting its stake in the Chinese firm.[224]

4.2.3 South China Sea and Alternate Networks

Another way in which China is attempting to shape submarine cable network dynamics is through its contested control over the South China Sea. Specifically, China's illegal claim over this strategic seascape is being pursued, in part, by denying cable installation and repair requests from non-Chinese firms.[225] Moreover, cable repairs in this relatively shallow sea are considerably delayed, and many applications are being rejected.[226] Vietnam's subsea conduits have been particularly affected by China's unlawful annexation of the South China Sea. In 2023, when all five of Vietnam's submarine cable networks were severed, repairs took eight long months to complete. Moreover, in April 2024 a cable ship working within Vietnam's Exclusive Economic Zone and escorted by a Vietnamese naval vessel was confronted by a Chinese coastguard ship demanding information about the cable ship's work and loitering near the cable grounds.[227] As a result of China's South China Sea claim and resulting interference in cable networks, non-Chinese installers are increasingly wary of working in this contested seascape, and many new submarine cable networks are, if possible, avoiding the sea altogether, for example, transiting the Indonesian Archipelago between Singapore and the Pacific Ocean – as discussed in more detail below. According to Mao Ning, a Chinese Foreign Ministry spokesperson, China 'has always taken a welcoming attitude and supported other countries and telecommunications companies in laying international submarine cables in waters under China's jurisdiction'.[228] However, evidence suggests this sentiment does not apply in the South China Sea.

China has moved quickly to secure its seabed lines of communication through high-level political strategies including the Digital Silk Road and through fostering a cable industry which can effectively lay and repair cable networks. While it's difficult to ascertain the exact nature of the

[224] Danny D'Cruze, 'US Warns Google, Meta about Risk of Chinese Repair Ships Tampering with Undersea Internet Cables', *Business Today*, 20 May 2024, www.businesstoday.in/technology/news/story/us-warns-google-meta-about-risk-of-chinese-repair-ships-tampering-with-undersea-internet-cables-430205-2024-05-20.

[225] Rebecca Tan, 'Escalating Contest over South China Sea Disrupts International Cable System', *The Washington Post*, 3 October 2024, Gale Academic OneFile, https://link.gale.com/apps/doc/A811068087/AONE?u=unimelb&sid=ebsco&xid=104fe9ce.

[226] Tan, 'Escalating Contest over South China Sea Disrupts International Cable System'.

[227] Tan, 'Escalating Contest over South China Sea Disrupts International Cable System'.

[228] Tan, 'Escalating Contest over South China Sea Disrupts International Cable System'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

relationship between Beijing and its submarine cable industry or the relationship between the Belt and Road Initiative and claimed BRI-backed cable network projects, it's clear that China has lofty ambitions for submarine cable connectivity and plans to dislodge the West's cable primacy.

4.3 The Quad

The preceding analysis groups the United States, India, Australia, Japan and India under a Quad umbrella, as this grouping has centralised various submarine cable network security initiatives. As such, the preceding analysis will detail common Quad initiatives before shifting to focus on how each Quad state is progressing on submarine cable security issues unilaterally. However, the preceding analysis proves that the unilateral versus multilateral distinction can be ambiguous, and at the time of writing, many of these efforts are still latent. The Quad grouping first announced its plans to shape submarine cable networks in May 2023 via a new 'Quad Partnership for Cable Connectivity and Resilience'.[229] At that time, according to a joint statement, the partnership was intended to 'strengthen cable systems in the Indo-Pacific, drawing on Quad countries' world-class expertise in manufacturing, delivering and maintaining cable infrastructure'.[230] As part of this partnership, Australia agreed to establish the 'Indo-Pacific Cable Connectivity and Resilience Program', later renamed the 'Cable Connectivity and Resilience Centre' and analysed below.[231]

On 21 September 2024, Quad heads of state released 'the Wilmington declaration' at the fourth Quad Leaders' Summit. In noting that 'the Quad is here to stay' and that 'robust funding' will be directed at Quad priorities, the Declaration celebrated the Quad Partnership for Cable Connectivity and Resilience's successes, including Australia's Cable Connectivity and Resilience Centre (outlined below), Japan's provision of technical assistance in the Pacific, and the United States' CABLES Program (outlined below) achievements.[232] The declaration noted plans

[229] 'Quad Leaders' Joint Statement', Government, Australian Department of the Prime Minister & Cabinet, 20 May 2023, www.pm.gov.au/media/quad-leaders-joint-statement.

[230] Australian Department of the Prime Minister & Cabinet, 'Quad Leaders' Joint Statement'.

[231] 'Quad Leaders' Summit 2023: Infrastructure', Government, Australian Government Department of the Prime Minister and Cabinet, 2023, www.pmc.gov.au/resources/quad-leaders-summit-2023/infrastructure.

[232] 'Joint Statement from the Leaders of Australia, India, Japan, and the United States: The Wilmington Declaration', Government, Australian Department of the Prime Minister & Cabinet, 21 September 2024, www.pm.gov.au/media/joint-statement-leaders-australia-india-japan-and-united-states.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

to connect all Pacific Island nations with cable networks and that since the previous Quad Leaders' Summit, US$140 million in cable network funding had been committed. The declaration noted that the leaders 'underscore our commitment to an inclusive, open, sustainable, fair, safe, reliable and secure digital future'.[233]

Several days later on 25 September 2024, a US-proposed statement titled 'The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World' was endorsed by Quad members, the UK and the EU, as well as Canada, the Federated States of Micronesia, Finland, France, the Marshall Islands, the Netherlands, New Zealand, Portugal, the Republic of Korea, Singapore, Tonga and Tuvalu. The 'New York Statement' acknowledged the criticality of submarine cable networks and society's corresponding dependency and vulnerability. Endorsers agreed to a range of principles including resilient and redundant design, use of 'secure and verifiable' suppliers with clear governance and ownership structures, close industry and government coordination, better spatial and route planning, best practice sharing, third-country influence risk assessments, data risk mitigation frameworks and, finally, adherence to international law.[234] Of note, the New York Declaration articulated how submarine cable networks regard not only the length of submerged cable but are also part of a broader ecosystem, which includes elements related to 'construction, operation, surveillance, maintenance and repair, such as landing stations, software, and the terrestrial parts of the submarine cable connecting to them, repair centers, as well as the fleet of deployment, maintenance and repair vessels'.[235]

Announced in late 2024 were plans to create a 'Quad Action Plan to Protect Commercial Undersea Telecommunications Cables', although at the time of writing this action plan has not yet materialised. The Trump Administration's approach to the Quad remains to be fully determined, though the grouping has continued to engage and the administration has not signalled an intention to abandon it.

[233] Australian Department of the Prime Minister & Cabinet, 'Joint Statement from the Leaders of Australia, India, Japan, and the United States: The Wilmington Declaration'.

[234] 'The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World', Government, Australian Department of Foreign Affairs and Trade, 25 September 2024, www.dfat.gov.au/international-relations/regional-architecture/quad/cable-connectivity-and-resilience-centre/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world, www.dfat.gov.au/international-relations/regional-architecture/quad/cable-connectivity-and-resilience-centre/new-york-joint-statement-security-and-resilience-undersea-cables-globally-digitalized-world.

[235] Australian Department of Foreign Affairs and Trade, 'The New York Statement'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

4.4 United States

The United States deploys several strategies to further submarine cable networks in its national interest. This section overviews US strategy concerning cable security and its 'Team Telecom' before examining the US' efforts at a cable repair fleet and its diplomatic efforts including the CABLES Program. At the time of writing, the impact of the Trump Administration on cable security policy issues is unclear. As is clear, the United States is a key player in subsea communications, and since 2018 has dramatically increased its efforts primarily at nullifying China's efforts at increased market capitalisation and also at cable flow resilience.

