ISSUE 11 / APRIL 2025

BLUE SECURITY

A MARITIME AFFAIRS SERIES

Securing Our Data: Subsea Cables and Maritime Security in Southeast Asia

Cynthia Mehboob
Fitriani

BLUE SECURITY
THE UNIVERSITY OF WESTERN AUSTRALIA | UWA DEFENCE & SECURITY
UNITED STATES STUDIES CENTRE
UNSW CANBERRA
AP4D Asia-Pacific Development, Diplomacy & Defence Dialogue
LA TROBE UNIVERSITY
GRIFFITH UNIVERSITY | GRIFFITH ASIA INSTITUTE

BLUE SECURITY

The Blue Security Program engages with and facilitates high quality research on issues of critical maritime security across the Indo-Pacific. Bringing together leading regional experts in politics, international law and strategic studies, Blue Security focuses on three key pillars of maritime security: order, law and power.

Blue Security is a collaboration between La Trobe Asia, Griffith Asia Institute (GAI), University of New South Wales Canberra (ADFA), University of Western Australia's Defence and Security Institute (DSI), United States Studies Centre at the University of Sydney (USSC) and the Asia-Pacific Development, Diplomacy & Defence Dialogue (AP4D).

Views expressed are solely of its author/s and not representative of the Maritime Exchange, the Australian Government, or any collaboration partner country government.

It produces working papers, commentaries, and scholarly publications related to maritime security for audiences across the Indo-Pacific.

The Blue Security consortium is led by Associate Professor Rebecca Strating (La Trobe Asia, La Trobe University), Professor Ian Hall (Griffith Asia Institute), Professor Douglas Guilfoyle (UNSW Canberra), Professor Peter Dean (United States Studies Centre), and Melissa Conley Tyler (Asia- Pacific Development, Diplomacy & Defence Dialogue).

Dr Troy Lee-Brown (Defence and Security Institute, University of Western Australia) is the Project Manager and Kate Clayton (La Trobe Asia) leads the emerging scholars program.

Blue Security receives funding support from the Department of Foreign Affairs and Trade, Australia.

@bluesecprogram

Cover image: Marisa Estivill

MARITIME AFFAIRS SERIES EDITORS

Professor Bec Strating

Bec Strating is the Director of La Trobe Asia and a Professor of Politics and International Relations at La Trobe University, Melbourne. Her research focuses on maritime disputes in Asia and Australian foreign and defence policy. She has an extensive track record in writing research publications including three monographs, most recently "Defending the Maritime Rules- Based Order" (2020). She is currently a non-visiting fellow at the Royal Australian Navy's Seapower Centre, a member of the East West Centre Council on Indo-Pacific Relations, and chair of the Women in International Security Australia's steering committee. Bec serves on the editorial boards of the Australian Journal of International Affairs and Journal of Maritime and Territorial Studies.

Dr Troy-Lee Brown

Troy Lee-Brown is a researcher in regional security, maritime security and international relations with a focus on the Indo-Pacific. He is currently the editor of the 'Black Swan Strategy Paper' and the project manager for 'Blue Security', a joint DSI-La Trobe Asia-Griffith Asia Institute-UNSW project which focuses on issues of maritime security in the Indo-Pacific. Troy has authored several journal papers with a focus on security issues in the Indo-Pacific, regionalism and maritime security. His research interests include the Indo-Pacific, India, Japan, maritime security, regionalism and climate change.

PRODUCTION COORDINATOR

Kate Clayton

Kate Clayton is a Senior Coordinator (Programs & Research) at La Trobe Asia. Her research areas include Australia, China, the Pacific Islands and the United States. Kate is interested in climate change, geopolitics and conceptions of security in policymaking. For Blue Security, Kate manages the early career researchers' program and is the publication production coordinator. Formally, Kate was a sessional academic in international relations at La Trobe University and the University of Melbourne. She is an alumnus of the US State Department's International Visitor Leadership Program, participating in program on enhancing regional maritime governance in the Quad.

MARITIME AFFAIRS SERIES AUTHORS

Cynthia Mehboob

Cynthia Mehboob is a doctoral scholar in the Department of International Relations at the Australian National University. Her research examines the complex interplay between human, non-human, and more-than-human elements in the securitisation of Australia's critical infrastructure, with a particular focus on the techno-politics of undersea cables in the Indo-Pacific. She is a 2024–2025 Women in the Alliance Fellow at the United States Studies Centre, Sydney. Beyond academia, Cynthia actively contributes to public discourse on digital infrastructure and national security, with her analysis featured in *The Interpreter (Lowy Institute), The Conversation, The Guardian Australia, NBC, Channel News Asia (CNA) Nikkei Asia, Baird Maritime, The Maritime Executive,* and the *Samoa Observer.* She has provided expert commentary on Australian radio and television, including ABC Australia and SBS News, and has appeared on several podcasts discussing the geopolitical stakes of undersea cable networks in the Indo-Pacific.

Fitriani

Dr Fitriani is a senior analyst at Australian Strategic Policy Institute (ASPI)'s Cyber, Technology and Security. Her research focuses on hybrid threats in the Indo Pacific, as well as foreign policy and non-traditional security issues. She has previously held appointments with the Centre for Strategic and International Studies; S. Rajaratnam School of International Studies, Nanyang Technological University; Dortmund University and the University of Indonesia.

CONTENTS

INTRODUCTION

Control over the undersea domain has long been a strategic imperative, but in recent years, the significance of submarine communication cables has surged, reshaping geopolitical dynamics both below and above water. The global economy's increasing reliance on digital infrastructure has driven a rapid expansion of submarine cable networks,[1] with profound implications for strategic and economic security.

Historically, three submarine cable companies – SubCom (originally part of Bell Labs[2] in the United States), Alcatel Submarine Networks, Inc. (France), and NEC Corporation (Japan) – dominated the subsea cable market.[3] However, since 2008, China's HMN Tech has expanded globally, offering competitively priced infrastructure solutions, particularly to countries in the Global South. The entry of other Chinese firms into the market, especially through Beijing's Digital Silk Road (DSR) initiative, has further altered the submarine cable manufacturing and funding landscape, appealing to nations seeking to bridge the digital divide.[4] However, this shift has raised concerns about strategic digital dependencies, particularly in regions where the intensifying US-China technological competition is viewed as a strategic dilemma for middle powers and island countries.[5]

Nowhere is this dynamic more pronounced than in Southeast Asia, the world's fastest-growing digital market.[6] With more than 125,000 new users joining the digital economy every day,[7] the region's monthly data consumption is expected to triple from 9.2 GB in 2020 to 28.9 GB per user by 2025.[8] Submarine cables, which carry around 99 per cent of all international data,[9] are a crucial yet under-secured part of Southeast Asia's digital and economic architecture. Yet, the strategic importance of Southeast Asia's digital infrastructure is complicated by its geopolitical context.

The South China Sea (SCS), the world's most militarised maritime zone,[10] is a flashpoint for territorial disputes involving China, Vietnam, Malaysia, Brunei, the Philippines, and Taiwan.[11] Taiwan is the only non-ASEAN claimant in this equation. The United States (US) has had a strong military footprint in the region since the end of WWII[12] to maintain its global strategic dominance. On the other hand, China's increasingly assertive posture in these waters in relation to other claimants has escalated tensions, raising the stakes for critical infrastructure that crosses these contested zones.[13]

Employing 'weaponised interdependence' as an analytical framework, this paper posits that the SCS constitutes a paradigmatic site for examining the strategic deployment of network centrality as a mechanism of geopolitical leverage. This framework elucidates how asymmetries in the global network topology enable great powers to consolidate power by instrumentalising infrastructural chokepoints to coerce, surveil, and dictate outcomes in transnational governance. Against this backdrop, the paper maps the unfolding dynamics of great power competition over submarine cable networks in the SCS, where material infrastructure intersects with the imperatives of sovereignty and national security.

The analysis foregrounds the politics of cable repair and maintenance regimes, particularly the regulation of licensing and permitting processes. These ostensibly technical practices, refracted through China's expansive territorial claims, exemplify how regulatory mechanisms are deployed to reinforce asymmetrical authority and shape the region's digital trajectory. The paper interrogates the cable protection regimes of all ASEAN SCS claimants and argues that ensuring subsea cable resiliency and unhampered digital connectivity requires the elimination of critical deficiencies in the existing cable protection frameworks of these actors. The study calls for stronger regional collaboration, public-private partnerships, and comprehensive policy frameworks to safeguard the region's undersea cables.

US – CHINA SUBSEA CABLES COMPETITION AND THE MILITARISATION OF DATA CABLES

NETWORK CENTRALITY AS CATALYST FOR CONTROL

During the last decade, particularly following the acceleration of China's DSR initiatives, the militarisation of submarine cables has intensified. China's status as a significant emerging player in cable manufacturing and deployment has amplified concerns about surveillance, infrastructure security, and the strategic implications of its expanding influence. The US and its allies, having long exploited similar advantages,[14] have been among the most vocal in raising alarms about China's involvement in cable projects, cognisant of the risks posed by Beijing's expanding control over this critical infrastructure.[15]

The centrality of the US in global internet infrastructure can be traced to its role as the internet's progenitor, allowing it to control critical submarine cable exchange points, which enabled extensive surveillance capabilities. Mass surveillance programs such as the National Security Agency's (NSA) BLARNEY, involved in the upstream collection of data, have been run since the 1970s in the US.[16] NSA's FAIRVIEW and PRISM programs leveraged (and sometimes created) new laws to coerce major telecommunication companies to share reports on global data flows with the US government.[17] According to the data leaked by Edward Snowden, an intelligence contractor, the NSA was able to sift data off of cables as it flowed past because of these partnerships,[18] which underscores the strategic utility of possessing network centrality for a state.

China's rise as a technological and infrastructural power mirrors the United States' earlier trajectory. In the era of intensifying US-China competition, one which borders on adversarial, China is faced with the possibility of being digitally isolated. Its strategic calculations now dictate that it utilises its state-controlled companies, such as Huawei and ZTE, and initiatives like the DSR to position itself as a dominant player in global communications infrastructure. Leading the development of 5G networks, constructing undersea cables, and financing critical projects in emerging markets, China is said to be a major force shaping digital landscapes in the Global South.[19] Domestically, China not only can summon data from its telecommunications companies by law,[20] but its Great Firewall program also exemplifies the Chinese Communist Party's (CCP) use of infrastructure as a mechanism of socio-political control to maintain internal stability via surveillance.[21]

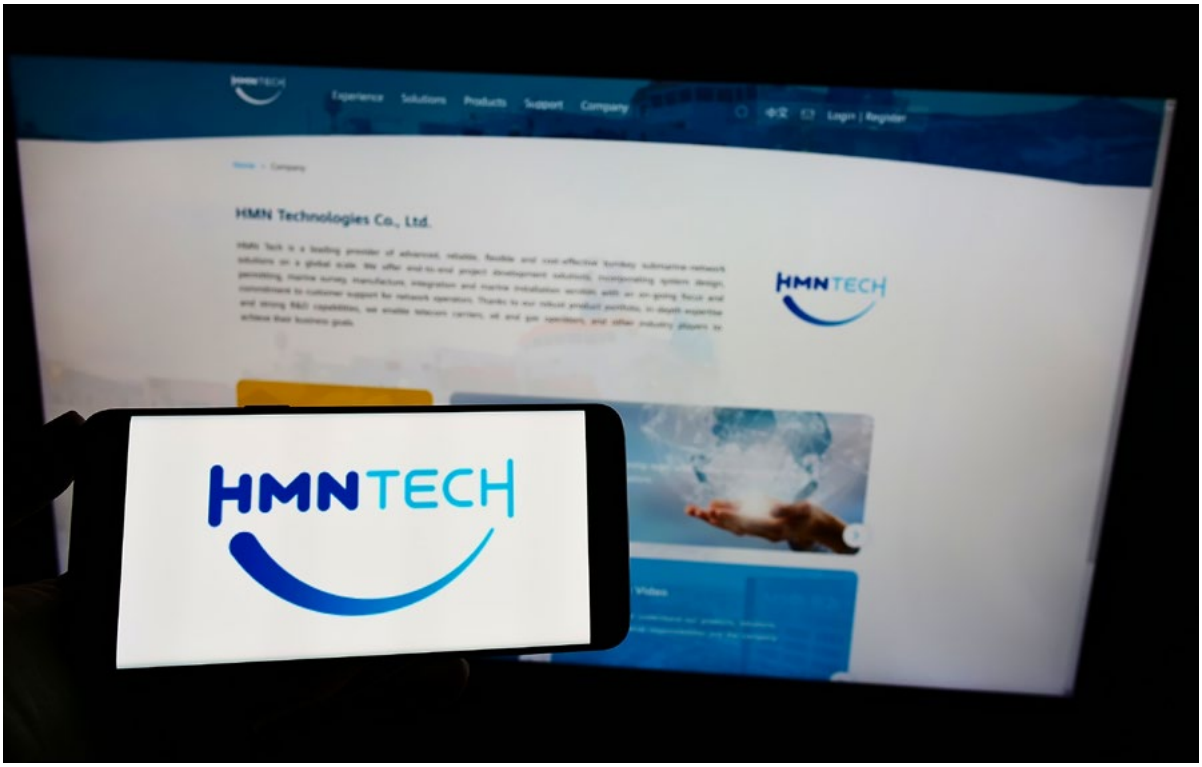
The dual-use advantages of subsea cables in the CCP's imaginary is evident in the remarks by a party official, who stated, 'Although undersea cable laying is a business, it is also a battlefield where information can be obtained.'[22] Such a perspective reinforces the view that China perceives subsea infrastructure as a critical component of its geopolitical and informational strategy, further consolidating its global position. With the launch of its DSR, China's stated aims included being able to control 60 per cent of the global subsea cables market.[23] While that ambition has not materialised, according to the China Academy of Information and Communications Technology (CAICT) – the country's top think tank on telecommunications – Chinese companies are expected to contribute 45 per cent of the total 770,000 km of cable set to be installed from 2023 to 2028.[24]

Pertinently, digital and technological offerings by Chinese companies are hardly benign. In 2013 Huawei, the parent company of HMN Technologies[25] (formerly Huawei Marine Networks, which provided subsea connectivity solutions and sold its share in the company in 2020), was implicated in intellectual property theft from the US worth $300 billion annually.[26] Washington at the time claimed that the Huawei theft on behalf of the CCP cost the US economy 2.1 million jobs per annum, and called it the greatest transfer of wealth in history.[27] The US still considers HMN Tech an affiliate of Huawei.[28] Initially, the US imposed tariffs on Huawei and then proceeded to systematically exclude it from the global networks by institutionalising its 2020 'Clean Network' initiative.[29] Over the years, the US and its allies have facilitated the ousting of Chinese cable companies from various projects such as the Coral Sea Cable and the SEA-ME-WE 6 system.[30]

Documented cases of submarine cable tapping exist against the US, notably during the Cold War and through the now-retired SEA-ME-WE3 cable.[31] It is noteworthy that disclosures about mass surveillance programs emerged from within the US. In contrast, similar disclosures are hard to expect from within China, where strict state control limits transparency. On the other hand, China's domestic practices, such as employing its Great Firewall for autocratic control and its ambition to wire as much of the world as possible through Chinese companies with a tainted reputation, and with a track record of surveillance and stealth at such a staggering scale, raise significant concerns about its intentions in the global technological arena.