4.4.1 Central and Foreign Strategy

At the strategic level, while not mentioning submarine cables specifically, the United States' 2022 'National Security Strategy' highlights technology as a core element of modern geopolitical competition – noting that 'the digital backbones of the modern economy must be open, trusted, interoperable, reliable, and secure'.[236] The National Security Strategy also commits US Government investment in 'high-quality digital infrastructure' in the Global South.[237] Likewise, the 2022 US Indo-Pacific Strategy committed the nation to promoting 'secure and trustworthy digital infrastructure' in the region.[238] The Biden Administration's March 2023 National Cybersecurity Strategy places a priority on international supply chains, noting how the US, in collaboration with partners and allies, will 'implement best practices in cross-border supply chain risk management and work to shift supply chains to flow through partner countries and trusted vendors'.[239] In May 2024, the US Department of State published its 'International Cyberspace & Digital Policy Strategy' which listed enhancing submarine cable resilience and security as a specific priority line of effort.[240] According to US assessments, cable disruption and destruction due to accidents, natural disasters or hostile actions

[236] *National Security Strategy* (The White House, 2022), 32–33, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf.
[237] *National Security Strategy*, 34.
[238] *Indo-Pacific Strategy of the United States* (The White House, 2022), 17, https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf.
[239] *National Cybersecurity Strategy* (The White House, 2023), 37, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[240] *United States International Cyberspace & Digital Policy Strategy*, Government (US Department of State, 2024), www.state.gov/wp-content/uploads/2024/06/United-States-International-Cyberspace-and-Digital-Strategy.pdf.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

are a key vulnerability. Also, the strategy articulates how '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'.[241]

Both the first Trump and subsequent Biden administrations implemented various diplomatic projects and initiatives which aimed at submarine cable security. Specifically, the Trump Administration launched its Digital Connectivity and Cybersecurity Partnership (DCCP) in 2018, which continued through the Biden Administration and concluded in 2024. Launched in July 2018 as a whole-of-government initiative with an initial US$25 million investment, the DCCP aimed to promote an 'open, interoperable, secure, and reliable Internet'.[242] The DCCP has been associated with various submarine cable projects, including the Central Pacific Cable[243] and submarine cable capacity in Bangladesh.[244]

The Partnership for Global Infrastructure and Investment (PGI) was established in 2022 in partnership with the G7 and was dubbed the 'G7's flagship infrastructure and investment initiative'.[245] The fund aimed to collectively mobilise US$700 billion (US$200 million from the US) by 2027 for 'sustainable infrastructure', and by 2024 the United States had 'mobilised' US$60 billion through 'federal financing, grants, and leveraged private sector investment'.[246] The US Department of State noted that 'PGI offers a positive alternative to the models of infrastructure financing and delivery that are often opaque, fail to uphold standards, exploit workers, and leave the recipient countries worse off'.[247] When it comes to submarine cables, according to a White House statement in 2024, a US

[241] *United States International Cyberspace & Digital Policy Strategy*, 27.

[242] 'Digital Connectivity and Cybersecurity Partnership', Government, US Department of State, 2018, https://2017-2021.state.gov/digital-connectivity-and-cybersecurity-partnership/.

[243] Winston Qiu, 'USTDA Funds Feasibility Study for the Central Pacific Cable', Submarine Cable Networks, 3 November 2023, www.submarinenetworks.com/en/systems/trans-pacific/central-pacific-cable/ustda-funds-feasibility-study-for-the-central-pacific-cable.

[244] 'USTDA Supports Subsea Cable Capacity in Bangladesh', SubTel Forum, 21 May 2024, https://subtelforum.com/ustda-supports-subsea-cable-capacity-in-bangladesh/.

[245] 'Fact Sheet: Partnership for Global Infrastructure and Investment at the G7 Summit', Government, The White House, 13 June 2024, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/06/13/fact-sheet-partnership-for-global-infrastructure-and-investment-at-the-g7-summit-2/.

[246] The White House, 'Fact Sheet'.

[247] 'Office of the U.S. Special Coordinator for the Partnership for Global Infrastructure and Investment', Government, US Department of State, 2022, www.state.gov/about-us-office-of-the-u-s-special-coordinator-for-the-partnership-for-global-infrastructure-and-investment/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

State Department's US$15 million investment in Pacific Island cable networks is a PGI investment.[248]

In addition, the Biden Administration's 2022 Indo-Pacific Economic Framework for Prosperity (IPEF) economic initiative had an opaque role in supporting submarine cable initiatives. According to the US Trade and Development Agency (USTDA – which administers many cable development projects), US assistance for various submarine cable projects advances the IPEF, including networks in Indonesia[249] and in Bangladesh.[250] In sum, the US Government included submarine cable network financing in various diplomatic and foreign assistance projects since 2018.

4.4.2 Team Telecom

Another key US initiative was the April 2020 Trump Administration's formalisation, via executive order, of a bureaucratic group dubbed 'Team Telecom'.[251] Based at the US Department of Justice's National Security Division, Team Telecom's members are derived from that department, as well as the Department of Defense and Department of Homeland Security.[252] Additionally, Team Telecom relies on a wide assortment of advisers, including the Secretaries of States, Treasury and Commerce, in addition to trade, intelligence, technology and White House representatives. This multidisciplinary team is tasked with advising the US Federal Communications Commission on law enforcement and national security considerations associated with telecommunications licences and telecommunications foreign ownership or control.[253] Concerning submarine cable security, Team Telecom is responsible for reviewing applications for new

[248] The White House, 'Fact Sheet'.

[249] 'USTDA, Super Sistem Partner on Subsea Cable for Indonesia', Government, US Trade and Development Agency, 11 July 2023, www.ustda.gov/ustda-super-sistem-partner-on-subsea-cable-for-indonesia/.

[250] SubTel Forum, 'USTDA Supports Subsea Cable Capacity in Bangladesh'.

[251] Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, Vol. 85, No. 68 Executive Order 13913 § Federal Register (2020), www.federalregister.gov/documents/2020/04/08/2020-07530/establishing-the-committee-for-the-assessment-of-foreign-participation-in-the-united-states.

[252] 'Team Telecom', Government, National Security Division, US Department of Justice, 11 September 2023, www.justice.gov/nsd/team-telecom.

[253] 'The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector', Government, National Security Division, US Department of Justice, 7 December 2021, www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

or transferred international telecommunication services to or from the US and for new or transferred submarine cable landing licences. While this initiative was officially country-agnostic, FCC Commissioner Brendan Carr singled out China upon its formalisation in April 2020, stating:

> The President's committee will have a full docket, and near the top of it, I recommend that the committee examine every carrier owned by the Chinese government that now connects to networks here in the U.S.—including China Unicom and China Telecom.[254]

4.4.3 Industry and the Cable Security Fleet

The United States has had a vibrant domestic submarine cable industry for many years. Its flagship submarine cable firm is SubCom. Established in 1955, SubCom has laid and deployed over 200 subsea systems which would traverse Earth over 21 times. The firm has a close working relationship with the US Government and military and played a key role in the US Cable Security Fleet. In 2019, US Congress passed a bill to establish a Cable Security Fleet which would consist of privately owned, US-documented and commercially viable ships 'to meet national security requirements' associated with submarine cable repair.[255] The legislation appropriated US$10 million per year (US$5 million per vessel per year) to be spent during fiscal years 2021 to 2035 inclusive and stipulated US citizenship requirements for owners and operators.[256] The Cable Security Fleet was implemented by the US Department of Transportation's US Maritime Administration and two SubCom-owned ships were acquired for the programme – CS *Dependable* which operated in the Pacific Ocean, and CS *Decisive* which operated in the Atlantic.[257] However, in 2022 the Department of Transportation (DoT) defunded the Cable Security Fleet[258] and in 2024 the Biden Administration cut funding for the initiative. According to retired US Navy Captain Douglas R. Burnett, while Congress recognised the pressing national security need for the CSF, 'DoT opposition is tied to bureaucratic complacency,

[254] 'Carr Praises Executive Order Enhancing National Security Review of Foreign Participation in U.S. Telecom Sector', Government, Office of Commissioner Brendan Carr, Federal Communications Commission, 6 April 2020, https://docs.fcc.gov/public/attachments/DOC-363550A1.pdf.

[255] 46 USC Ch. 532: Cable Security Fleet (2019), https://uscode.house.gov/view.xhtml?edition=prelim&req=granuleid%3AUSC-prelim-title46-chapter532&utm_source=chatgpt.com.

[256] 46 USC Ch. 532: Cable Security Fleet.

[257] Douglas Burnett, 'Repairing Submarine Cables Is a Wartime Necessity', *U.S. Naval Institute*, 1 October 2022, www.usni.org/magazines/proceedings/2022/october/repairing-submarine-cables-wartime-necessity.

[258] Burnett, 'Repairing Submarine Cables Is a Wartime Necessity'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

outdated misconceptions of modern international communication technology and potential disruptive impacts, and an unexplained view that protecting cables is not important or is a problem for others'.[259] Republican Senator Ted Cruz voiced his dismay in August 2024 at Biden's decision to cut funding for the CSF, arguing, 'The security of undersea cables depends on having access to these "trusted" ships for maintenance and repair of cables, rather than relying on foreign-flagged repair ships sometimes owned by foreign adversaries, which may be recalled to their home countries or otherwise pose risks and reliability concerns during conflict.'[260] It is unclear whether the Trump Administration will reinstate the CSF.

4.4.4 CABLES Program

Another line of US Government effort to shape global submarine cable network dynamics is the Department of State's CABLES Program. Established and implemented by US-based connectivity and digital infrastructure consultancy APTelecom, the CABLES Program utilises its US$5 million budget to build regional capacity and provide technical assistance to regional submarine cable network stakeholders. According to the US International Cyberspace & Digital Policy Strategy, the Cables Program works 'throughout the East Asia Pacific region, responsibly informing essential telecommunications and cables infrastructure stakeholders of the perils of choosing untrusted suppliers'.[261] While public details are scarce, the CABLES Program is primarily a diplomatic effort at dissuading foreign telecommunications officials from contracting Chinese firms associated with submarine cable networks.

In sum, the United States' efforts primarily revolve around defending its dominant position in the submarine cable market from China while its efforts at a sovereign cable repair capacity have stalled. In addition to these formal initiatives, recent press reports also note how the United States lobbies foreign officials against using Chinese vendors for submarine cable networks. According to reports, the United States lobbied Vietnam to avoid Chinese suppliers and also lobbied firms planning to lay trans-Pacific cables to route around the South China Sea.[262] Reuters reports that American lobbying efforts on consortium members of the SeMeWe-6 cable

[259] Burnett, 'Repairing Submarine Cables Is a Wartime Necessity'.
[260] Ted Cruz, 'Biden-Harris Admin Defunds National Security Program For Woke Liberal Initiatives', Letter, 8 August 2024, www.commerce.senate.gov/services/files/386B13FE-78EA-40B7-AB14-0F6A4F762A13.
[261] *United States International Cyberspace & Digital Policy Strategy*.
[262] Tan, 'Escalating Contest over South China Sea Disrupts International Cable System'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

successfully flipped the project from HMN Tech to SubCom.[263] While the Trump Administration was re-inaugurated in 2025, his Administration has not implemented any unique programmes which secure submarine cables specifically, despite various executive orders pertaining to maritime strategy, maritime energy and seabed mining.[264] In combination, the United States has pivoted since 2018 and is now actively defending its position as a market leader in submarine cable network installation.

4.5 Australia

While a middle power in Indo-Pacific strategic affairs, Australia plays an active role in submarine cable network security in this new geopolitically charged environment. Indeed, for several decades Australia has enforced submarine cable 'protection zones' off its western and eastern coasts. Although legislative improvements could be made, these zones, which criminalise a range of actions which damage or could foul submarine cable networks,[265] are nevertheless viewed as an international 'gold standard' and a legislative model which other states could adapt and adopt. As these protection zones were enacted primarily to deter accidental and negligent seafaring practices – rather than to respond to seabed warfare and geopolitical competition – this section will instead focus on Australia's Cable Connectivity and Resilience Centre as well as its 'Australian Infrastructure Financing Facility for the Pacific (AIFFP)' – both established to thwart China's forays into the submarine cable market and promote Internet connectivity in line with Australia's security interests. Indeed, according to its '2023–2030 Australian Cyber Security Strategy', connectivity and cyber resilience in the Indo-Pacific can be consolidated through submarine cable infrastructure investments.[266]

4.5.1 Australian Infrastructure Financing Facility for the Pacific

The Australian Infrastructure Financing Facility for the Pacific, part of Australia's Department of Foreign Affairs and Trade, was announced

[263] Brock, 'U.S. and China Wage War beneath the Waves – over Internet Cables'.

[264] April Herlevi, 'What Lies beneath: Trump and the Security of Subsea Cables', *The Interpreter, The Lowy Institute*, 10 June 2025, www.lowyinstitute.org/the-interpreter/what-lies-beneath-trump-security-subsea-cables.

[265] Stuart Kaye, 'The Protection of Platforms, Pipelines and Submarine Cables under Australian and New Zealand Law', in *Maritime Security : International Law and Policy Perspectives from Australia and New Zealand*, ed. Natalie Klein et al. (Routledge, 2010), 199.

[266] *2023–2030 Australian Cyber Security Strategy* (Australian Government, 2023), www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

in November 2018 and operational in July 2019. The AIFFP partners with Indo-Pacific states and private entities to invest in a range of infrastructure across the Pacific (plus Timor-Leste), including energy, water, transport and telecommunications. According to the AIFFP, the facility designs and delivers 'high impact, safeguarded projects',[267] which has included a range of submarine cable network infrastructure.

The AIFFP was established in tumultuous times and was an initiative implemented under Australia's 'Pacific Step-up' – in part a response to Beijing's increasing influence amongst Pacific island nations. Identified in Australia's 2017 Foreign Policy White Paper, support for Pacific island nations was prioritised, as Australian foreign policy officials admitted that 'like all great powers, China will seek to influence the [Indo-Pacific] region to suit its own interests'.[268] In 2018, Australia's then foreign minister Julie Bishop claimed that China was engaging in 'dept trap diplomacy', whereby Pacific island states were being 'trapped into unsustainable debt outcomes', adding that the 'trap can then be a debt-for-equity swap and they have lost their sovereignty'.[269]

Since its inception and with a budget of AU$2 billion, the AIFFP has been Australia's vehicle for cable infrastructure financing, via both grants and loans. Of the 20 projects listed online at the time of writing in 2026[270] as either 'completed' or 'signed and announced', six pertain to submarine cable network infrastructure projects (see Table 1). As Table 1 illustrates, Australia's projects avoid Chinese suppliers, favouring American, Japanese and Australian firms. It also demonstrates the collaborative nature of Australia's submarine network investments, including Quad nations, as well as New Zealand and Taiwan in some instances.

4.5.2 Cable Connectivity and Resilience Centre

Under the Quad umbrella, in July 2024 Australia launched its Cable Connectivity and Resilience Centre. With a budget of AU$18 million over a four-year period and an Indo-Pacific-wide mandate, the Cable Connectivity

[267] 'About', Government, Australian Infrastructure Financing Facility for the Pacific, 2025, www.aiffp.gov.au/about.

[268] *Foreign Policy White Paper*, Government (Australian Department of Foreign Affairs and Trade, 2017), 26, www.dfat.gov.au/sites/default/files/2017-foreign-policy-white-paper.pdf.

[269] Ben Doherty, 'Experts Dispel Claims of China Debt-Trap Diplomacy in Pacific but Risks Remain', World News, *The Guardian* (Canberra), 20 October 2019, www.theguardian.com/world/2019/oct/21/chinese-loans-expose-pacific-islands-to-risk-of-unsustainable-debt-report-finds.

[270] Projects listed as 'Pacific Climate Infrastructure Financing Partnership' – a separate but related Australian Government initiative – are not included in this table.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Table 1 AIFFP submarine cable network infrastructure projects.

Project	Countries connected	Delivery partners	Supplier	AIFFP contribution (in million)
Adamasia Cable System 1	Solomon Islands	Solomon Islands Submarine Cable Company Limited	SubCom	AU$104
Timor-Leste South Submarine Cable	Timor-Leste	Government of Timor-Leste	Vocus Group	AU$7.2
Palau ECHO Submarine Cable Branch System	Pulau	Belau Submarine Cable Corporation National Government of Palau Government of Japan Government of the United States	NEC	AU$14.8
Tonga Hawaiki Submarine Cable Branch System	Tonga	Government of the Kingdom of Tonga Government of New Zealand Tonga Cable Limited	SubCom	AU$35.6
East Micronesia Cable System	Federated States of Micronesia Narau Kiribati	Government of the Federated States of Micronesia Government of the Republic of Nauru Government of the Republic of Kiribati Government of Japan Government of the United States Government FSM Telecommunications Cable Corporation BwebwerikiNET Limited of Kiribati Nauru Fibre Cable Corporation NEC Corporation	NEC	AU$65

Hawaiki Nui and Google Regional Submarine Cable Branching Units	Not specified	Not specified	BW Digital	Not specified
Tuvalu Vaka Cable	Tuvalu	Government of Tuvalu Tuvalu Telecommunications Corporation Google Government of Japan Government of New Zealand Government of Taiwan Government of the United States	SubCom	Up to AU$53

'Investment Map', Government, The Australian Infrastructure Financing Facility for the Pacific, 2025, www.aiffp.gov.au/investments.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

and Resilience Centre will commission policy-relevant research and analysis to inform regulations, policy development and decision-making, provide training and technical assistance, and share information between governments and industry, including by hosting international dialogues.[271] According to Australia's Foreign Minister Penny Wong, the Centre's 'work is integral to the prosperity and security of our region'.[272] As of 2026 the Centre has hosted a series of workshops across the Indo-Pacific on cable network futures, has funded several research projects and has appointed EY, a consulting firm, to implement its programme of work.