These incidents present useful insights into how nation-states leverage the internet and related infrastructure for strategic gains. The US and now China's behaviour concerning undersea cables can be described using the weaponised interdependence framework. 'Weaponised interdependence' is a term used to refer to states leveraging global informational and financial networks for strategic purposes in the international system, a concept advanced by Henry Farrell and Abraham Newman.[32] They contend that network topographies, characterised by asymmetries in connectivity, allow states with jurisdiction over central nodes and the requisite domestic institutions to exploit these structural advantages for coercive ends, employing mechanisms such as the 'panopticon effect' (strategic information gathering) and the 'chokepoint effect' (denial of access).[33] Farrell and Newman argue that key global networks tend to be self-reinforcing and asymmetrically distributed, reinforcing power imbalances. These networks, exemplified by systems like SWIFT and the internet, are increasingly centralised in a 'hub-and-spoke' configuration, consolidating power in a limited number of intermediaries and contradicting the expectations of Keohane and Nye's theories of global cooperation.[34]

The weaponisation of infrastructure, as evidenced by both the US and China, is not a moral failing specific to any one state but rather a natural consequence of strategic anxiety and capacity-meeting opportunity. The US's early actions in the internet era, far from being a departure from geopolitical norms, can be viewed as an extension of established national security practices – a trend China now follows as its infrastructural capacities grow. Beijing is now seen acting in ways consistent with the structural imperatives of a state capable of achieving increasing centrality in regional, if not global, communications. Both cases illustrate that technological dominance naturally lends itself to exploitation by states seeking to extend their influence and secure their strategic interests.



SOUTH CHINA SEA AND THE US-CHINA GEOPOLITICAL COMPETITION

The SCS is a region characterised by territorial tensions between several claimants, including China, Malaysia, Taiwan, Vietnam, Brunei, and the Philippines. The territorial claims of Taiwan and China mirror each other, while other states have competing and overlapping claims too. US alliances, such as those with the Philippines[35] and Taiwan,[36] create a complex web of military and political commitments, including defence treaties and the establishment of military bases. China's strategic concerns are centred around territorial claims and access to strategic waterways such as Miyako and Taiwan Strait, and the Bashi Channel,[37] intensifying regional tensions.

The SCS is simultaneously a vital corridor for subsea cables,[38] providing the most efficient route to connect East Asia with the broader Asian continent and onward to Africa. The strategic importance of this route cannot be overstated, as it facilitates a significant portion of the region's digital connectivity. Given the contested nature of this maritime zone, laying a new cable system in these waters or repairing damaged cables requires the industry to seek permits from all parties claiming a particular maritime zone. Undersea data cables are transnational objects. Even in regions where there are no competing maritime claims, this critical infrastructure is highly vulnerable. They can be snagged by trawlers and severed by anchors. According to the International Cable Protection Committee (ICPC), over 70 per cent of all cable faults globally can be attributed to fishing and anchoring activities, while natural hazards account for less than 20 per cent.[39] High-vessel traffic areas, combined with shallow waters, spell damage to these cables. The SCS is relatively shallow, with nearly half of its seabed consisting of continental shelf areas at depths of less than 650 feet.[40] Only 16 per cent of the sea consists of deep basins, such as those reaching over 16,400 feet.[41] It is no wonder, then, that over half of all cable faults globally are reported in the SCS. More than 50 per cent of global fishing vessels operate in these waters, too, underscoring the vulnerability and strategic significance of this underwater infrastructure.[42]

Human fishing-related activities and natural hazards aside, the geopolitical landscape of the region puts the security of this critical infrastructure at further risk. In 2013, the Philippines initiated arbitration to clarify the legal status of the waters and islands in the SCS, challenging China's sweeping claims. In 2016, the Permanent Court of Arbitration in The Hague ruled that the majority of China's claims under its 'nine-dash line' were unlawful.[43] While the ruling affirmed China's legal claim to only 20 per cent of the SCS, Beijing has continued to assert control over 90 per cent of the region,[44] dismissing the ruling.

Over the years, subsea cables have become an integral part of China's strategic plan to assert its illegal maritime claims in the SCS. China has markedly expanded its underwater capabilities in the SCS.[45] Central to this effort is the development of a sophisticated underwater surveillance network, often described as the 'Great Underwater Wall.'[46]

Utilising a combination of sensors, unmanned underwater vehicles, and intelligence-gathering operations, this network monitors maritime activity, granting Beijing a strategic advantage in situational awareness and maritime security. The Asia Maritime Transparency Initiative (AMTI) noted in 2020 that China has deployed a robust array of sensors and communication systems between Hainan Island and the Paracel Islands, forming a part of the 'Blue Ocean Information Network.'[47] Developed by the state-owned China Electronics Technology Group Corporation (CETC), this network is officially framed as an environmental monitoring and communication system. However, its dual-use potential is evident, with capabilities that extend into military applications. The system's most visible components are the 'Ocean E-Stations,' or floating integrated information platforms (IIFPs), and the 'island reef-based integrated information systems' (IRBIS).[48] Together, these floating and fixed platforms enhance China's ability to control and surveil the maritime environment, raising significant cable-related security concerns for other SCS claimant states and global maritime stakeholders.

China is not alone in deploying oceanographic research assets. The US has engaged in underwater espionage since, arguably, the Cold War;[49] and China has accused the US of deploying surveillance vessels in the SCS on several occasions.[50] Strategically, underwater surveillance by external actors in the SCS poses a heightened threat to China, as these waters host a substantial portion of its undersea cable infrastructure, critical to its national and regional connectivity.

At the time of writing, China's cable map, as captured by Telegeography, is as follows:

No	China's cables	Ready for service (RFS)	Cable Length	Supplier	Owners	Shared with other SCS claimants
1	APCN-2	2001		NEC	AT&T, BT, China Telecom, China Unicom, Chunghwa Telecom, HKBN, KDDI, KT, LG Uplus, NTT, Orange, PCCW, PLDT, Singtel, Singtel Optus, Softbank Corp, Starhub, Tata Communications, Telekom Malaysia, Telstra, Verizon, Vodafone	Malaysia, Philippines, Taiwan
2	Asia Africa Europe-1 (AAE-1)	2017		NEC, SubCom	China Unicom, Djibouti Telecom, Etisalat UAE, Hyalroute, Metfone, Mobily, National Telecom, OTEGLOBE, Omantel, Ooredoo, PCCW, Pakistan Telecommunications Company Ltd., Reliance Jio Infocomm, Retelit, TIME dotCom, TeleYemen, Telecom Egypt, VNPT International, Viettel Corporation	Malaysia, Vietnam
3	Asia-America Gateway (AAG) Cable System	2009		ASN, NEC	AT&T, BT, Bharti Airtel, Eastern Telecom, Ezecom, Globe Telecom, Indosat Ooredoo, National Telecom, PLDT, Saigon Postel Corporation, Spark New Zealand, Starhub, Telekom Malaysia, Telkom Indonesia, Telstra, Unified National Networks (UNN), VNPT International, Viettel Corporation	Brunei, Malaysia, Philippines, Vietnam
4	Asia Direct Cable (ADC)	2024 (Q4)		NEC	China Telecom, China Unicom, National Telecom, PLDT, Singtel, Softbank Corp, Tata Communications, Viettel Corporation	Philippines, Vietnam
5	Asia Link Cable (ALC) (2026)	2026 (Q1)	7,200 km	HMN Tech	China Telecom, China Unicom, DITO Telecommunity, FPT Telecom, Globe Telecom, Singtel, TIME dotCom, Telekom Malaysia, Unified National Networks (UNN), VNPT, Viettel Corporation	Malaysia, Philippines, Veitnam
6	Asia Pacific Gateway (APG)	Nov 2016	10,400m	NEC	China Mobile, China Telecom, China Unicom, Chunghwa Telecom, KT, LG Uplus, Meta, NTT, National Telecom, Starhub, TIME dotCom, VNPT International, Viettel Corporation	Malaysia, Taiwan, Veitnam
7	Asia Submarine-cable Express (ASE)/Cahaya Malaysia	Aug 2012	8,148 km	NEC	NTT, PLDT, Starhub, Telekom Malaysia (Telekom Malaysia owns two fibre-pairs, which it refers to as the Cahaya Malaysia system. NTT, PLDT, and Starhub jointly own the other four fibre pairs.)	Malaysia, Philippines

No	China's cables	Ready for service (RFS)	Cable Length	Supplier	Owners	Shared with other SCS claimants
8	Cambodia-Hong Kong	July 2025	2,175 km	China's Unicom Group	Government of Cambodia	Landing points uncertain
9	Cross-Straits Cable Network (CSCN)	Aug 2012 Estimates Aug 2037	21 km	China	China Mobile, China Telecom, China Unicom, Chunghwa Telecom	Taiwan
10	Dalian-Yantai Cable	March 1998	146 km	ASN	China Telecom	Domestic cable
11	EAC-C2C (East Asia Crossing – City to City)	Nov 2002	36,500 km	Initially constructed by Asia Global Crossing	Telstra	Philippines, Taiwan
12	FLAG Europe-Asia (FEA)	Nov 1997	28,000 km	SubCom	Global Cloud Xchange	Malaysia
13	FLAG North Asia Loop/REACH North Asia Loop	June 2001	9,504 km	ASN, Fujitsu	Global Cloud Xchange, PCCW, Telstra (Global Cloud Xchange owns 3 fiber pairs which it refers to as FLAG North Asia Loop. Of the three remaining fiber pairs comprising the REACH North Asia Loop, Telstra owns one fiber pair, PCCW owns one fiber pair, with the final fiber pair is jointly owned by Telstra and PCCW).	Taiwan
14	Haikou-Beihai Cable	1999	198 km	ASN	China Telecom	Domestic cable
15	Hainan to Hong Kong Express (H2HE)	Sep 2021	675 km	HMN Tech	China Mobile	Domestic cable
16	New Cross Pacific (NCP) Cable System	May 2018	13,618 km	SubCom	China Mobile, China Telecom, China Unicom, Chunghwa Telecom, KT, Microsoft, Softbank Corp	Taiwan
17	Ningbo-Zhoushan Cable	July 1998	35 km	ASN	China Telcom	Domestic cable
18	SEA-H2X	2025 (Q3)	5,000 km	HMN Tech	China Mobile, China Unicom, Converge ICT, Sonia Satellite Services Sdn Bhd	Malaysia, Philippines

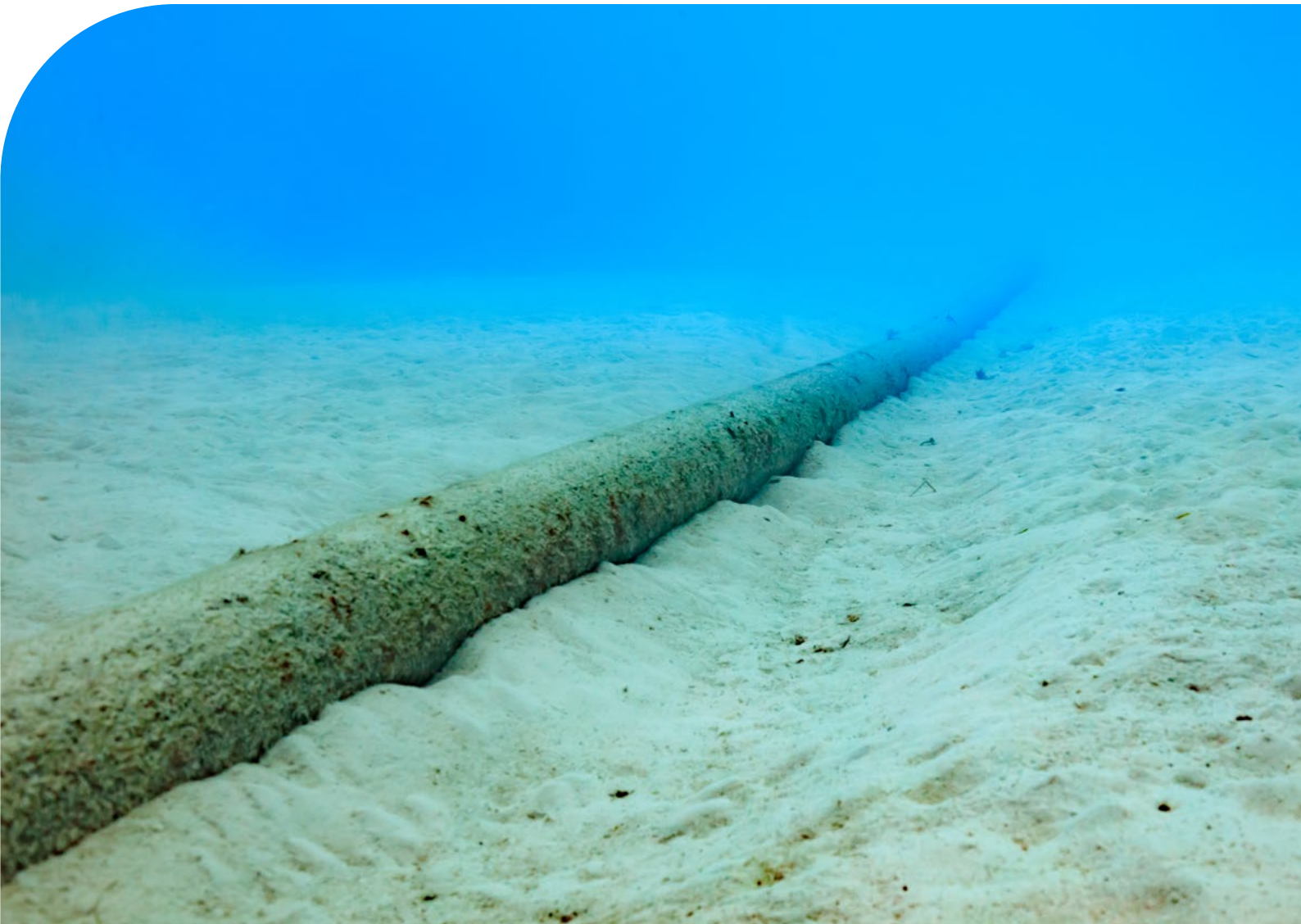
No	China's cables	Ready for service (RFS)	Cable Length	Supplier	Owners	Shared with other SCS claimants
19	SeaMeWe-3 (Retired on 2 December 2024 after 25 years of service)	Sep 1999	39,000 km	ASN, Fujitsu, SubCom	A1 Telekom Austria, AT&T, Altice Portugal, BICS, BT, CTM, China Telecom, Chunghwa Telecom, Cyta, Deutsche Telekom, Djibouti Telecom, Embratel, Etisalat UAE, Indosat Ooredoo, Jabatan Telecom Brunei, KDDI, KPN, KT, LG Uplus, Maroc Telecom, Myanmar Post and Telecommunication (MPT), National Telecom, OTEGLOBE, Omantel, Orange, Orange Polska, PCCW, PLDT, Pakistan Telecommunications Company Ltd., Rostelecom, Saudi Telecom, Singtel, Singtel Optus, Softbank Corp, Sparkle, Sri Lanka Telecom, Tata Communications, Telecom Argentina, Telecom Egypt, Telekom Malaysia, Telkom South Africa, Telstra, Tunisia Telecom, Turk Telekom, Ukrtelecom, VNPT International, Verizon, Vocus Communications, Vodafone, eir	Brunei, Malaysia, Philippines, Taiwan, Vietnam
20	Southeast Asia-Japan Cable 2 (SJC2) 2025	2025 (Q1)	10,500 km	NEC	China Mobile, Chunghwa Telecom, DongHwa Telecom, KDDI, Meta, SK Broadband, Singtel, Telin, True Corporation, VNPT-Vinaphone	Taiwan, Vietnam
21	Southeast Asia-Japan Cable (SJC)	June 2013	8,900 km	NEC, SubCom	China Mobile, China Telecom, Chunghwa Telecom, Globe Telecom, Google, KDDI, National Telecom, Singtel, Telkom Indonesia, Unified National Networks (UNN)	Brunei, Philippines
22	Taiwan Strait Express-1 (TSE-1)	Jan 2013	260 km	HMN Tech	China Mobile, China Unicom, Chunghwa Telecom, Far EasTone (FET), Taiwan International Gateway Corporation, Taiwan Mobile	Only connects China and Taiwan
23	Tata TGN-Intra Asia (TGN-IA)	March 2009	6,700 km	SubCom		Only 4 landing points (Singapore), Philippines, Vietnam
24	TKO Connect	Sep 2023	6 km		HKBN, SUNeVision	Domestic cable
25	Trans-Pacific Express (TPE) Cable System	Aug 2008	17,968 km	SubCom	AT&T, China Telecom, China Unicom, Chunghwa Telecom, KT, NTT, Verizon	Taiwan

Table 1: A snapshot of China's subsea cables map.
All the data used to populate this table has been generated from TeleGeography's Submarine Cable Maps web resource[51]

As detailed in the table, after SEA-ME-WE 3's recent retirement, there are 24 submarine cable systems (active and planned) connecting China to global digital networks. Of these, 20 are already operational, and 4 are set to go live between 2025-2026. Notably, 19 of these systems feature connection points in other SCS claimant states, while the remaining 5 are purely domestic cables enhancing connectivity within China. The only new planned system with potential regional reach, the Cambodia-Hong Kong cable, is scheduled for activation in 2025, though its future connections to other claimants remain uncertain at this stage.

At the time of writing, of all SCS claimants, China has the highest number of cables landing on its shores, with most cables of other claimants having at least one landing point in China. This dynamic affords Beijing 'network centrality', a concept at the core of Newman and Farrell's arguments. It highlights how control over critical digital infrastructure can amplify a node's global influence.[52] Examples of the benefits of network centrality can be seen in how the US historically leveraged this advantage to gain geopolitical advantages. As Newman and Farrell explain, the United States has long recognised that communication traffic – whether phone calls, emails, or chats – typically follows the cheapest available route rather than the most physically direct one.[53] Nonetheless, as part of its PRISM and other mass surveillance programs, the NSA encouraged telecommunication companies to prioritise the transfer of data via the US before being routed to its final destinations. Farrell and Newman argue that gaining network centrality is the consequence of deliberate policy and not an accidental achievement.[54]

This carefully crafted engineering of network centrality amplified US power over global information flows. Given the US's effective use of network centrality to shape global dynamics, it is fair to assert that China's drive to replicate this model is both logical and strategic.



CHINA'S QUEST FOR NETWORK CENTRALITY IN THE SOUTH CHINA SEA

After the installation of the physical layer of submarine cables, one of the network management software used to operationalise these cables is the Software-Defined Networking (SDN) application.[55] It is used to enhance the utilisation of the physical layer of the infrastructure while improving network efficiency. Analysts argue that Chinese companies are leading the way in the creation of this software. During a period of intensified tensions in the SCS region, the Southeast Asia-Japan Cable (SAJC), manufactured by SubCom and NEC, with connection points in China and responsible for connecting Japan to Singapore, became a victim of SDN misuse. Data bound for Japan was being routed through Hainan Island, which falls under China's jurisdiction.[56]

Table 1 illustrates that all claimant states in the SCS currently have various subsea cables landing in China. Just as cables landing in any other country, these are susceptible to being tapped or the data to being re-routed on occasion – such is the nature of this network. The SDN example above demonstrates the advantages of several claimant cables landing on China's shores and their role in materialising Beijing's strategic interests.

Based on the logic of the benefits offered by network centrality, the table demonstrates that China seems to be strategically embedding itself within regional SCS connectivity systems, prioritising redundancy. Despite ongoing tensions, the network architecture in the SCS has created a scenario where China and other claimant states are intertwined, in what we term a complex 'digital embrace.' According to an industry professional,[57] any harm to cables in the SCS waters harms China's connectivity, too. Therefore, physical harm to a cable system entangled with those of other claimants will affect the connectivity of several stakeholders. This creates a 'shared risk' scenario, making deliberate sabotage to the physical layer of cable infrastructure unlikely.

However, by the strategic awarding of cable-related permits in SCS, China seems to be deliberately engineering a position of centrality, using the regulatory tools at its disposal to create infrastructural interdependence in the region it seeks to dominate. This is underpinned by several factors:

CABLE MANUFACTURING TRENDS

Of the 20 active cables connecting China with other SCS claimants, 16 were manufactured by Western and Japanese companies, with only 4 – two of which are smaller, domestic cables – produced by Chinese firms. Among the 5 planned systems, NEC Japan is responsible for two, while the other three will be manufactured by Chinese companies. This shift towards Chinese-manufactured infrastructure is an emerging trend that cannot be ignored.

Several factors contribute to this shift. Chinese-made cables are not only cheaper, making them an attractive option for countries seeking cost-effective solutions, but they also allow China to maintain greater control over the infrastructure. Chinese companies are legally obligated to cooperate with the government and provide data upon request,[58] which gives China an additional layer of control over digital flows in the region.

CABLE LIFESPAN AND REPLACEMENT

The typical operational lifespan of modern fibre-optic cable systems is around 12 to 17 years,[59] older systems often remain in service for over 25 years.[60] Newer systems, however, are retired sooner due to rapid innovation in the cable industry and the growing demand for higher capacity across all networks. Additionally, older systems become more expensive to maintain on a per-terabyte basis.[61] As shown in Figure 1, the average age of the 16 Western-manufactured cables connecting China to other SCS claimant states is approximately 18 years, indicating that these systems are past their optimal service life.

From this perspective, it is plausible to deduce that China's restriction on new permits for Western companies is part of a broader strategic calculus:

a) **Ensuring Future Undersea Infrastructure Dominance:** At the time of writing, the last instance of a non-Chinese vendor successfully laying a subsea cable in the SCS was the Asia Direct Cable (ADC) by NEC, a Japanese company, which received a permit in 2019.[62] Since then, there has been a marked absence of new licenses issued to non-Chinese entities. By denying access to foreign companies, China can gradually ensure that future cables connecting its territory are domestically manufactured, thereby consolidating its control over the infrastructure. This move will not only enhance the security of its own networks but will also diminish the influence of external actors in the region's digital sphere.

b) **Maintaining Digital Interdependence:** In the SCS, any route planning, surveying, or construction inherently involves Chinese permission and oversight, further cementing Beijing's strategic position. Infrastructural interdependence also abates China's own strategic anxieties concerning physical infrastructure in the region, given the entangled nature of the submarine cable networks.

The implications of this strategy are profound. As existing Western-manufactured cables near the end of their lifespan, SCS claimants, including ASEAN members and Taiwan, are faced with a strategic dilemma. Relying on established connections, which increasingly lead back to Chinese-controlled infrastructure, may offer the path of least resistance but also risks entrenching Chinese influence over their digital futures. Western companies are increasingly circumventing SCS for future cables for the same reason.[63]

Increases in regulations, permitting issues, and cable repair times add another layer of strategic complexity to the region at a time when Southeast Asia is increasingly positioning itself as a prime destination for global tech operators seeking to establish data centre bases. Singapore, Malaysia, Thailand, Indonesia, and Vietnam have emerged as the region's top five hubs.[64] Notably, two of these – Malaysia and Vietnam – are SCS claimant states. As data centres proliferate across Southeast Asia, regional governments are locked in a competitive race to attract investment, with Singapore leading for now.[65]

The table below provides a comparative snapshot of the economic and digital infrastructure of SCS claimant states, emphasising their reliance on undersea cables for connectivity and economic growth:

Country	Total GDP in billions (USD)	Digital economy contribution to GDP in percentage (%) in 2023	Number of Data Centres	Annual Revenue from Data Centres (USD)	Total Number of Active International Submarine Systems	Number of Active International Cables Connected to China	Planned systems	Planned systems connected to China	No. of planned systems designed to crisscross SCS
Malaysia	445.52	23 %	~50	812 mil (2024 projection)	21	8	6	2	2
Vietnam	465.81	12 %	~30	561 mil (2022), 685mil (2023) projected 1.44 bn by 2029	5	5	4	3 (no details available for the fourth system)	3
Taiwan	802.96	29.9 %	27	1.47 bn (2023), projected 3.45 bn by 2029	11	9	3	1	1
Philippines	471.52	8.5 %	~22	750 mil (2023) projected 1.61 bn by 2029	10	7	7	3	3
Brunei Darussalam	15.51	3.12 %	1	Not specified	4	3	1	1	1

Table 2: All data presented in columns 6-10 is collected from TeleGeography's web resource 'Submarine Cable Map'.[66]

The figures reveal key strategic dependencies and economic vulnerabilities that are deeply intertwined with the economic and national security situations of SCS claimants, especially in the context of US-China competition for influence in the region. Unlike the US, which relies on freedom of navigation operations, lobbying, and diplomatic leverage, China wields direct regulatory power in the SCS waters.

This paper argues that, in the context of the SCS region, China holds a stronger strategic position than the US in the competition over submarine cables. China asserts claims to 90 per cent of the SCS[67] and mandates that cable repair and maintenance vessels obtain permits to operate within its EEZ – a requirement that contravenes the provisions of the United Nations Convention on the Law of the Sea (UNCLOS). This effectively means that any entity seeking to lay, operate, maintain, or repair subsea cable systems in these waters must secure China's approval as a permitting authority, even though such approval exceeds its legal rights.

MAINTENANCE AND REPAIR IN THE SOUTH CHINA SEA

The SCS is one of the busiest maritime regions in the world, with an estimated $5.3 trillion in trade passing through its waterways annually.[68] Its geopolitical significance is further underscored by the presence of critical undersea infrastructure, particularly at least 11 submarine cable systems,[69] that connect Southeast Asian nations to global communication networks.

In the SCS, where multiple nations claim the same waters, efforts to repair or maintain these cables can be hindered by territorial disputes. If a cable running through disputed waters is damaged, a country's attempts to repair it might be viewed as an infringement on another claimant's sovereignty. China's harassment of a private repair vessel, escorted by a Vietnamese naval ship within the Vietnamese EEZ in April 2024, is a case in point.[70] Legal and political complexities such as these add to the already difficult task of maintaining and securing submarine cables in Southeast Asia.

CABLE MAINTENANCE AGREEMENTS APPLICABLE TO THE SOUTH CHINA SEA

There are two primary types of maintenance agreements for submarine cables: geographical zone-based Cable Maintenance Agreements (CMAs), wherein cable owners coordinate maintenance on a regional basis, and private ad-hoc agreements, which involve maintenance providers offering services for individual cables. In the latter arrangement, contracts are established for each cable, with specified priorities for intervention in the event of multiple faults. Additionally, service providers typically maintain depot facilities and base ports; however, vessels may also be utilised for other operations, which can result in delayed mobilisation for cable repairs.[71]

Repair capabilities for submarine cables in Southeast Asia are governed by three key frameworks: the Southeast Asia and Indian Ocean Cable Maintenance Agreement (SEAIOCMA), the Yokohama Zone (YZ) agreement, and the Asia Pacific Marine Maintenance Service Agreement (APMMSA). SEAIOCMA and YZ are consortium-based agreements, while APMMSA is a private zone agreement.[72]

SEAIOCMA, which, according to industry sources, covers 45 cables with 47 cable owners and spans regions from Djibouti to Guam and Taiwan to Australia, relies on support from ASEAN Cableship Pte Ltd, Indian Ocean Cableship Pte Ltd, and Global Marine Systems Ltd, with base ports in Singapore, Sri Lanka, and the Philippines. YZ is currently responsible for 20 cables and includes 27 cable owners as members. It maintains two cable ships and strategically located depots to ensure rapid repairs. The provisions of these contracts stipulate that cable repair ships, along with their highly skilled crews, will commence sailing within 24 hours of being notified of a fault in the cable system.[73] YZ is serviced by three ship operators: Chinese SBSS, Japanese KSC – KDDI Cableships and Subsea Engineering Inc., and Korean LS Marine Solutions. Chinese company SBSS is contracted to service the Yokohama Zone for six months of the year,[74] according to Mike Constable, former CEO of Huawei Marine Networks (later rebranded as HMN Tech) and a recognised authority on the strategic, commercial, and regulatory aspects of submarine cable system development and deployment. YZ and SEAIOCMA together have a joint agreement – the Pacific and Indian Ocean Cable Maintenance Agreement (PIOCMA) – that addresses the overlap between their respective zones, enabling assets from each to provide coverage in the overlap area. The current YZ agreements expired in late 2024,[75] while SEAIOCMA's agreements will expire at the end of 2025.[76]

APMMSA is now solely managed by ASN following SubCom's 2023 withdrawal from maintenance activities, and provides coverage for the Pacific and Indian Oceans.[77] SubCom (a US company that, Reuters notes,[78] was historically a US Cold War project) withdrew from the APMMSA, a private-sector consortium for cable maintenance, in 2023. This move coincided with SubCom's parent company acquiring land for a cable depot in the Philippines, aligning with the US Department of Defense's expanded military presence in the region under the Enhanced Defense Cooperation Agreement (EDCA) signed in April 2023.[79] The timing is significant, as it reflects the US race to secure control over critical subsea infrastructure – particularly in the face of China's growing regulatory dominance in the SCS.