4.6 Trilateral Partnership for Infrastructure Investment in the Indo-Pacific

Another grouping formed to support submarine cable projects (amongst other infrastructure developments) is the Australia–Japan–United States 'Trilateral Partnership for Infrastructure Investment in the Indo-Pacific'. This partnership, between the Australian Department of Foreign Affairs and Trade, the United States Overseas Private Investment Corporation (OPIC), and the Japanese Bank for International Cooperation, was announced in July 2018.[273] According to the joint statement, the three nations expressed 'the belief that good investments stem from transparency, open competition, sustainability, adhering to robust global standards, employing the local workforce, and avoiding unsustainable debt burdens'.[274]

The partnership's first project, announced in October 2020, was the US$30 million Palau spur cable.[275] The spur was designed to connect Palau to the Meta and Google-owned (NEC built) Echo cable, which will connect Singapore, Jakarta, Guam and California via the Indonesian archipelago, thus avoiding the South China Sea. The Echo Cable is scheduled for completion in the fourth quarter of 2025 and will

[271] 'Launch of the Cable Connectivity and Resilience Centre', Government, Australian Department of Foreign Affairs and Trade, 29 July 2024, www.foreignminister.gov.au/minister/penny-wong/media-release/launch-cable-connectivity-and-resilience-centre, www.foreignminister.gov.au/minister/penny-wong/media-release/launch-cable-connectivity-and-resilience-centre.

[272] Australian Department of Foreign Affairs and Trade, 'Launch of the Cable Connectivity and Resilience Centre'.

[273] 'Australia, US and Japan Announce Trilateral Partnership', Export Finance Australia, 2018, www.exportfinance.gov.au/newsroom/australia-us-and-japan-announce-trilateral-partnership/.

[274] Export Finance Australia, 'Australia, US and Japan Announce Trilateral Partnership'.

[275] 'Australia Partnering with Japan and the United States to Finance Palau Undersea Cable', Government, Australian Infrastructure Financing Facility for the Pacific, 28 October 2020, www.aiffp.gov.au/news/australia-partnering-japan-and-united-states-finance-palau-undersea-cable.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

be Palau's second submarine cable connection. Other submarine cable projects funded under the partnership include the NEC-supplied East Micronesia Cable System, which will connect Tarawa (Kiribati), Kosrae (Micronesia) and Yaren (Naru) to Pohnpei (Micronesia) – which has an existing link to the SubCom-laid HANTRU1 Cable System that connects to the Pacific Ocean cable hub of Guam.[276] The East Micronesia Cable System has an estimated cost of AU$135 million and is scheduled for completion late 2025. According to one senior US official commenting on the East Micronesia Cable System, 'secure and resilient digital connectivity has never been more important'.[277]

In sum, Australia, the United States and Japan have mobilised this new multilateral grouping to tackle regional submarine cable connectivity gaps by subsidising cables in the Pacific Ocean, thereby thwarting China's attempts at laying networks via HMN Tech.

4.7 Japan

Tokyo has made various unilateral efforts to further submarine cable resilience, regional connectivity and supply chain security in line with its national interests. Industrially, Japan's NEC is a leading submarine cable network player and has laid over 400,000 kilometres of subsea cable globally, with close ties to the Japanese Government. In 2008, NEC acquired OCC Corporation (Ocean Cable & Communications) which manufactures optical submarine cables domestically in Japan.[278] This acquisition reportedly took place amid concern within NEC that China's Huawei would acquire the strategically important Japanese cable manufacturer.[279] In July 2024 then US Secretary of State Antony Blinken visited NEC's Tokyo headquarters, where he was briefed on a range of technologies, including submarine cable technologies. Blinken noted to the press that 'the leading edge work that [NEC] are doing on undersea cables and communications systems … are the future for digital communications',

[276] 'Work to Start on East Micronesia Cable Following Contract Signing', Australian Department of Foreign Affairs and Trade, 6 June 2023, www.dfat.gov.au/news/media-release/work-start-east-micronesia-cable-following-contract-signing.

[277] Australian Department of Foreign Affairs and Trade, 'Work to Start on East Micronesia Cable Following Contract Signing'.

[278] 'NEC and Sumitomo Electric to Acquire Leading Submarine Cable Manufacturer', NEC Corporation, 1 July 2008, www.nec.com/en/global/prod/nw/submarine/news/2008/20080701.html.

[279] Kanako Tanaka and Takeshi Narabe, 'Japan Fighting Uphill Battle in Protecting Web of Undersea Cables', The Asahi Shimbun, 31 January 2025, www.asahi.com/ajw/articles/15578284.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

lauding NEC as a 'trusted vendor'.[280] However, according to NEC President and CEO Takayuki Morita in 2025, the Japanese government provides little assistance to NEC amid global competition, noting that 'we are the only one fighting with no support'.[281] Amid this discontent, in late 2025 reports emerged that Tokyo may support NEC to acquire a cable installation and repair fleet – pending approvals.[282]

Tokyo has also announced a range of submarine cable network initiatives, but implementation has been patchy. In 2021, Prime Minister Kishida Fumio announced plans to create a subsea 'Digital Garden City Superhighway' which would encircle Japan, economically revitalise Japan's regions and be part of Tokyo's Digital Garden City Nation vision.[283] While this project was expected to be completed by 2025, the originally proposed new submarine cable network is yet to be installed. In addition, in 2022, Tokyo announced it will spend US$440 million to geographically decentralise submarine cable-landing stations and data centres, citing both economic and security justifications.[284] In early 2025, Nikkei Asia reported that Japanese ministries are planning to support capital investment in subsea networks and subsidise investment in cable laying vessels.[285] In foreign relations beyond the Indo-Pacific, Tokyo inked an MoU with the European Union on 3 July 2023 to further 'secure, resilient and sustainable global connectivity', although the agreement did not commit either side to any specific joint projects.[286] Japan's Ministry of Economy, Trade, and Industry in April 2025 announced that submarine cable policy would be integrated into its purview.[287] Despite intentions,

[280] Blinken, 'Secretary Antony J. Blinken Remarks to the Press'.

[281] Tanaka and Narabe, 'Japan Fighting Uphill Battle in Protecting Web of Undersea Cables | The Asahi Shimbun'.

[282] 'Japan Expands Subsea Fleet', *Submarine Cables Singapore 2026*, 1 December 2025, www.asia.submarine-cables-summit.com/news/japan-unleashes-subsea-fleet-to-power-asia-pacific-connectivity.

[283] Kishida Fumio, 'Policy Speech by Prime Minister Kishida Fumio to the 207th Session of the Diet', Speech, Tokyo, 6 December 2021, https://japan.kantei.go.jp/101_kishida/statement/202112/_00002.html.

[284] Justin Sherman, 'Improving Indo-Pacific Cable Security and Resilience: Investment, Licensing, and Repair', *Indo-Pacific Outlook* 1, no. 4 (2024): 7, https://hdl.handle.net/10125/107696.

[285] Kiu Sugano, 'Japan to Back Undersea Cable Investments for National Security', *Nikkei Asia* (Tokyo), 26 February 2025, https://asia.nikkei.com/Business/Telecommunication/Japan-to-back-undersea-cable-investments-for-national-security.

[286] 'Memorandum of Cooperation on Submarine Cables for Secure, Resilient and Sustainable Global Connectivity', European Commission, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2371.

[287] Erin L. Murphy and Thomas Bryja, *The Strategic Future of Subsea Cables: Japan Case Study* (Center for Strategic and International Studies, 2025), www.csis.org/analysis/strategic-future-subsea-cables-japan-case-study.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Tokyo's efforts at intervention in the submarine cable network market have largely focussed on subsidising regional networks, and unilateral cable resiliency efforts have yielded mixed results at the time of writing. Nevertheless, these efforts to date demonstrate Tokyo is motivated to better secure its cable networks, even if implementation has been uneven.

4.8 India

Despite India's Quad membership, the key South Asian state is currently prioritising its submarine cable security over promoting regional resilience.[288] New Delhi's telecommunications regulators are encouraging the nation's cable operators to invest in a sovereign India-flagged repair capacity, to diversify the geographic spread of cable landing locations and to connect coastal Indian cities (and new data centres) via domestic submarine cable networks.[289] Despite these policy priorities, India currently lacks any regional strategy for cable connectivity in either the India Ocean or the wider Indo-Pacific and does not currently invest in cable networks for neighbouring nations. According to a September 2024 joint Quad statement, India recently commissioned a feasibility study to assess expanding 'undersea cable maintenance and repair capabilities in the Indo-Pacific'.[290]

Opportunities exist for India to foster a domestic submarine cable manufacture capacity – whether by encouraging Indian firms or inviting foreign entities to establish factories. Furthermore, at least publicly, India has not articulated how its national security apparatus will respond to the increasing instances of seabed warfare or how India will protect the cable networks beyond its EEZ. According to scholar Jagannath Panda, while India's key role in the emerging Indo-Pacific security architecture is clear, the country should integrate submarine cable networks into its regional deterrence strategy, especially vis-à-vis China.[291] In comparison to its Quad partners, India is the least active player in submarine cable

[288] Samuel Bashfield, 'Digital Sovereignty: Securing India's Submarine Cables', *The Diplomat*, 26 December 2024, https://thediplomat.com/2024/12/digital-sovereignty-securing-indias-submarine-cables/.