SubCom's exit from APMMSA also suggests a move away from agreements that may limit US influence over infrastructure, while the Philippines depot allows for rapid maintenance of cables critical to global communications, particularly in contested areas. The strategic positioning of this depot is not only about infrastructure but also about reinforcing US geopolitical objectives, ensuring key subsea routes remain accessible to allies and out of China's reach. Some of these tactics may be deemed responsible for Bejing's more time-consuming approach[80] to issuing licences and permits for cable repairs and maintenance.

While Southeast Asian nations own, register, and operate some cable-laying and repair ships – 11 of the over 59[81] installation and maintenance assets[82] – the ability to perform quick and cost-effective repairs is not always guaranteed. Factors such as vessel and crew availability, weather conditions, and the need to obtain necessary permits or licenses can complicate the repair process.

As per unpublished industry data, 206 cable faults were reported worldwide in 2023, with the average notification to departure time for repair vessels being 21 days. Numbers on global repair distribution indicate that 44 per cent of the faults occurred within territorial waters, 54 per cent within EEZ, and only 2 per cent in the high seas. The same unpublished data from 2023 shows that the eastern hemisphere's maintenance agreements, which include SEAIOCMA, Yokohama and APMMSA, saw a rise in repair vessel response time.[83] The reason provided for this delay is the backlog of repair time in the Asia region. According to recent industry data, the high vessel utilisation rate within SEAIOCMA could be deemed one of the reasons for the delay in repair vessel response time, with the vessel utilisation rate within SEAIOCMA and YZ sitting at approximately 84 and 40 per cent, respectively.[84] This backlog, according to other unnamed industry sources, can also be attributed to reasons related to operational and security permits and regulations[85] by the very states that have their connectivity disrupted due to cable breaks. In 2023, the mean time for a vessel to commence repair was over 40 days.[86]

'China's possession of fewer than ten cable-laying vessels'[87] – some of which are newly acquired, including the largest cable-laying vessel – adds complexity to the situation. China's intent behind expanding its fleet of cable-laying vessels is often framed as serving both domestic and geopolitical objectives.[88] However, some industry analysts,[89] including Constable, argue that given HMN Tech's possession of only one new vessel, Beijing's primary priority is securing assets to deploy and maintain China's infrastructure. This is vital for mitigating the risk of exclusion from the global cable ecosystem, which remains heavily influenced by US policies and the broader Western-led digital infrastructure landscape. In fact, according to industry sources like Constable, who has extensive experience in industry developments, HMN Tech has faced challenges in offering maintenance solutions to investors, with its limited vessel assets presenting a significant barrier. Despite this, industry sources claim that China offered a repair vessel to SEAIOCMA, but the proposal was not accepted by its members.[90] This, arguably, reflects the industry's reluctance to become entangled in great-power rivalry.

While China's strategic withholding of licenses for Western companies to conduct cable-laying operations in the SCS has placed increasing pressure on claimant states, two HMN Technologies-led projects are on track to come online next year. These projects, which run through the SCS, have faced no such permitting issues, with an involved executive at a Chinese telecom company stating, 'We have not seen any issues'.[91] According to the Washington Post, bypassing the SCS would require additional cable and extended installation periods. Moreover, certain alternative routes pass through shallower waters, which increases the vulnerability of the cables to faults. Given the limited number of cables operating along these routes, rerouting traffic in the event of a disruption would prove challenging, heightening the risks to connectivity and system reliability for all states in the region.[92]

The extent of China's regulatory control on permits raises critical questions about the role of international legal frameworks and regulatory mechanisms. Understanding how these frameworks are structured, enforced, and navigated by various states is crucial in determining whether the region can maintain a balanced digital ecosystem or if it will see a shift towards a more consolidated, China-centric model. The next section will explore the regulatory frameworks of SCS claimant states in greater detail, assessing the extent to which they offer resilience against strategic monopolisation and the pressures they face in an era where digital and physical infrastructures are increasingly interlinked.

THE INSUFFICIENCY OF EXISTING CABLE PROTECTION REGIMES IN THE SOUTH CHINA SEA

HISTORICAL LEGAL FRAMEWORKS

The first significant international agreement to address submarine cables was the 1884 Convention for the Protection of Submarine Telegraph Cables. It laid the foundation for the legal status of undersea cables by affirming the freedom to lay and repair them across international waters. Legal experts note that the international legal regime for protecting and managing submarine cables has remained largely unchanged since 1884.[93] Unsurprisingly then, the legal provisions under the 1884 Convention were more relevant to a time when submarine cables played a peripheral role, primarily for telegraphic communication. Its limitations are evident in that it does not restrict belligerent actions against these cables, making it ill-suited to deter modern sabotage and hostile activities.[94]

Subsequent international agreements, such as the 1958 Geneva Convention on the High Seas and the 1982 UNCLOS, expanded on these freedoms. UNCLOS in particular provides the most comprehensive international legal framework for the laying, operation, and maintenance of submarine cables. Article 58 of UNCLOS stipulates that all states, whether coastal or landlocked, enjoy freedoms of navigation, overflight, and the laying of submarine cables and pipelines within the EEZ of coastal states. Importantly, UNCLOS recognises that beyond the 12-nautical mile territorial sea, coastal states may not unduly impede the maintenance and repair of these cables, effectively granting cable operators the right to maintain and repair existing infrastructure across international waters. Additionally, UNCLOS Articles 113, 114, and 115 mandate that states criminalise the wilful or negligent damage of cables, ensure reimbursement for damages, and compensate shipowners who sacrifice equipment to avoid cable damage. These updates reflect a progression toward better protection and maintenance of global undersea infrastructure, though gaps remain in addressing modern security threats.

Pertinently, despite the extensive legal provisions offered by UNCLOS, the United States has neither signed nor ratified the treaty. As a non-party to UNCLOS, the US is limited to relying on the 1884 Convention rules to protect its undersea cables. The 1884 Convention – which the US incorporated into law – prohibits the intentional breaking of cables, though this ban notably does not apply in wartime.[95]

MAINTENANCE AND REPAIR RIGHTS UNDER UNCLOS

While UNCLOS does not explicitly mention maintenance activities, the general understanding supported by legal scholars, is that the freedom to lay cables includes the right to maintain and repair them.[96] Articles 58 and 79 of UNCLOS collectively affirm this interpretation, ensuring that states must not obstruct these activities. During the negotiations leading to the adoption of UNCLOS, there were debates about what constituted 'internationally lawful uses of the sea' related to submarine cables. Scholars such as Burnett, Davenport,[97] and Beckman[98] argue that this expression should encompass not only the laying but also the maintenance and repair of cables, which is essential to keep them operational.

Furthermore, this understanding is significant when considering that submarine cables are vital components of the global information infrastructure; hence, legal frameworks need to account for ensuring their continuous operation. Despite this, UNCLOS does not provide clear directives on addressing cable sabotage or deliberate damage, leaving a gap in legal coverage that could be exploited by state or non-state actors. This vulnerability has been highlighted by recent events and disputes, such as those in the SCS region, where geopolitical rivalries have raised concerns over the security of submarine cables.

REGIONAL DEVELOPMENTS ASEAN'S GUIDELINES

While global efforts to update and expand the legal frameworks have been slow, regional initiatives have started to address specific issues, particularly in Southeast Asia. In October 2019, the Association of Southeast Asian Nations (ASEAN) adopted the ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables.[99] These guidelines, while non-binding, represent a significant step forward in recognising the strategic importance of swift cable repairs. The guidelines also advocate for streamlining the permitting process for submarine cable repairs, encouraging transparency and simplification of regulations.

To complement the provisions of UNCLOS, individual SCS claimants have implemented national regulations to enhance the security of undersea cables. However, these regulatory frameworks exhibit significant variation across different jurisdictions. The following section undertakes a detailed examination of these frameworks, aiming to reveal how distinct national priorities shape regulatory approaches and to identify critical gaps in security. This analysis will offer insights into the inconsistencies and vulnerabilities that persist in the protection of undersea cable infrastructure.

DOMESTIC TELECOMMUNICATIONS LEGISLATIVE FRAMEWORKS SCS CLAIMANTS OTHER THAN CHINA

In this section, we discuss the legislative frameworks by SCS claimants. The fact that they have enacted regulations on subsea cables – albeit limited in their implementing capacity and relative power of assertion compared to the great powers dominating the contested waters – demonstrates their agency in independent decision-making in this critical area. This showcases regional stakeholders not as passive actors bending to external pressures, but as agentic participants shaping their destinies amidst complex geopolitical dynamics.

BRUNEI

Brunei, with its ambitious digital transformation agenda, aims to position itself as a 'Connected Smart Nation,' driven by the Authority for Info-communications Technology Industry of Brunei Darussalam (AITI).[100] With 95% of its population connected to the internet, Brunei has laid out a strategic five-year 'Digital Economy Master Plan'[101] to enhance digital connectivity.

As a claimant in the SCS, Brunei relies on robust connectivity to global networks, supported by four existing submarine cable systems. To bolster regional interconnectivity, Brunei has embarked on the Asia Link Cable (ALC) project, set to be completed by 2025.[102] This 7,200 km, $300 million[103] initiative aims to connect key regional hubs such as Hong Kong SAR, Singapore, the Philippines, Brunei, and Hainan, China,[104] thereby reinforcing Southeast Asia's economic integration. The addition of the ALC reflects a strategic move to diversify connectivity routes and enhance redundancy. However, the recent retirement of the SEA-ME-WE 3 cable, which has been a critical link since 2000, underlines the urgency of updating and expanding Brunei's digital infrastructure.

In 2023, Brunei issued a Telecommunications Code under the existing 2001 Telecommunications Order, representing a strategic move to regulate the telecommunications sector through a structured legal framework.

The 2023 Telecommunications Code[105] introduces a comprehensive regulatory structure aimed at promoting sustainable competition, technological neutrality, and efficient infrastructure usage. This code, however, appears more focused on domestic network expansion and digital connectivity than on safeguarding the physical infrastructure that enables these services. For cable security, it continues to rely on the outdated 2001 Telecommunications Order, which raises significant concerns.

The regulation of submarine cables in Brunei falls under the Telecommunications Order of 2001,[106] which established AITI as the principal body overseeing the sector. While AITI has broad authority over telecommunications systems – including submarine cables – the legal framework remains ambiguous about its jurisdiction over cables in Brunei's EEZ and CS.[107] Although the 1954 Continental Shelf Proclamation suggests these areas fall under Brunei's jurisdiction, the lack of explicit legal provisions raises questions about enforcement and regulatory oversight, particularly in contested maritime zones.

Brunei's licensing framework, notably the Infrastructure Provider for the Telecommunications Industry (INTI) License,[108] empowers operators to manage and control the necessary infrastructure, yet it does not impose restrictions on foreign ownership.[109] This openness to foreign investment has facilitated the development of cross-border digital trade by minimising regulatory compliance costs. However, it also introduces potential security risks as control over strategic assets may be influenced by external interests, particularly in a region marked by geopolitical tensions.

While Brunei has made commendable strides towards becoming a digitally connected nation,[110] the ambiguity over jurisdictional authority, especially in maritime zones, presents strategic vulnerabilities. As Brunei moves forward with projects like the Asia Link Cable, strengthening regulatory clarity and enhancing enforcement mechanisms will be essential to ensuring the resilience and security of its digital infrastructure amidst an increasingly complex geopolitical landscape.

PHILIPPINES

The Philippines, strategically positioned in Southeast Asia, plays a crucial role in the region's digital connectivity through its extensive network of submarine cables. It is increasingly referred to as the emerging 'Mid-Asia hub.' This shift is attributed to Hong Kong's marginalisation following its annexation by China, with Japan serving as the northern hub and Singapore as the southern one in the regional network. Currently, the country hosts 19 active cables, with an additional 7 slated to be operational between 2024 and 2028.[111] Despite this vital role, the regulatory framework governing submarine cables in the Philippines remains fragmented, revealing significant vulnerabilities that could undermine national security and economic interests, particularly in the contested waters of the SCS.

The principal legislation governing telecommunications in the Philippines is the 1995 Public Telecommunications Policy Act (R.A. No. 7925).[112] This law establishes the National Telecommunications Commission (NTC) as the primary regulatory authority responsible for the regulation of telecommunications services, including submarine cables. The NTC is tasked with ensuring quality, reliability, and security across telecommunications infrastructure and promoting fair market conduct. However, while R.A. No. 7925 provides the general framework, it does not address the specific and unique vulnerabilities associated with submarine cables, leaving a critical gap in the legal protections needed for these essential digital arteries.

Telecommunications companies operating submarine cables must obtain franchises from Congress, which grants them the authority to lay and maintain these cables within Philippine waters. However, these franchises are primarily focused on operational aspects and lack explicit provisions related to security and strategic protection, particularly against threats posed by foreign entities. Moreover, while environmental permits are essential for protecting biodiversity in a climate-vulnerable country like the Philippines, the reliance on multiple permits and clearances including from environmental agencies adds layers of bureaucracy that hinder quick response times.

In 2021, the Congress of the Philippines amended Act No. 146 of the Public Service Act and enacted R.A.11659.[113] Section 2(m) of the amendment classifies telecommunications infrastructure, including submarine cables, but does not explicitly designate it as critical infrastructure. This law imposes restrictions on foreign ownership, capping it at 50% unless reciprocal rights are provided to Philippine nationals in the foreign entity's home country. While this regulation aims to safeguard national interests, it fails to account for the specific strategic risks associated with submarine cables, particularly in international waters.

Additionally, the Philippines signed the Anti-Cable Television and Cable Internet Tapping Act in 2013 (R.A. No. 10515).[114] The act penalises unauthorised damage, theft, or interception of telecommunications infrastructure, including submarine cables. Recent enforcement of this law by major telecom companies, such as Globe Telecom and PLDT, has led to legal action against hundreds of individuals involved in cable theft.[115] However, the law's jurisdiction is limited to Philippine territorial waters, leaving activities on the high seas unregulated. This limitation exposes a significant gap, as the country has yet to enact legislation that would penalise intentional cable cutting by Philippine-registered vessels on the high seas – a requirement under the UNCLOS.

The Maritime Industry Authority (MARINA), established under Presidential Decree No. 474[116] in 1974, oversees maritime operations, including the regulation of cable-laying activities within Philippine waters. MARINA issues special permits to domestic entities using foreign-registered vessels for these operations. However, such projects also require clearance from the National Security Council (NSC), enforcing an additional bureaucratic layer and undermining the agility needed to address cable disruptions swiftly.[117] In an environment like the SCS, where geopolitical tensions can exacerbate strategic vulnerabilities, such delays could have far-reaching consequences.

Recognising the challenges posed by the current regulatory environment, President Ferdinand Marcos Jr. issued Executive Order No. 32 in 2023[118] to streamline the permitting process for telecommunications infrastructure, including submarine cables. This directive limits the requirements needed for construction, installation, and maintenance, making it easier for companies to undertake necessary projects. However, while this order simplifies certain processes, the overall regulatory structure remains fragmented, with responsibilities dispersed across various agencies, each with its own set of mandates.

The patchwork of regulations governing submarine cables in the Philippines is symptomatic of a broader issue: the absence of a centralised, cohesive regulatory framework. This fragmented approach, involving entities like the NTC, MARINA, and the NSC, has the potential to hinder efficient coordination and create delays that could be strategically damaging, particularly in a region as sensitive as the SCS.

Centralising oversight under a dedicated authority is essential to streamline coordination, enhance efficiency, and ensure rapid responses to disruptions. Such an authority should oversee permits, maintenance, and enforcement against threats, while legislative reforms must designate submarine cables as critical infrastructure. Extending regulatory reach beyond national waters under UNCLOS would further bolster protection against illegal activities on the high seas.

VIETNAM

Vietnam has become a key battleground in the strategic contest between the US and China over control of undersea cable networks.[119] Currently, the country operates five active undersea cable networks,[120] which are, on average, 14 years old. With infrastructure aging, Vietnam faces significant connectivity challenges, and this was starkly highlighted in early 2023 when all five cables experienced simultaneous service disruptions.[121] While some attributed these failures to the aging network, US officials, while dissuading Vietnam from engaging in cable deals with Chinese companies, alleged sabotage by China, pointing to rising geopolitical tensions in the region.[122]

Amidst this backdrop, Vietnam is actively seeking to bolster its digital infrastructure. In April 2023, the state-owned telecommunications firm Viettel partnered with Singapore's Singtel to announce plans for a new undersea cable connecting southern Vietnam to Singapore.[123] The planned route would strategically bypass contentious areas of the SCS claimed by Beijing,[124] underscoring Vietnam's intent to diversify and secure its connectivity. Although the tender for this project has yet to be launched, it represents a move to strengthen ties with key digital hubs such as Singapore, Hong Kong, and Japan while maintaining flexibility to adapt and expand Vietnam's network.

Looking towards the future, Vietnam has laid out an ambitious strategy to expand its undersea cable network by 2030.[125] Since early 2024, Prime Ministerial Decision 1132/QD-TTg, Decision No. 805/QD-TTg, and Decision No. 36/QD-TTg have been issued and approved by the Ministry of Information and Communications (MIC). The directives lay out an *Informational Communication Infrastructure Master Plan* for 2021 to 2030, seeking to deploy at least ten new undersea cables,[126] bringing the total to 15. One of the new systems will be state-owned.[127] This initiative is part of a broader effort to solidify the country's position as a regional digital hub and to ensure robust international connectivity. In addition, the government plans to establish two new international land fibre optic routes by 2030, designed to handle at least 15% of the total capacity currently managed by marine systems. By 2027, Vietnam aims to have four new undersea cables in operation, boosting its data transmission capacity to at least 134 terabytes per second (Tbps).[128]

Vietnam's legal framework for the protection of submarine cables presents a robust approach, combining multiple regulatory instruments. Vietnam's regulation on submarine cables is primarily governed by two core legal instruments: the Law of the Sea 2012[129] and the Telecommunications Laws (2009, updated in 2023).[130] Together, these laws outline the rights and obligations associated with the installation, operation, and maintenance of submarine cables within Vietnam's maritime zones.

Vietnam's Law of the Sea (2012), which adheres to international standards, respects the principle of freedom to lay submarine cables on the continental shelf as enshrined in UNCLOS. At the same time, it mandates that any party wishing to lay cables within Vietnam's EEZ or continental shelf must obtain written consent from competent authorities. This regulatory measure ensures that activities align with national interests, allowing Vietnam to exercise its sovereign rights while upholding international commitments.

The updated Telecommunications Law (2023) forms the core of Vietnam's legal framework by establishing stringent conditions for granting licenses to entities seeking to install submarine cables. These conditions emphasise compliance with national defence requirements, environmental protection standards, and Vietnamese legal frameworks. The law ensures that entities adhere to strict guidelines from the outset, thereby maintaining the integrity of submarine cable installations. Supplementing this, decrees like No. 174/2013/ND-CP[131] set out clear penalties for violations, reinforcing the state's commitment to protecting these vital infrastructures. The classification of multinational telecommunications lines as high-priority constructions further underscores the strategic significance Vietnam assigns to its connectivity infrastructure.

Vietnam's multi-agency approach integrates several key players. Article 25 of Decree 25/2011/ND-CP[132] stipulates that after a license is approved, the specialised telecommunications management agency coordinates with the General Staff of the Ministry of Defence. This collaboration is crucial, as it facilitates the entry of vessels into Vietnamese waters for surveying, installing, maintaining, and repairing submarine cables under the provisions of law. This regulatory oversight ensures that all activities are conducted within the bounds of national security protocols.

Prime Minister's Directive No. 30/2007/CT-TTg[133] enhances these efforts by mandating that the Border Guard, Navy, and Vietnam Coast Guard – under the Ministry of National Defence (MND) – ensure the security of telecommunication submarine cables. This directive ensures that defence forces play an active role in safeguarding these infrastructures, reflecting a strong integration of national security into telecommunications management. Additionally, the police coordinate with telecommunication companies to protect the security of landing stations and handle legal actions against acts of sabotage.[134] Local governance also plays a role; the People's Committees of Coastal Areas[135] are tasked with raising public awareness about the importance of these cables and educating communities on their significance and security.

Further supporting this framework, Official Document No. 3591/VPCP-CN[136] establishes a collaborative mechanism to prevent damage to undersea cables. In cases of illegal undersea cable exploitation, various ministries, including the Ministry of Natural Resources and Environment (MONRE), Ministry of Information and Communications (MIC), Ministry of National Defence (MND), Ministry of Public Security, and Ministry of Culture and Information work in conjunction with the People's Committees of coastal provinces. The MIC, for instance, is responsible for issuing licenses and regulating the telecommunications sector, while the MND provides physical security through surveillance and enforcement capabilities. Meanwhile, MONRE ensures compliance with environmental standards, particularly during the installation and maintenance of cable systems.

Vietnam's approach is commendable for its alignment with UNCLOS principles and its recognition of telecommunications infrastructure as a strategic asset. The clear licensing procedures detailed in the Telecommunications Law ensure that only compliant entities are granted permissions, with requirements that include rigorous adherence to national security and environmental protocols. Enforcement mechanisms are also in place, with Vietnam's Criminal Code and related decrees – such as Decree No. 162/2013/ND-CP60[137] and No. 174/2013/ND-CP61[138] – establishing clear penalties for illegal activities such as unauthorised cable installations. The active engagement of the defence sector, directed by Prime Ministerial mandates, reflects a strong commitment to safeguarding these infrastructures from potential threats.

Vietnam's regulatory framework for the protection of submarine telecommunications cables exemplifies a comprehensive, 'whole-of-government' approach[139] characterised by the integration of legal provisions and multi-agency collaboration. This coordinated strategy enhances oversight and reinforces the defence of critical infrastructure, aligning with national security and economic objectives.

Nevertheless, this extensive inter-agency model is not without its inherent challenges. The involvement of multiple governmental bodies can lead to jurisdictional overlaps and ambiguities, particularly during crises, where a lack of clear authority may result in delayed response times. Addressing this issue through the establishment of a dedicated task force for submarine cable security could mitigate coordination challenges, ensuring a unified, efficient response across relevant stakeholders.

MALAYSIA

Malaysia's ambition to position itself as a key hub for submarine cable landings in Southeast Asia is clearly articulated in its Digital Economy Blueprint,[140] which aims to capitalise on the nation's strategic location and enhance its digital connectivity by 2025. Currently, 23 international cable systems[141] connect Malaysia to global communication networks – a critical infrastructure supporting the nation's economic growth, as reflected in the 23 per cent contribution of the digital economy to Malaysia's GDP in 2023.

The regulation of telecommunication submarine cables in Malaysia is governed by the Communications and Multimedia Act 1998[142] and its related instruments. This act requires entities to obtain a license from the Minister of Communications and Multimedia to own or provide network facilities, broadly defined to include physical infrastructure such as cables and landing centres. The Communication and Multimedia (Licensing) Regulations 2000[143] allow licenses for fixed links, cables, and submarine cable infrastructure, stipulating that licensees must be companies incorporated in Malaysia. License approvals are also contingent on securing permissions from relevant authorities for the placement, installation, and maintenance of network facilities across different terrains.[144]

Further, other key regulations include the Exclusive Economic Zone Act 1984 (Act 311),[145] which provides the legal basis for cable operations within Malaysia's EEZ and continental shelf. Section 22 of this act mandates that any installation of submarine cables in these areas requires government consent, giving authorities significant control over such activities. However, while this law allows for regulatory oversight, it can also lead to administrative bottlenecks that hinder swift responses to urgent maintenance and repair needs. Additionally, Section 23 imposes further responsibilities on cable operators by requiring the removal of disused or irreparable cables. These provisions primarily address activities within the EEZ, leaving regulatory gaps within Malaysia's territorial waters.

The Territorial Sea Act 2012[146] complements this framework by extending Malaysian sovereignty to its territorial seas, where authorisation is also required for any cable installation. Meanwhile, the Merchant Shipping Ordinance (MSO) 1952 (Section 491B),[147] introduced in Malaysia in 1980, mandates that operators notify the Director of the Marine Department before undertaking cable-laying activities. Despite these clear intentions to regulate submarine cable operations, the involvement of multiple agencies, including the Ministry of Transport, Malaysia Marine Department, and the Department of Fisheries creates a convoluted process with unclear hierarchy, often resulting in delays. These inefficiencies hinder Malaysia's strategic positioning as a digital infrastructure hub.

One of the most significant challenges to Malaysia's submarine cable infrastructure stems from its cabotage policy under the MSO 1952 (Part IIB). MSO's section 65L requires non-Malaysian vessels to secure a Domestic Shipping License Exemption (DSLE) before conducting repairs on submarine cables. This process, which averaged 27 days prior to January 2019, was considerably slower than the global standard of one week, leading to operational risks, increased costs, and extended network downtimes. Over a year, these delays could accumulate to nearly 100 days, deterring international investors from considering Malaysia as a viable connectivity hub.[148]

Efforts to streamline the DSLE process have been made, but disputes[149] between the Malaysian Shipowners Association (MASA) and cable operators over vessel suitability often lead to further delays.[150] Though Malaysia lifted cabotage restrictions in May 2024,[151] allowing foreign vessels to conduct repairs without needing a DSLE, the policy remains inconsistently applied. For example, Sarawak chose to reinstate the cabotage policy within its jurisdiction, citing the protection of local shipping industries.[152] Such inconsistencies undermine Malaysia's ambitions to be a regional digital hub by affecting the reliability of its submarine cable infrastructure.

The fragmented nature of Malaysia's regulatory oversight extends to security coordination. The National Security Council (MKN) is the lead agency overseeing the protection and security of submarine cables, coordinating with other bodies such as the Ministry of Transport and Malaysia Marine Department.[153] However, the lack of a cohesive inter-agency framework leads to inefficiencies, slow response times, and vulnerabilities, especially when incidents require urgent repairs. Service providers like Telekom Malaysia collaborate with the Malaysian Maritime Enforcement Agency for physical security, but comprehensive oversight remains fragmented and unclear. This regulatory disarray could threaten Malaysia's security and its ambitions as a regional connectivity hub, particularly given its strategic location in the SCS.

Malaysia's Penal Code 431A[154] criminalises intentional damage to telegraph cables, including submarine communication lines, with offenders facing up to two years of imprisonment, a fine, or both. However, this legislation is limited to general acts of 'mischief' and does not adequately address the modern complexities of protecting submarine cables from sabotage, cyber threats, or espionage. As the SCS is a geopolitically sensitive region, Malaysia must develop legislation that explicitly addresses these security challenges, emphasising the critical infrastructure's strategic importance.

Malaysia's broader digital strategy, articulated through initiatives such as the MyDigital Blueprint and the National Cyber Security Agency's (NACSA) Cybersecurity Strategy,[155] indirectly supports submarine cable security by underscoring the importance of digital infrastructure. However, these initiatives lack explicit recognition of submarine cables as part of the Critical National Information Infrastructure (CNII).[156] This oversight limits the applicability of robust legal protections, despite the cables' critical role in carrying 99 per cent of Malaysia's internet traffic.

To truly position itself as a digital leader in Southeast Asia, Malaysia must undertake a comprehensive overhaul of its submarine cable policies. This reform should include streamlining permitting processes, establishing clear and cohesive inter-agency coordination, and updating legal protections to explicitly address modern threats. Recognising submarine cables as critical national infrastructure would further enhance Malaysia's strategic resilience, ensuring the secure and efficient operation of its digital networks.

KEY ISSUES IN THE LEGAL AND CABLE PROTECTION FRAMEWORKS OF SCS CLAIMANTS

The strategic importance of undersea cables in the SCS region cannot be overstated, yet the legal and security frameworks of the region's claimants reveal significant vulnerabilities. As China consolidates its control over key maritime routes and exercises leverage over licensing and repair permits, the inadequacies in the regulatory frameworks of other SCS claimants pose a serious threat to regional digital security. These gaps hinder the ability of SCS claimants to develop a cohesive strategy against potential disruptions, coercive tactics, or strategic isolation.