[289] *Consultation Paper on Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India*, no. 15/2022 (Telecom Regulatory Authority of India, 2022), www.trai.gov.in/sites/default/files/2024-09/CP_23122022_0.pdf.

[290] Australian Department of the Prime Minister & Cabinet, 'Joint Statement from the Leaders of Australia, India, Japan, and the United States: The Wilmington Declaration'.

[291] Jagannath Panda, 'India's Emerging Undersea Cable Landscape: Varied Indo-Pacific Partnerships to Boost Geopolitical Ambitions?', *Marine Policy* 171 (January 2025): 8, https://doi.org/10.1016/j.marpol.2024.106417.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

network intervention and currently focusses its efforts on domestic rather than regional initiatives. Like Japan, despite patchy implementation to date, India's efforts nevertheless demonstrate that New Delhi is taking the security of its cable networks seriously, working internally through policy options for future implementation.

4.9 Conclusion

This empirical mapping proves systemic yet evolving state competition in the Indo-Pacific to control cable networks. China's Digital Silk Road is pitted against the more fragmented Western counter-measures, as each side seeks to exclude respective rivals and reduce respective vulnerability by securing a favourable network position. Other initiatives detailed, including Australia's AIFFP, the US' Team Telecom and the Trilateral Partnership show how states mobilise diplomatic and financial tools to dictate network topologies. However, various of these efforts remain challenging to implement, such as the US' Cable Security Fleet, Japan's resiliency initiatives and India's repair strategy. This variation may reflect varying state capacities, threat perceptions, and industrial bases – rather than an absence of competitive dynamics. While this section has focussed on major and selected middle powers, smaller Indo-Pacific states are also navigating this competition, whether as increasingly active cable policy actors or as policy takers caught between competing US and Chinese connectivity offers. A fuller treatment of these states' responses remains an important avenue for future research. Nevertheless, the subsequent fifth section categorises these responses within a nodes-flows-production typology, showing how key Indo-Pacific states compete for structural positions which lessen dependency risk, which simultaneously create conditions which could be weaponised.

5 The Nodes-Flows-Production Contest

Major powers in the Indo-Pacific are responding in a variety of ways to submarine cable network competition in this era of heightened Sino-US geopolitical competition. Drawing on cases from the preceding empirical sections, this final analytical section examines and categorises state imperatives to intervene in submarine cable networks, positing three broad categories – *nodes*, *flows* and *production* (see Figure 3). While some overlap exists between these three categories, this distinction is a useful lens to understand how network-based competition is operationalised in the Indo-Pacific – how states control regional network nodes, how flows

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

are defended and exploited and how production is secured. The following analysis interweaves network-based competition perspectives to better illustrate how states are responding to this renewed, perceived seabed connectivity threat and to illuminate various implications for international relations as states are driven to pursue network centrality.

5.1 Nodes

In the Indo-Pacific, funding, laying and operating new and existing regional submarine cable networks is a key battleground between the United States and China. I argue that control over regional connectivity is a key state imperative and is driving network competition in the Indo-Pacific. Control is exerted through influencing network geographical contours (including cable routes and landing station locations), through selecting installers and facilitated through new bureaucratic infrastructures. Major Indo-Pacific powers such as the United States, China and India, plus middle powers such as Australia, are relatively sufficiently connected with commercially viable networks and can veto any 'untrusted' suppliers which intend to connect respective shores. As such, emphasis is placed by these wealthier nations on intervening in regional connectivity – submarine cable networks that connect regional neighbours. Ultimately, states are sovereign and can decide on the nature and variety of respective connections; however, pressure and subsidies by powerful states can influence network characteristic choices. Immense efforts are being undertaken by great and middle powers to dictate regional connectivity – the network's nodes.

As this Element has outlined, submarine cable connectivity is vital for economic growth and global competitiveness, for national security, as well as for the functioning of modern digital societies. As demand for bandwidth from states, businesses and societies grows, submarine telecommunication networks provide the only reliable, stable and cost-effective method of data transmission between continents and islands. Despite advances in satellite data transmission capacities, submarine cables remain the backbone of modern information flows. Moreover, cable connectivity is expensive, and new projects require either a strong business case to attract investors or be subsidised/funded through a state (often through a state-owned telecommunications company). Alternatively, submarine cable network projects are funded (to varying degrees) by multilateral institutions, including the World Bank and the Asian Development Bank. Therefore, nodal connectivity refers to efforts

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

by states to influence the contours of new regional cable networks and to influence the choice of suppliers (as distinct from supply chains). In exerting influence over regional connectivity projects, restricting adverse suppliers is usually a high priority and a method of exclusion.

In this context, an underlying motivation behind initiatives like the Digital Silk Road and the Trilateral Partnership for Infrastructure Investment in the Indo-Pacific is to exclude rivals. Exclusionary policies by the United States and its allies are designed to perpetuate the West's central role in submarine cable networks and to hobble attempts by China to make inroads. Conversely, China's ambitions in the cable market are designed to dislodge the West's central position in digital connectivity and build alternative competing networks. Due to the immense costs associated with submarine cable network design, installation and operation, many smaller countries are forced to make a choice between these competing poles, which naturally excludes the losing side from the infrastructure network. Network exclusion diminishes regional influence, which in turn diminishes relative power. Hence, excluding rivals from new subsea networks has considerable strategic implications for both the winners and losers.

Moreover, states are dictating network geographical characteristics, including landing points (such as deciding which states and cities are to be connected) and routing (such as avoiding hostile or unstable zones) which can create or alleviate dependencies. For example, China has effectively locked the South China Sea to non-Chinese subsea fibre projects by enforcing onerous permitting requirements in that region. As a result, various new trans-Pacific cable projects from Singapore to the United States are transiting the Indonesian archipelago rather than the South China Sea. By influencing cable routes, states can pursue strategic connections and exclude rivals. As a result, submarine cable networks help to bolster trade, military or diplomatic ties between a state and states connected to the network.

In order to pursue network centrality in submarine cable nodes, new bureaucratic infrastructures have been established to rapidly respond, intervene and exclude rivals. As the previous section illustrated, a range of new multilateral initiatives and (intra)governmental groupings have been created to better control new network nodes. For example, the United States established its Digital Connectivity and Cybersecurity Partnership, plus the Partnership for Global Infrastructure and Investment in part to establish its strategic position in subsea networks. Likewise, Australia rapidly stood up the Australian Infrastructure Financing Facility for

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

the Pacific in addition to the Cable Connectivity and Resilience Centre to further its influence over regional subsea network connectivity. Moreover, multilateral architecture, including the Trilateral Partnership for Infrastructure Investment in the Indo-Pacific is a Western attempt at maintaining its strategic position in cable networks and excluding alternative Chinese networks. China too has launched its Digital Silk Road in 2015 with a view to enhancing its centrality in subsea networks for strategic reasons. In this new era, states are investing directly or through multilateral arrangements in new regional cable networks.

As a result of this new bureaucratic architecture that has been established since 2015, in several cases new submarine cable network projects are being determined by strategic state investment and subsidies rather than commercial and market dynamics. Moreover, this new bureaucratic architecture is resulting in swifter and more discrete state intervention than was the case in the late 2010s and early 2020s. For example, international diplomatic controversies ensued in 2016 and 2020 when Chinese firms were set to win submarine cable installation contracts in the Solomon Islands, and then Kiribati, Micronesia and Narau, respectively. In both of these cases, Western nations stepped in to thwart Chinese bids, in the process establishing bureaucratic infrastructure which has since been mobilised to subsidise or fund regional cable networks before China can mount a compelling offer. Moreover, these bureaucratic architectures are not being implemented unilaterally but are being coordinated amongst partners for maximum effect. As outlined in an earlier section, the Trilateral Partnership for Infrastructure Investment in the Indo-Pacific combines American, Japanese and Australian state capital to circumvent China's cable network-laying ambitions and advance collective nodal control amongst like-minded democracies.

By intervening in regional submarine cable network design, states are able to both exert regional influence and promote respective notions of 'data integrity'. Just as states invest in physical infrastructure in developing states to build influence, centrality in physical submarine cable networks is likewise used as a tool of statecraft and as a source of power. Functioning cable networks can be used as a tool of geopolitical leverage, of economic control, of soft power and of technological standards leadership. For many small islands and less developed states which receive a subsidised or externally funded cable network, continued access to the data conduit is often an existential issue. Concurrently, by intervening in network nodal connectivity, middle and great powers can dictate network security, thereby setting and enforcing rules and standards. Specifically, states can ensure

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

networks avoid hostile states (and associated territories) which could gain physical or digital access to the network or subject the network to undue monitoring. While these network infrastructures may not be otherwise commercially viable, by subsidising or investing in networks directly, powerful states can determine routing decisions to accommodate respective national security imperatives.