FRAGMENTED REGULATORY STRUCTURES

Across the region, legal frameworks governing undersea cables are dispersed across multiple legislative instruments, agencies, and regulations, leading to bureaucratic inefficiencies. Vietnam, for example, relies on a patchwork of decrees, directives, and laws from various ministries, including the Ministry of Information and Communications (MIC) and the Ministry of National Defense (MND). Similarly, the Philippines lacks a dedicated regulatory body, with oversight split between entities such as the National Telecommunications Commission (NTC), the Maritime Industry Authority (MARINA), and the National Security Council (NSC). This fragmented approach complicates decision-making, leading to delays in issuing permits, coordinating repairs, and managing security threats.

REPAIR HURDLES

A major challenge to maintaining resilient undersea cable networks in the SCS is the stringent regulatory requirement for prior authorisation to conduct repairs. ASEAN coastal states, including Vietnam, the Philippines, and Malaysia, extend these permit requirements beyond their territorial waters into their EEZs and continental shelves (CSs), while Brunei's stance remains unclear, adding to the regulatory complexity. These rules conflict with the freedom of repair principle under the UNCLOS, which prohibits coastal states from impeding cable maintenance beyond their territorial seas. Requiring permits in the EEZ and CS introduces bureaucratic delays that can prolong critical repair operations by weeks, undermining regional digital connectivity and increasing the risk of strategic disruptions. The situation is further exacerbated by the need for multiple approvals from different agencies.

INSUFFICIENT LEGAL PROTECTIONS AGAINST FOREIGN INTERFERENCE

SCS claimants, such as the Philippines, have yet to implement robust legal frameworks to address extraterritorial threats. The Philippines has not fulfilled its obligations under UNCLOS to penalise intentional interference by Philippine-registered vessels on the high seas, leaving critical gaps in legal protections.

OVERLAPPING JURISDICTION AND COORDINATION CHALLENGES

Coordination across various agencies remains a critical weakness. Vietnam's 'whole-of-government' approach may result in overlapping responsibilities that delay actions during emergencies. In the Philippines, MARINA requires special permits for foreign vessels involved in cable laying, but projects also need clearance from the NSC, leading to a multilayered approval process that can hinder swift responses. This lack of streamlined coordination can prevent these states from acting quickly in case of deliberate disruptions, such as sabotage or geopolitical coercion.

LIMITATIONS ON FOREIGN INVESTMENT AND OWNERSHIP

The regulatory environment of many SCS claimants places restrictions on foreign investment in the telecommunications sector, aiming to safeguard national security. The Philippines imposes conditional ownership rights based on reciprocal agreements. While these measures protect national interests, they also restrict the influx of foreign capital and technological expertise necessary for diversifying cable networks. Vietnam's recent regulatory updates allow for 100 per cent foreign ownership in non-traditional telecommunications services like data centres; yet, submarine cables remain outside this purview, reflecting a need for clearer, more inclusive policies.

DEPENDENCY ON EXISTING ROUTES AND GEOPOLITICAL VULNERABILITIES

Many claimants, including Vietnam and Taiwan, rely heavily on existing undersea routes that pass through contested areas of the SCS. This dependency makes them vulnerable to potential disruptions, whether from accidents, natural disasters, or deliberate actions. Vietnam's new partnership with Singapore to develop a cable bypassing disputed regions and new planned systems indicates a strategic attempt to mitigate this risk, yet the overall reliance on China-connected cables still persists. In scenarios where China controls the issuance of permits for repairs in SCS, these nations face the risk of strategic digital isolation.

INADEQUATE ENFORCEMENT AND MONITORING

Despite efforts to enhance cable security, enforcement remains weak. The Philippines' Anti-Cable Television and Cable Internet Tapping Act penalises damage within its territory but does not extend to the high seas, where cables are equally vulnerable.

LACK OF REGIONAL COLLABORATION ON CABLE SECURITY

Regional frameworks, such as the ASEAN Maritime Outlook, emphasise Maritime Domain Awareness, but they do not explicitly address undersea cable security; consequently, the legislations reflect a lack of focus on promoting Underwater Domain Awareness. While MDA initiatives with partners like the EU and the US are promising, the omission of specific undersea infrastructure concerns leaves a critical gap. Without a cohesive regional policy, individual states are left to manage their own cable security, making it easier for external actors to exploit these vulnerabilities.

RECOMMENDATIONS FOR ENHANCING SUBMARINE CABLE SECURITY IN SOUTHEAST ASIA

Below are recommendations to enhance submarine cable security that can be applied in the context of Southeast Asia and the wider Indo-Pacific region.

STRENGTHENING REGIONAL COOPERATION MECHANISMS THROUGH AN ASEAN SUBMARINE CABLE PROTECTION TASK FORCE

The most immediate step towards bolstering regional cable security is to streamline the often cumbersome regulatory processes governing undersea cables. Bureaucratic delays in issuing permits for cable surveys and repairs have proven to be a significant bottleneck, leading to prolonged disruptions and strategic vulnerabilities. A dedicated ASEAN Submarine Cable Protection Task Force could address these issues by serving as a central coordination platform, ensuring more efficient handling of permit applications and regulatory compliance.

This task force could act as a centralised platform for member states to coordinate efforts, share best practices, and respond swiftly to incidents of cable damage. It would involve representatives from relevant national agencies, including the ICPC, International Telecommunications Union (ITU), telecommunications regulators, maritime authorities, military and naval forces, cable operators and maintenance providers. While similar initiatives have been successfully implemented in regions such as the United Kingdom, the US, and the European Union, the full enactment of such a task force within ASEAN will require overcoming political and logistical challenges. By leveraging the existing ASEAN framework, this platform could streamline coordination, reduce regulatory fragmentation, and foster a regional approach to securing vital digital infrastructure.

The task force should prioritise:

- **Harmonising Permitting Processes:** Develop unified protocols for issuing permits across member states, reducing the need for multiple approvals from different agencies.
- **Legal Clarity and Operational Jurisdiction:** Address existing ambiguities by establishing clear legal frameworks that define responsibilities and streamline the process of securing approvals, especially in contested maritime zones. This would include the authority to operate and conduct repairs beyond national territorial waters, with mechanisms in place to address cross-border cooperation and jurisdictional challenges.

- The task force could support a framework that enables legal and diplomatic mechanisms to address incidents of deliberate cable damage. Establishing regional agreements that clearly outline jurisdictional responsibilities and procedures for cross-border cooperation would help strengthen deterrence and regional security. Additionally, encouraging the development of a code of conduct for actions in shared and contested waters would help manage tensions and provide a framework for handling incidents involving foreign actors, focusing on non-military solutions to conflict. By combining a diplomatic, legal, and technical approach, the task force can promote a practical, cooperative strategy for regional security.
- **Including Taiwan in the ASEAN Task Force Through Structured Partnerships**
  Given Taiwan's strategic position and its substantial involvement in SCS regional submarine cable networks, it is vital to facilitate its engagement within the ASEAN Submarine Cable Protection Task Force. While formal membership may be diplomatically challenging, Taiwan can be integrated through structured partnerships that reflect its importance to regional digital infrastructure without politicising the collaboration. This approach emphasises mutual security and connectivity, allowing Taiwan to contribute its technical expertise and advanced capabilities in a manner that aligns with broader regional objectives.

Taiwan's engagement can be structured through a few practical mechanisms:

- **Establish Observer Status:** Granting Taiwan observer status within the task force would enable it to participate in discussions, share information, and contribute resources without necessitating full membership. This arrangement could be modelled on existing partnerships ASEAN has with other dialogue partners, including the Quad nations, thus providing a precedent for engagement without formal integration.
- **Business Conduct Agreements with ASEAN States:** Encouraging business conduct agreements between Taiwan and individual ASEAN members can facilitate its participation in task force activities. These agreements would allow Taiwan to assist in joint monitoring, provide data from its own cable networks, and enhance rapid response capabilities through shared protocols.
- **Structured Technical Partnerships:** Taiwan's technological prowess, particularly in sectors like data analytics and cyber resilience, can be leveraged through structured technical partnerships. By contributing advanced monitoring technologies, Taiwan could enhance the task force's overall capabilities. Joint training exercises and technology transfers would foster deeper integration without challenging the regional diplomatic balance.
- **Building on Existing Dialogue Channels:** ASEAN can work with dialogue partners, such as Japan, the US, and Australia, who already maintain robust relations with Taiwan. By aligning Taiwan's inclusion with ongoing Quad initiatives, ASEAN can frame this cooperation as a technical necessity rather than a political stance, facilitating smoother integration.

DUAL TRACK ENGAGEMENT

To ensure stability and maintain a balanced approach while integrating Taiwan into regional frameworks, it is essential to simultaneously and constructively engage China. This engagement should be aimed at reducing tensions, fostering mutual understanding, and highlighting shared interests in protecting critical infrastructure. Below are strategic ways to engage China:

- **Establish collaborative dialogue on cable security:** Initiate bilateral discussions between ASEAN and China on submarine cable security as part of the broader ASEAN-China partnership. These discussions could focus on technical, non-political aspects of cable protection, such as repair protocols and environmental preservation.
- **Technical cooperation framework:** Propose a joint initiative where ASEAN and China share information on cable routes, vulnerabilities, and threats using neutral, non-political platforms for data exchange. ASEAN can also invite China to contribute to a regional centre focused on submarine cable resilience and repair. Additionally, subsea cable security can be included in the ongoing negotiations for the Code of Conduct in the South China Sea (COC), emphasising that shared concern may reduce suspicions and create a cooperative framework for addressing threats.
- **Conflict prevention mechanism:** Work with China to establish clear, de-escalation protocols for cable repair and maintenance in the disputed maritime zone. These protocols should focus on safety and efficiency while avoiding sovereignty disputes and highlighting shared economic interests of maintaining trade and financial networks.

LEVERAGING EXISTING MARITIME DOMAIN AWARENESS FRAMEWORKS

Expanding MDA frameworks to explicitly include submarine cable security is a vital step. Existing partnerships, particularly with the European Union, the United Kingdom, the US, and the Quad,[157] can serve as platforms for incorporating cable monitoring into MDA initiatives. Utilising technologies like the Automatic Identification System (AIS) alongside satellite-based monitoring can help track vessels near cable routes, identifying potential threats such as illegal fishing, anchoring, or unauthorised activities. Enhancing MDA's scope to include submarine cable positioning[158] will improve regional actors' ability to detect and respond to threats to these critical infrastructures, promoting greater stability and cooperation.

PRIORITISE UNDERWATER DOMAIN AWARENESS

While MDA provides essential surface-level monitoring, it does not account for the complexities of the underwater environment. A dedicated focus on UDA[159] is crucial for a holistic security posture. UDA incorporates specialised underwater surveillance technologies, such as Autonomous Underwater Vehicles (AUVs) equipped with sonar and imaging capabilities, to monitor cable conditions, detect anomalies, and respond to subsurface threats like sabotage or accidental damage from dredging and anchoring. Integrating UDA with MDA will enable states to develop a comprehensive threat assessment.

STRENGTHENING PUBLIC-PRIVATE PARTNERSHIPS

The integration of MDA and UDA requires robust collaboration across regional states, defence agencies, and industry. Telecommunications companies can provide critical data on cable vulnerabilities, while the private sector can contribute innovative research technologies, such as AI-powered analytics and low-cost commercial satellites. Furthermore, public-private partnerships offer a potential solution to the financial challenges faced by some nations in acquiring or building new repair vessels, as current commercial constraints are limiting the construction of new ships. Encouraging partnerships, especially in the vessel asset acquisition domain, can improve regional preparedness.

EXTENDING THE QUAD FRAMEWORK FOR CABLE SECURITY

The Quad's regional initiatives in critical infrastructure present a strategic opportunity to enhance subsea cable protection. The Quad, with Australia positioned near the SCS, can leverage its partnership to develop secure and reliable cable networks. For instance, the upcoming Asia Connect Cable, set to be operational in 2026, will link the Philippines, Indonesia, Singapore, and Australia, providing an alternative route for data connectivity. Moreover, ASEAN can strengthen its collaboration with the Quad, as all its members – Japan, Australia, the US, and India – are dialogue partners of ASEAN. These nations can be approached to offer technical expertise, financial support, and training in advanced technologies for the monitoring and maintenance of undersea cables.

ADVOCATING FOR TECHNOLOGY FOCUSED SOLUTIONS AND POLICY INTEGRATION

Non-China claimant states must integrate technology-facilitated submarine cable security into national and regional policies. This includes lobbying for the inclusion of both MDA and UDA in regional maritime security strategies, reflecting the interconnectedness of these frameworks.

CONCLUSION

Submarine cables are vital to global communications and play a key role in 'making things international.'[160] However, in Southeast Asia, the geopolitical complexities of the SCS conflict pose significant risks to this infrastructure. The SCS is one of the world's most contested regions, with overlapping claims from China, Vietnam, the Philippines, and Malaysia, which heighten the risk that submarine cables could be targeted or become collateral damage in these disputes.

While UNCLOS provides a general legal framework for protecting submarine cables, its enforcement is inconsistent, especially in regions where territorial disputes create legal ambiguities. The fragmented nature of national and regional regulations exacerbates these challenges, and the region has yet to develop a comprehensive strategy to address them. At the time of writing, there is no dedicated, legally binding, multilateral mechanism for protecting submarine cables in Southeast Asia. Although international actors like the US, Japan, and the European Union offer support, their efforts remain fragmented. ASEAN's current focus on broader maritime security issues has not yet extended to comprehensive cable protection, leaving networks exposed to threats from both state and non-state actors.

The article recommends that ASEAN establish a dedicated Submarine Cable Protection Task Force to coordinate regional efforts, share information, and collaborate closely with ICPC and ITU. Additionally, improving maritime and underwater domain awareness should be prioritised. This can be achieved through updating national legal frameworks to protect submarine cables while ensuring alignment with UNCLOS provisions, as well as by engaging local communities. External stakeholders such as Japan, India, the US, and Australia, through the Quad, can support Southeast Asian nations by providing technical expertise, financial assistance for buying new repair vessels, and training in advanced technologies for monitoring and repairing cables.

Ultimately, the protection of submarine cables must be integrated into Southeast Asia's broader maritime security strategies. Addressing physical vulnerabilities, resolving jurisdictional disputes, and fostering regional and international cooperation are essential to ensuring the long-term security and stability of the region's critical communication infrastructure. By adopting a comprehensive approach, Southeast Asian nations can safeguard their economies, maintain secure communications, and contribute to regional stability.

ENDNOTES

1 The Insight Partners, "Submarine Cable System Market Worth $30.50 Billion," Globe News Wire, August 28, 2024, https://www.globenewswire.com/news-release/2024/08/28/2937018/0/en/Submarine-Cable-System-Market-Worth-30-50-Billion-Globally-by-2030-Exclusive-Report-by-The-Insight-Partners.html#.

2 Nadine Hawkins, "The Underwater Digital Super Highway," *Capacity Media*, March 11, 2024, https://www.capacitymedia.com/article/2cxmm34wcyeqqxqoo54w0/big-interview/the-underwater-digtal-super-highway.

3 Nicole Starosielski, "The Politics of Cable Supply from the British Empire to Huawei Marine," in *Assembly Codes*, ed. Matthew Hockenberry, Nicole Starosielski, and Susan Zieger, 1st ed. (Duke University Press, 2021), 190–206, https://doi.org/10.2307/j.ctv1tfw0qk.15.

4 Wang Zheng, "China's Digital Silk Road (DSR) in Southeast Asia: Progress and Challenges," *ISEAS Yusof Ishaq Institute*, no. 1 (2024): 1–16, https://www.iseas.edu.sg/wp-content/uploads/2024/01/ISEAS_Perspective_2024_1.pdf.

5 Simona A. Grano and David Wei Feng Huang, China – US Competition: Impact on Small and Middle Powers' Strategic Choices, *China – US Competition: Impact on Small and Middle Powers' Strategic Choices*, 2023, https://doi.org/10.1007/978-3-031-15389-1.

6 Adam Bruns, "How Undersea Cables Drive Onshore Site Decisions The Submarine Fiber Industry Added an Average of 32 % Capacity Annually," Site Selection, March 2020, https://siteselection.com/issues/2020/mar/data-centers-how-undersea-cables-drive-onshore-site-decisions.cfm.

7 "ASEAN Identifies Key Opportunities and Challenges in the Digital Transformation of Media – ASEAN Main Portal," ASEAN, March 19, 2024, https://asean.org/asean-identifies-key-opportunities-and-challenges-in-the-digital-transformation-of-media/.

8 Aziz Zaman, "How Digitalization Is Making South and Southeast Asia Engines of Growth | World Economic Forum," World Economic Forum, February 10, 2022, https://www.weforum.org/agenda/2022/02/digitalization-south-southeast-asia/.

9 Alan Mauldin, "Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic?," Telegeography, May 4, 2023, https://blog.telegeography.com/2023-mythbusting-part-3.

10 Timothy Mclaughlin, "Between a Rock and a Hard Place in the South China Sea," *The Atlantic Monthly*, June 2024, https://www.theatlantic.com/international/archive/2024/06/thitu-island-south-china-sea-tension/678692/

11 Timothy Mclaughlin, "The Most Dangerous Conflict No One Is Talking About," *The Atlantic Monthly*, December 2023, https://www.theatlantic.com/international/archive/2023/12/south-china-sea-philippines-dispute-explained/676218/.

12 Gregory B Poling, "The United States Is Deeply Invested in the South China Sea.," *Foreign Policy*, August 14, 2022, https://foreignpolicy.com/2022/08/14/the-united-states-is-deeply-invested-in-the-south-china-sea/.

13 Rebecca Tan, "Rising Tension in South China Sea Disrupts Asia's Subsea Cable System," *The Washington Post*, October 3, 2024, https://www.washingtonpost.com/world/2024/10/03/south-china-sea-underwater-cables/.

14 Philip Dorling, "Australian Spies in Global Deal to Tap Undersea Cables," *The Sydney Morning Herald*, August 29, 2013, http://newsstore.fairfax.com.au/apps/viewDocument.ac;jsessionid=2B8F003F4661E49DA823E4DB209ED054?sy=afr&pb=all_ffx&dt=selectRange&dr=1month&so=relevance&sf=text&sf=headline&rc=10&rm=200&sp=brs&cls=2220&clsPage=1&docID=AGE130829IP7OI68TECV.

15 Henry Farrell and Abraham Newman, "The STORMBREW Map," in *Underground Empire. How America Weaponized the World Economy*, 1st ed. (New York: Henry Holt and Company, 2023), 46–79.

16 American Civil Liberties Union, "BLARNEY Exploits the Social Network via Expanded Facebook Collection," *American Civil Liberties Union (ACLU FOIA)*, 2014, https://www.aclu.org/documents/blarney-exploits-social-network-expanded-facebook-collection.

17 Ewen Macaskill and Gabriel Dance, "NSA Files: Decoded," *The Guardian*, November 1, 2013, https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

18 Ryan Gallagher, "New Snowden Documents Show NSA Deemed Google Networks a 'Target,'" *Slate*, September 2013, https://slate.com/technology/2013/09/shifting-shadow-stormbrew-flying-pig-new-snowden-documents-show-nsa-deemed-google-networks-a-target.html.

19 Richard Heeks et al., "China's Digital Expansion in the Global South: Systematic Literature Review and Future Research Agenda," *Information Society* 40, no. 2 (2024): 69–95, https://doi.org/10.1080/01972243.2024.2315875.

20 Micah McCartney, "Is China Hacking Undersea Cables? What We Know," Newsweek, May 21, 2024, https://www.newsweek.com/china-hacking-undersea-cables-1902970.

21 Julia Brackup, Sarah Harting, and Daniel Gonzales, *Digital Infrastructure and Digital Presence* (Santa Monica: RAND Corporation, 2022), https://www.rand.org/pubs/research_reports/RRA877-1.html.

22 Geoffrey Starks, "Statement of Commissioner Geoffrey Starks," no. 16 (2020): 13–15, https://docs.fcc.gov/public/attachments/DOC-367238A6.pdf.

23 Dale Aluf, "China's Subsea-Cable Power Play in the Middle East and North Africa," 2023, https://www.atlanticcouncil.org/wp-content/uploads/2023/05/ChinasGrowingInfluence_052423-1.pdf.

24 Cheng Ting-Fang et al., "China's Subsea Cable Drive Defies US Sanctions," June 26, 2024, https://asia.nikkei.com/Spotlight/The-Big-Story/China-s-undersea-cable-drive-defies-U.S.-sanctions.

25 HMN Technologies Co. Ltd, "HMN Tech," accessed December 10, 2024, https://www.hmntech.com/enNewBuild.jhtml.

26 Jeffrey Brown, "Opposing Views on Congress' Claims Huawei Technologies," (PBS NewsHour, October 10, 2012), https://www.youtube.com/watch?v=DKYmL4JwNsY.

27 The Commission on the Theft of American Intellectual Property, "The Intellectual Property Commission Report. The Report of the Commission on the Theft of American Intellectual Property," December 5, 2013, https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf.

28 Francesco Guarascio, Phuong Nguyen, and Joe Brock, "Exclusive: Inside the US Push to Steer Vietnam 's Subsea Cable Plans Away from China," *Reuters*, September 18, 2024, https://www.reuters.com/business/media-telecom/inside-us-push-steer-vietnams-subsea-cable-plans-away-china-2024-09-17/.

29 Rogier Creemers, "China's Long and Winding Road in Global Cyberspace: Great Power Relationships or Common Destiny?," *SSRN Electronic Journal* (January 31, 2021), https://doi.org/10.2139/ssrn.3776814.

30 Anna Gross et al., "Subsea Cables: How the US Is Pushing China out of the Internet's Plumbing," *Financial Times,* June 13, 2023, https://ig.ft.com/subsea-cables/.

31 Dorling, "Australian Spies in Global Deal to Tap Undersea Cables."

32 Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (July 1, 2019): 42–79, https://doi.org/10.1162/isec_a_00351.

33 Ibid.

34 Robert J Keohane and Joseph Nye, *Power and Interdependence (Longman Classics in Political Science), Grupo Editor Latinoamericano,* 4th ed. (Pearson, 2012).

35 Renato Cruz De Castro, "Abstract of Crisis in Philippine-U.S. Security Relations: From an Alliance to a Security Partnership?," Pacific Review 35, no. 3 (2022): 477–505, https://doi.org/10.1080/09512748.2020.1845227.the Philippines doubted the U.S.'s often-repeated commitment to assist its ally because the 1951 Philippine-U.S. Mutual Defence Treaty (MDT

36 Bonnie S. Glaser, Jessica Chen Weiss, and Thomas J. Christensen, "Taiwan and the True Sources of Deterrence," *Foreign Affairs* 103, no. 1 (2024): 88–100, https://heinonline.org/HOL/PrintRequest?collection=journals&handle=hein.journals/fora103&div=11&print=section&format=PDFsearchable&submit=Print%2FDownload&id=90.

37 Tetsuo Kotani, "China's 'Nine Gates' and Security Policy in the Indo-Pacific Challenges for Japan," *International Affairs* 4, no. 1 (2020): 21–30, https://jiia.repo.nii.ac.jp/?action=repository_uri&item_id=1238&file_id=14&file_no=1.

38 Elina Noor, "Entangled: Southeast Asia and the Geopolitics of Undersea Cables," I*ndo-Pacific Outlook 1,* no. 5 (2024): 1–10, https://manoa.hawaii.edu/indopacificaffairs/wp-content/uploads/sites/106/2024/02/Noor-Entangled.pdf.

39 Camino Kavanagh, "Wading Murky Waters: Subsea Communications Cables And Responsible State Behaviour," 2023, https://unidir.org/wp-content/uploads/2023/05/UNIDIR_Wading_Murky_Waters_Subsea_Communications_Cables_Responsible_State_Behaviour.pdf.

40 Ibid.

41 Ibid.

42 Lawson W. Bigham, "The South China Sea: Complex and Changing," *Proceedings - The U.S. Naval Institute Magazine* 149, no. 1 (January 2023), https://www.usni.org/magazines/proceedings/2023/january/south-china-sea-complex-and-changing.

43 Angela Poh, "The Myth of Chinese Sanctions over South China Sea Disputes," *Washington Quarterly* 40, no. 1 (2017): 143–65, https://doi.org/10.1080/0163660X.2017.1302744.

44 Henry S. Bensurto, "Archipelagic Spratlys": *China's Desperate Attempt to Preserve Expansionist Policy? Peaceful Maritime Engagement in East Asia and the Pacific Region,* 2023, https://doi.org/10.1163/9789004518629_009.

45 See also, John Pollock and Damien Symon, "How Beijing Is Closing Surveillance Gaps in the South China Sea," Chatham House, October 17, 2024, https://www.chathamhouse.org/publications/the-world-today/2024-09/how-beijing-closing-surveillance-gaps-south-china-sea.

46 Dolma Tsering, "China's 'Undersea Great Wall' Project: Implications," National Maritime Foundation, 2016, http://www.maritimeindia.org/.

47 "Exploring China's Unmanned Ocean Network," Asia Maritime Transparency Initiative (AMTI), 2020, https://amti.csis.org/exploring-chinas-unmanned-ocean-network/.

48 Ibid.

49 Joe Brock, "U.S. and China Wage War beneath the Waves – over Internet Cables," Reuters, March 24, 2023, https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

50 "US Deploys 3 Surveillance Ships in South China Sea – Radio Free Asia," *Radio Free Asia,* March 25, 2022, https://www.rfa.org/english/news/china/usa-southchinasea-03252022145749.html.

51 TeleGeography, "Submarine Cable Map," Submarine Cable Map, 2024, https://www.submarinecablemap.com/.

52 Farrell and Newman, "Weaponized Interdependence".

53 Farrell and Newman, "The STORMBREW Map."

54 Ibid., 58.

55 Carlo J.V. Caro, "Underwater Geopolitics," *Real Clear Defence,* November 2024, https://www.realcleardefense.com/articles/2024/11/26/underwater_geopolitics_1074698.html.

56 Ibid.

57 Interview with an anonymous industry insider, data collected on 30-09-24.

58 McCartney, "Is China Hacking Undersea Cables?"

59 Alan Mauldin, "Is the Lifespan of a Submarine Cable Really 25 Years?," TeleGeography, April 20, 2023, https://blog.telegeography.com/2023-mythbusting-part-2.

60 Geoff Bennett, "Extending the Economic Life of Submarine Cables," Capacity Media, December 5, 2022, https://www.capacitymedia.com/article/2ay2px8kc1mtygh3sd7nk/industry-voices/extending-the-economic-life-of-submarine-cables.

61 Sebastian Moss, "Fortune on the High Seas," Data Centre Dynamics, 2016, https://www.datacenterdynamics.com/en/analysis/fortune-on-the-high-seas/.

62 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 (June 28, 2024), https://doi.org/10.1007/s44216-024-00029-1.

63 Ting-Fang et al., "China's Subsea Cable Drive Defies US Sanctions."

64 Kang Wan Chern, "South-East Asia Emerges as Global Data Centre Hot Spot as AI Usage Rises," *The Straits Times,* October 14, 2024, https://www.straitstimes.com/business/south-east-asia-emerges-as-global-data-centre-hot-spot-as-ai-usage-rises.

65 Adrian Ashurst, "The Race to Build Data Centres in Southeast Asia," FEBIS, May 24, 2024, https://www.febis.org/2024/05/24/the-race-to-build-data-centres-in-southeast-asia/.

66 TeleGeography, "Submar. Cable Map."

67 Rex Lien Doan, "The Conflict of Laws in the South China Sea and Its Threats to the Indo-Pacific Rules-Based Order," *Loyola University Chicago Law Journal* 55, no. 1 (2024): 8–72, https://loyola-chicago-law-journal.scholasticahq.com/article/117067-the-conflict-of-laws-in-the-south-china-sea-and-its-threats-to-the-indo-pacific-rules-based-order/attachment/225480.pdf.

68 R. S. Aswani, Shambhu Sajith, and Anil Kumar, "Can Offshore Wind Energy Bridge Geopolitical Asymmetries through Cooperative Sustainable Development in South China Sea?," *Asian Journal of Political Science* 31, no. 2 (2023): 140–60, https://doi.org/10.1080/02185377.2023.2227162.

69 "TeleGeography | Home," 2024, https://www2.telegeography.com/?_hstc=196094579.f9a84f603cd9113be00a7d1e2b7fb1ce.1706616364059.1711544351960.1711679306776.14&_hssc=196094579.3.1711679306776&_hsfp=504977917.

70 Tan, "Rising Tension in South China Sea Disrupts Asia's Subsea Cable System."

71 Georgia Bafoutsou et al., "What Is At Stake?," 2023, https://www.enisa.europa.eu%2Fsites%2Fdefault%2Ffiles%2Fpublications%2FUndersea%2520cables%2520-%2520What%2520is%2520a%2520stake%2520report.pdf&psig=AOvVaw3gE0X4MnB4n_hb6PqtFlaY&ust=1740620068125000&source=images&cd=vfe&opi=89978449&ved=0CAYQrpoMahcKEwjYxMK1meCLAxUAAAAAHQAAAAQBA.