As outlined, states are increasingly intervening in new submarine cable network designs to further visions of regional connectivity, according to respective national interests, which can create the conditions for weaponisation. As these connectivity ideals are sometimes not commercially viable, states are increasingly subsidising and investing to better control future network contours. This competition to control the contours of subsea digital connectivity positions states for future possible leverage. Simply put, in this era of heightened geopolitical competition, Indo-Pacific great and middle powers are vexed by the contours of new regional submarine cable networks and how centrality in these networks can be used to further a favourable balance of power.

5.2 Flows

The second imperative driving states to intervene in the global submarine cable ecosystem is flow control – defending the data that transits submarine cable networks from accidental, negligent and intentional incidents. Moreover, flow control can also result in weaponising data flows and exploiting these transmissions for strategic purposes – as Farrell and Newman describe as the 'panopticon effect' – which is 'the ability to glean critical knowledge from information flows'.[292] The digital interconnectedness afforded by submarine cable networks results in both strategic benefits and also strategic vulnerabilities. Even though the overwhelming majority of cable faults occur due to accidents, negligence and natural phenomena, in this era of heightened geopolitical tensions between China and the United States, the fear of hostile cable incidents and espionage is driving state intervention.

Unlike strategies to intervene in network nodes (as articulated above), Indo-Pacific nations have been slow and/or reluctant to articulate public strategies to defend submarine cable networks. While counterparts in Europe – both nation-states and regional organisations such as NATO and the European Union – have publicised investment into cable

[292] Farrell and Newman, 'Weaponized Interdependence', 55.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

protection strategies, states in the Indo-Pacific have thus far been reluctant to likewise articulate defensive plans against hostile actions.[293] This reluctance is due to the lack of suspicious seabed incidents which have taken place in the Indo-Pacific, compared with the various high-profile suspicious examples in Europe this Element has detailed. While in late 2025 Australia's Chief of Navy said publicly that the loss of Australia's submarine cable networks would be an 'existential threat',[294] the country's 2024 Civil Maritime Security Strategy does not consider the particulars of seabed critical infrastructure,[295] and Australia's 2024 National Defence Strategy likewise does not engage with seabed lines of communication.[296] Moreover, little is publicly known about the offensive seabed warfare and cable disruption plans of Indo-Pacific nations – information which is a closely guarded secret.

Nevertheless, Indo-Pacific states are pursuing network flow resilience through various softer strategies, including advisory functions and best-practice strategies. For example, the multilaterally endorsed 'New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World', as noted above, advocates for submarine cable network design prioritising 'resilience, redundancy, and security', in addition to 'spatial and route planning to promote coordinated use of seabeds, protect cables from natural or man-made hazards, ease chokepoints, and reduce risk of inadvertent disruption while expanding global connectivity'.[297] Likewise, the United States' Office of Economic Security, the Supply Chain Resilience Center, and the Cybersecurity and Infrastructure Security Agency collaboratively published a report in 2024 titled 'Priorities for DHS [Department of Homeland Security] Engagement on Subsea Cable Security & Resilience', which advocates for better public–private coordination and streamlined permitting, licencing

[293] Samuel Bashfield and Oscar Youlten, 'Seabed Critical Infrastructure Protection: Resilience vs. Connectivity', *Asia Maritime Transparency Initiative, Center for Strategic & International Studies*, 14 May 2025, https://amti.csis.org/seabed-critical-infrastructure-protection-resilience-vs-connectivity/.

[294] Mark Hammond, 'Indo Pacific Sea Power Conference 2025 Opening Address', Speech, Indo Pacific Sea Power Conference, Royal Australian Navy, 4 November 2025, www.navy.gov.au/about-navy/leaders/chief-navy/speeches/2025-11-04/indo-pacific-sea-power-conference-2025-opening-address.

[295] *Australian Government Civil Maritime Security Strategy* (Australian Department of Home Affairs, 2022), 48, www.homeaffairs.gov.au/nat-security/files/australian-government-civil-maritime-security-strategy.pdf.

[296] *2024 National Defence Strategy*, Government (Australian Department of Defence, 2024), www.minister.defence.gov.au/media-releases/2024-04-17/2024-national-defence-strategy.

[297] Australian Department of Foreign Affairs and Trade, 'The New York Statement'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

and regulation, in addition to clearer emergency management and incident response arrangements.[298]

Moreover, the International Cable Protection Committee (ICPC), which has an extensive membership primarily consisting of industry players in addition to key governments and public agencies including the governments of Australia and India, plus the US Navy and China Telecommunication Corporation, advocates for effective submarine cable security and resilience amongst governments globally. The ICPC's flagship 'Government Best Practices for Cable Protection Resilience' publication is a guide for public officials to security cable networks, advising best practices across key issues including fishing and anchoring risks, seabed spatial separation, charting, domestic protective legislation frameworks, government points of contact, regulatory ease of repair, critical infrastructure designation and data sharing.[299] Through joining and supporting the work of the ICPC, these key Indo-Pacific governments and agencies are attempting to further the resilience and security of global subsea connectivity through public policy advocacy.

Exploiting submarine cable flows in the modern era is likewise little understood publicly due to security classification barriers but, nevertheless, drives submarine cable flow policies and explains why states pursue centrality. The Snowden revelations in 2013 laid bare how submarine cable landing stations can be sites of monitoring and signals intelligence collection. Indeed, cable networks presumably remain a key enabler of data interception and signals intelligence collection in the modern era, although details are difficult to ascertain. Securing flows can be understood by the 'panopticon effect', which articulates how control of network infrastructure can permit data monitoring. In this sense, China's efforts at installing an alternate network of submarine cables – via its Digital Silk Road – can be posited as a push to simultaneously escape the West's panopticon, and perhaps enable its own.

Securing cable flows from disruption is currently the least developed imperative for Indo-Pacific states, unlike for European counterparts. This

[298] *Priorities for DHS Engagement on Subsea Cable Security & Resilience: A White Paper by the Office of Economic Security, the Supply Chain Resilience Center, and the Cybersecurity and Infrastructure Security Agency* (US Department of Homeland Security, Supply Chain Resilience Center, Cyber & Infrastructure Security Agency, 2024), www.dhs.gov/sites/default/files/2024-12/24_1218_scrc_Priorities-for-DHS-Engagement-on-Subsea-Cable-Security-Resilience_18-Dec-24.pdf.

[299] *Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables*, 1.1 (International Cable Protection Committee, 2021), www.iscpc.org/publications/icpc-best-practices/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

perceived latency is due to a lack of urgency in the Indo-Pacific to actively defend these networks and hampered by a methodological difficulty to ascertain how militaries are preparing for seabed warfare due to security classification restrictions. We cannot assume that just because Indo-Pacific states do not publicly link undersea warfare capability development with submarine cable protection, that these seabed infrastructures are being neglected by militaries. However, this public sluggishness may be strategic rather than permanent. As future cable incidents occur in the Indo-Pacific, these soft governance mechanisms outlined above may be deemed inadequate, and submarine cable defence may be formalised and publicised.

5.3 Production

The third imperative driving states to intervene in the submarine cable ecosystem is perceived production and supply chain vulnerabilities. As this Element illuminates, supporting sovereign or allied cable network suppliers is a foremost consideration when considering new networks. States can hobble hostile suppliers through sanctions, through onerous permitting requirements, by avoiding particular firms in new projects and by banning cables landing within jurisdictions. In this context, supply chains refer not only to the raw materials and components which make up cable networks but also to repair capacities and sovereign industry capabilities. Assured access to cable network materials, components, expertise and repair capabilities is fundamental in driving resilience and connectivity, as outlined above.

Submarine cable networks consist of many materials and components. The average length of cable alone consists of a range of materials, including (from outside in) tar-soaked nylon yarn, galvanised armour wires, nylon yarn bedding, polyethylene insulator, copper sheath, ultra-high strength steel wires, buffering material (plastic/steel) and silicone gel, before ultimately the optical fibres.[300] Most cables are also powered to operate underwater repeaters, utilise branching units and Reconfigurable Optical Add/Drop Multiplexers, and landing stations require a range of specialised equipment. The origin and sources of these materials and components are being increasingly scrutinised. States are increasingly aware of these supply chain issues to ensure availability in a crisis. Fears over inbuilt backdoors and compromised equipment also drive supply chain scrutiny. As submarine cable networks have been key sites of signals

[300] TeleGeography, 'Submarine Cable FAQs'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

intelligence collection and espionage, concerns over technically compromised equipment abound.

States' fears of being strategically dependent on others for these key components and materials are driving policy responses and intervention. By extension, many major and middle powers are attempting to onshore or 'friendshore' submarine cable manufacture and operation capabilities or support existing sovereign industry.[301] American efforts at obstructing China's submarine cable industry are evidenced through its addition of Huawei Marine Networks in 2020 to the 'entity list', resulting in its divestment from Huawei and phoenixing as HMN Tech under a new parent company.[302] After the United States successfully thwarted HMN Tech's bid to install the intercontinental SeaMeWe-6 cable network, China's foreign ministry issued a statement noting that the United States 'should stop fabricating and spreading rumours about so-called "data surveillance activities" and stop slandering and smearing Chinese companies'.[303]

Sovereign cable repair capacity has become an issue of interest and action amongst Indo-Pacific states. While cable resilience in peacetime is largely managed by the private sector, conflict would entail a new set of considerations. As this Element has illuminated, during conflict submarine cable networks and associated installation and repair vessels become a target as maintaining network uptime is paramount. Ensuring submarine cable network resilience during a conflict would take a coordinated approach from military assets, coastguard vessels, cybersecurity specialists, the cable industry and policy coordination departments. Militaries and coast guards would be required to defend not only military seabed infrastructure but also civilian telecommunications cables, which would likewise be targeted during a confrontation. As submarine cable networks have not been targeted in a full-scale conflict since the Second World War (when telegraph cables were linking the globe), how optical fibre cables would be targeted (e.g. kinetically or virtually) and affect the outcome of a war is uncertain. However, in today's digitally interconnected society, targeting submarine cable networks during a conflict would have devastating ramifications for the populations and communities affected. During a conflict, whereby flows of goods and services are interrupted and cables are targets, a sovereign cable industry would be a vital component of national power. From an American perspective, analysts Daniel

[301] Bashfield and Strating, '"Friendshoring" the Seabed'.
[302] HMN Tech, 'Huawei Marine Networks Rebrands as HMN Technologies'.
[303] Brock, 'Exclusive'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

F. Runde, Erin L. Murphy and Thomas Bryja argue that 'the overreliance on Chinese [cable] repair ships due to limited alternatives in the marketplace is another vulnerability if, during a time of military conflict, the Chinese government prohibits access to its repair ships'.[304]

Submarine cable repairs are generally coordinated and undertaken through cable maintenance zone agreements, which pool cable repair ships within specified maritime areas or individual maintenance contracts. While these agreements have operated largely successfully for many years, many states are increasingly concerned about the availability of these vessels in a crisis and a state's inability to dictate repair priorities. While submarine cable repair hubs (docks and depots) and repair ship flags have been decided by commercial factors, geopolitical factors are changing the geography of these repair infrastructures. States are increasingly attempting to intervene in submarine cable repair arrangements in order to dictate repair prioritisation, such as the (now defunded) United States Cable Security Fleet, China's involvement in S.B. Submarine Systems and India's feasibility studies into sovereign repair fleets. Also, by controlling cable repair infrastructures, these services can be shared with partners and be used as a tool of statecraft while also mitigating the possibility that cable engineers interfere with submarine cables while undertaking repairs or introduce backdoors or otherwise compromise the networks.

By supporting the production of sovereign and/or friendly submarine cable network supply chains, these firms can be instrumentalised by states and be incorporated as an element of statecraft – the possible limitations of which are engaged with in Section 6. Due to the close relations these firms have with respective governments – including financial – an alignment with national security objectives is expected. As a result, states could leverage respective firms to further national security objectives and implement defence and foreign policy agendas with geopolitical implications. As a result, there emerges a blurring between the commercial and security logics which drive submarine cable network design and maintenance. While in the post–Cold War era cable networks were largely driven by commercial considerations, geopolitical factors are increasingly dictating network dynamics, including supply chains and industry considerations. In sum, submarine cable supply chains, whether they be materials or components, the cable industry or repair capabilities, are being increasingly scrutinised

[304] *Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition* (Center for Strategic and International Studies, 2024), 3, www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

by states seeking greater control. By controlling the supply, states can ensure sovereign oversight of these critical infrastructures and improve connectivity on respective terms, simultaneously furthering geopolitical goals of attaining or maintaining network centrality.

5.4 Conclusion

In the Indo-Pacific, efforts at network centrality are driving state intervention into submarine cable network nodal control, flow rule and production dominance. Indo-Pacific states have made considerable efforts to control network nodes through subsidies and bureaucratic infrastructure – evidenced by China's Digital Silk Road and Western competing initiatives. These initiatives secure network positions that reduce vulnerability to adversary control. In contrast, efforts at controlling flows have remained relatively mild in the Indo-Pacific, as states focus on softer governance and advisory resilience initiatives to date, rather than military responses (at least articulated publicly). Despite this, the panopticon effect, and ability to monitor data traffic, does explain the value in, and efforts to, control network flows. Controlling production is a significant line of effort amongst Indo-Pacific states, which can blur the line dividing security and commercial logics. This analysis demonstrates how states in the Indo-Pacific compete for network centrality to mitigate vulnerabilities, though structural competition creates conditions that risk weaponisation – echoing Farrell and Newman's warning. However, limitations to this weaponisation possibility exist, which are engaged in the following concluding section.

6 Conclusion: The Seabed and Indo-Pacific Security

As Sino-US competition revolves around network centrality – and the global order continues to fracture – submarine cable networks will remain a focus of geopolitical competition. States in the Indo-Pacific are adapting to this age of heightened geopolitical competition and securing seabed lines of communication accordingly. As I outlined in this Element, various key Indo-Pacific states have already adapted policies to maintain centrality in submarine cable networks, and further steps are expected in the coming years. As these networks are vital to the functioning of our modern digital societies, maintaining uptime on 'trusted' subsea networks is a paramount national security consideration for many leaders. According to historian Richard Dunley:

> In wartime, arguably more than at any other time, information is power. It is through this lens that we must view the global submarine cable

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

> network. Cutting and tapping cables is important, but these tend to be the acts of a disruptor. Western nations [and indeed all major powers] need to think once again about how they would exploit their control of the global commons in time of war to control the global communications infrastructure, and the knowledge that flows across it.[305]

This Element first outlined the historical progression from the telegraph era to modern optical fibre networks, finding that submarine cable networks are perceived as vulnerable as these networks rapidly transmit information between continents and islands, geographically traverse maritime and coastal zones, and physically constrict and aggregate information flows through limited chokepoints. Second, after outlining modern Sino-US competition over technological primacy, I posited network-based competition and weaponised interdependence frameworks, and articulated a novel policy typology to analyse how Indo-Pacific states are responding to seabed insecurity. Third, this Element analysed a range of contemporary cable cuts and suspicious incidents in both the Indo-Pacific (Taiwan and Red Sea) and extra-regionally (Baltic Sea) to illustrate why submarine cable security is now receiving renewed policy attention. Fourth, this Element focussed on how key Indo-Pacific states and the Quad are responding to perceived submarine cable insecurity, primarily across foreign and defence policy domains. The final analytical section posited a novel nodes, flows and production framework to understand and examine the goals of various Indo-Pacific states and how these efforts point to a network-based competition model through which interdependence could be weaponised. The competition I illustrated in this Element over submarine cable networks is a microcosm of broader Sino-US competition centred around networks – whether digital, infrastructural, capital or production.

This Element examined how states are pursuing network centrality to reduce vulnerability in seabed digital connectivity, rather than whether these efforts are successful. Indeed, according to Gjesvik, private corporations can 'resist state attempts at weaponization'.[306] According to Gjesvik:

> The ability of states to reach into, mobilize, and benefit from their centrality in the network has therefore weakened as corporations gain in relative strength. The strong position of the market players in turn affords them greater agency to pursue their own interests, that are often at odds with the interests of states.[307]

[305] Dunley, 'Undersea Cable Control'.
[306] Gjesvik, 'Private Infrastructure in Weaponized Interdependence', 724.
[307] Gjesvik, 'Private Infrastructure in Weaponized Interdependence', 740.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Gjesvik captures an inherent tension and highlights that despite state attempts to control these networks, success may be limited by corporate interest and market dynamics. However, Gjesvik's views, using trans-Atlantic cables as a case study, may not give adequate weight to the tools states have available, including landing licences, national security legislation, entity lists and direct subsidies. Indeed, the ability of a state to mobilise respective central positions in networks will be limited to a degree by the network owners and/or operators. Likewise, states will be limited by the imposition of technical and geographical realities, for example, fibre optic cables are more difficult to clandestinely tap without access to landing stations, fibre optic networks can more easily re-route data to avoid single-point disruptions, and the Indo-Pacific's vast geography and correspondingly distributed cable routes are more challenging to patrol than the Baltic Sea. As a result, network-based competition is both intensifying yet constrained, as fierce competition ensues to control networks that perhaps cannot be fully managed.

Competition to lay and operate rival submarine cable networks raises questions over 'bifurcation' of the Internet – meaning the creation of distinct and disconnected American- and Chinese-led Internets. However, while potentially causing nominal data transfer delays, analysts Jocelinn Kang and Jessie Jacob note that due to the Internet's 'circuitous' nature in which data is 'dynamically reroute[d]', such network bifurcation will have a 'minimal impact' on network performance.[308] Ultimately, despite a potential lack of direct connections between China and the United States, for example, data will still flow via intermediaries. However, as Dwayne Woods and Junda Li argue, this bifurcation, articulated as the 'proactive reshaping of network topologies by states seeking to mitigate these very vulnerabilities' is not adequately considered by the weaponised interdependence framework.[309] Indeed, even if submarine cable network bifurcation has a negligible technical effect on global data transfer between these two blocs, the existence of two networks challenges the panopticon effect and reduces dependency vulnerabilities as competitors build and use respective 'trusted' networks. This Element has highlighted these various efforts in the Indo-Pacific, supporting Woods and Li's contention

[308] Jocelinn Kang and Jessie Jacob, *Connecting the Indo-Pacific: The Future of Subsea Cables and Opportunities for Australia*, Policy Brief (Australian Strategic Policy Institute, 2024), 17, www.aspi.org.au/report/connecting-indo-pacific-future-subsea-cables-and-opportunities-australia/.

[309] Woods and Li, 'Dangerous Depths of Bifurcation: The Rise of "Inter-National Security Narcissists" and Undersea Cable (Dis)Connections', 107.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

that the potential for interdependence to be weaponised is slowly leading to subsea network bifurcation.

According to Schindler and colleagues, when Sino-US competition is centred on network centrality, 'it is very difficult to imagine either side achieving a resounding victory'.[310] Victory will remain elusive as smaller states can pursue strategies of 'omni-alignment' and resist choosing sides.[311] When it comes to cable networks, smaller states can hedge, for example, permitting HMN Tech to install some networks and Western firms to install others. Moreover, the choice of submarine cable network supplier origin can differ from alignment in other networks – whether it be finance, infrastructure or production. How third states respond to Sino-US competition for network centrality will influence which pole dominates. As this competition progresses, winners and losers can be identified.

How the second Trump Administration perpetuates intervention in submarine cable networks and pursues network centrality, amid its efforts to disengage globally, is at the time of writing still unclear. According to Winecoff, the US could give up its structural power through 'malintent and/or short-sightedness', warning that while 'the United States possesses network prominence now [writing in 2020]. In the 21st century it should prioritize good stewardship of it'.[312] However, Trump is not stewarding the United States' leading global role, and future researchers should monitor how Trump's non-traditional foreign and national security policies play out on the seabed.

One key technological factor that will determine the future of the Indo-Pacific's submarine cable networks and corresponding Sino-US competition is sensing technology. A range of new sensing technologies are being installed on submarine cable networks, which I overviewed briefly in the preceding sections. These new sensing technologies have the potential to further network resilience by enabling real-time network monitoring, which means that negligent or malicious actors can be interdicted before cable damage occurs. These technologies can also streamline repairs by better pinpointing fault locations and assisting to more efficiently schedule maintenance before outages occur. However, these sensors can also monitor the seabed and underwater domain and can provide useful intelligence to militaries pertaining to surface and subsurface vessel movements and other events. By turning submarine telecommunication

[310] Schindler et al., 'The Second Cold War', 1107.
[311] Schindler et al., 'The Second Cold War', 1108.
[312] Winecoff, '"The Persistent Myth of Lost Hegemony," Revisited: Structural Power as a Complex Network Phenomenon', 243.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

cables into sensing networks, these cables may become more vulnerable in a conflict as the infrastructures take on a distinct military value.

This Element has provided a succinct analysis of Indo-Pacific submarine cable geopolitics and posited a novel typology to understand how competition over this distinct infrastructure is regionally generalisable, under a network-based competition model. Nevertheless, this study faced limitations. Notably, due to the sensitive nature of undersea warfare, security classifications restrict our understanding of how Indo-Pacific states are adapting to seabed insecurity, vis-à-vis cables. Likewise, commercial sensitivities limit available data pertaining to network dynamics and state-industry relations. Moreover, the focus on Indo-Pacific dynamics inherently limits detailed comparisons with other regions, including Europe, in which seabed insecurity is perhaps more acute. Also, this Element has focussed on middle and major powers in the Indo-Pacific at the expense of smaller nations, including those in the Indian Ocean, Southeast Asia and the Pacific, which collectively have considerable influence to determine which pole succeeds in attaining a more prominent position of network centrality. Lastly, as the months and years progress, Indo-Pacific state submarine cable policy responses will continue to mature and evolve as future seabed incidents occur – meaning this study is but a preliminary examination of this fast-moving policy domain.

Further in-depth study is needed to better understand how conflict has played out on the seabed historically, the often-opaque relations between governments and respective submarine cable industries, the new geographies of future networks, the corresponding future repair requirements, and how other states are adapting. As the seabed becomes more congested, further instances of seabed warfare take place (whether confirmed or suspected), civillian cable networks become seabed sensors and great powers funnel ever more money into respective cable industries, Indo-Pacific seabed connectivity will remain at the forefront of Sino-US strategic competition. As geopolitical tensions heighten across the Indo-Pacific, cable policy will no longer be the domain of telecommunications and foreign policy agencies, but coastguards and navies will play an increasingly prominent role – as is happening in Europe. As China and the United States (and partners) compete for centrality in submarine cable networks, these nations should operate deftly so as to not weaponise the very networks these states are attempting to secure.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Acknowledgement

I'd like to acknowledge the excellent research assistance undertaken by Mr Shengzhe (Toby) Shen, Miss Tilly Robson, Mr Oscar Youlten and Ms Inès Carlier who contributed to the research of this Element. Thanks are also due to colleagues who reviewed earlier versions of this Element, including Dr David Brewster and Dr Anthony Bergin. This Element was written as part of the Australian Department of Defence-funded Strategic Policy Grant Program project '2024-053: Defending Critical Seabed Infrastructure', which I lead through the University of Melbourne. The ideas put forth in this Element are solely my own and do not reflect Australian Department of Defence policy or the policy of any other department, agency or organisation. All errors remain my own.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Cambridge Elements

Indo-Pacific Security

Kai He

Griffith University

Kai He is Professor of International Relations at Griffith University, Australia. He has authored or co-authored six books and edited or co-edited six volumes. Among his notable works are *Institutional Balancing in the Asia Pacific* (Routledge, 2009), *China's Crisis Behavior: Political Survival and Foreign Policy* (Cambridge, 2016), and *After Hedging* (Cambridge Elements in International Relations in 2023).

Steve Chan

University of Colorado Boulder

Steve Chan is College Professor of Distinction (Emeritus) at the University of Colorado Boulder. His publications include twenty-five books and about two hundred articles and chapters. His most recent book is *Culture, Economic Growth, and Interstate Power Shift: Implications for Competition between China and the United States* (Cambridge University Press, 2024).

Rumi Aoyama

Waseda University

Rumi Aoyama is Professor at the Graduate School of Asia-Pacific Studies at Waseda University, and director of Waseda Institute of Contemporary Chinese Studies. Her publications include thirteen books and more than one hundred and fifty articles and chapters. Her book, *Contemporary China's Foreign Policy* [Gendai chuugoku no gaikou] was honored with the 24th Masayoshi Ohira Foundation Memorial Prize.

Advisory Board

Amitav Acharya, *American University*

Dewi Fortuna Anwar, *National Research and Innovation Agency (BRIN), Indonesia*

Mely Caballero-Anthony, *Nanyang Technological University*

Rosemary Foot, *University of Oxford*

Evelyn Goh, *Australian National University*

Deborah Larson, *University of California, Los Angeles*

T. V. Paul, *McGill University*

Yan Xuetong, *Tsinghua University*

About the Series

Elements in Indo-Pacific Security publishes original and authoritative works on diverse security topics, encompassing not only traditional issues of war and peace but also emerging concerns such as space competition and climate change. It also explores interactions among actors within this region and between them and others beyond it.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110

Cambridge Elements

Indo-Pacific Security

Elements in the Series

Taiwan and the Danger of a Sino-American War
Steve Chan

Factional Politics in the Liberal Democratic Party: Explaining Change and Continuity in Japan's Economic Statecraft
Michael J. Gigante and Ming Wan

The Hedgers: How the Global South Navigates the Sino-American Competition
Zaki Laïdi and Yves Tiberghien

Green BRI as the New BRI: Domestic Drivers and International Implications
Min Ye and Jiaqi Wang

Bounded Ambition: China as a Multilateral Actor in World Politics
Rosemary Foot and Xueying Zhang

Indian Public Opinion toward the Major Powers
Aidan Milliff and Paul Staniland

South Korea's Soft Power: The Korean Wave
Uk Heo and Sooho Song

Decolonizing Security in East Asia: Towards Pluriversal Coexistence
Chih-yu Shih, Chiung-Chiu Huang, and Yih-Jye Hwang

Submarine Cables
Samuel Bashfield

A full series listing is available at: www.cambridge.org/EIPS

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 20:30:23, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009651110