72 Cynthia Mehboob's personal communication with Mr. Mike Constable, 5 December 2024.

73 Douglas R. Burnett and Kristin Berdan, "To Secure Undersea Cables, Take Lessons from the British Empire's All-Red Line | Proceedings – July 2024 Vol. 150/7/1,457," U.S. Naval Institute 150, no. 7 (July 2024), https://www.usni.org/magazines/proceedings/2024/july/secure-undersea-cables-take-lessons-british-empires-all-red-line.

74 Cynthia Mehboob's personal communication with Mr. Mike Constable, 5 December 2024.

75 Simon Dux, "Ciena: Global Undersea Network Is More Resilient, but Threats Remain," *Mobile Europe,* 5 October 2023, https://www.mobileeurope.co.uk/ciena-global-undersea-network-is-more-resilient-but-threats-remain/.

76 Cynthia Mehboob's personal communication with Mr. Mike Constable, 5 December 2024.

77 Ibid.

78 Brock, "U.S. and China Wage War beneath the Waves"

79 U.S Department of Defense, "Philippines, U.S. Announce Four New EDCA Sites," 2023, https://www.defense.gov/News/Releases/Release/Article/3285566/philippines-us-announce-four-new-edca-sites/.

80 Tan, "Rising Tension in South China Sea Disrupts Asia's Subsea Cable System".

81 Unpublished data provided by Mr. Mike Constable, personal communication with Cynthia Mehboob, 5 December 2024.

82 Unpublished data provided by Mr. Mike Constable, personal communication with Cynthia Mehboob, 5 December 2024.

83 Unpublished data provided by an anonymous Senior Industry Professional, personal communication with Cynthia Mehboob, 10 October 2024.

84 Unpublished data provided by Mr. Mike Constable, personal communication with Cynthia Mehboob, 5 December 2024.

85 Unpublished data provided by an anonymous Senior Industry Professional, personal communication with Cynthia Mehboob, 10 October 2024.

86 Noor, "Entangled: Southeast Asia and the Geopolitics of Undersea Cables."

87 Ting-Fang et al., "China's Subsea Cable Drive Defies US Sanctions."

88 Ibid.

89 Cynthia Mehboob's personal Communication with an anonymous industry insider, 23 August 2024.

90 Cynthia Mehboob's personal communication with Mr. Mike Constable, 5 December 2024.

91 Tan, "Rising Tension in South China Sea Disrupts Asia's Subsea Cable System."

92 Ibid.

93 Jason Petty, "How Hackers of Submarine Cables May Be Held Liable Under the Law of the Sea.," *Chicago Journal of International Law,* vol. 22, 2021, https://chicagounbound.uchicago.edu/cjil/vol22/iss1/18.

94 See Jason Halog, Paul Margat, and Michael Stadermann, "Legal Considerations on the Protection of Subsea Cables in the International and National Legislative Framework," *Transactions on Maritime Science* 13, no. 1 (2024), https://www.toms.com.hr/index.php/toms/article/view/739.

95 Kevin Frazier, "Policy Proposals for the United States to Protect the Undersea Cable System," *Journal of Law, Technology & the Internet*. 13, no. 1 (2021): 233–56, https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1133&context=jolti.

96 Hai Dang Vu, "Improving the Freedom of Repairing Telecommunication Submarine Cables in Southeast Asia: Next Steps for ASEAN," *Asia-Pacific Journal of Ocean Law and Policy,* 6, no. 1 (2021), 66–93. https://doi.org/10.1163/24519391-06010004.

97 Tara Davenport, "Submarine Cables, Cybersecurity and International Law: An Analysis," J*ournal Law & Technology* 24, no. 1 (2015): 57–109, https://scholarship.law.edu/jlt/vol24/iss1/4?utm_source=scholarship.law.edu%2Fjlt%2Fvol24%2Fiss1%2F4&utm_medium=PDF&utm_campaign=PDFCoverPages.

98 Robert Beckman et al., "Enhancing the Security of Singapore's Submarine Cables: Strengths, Challenges, and Opportunities", Nanyang Technological University Policy Report (Singapore, 2024), https://www.rsis.edu.sg/wp-content/uploads/2024/05/PR240521_Enhancing-the-Security-of-Singapores-Submaring-Cables.pdf.

99 ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), "ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables," *ASEAN TELMIN,* 2019, .https://asean.org/wp-content/uploads/2012/05/ASEAN-Guidelines-for-Strengthening-Resilience-and-Repair-of-Submarine-Ca....pdf

100 Vanne Khut, "Brunei: Challenges and Opportunities in Becoming a 'Smart Nation'," *The Scoop,* June 24, 2024, https://thescoop.co/2024/06/24/brunei-challenges-and-opportunities-in-becoming-a-smart-nation/.

101 Brunei Darussalam Digital Economy Council, "Digital Economy Master Plan 2025," 2020, https://www.mtic.gov.bn/DE2025/documents/Digital Economy Masterplan 2025.pdf.

102 James Kon, "UNN Invests BND85M in New Undersea Cable | Borneo Bulletin Online," *Borneo Bulletin,* November 9, 2022, https://borneobulletin.com.bn/unn-invests-bnd85m-in-new-undersea-cable-2/.

103 Hazel Moises, "Installation of the Asia Link Cable Subsea Network Begins in 2024," W Media, January 5, 2023, https://w.media/installation-of-the-asia-link-cable-subsea-network-begins-in-2024/.

104 Asia Link Cable, "Submarine Cable Map," Submarine Cable Maps, October 22, 2024, https://www.submarinecablemap.com/submarine-cable/asia-link-cable-alc.

105 Authority for Info-communications Technology Industry of Brunei Darussalam, "Telecommunications Order, 2001 Code of Practice for the Telecommunications Sector (Telecommunications Code)" (rev. 2023), https://aiti.gov.bn/media/5icct3re/tc-aiti-telecommunications-code.pdf

106 Constitution of Brunei Darussalam, "Telecommunications Order, 2001 (Order under Section 83(3))" (2001), https://www.mtic.gov.bn/Documents/Acts and Orders/Telecommunications Order,2001.pdf.

107 Dang Vu, "Improving the Freedom of Repairing Telecommunication Submarine Cables in Southeast Asia."

108 Authority for Info-Communications Technology Industry of Brunei Darussalam, "Licensing & Regulatory Framework-Operational Framework for AiTi," January 2005, www.aiti.gov.bn.

109 US Department of State, "Investment Climate Statements: Brunei", 2023, https://www.state.gov/reports/2023-investment-climate-statements/brunei/.

110 See: Khut, "Brunei: Challenges and Opportunities in Becoming a 'Smart Nation'."

111 TeleGeography, "Submar. Cable Map."

112 Congress of the Philippines, "Republic Act No. 7952. An Act to Promote and Govern the Development of Philippine Telecommunication and the Delivery of Public Telecommunications Services" (1995), https://lawphil.net/statutes/repacts/ra1995/ra_7925_1995.html.

113 Congress of the Philippines, "Republic Act No. 11659. An Act Amending Commonwealth Act No. 146, Otherwise Known as the Public Service Act" (2021), https://www.officialgazette.gov.ph/downloads/2022/03mar/20220321-RA-11659.pdf.

114 Congress of the Philippines, "Republic Act No. 10515. An Act Prohibiting And Penalizing Unauthorized Interception, Reception Or Use Of Any Signal Or Service Over A Cable Television System Or Cable Internet System And/Or Network, And For Other Purposes," Republic of the Philippines § (2012), https://lawphil.net/statutes/repacts/ra2013/ra_10515_2013.html.

115 ABS-CBN News, "Globe Partners with Law Enforcers to Curb Cable Cutting, Stealing," *ABS-CBN News,* July 15, 2022, https://news.abs-cbn.com/business/07/15/22/globe-partners-with-law-enforcers-to-curb-cable-cutting-stealing.

116 Congress of the Philippines, "Presidential Decree No. 474, Providing for the Reorganisation of Maritime Functions in the Philippines, Creating the Maritime Industry Authority, and for Other Purposes" (1974), https://pqf.gov.ph/Uploads/Legal Basis/PD 474 MARINA.pdf

117 Academic Reports on Submarine Cables, *Regulation and Protection of Submarine Cables in ASEAN,* ed. Robert Beckman and Joel Ong, International Cable Protection Committee, 2024, https://cil.nus.edu.sg/wp-content/uploads/2024/05/Combined-ASEAN-Academic-Reports-on-Cables_4-Jun-24-final.pdf.

118 The President of the Philippines, "Executive Order No. 32" (2023), https://lawphil.net/executive/execord/eo2023/eo_32_2023.html.

119 Guarascio, Nguyen, and Brock, "Exclusive: Inside the US Push to Steer Vietnam's Subsea Cable Plans Away from China."

120 Submarine Cable Map – Vietnam, "Submarine Cable Map," Submarine Cable Map-TeleGeography, October 22, 2024, https://www.submarinecablemap.com/country/vietnam.

121 Matthew Connatser, "Vietnam's Internet Again in Trouble as 3/5 Sub Cables Cut • The Register," *The Register,* June 18, 2024, https://www.theregister.com/2024/06/18/vietnam_internet_cables/#.

122 Guarascio, Nguyen, and Brock, "Exclusive: Inside the US Push to Steer Vietnam's Subsea Cable Plans Away from China."

123 Niva Yadav, "Viettel and Singtel Partner for Vietnam-Singapore Submarine Cable," *Data Center Dynamics,* 2024, https://www.datacenterdynamics.com/en/news/viettel-and-singtel-partner-for-vietnam-singapore-submarine-cable/#.

124 Tsubasa Suruga, "Asia's Internet Cable Projects Delayed by South China Sea Tensions," *Nikkei Asia,* May 19, 2023, https://asia.nikkei.com/Business/Business-Spotlight/Asia-s-internet-cable-projects-delayed-by-South-China-Sea-tensions.

125 The Prime Minister of Vietnam, "Decision 1132/QD-TTg 2024 Approving the Digital Infrastructure Strategy through 2025, with an Orientation towards 2030" (2024), https://english.luatvietnam.vn/thong-tin/decision-1132-qd-ttg-2024-digital-infrastructure-strategy-through-2025-367845-d1.html.

126 "Vietnam to Have 10 New Undersea Fibre Optic Cable Lines," *Vietnam Plus,* June 20, 2024, https://en.vietnamplus.vn/vietnam-to-have-10-new-undersea-fibre-optic-cable-lines-post288850.vnp.

127 Laura Dobberstein, "Vietnam Plans to Convert All of Its Networks to IPv6," *The Register,* October 14, 2024, https://www.theregister.com/2024/10/14/vietnam_digital_infrastructure_policy/.

128 Ibid.

129 Order No 16/2012/L-CTN of July 2 2012 on the promulgation of law, "Law of the Sea of Vietnam" (2012), https://faolex.fao.org/docs/pdf/vie124619.pdf.

130 The National Assembly-the Socialist Republic of Vietnam, "Law 24/2023/Vietnam on Telecommunications " (2023), https://dazpro.com/law24-2023-vietnam-on-telecommunications/.

131 Socialist Republic of Vietnam, "174/2013/ND-CP in Vietnam, Decree 174/2013/ND-CP Penalties Administrative Violations Post Information Technology Radio Frequency in Vietnam," Decree No. 174/2013/N D-CP § (2013), https://thuvienphapluat.vn/van-ban/EN/Thuong-mai/Decree-174-2013-ND-CP-penalties-administrative-violations-post-information-technology-radio-frequency/352240/tieng-anh.aspx.

132 Socialist Republic of Vietnam, "25/2011/ND-CP in Vietnam, Decree No. 25/2011/ND-CP Detailing and Guiding the Implementation in Vietnam" (2011), https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Decree-No-25-2011-ND-CP-detailing-and-guiding-the-implementation/123358/tieng-anh.aspx.

133 Academic Reports on Submarine Cables, *Regulation and Protection of Submarine Cables in ASEAN.*

134 Vu Hai Dang and Nguyn Quy Binh, "Ocean Governance Study of Vietnam," February 2023, www.un.org/oceancapacity/norway.

135 Ibid.

136 Socialist Republic of Vietnam, "No. 3591/VPCP-CN Regarding Prevention of Infringement of Submarine Telecommunication Cables at Sea" (2007), https://thuvienphapluat.vn/cong-van/Cong-nghe-thong-tin/Cong-van-3591-VPCP-CN-phong-chong-xam-hai-cap-vien-thong-ngam-tren-bien/83274/noi-dung.aspx.

137 The Socialist Republic of Vietnam, "162/2013/ND-CP in Vietnam, Decree 162/2013/ND-CP Administrative Violations Committed within Territorial Waters of Vietnam in Vietnam" (2013), https://thuvienphapluat.vn/van-ban/EN/Vi-pham-hanh-chinh/Decree-162-2013-ND-CP-administrative-violations-committed-within-territorial-waters-of-Vietnam/380596/tieng-anh.aspx.

138 Socialist Republic of Vietnam, 174/2013/ND-CP in Vietnam, Decree 174/2013/ND-CP penalties administrative violations post information technology radio frequency in Vietnam.

139 Academic Reports on Submarine Cables, *Regulation and Protection of Submarine Cables in ASEAN*.

140 Economic Planning Unit, "Malaysia Digital Economy Blueprint" (Putrajaya, February 19, 2021), https://www.ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf.

141 Submarine Cable Map, "Submarine Cable Map – Malaysia," Submarine Cable Map – TeleGeography, October 11, 2024, https://www.submarinecablemap.com/country/malaysia.

142 The Commissioner of Law Revision, "Communications and Multimedia Act 1998, Laws of Malaysia" (2006), https://www.vertic.org/media/National Legislation/Malaysia/MY_Communications_and_Multimedia_Act.pdf.

143 Communications and Multimedia Act 1998 [Act588], "Communications and Multimedia (Licensing) Regulations 2000 [P.U.(A) 129/2000]," (2001), https://mcmc.gov.my/en/legal/acts/communications-and-multimedia-act-1998-reprint-200/communications-and-multimedia-(licensing)-regulati?nid=994.

144 Dang Vu, "Improving the Freedom of Repairing Telecommunication Submarine Cables in Southeast Asia"

145 Malaysian Federal Government (MFG), "Malaysia Exclusive Economic Zone Act 1984 (Act 311) – An Act Pertaining to the Exclusive Economic Zone and Certain Aspects of the Continental Shelf of Malaysia and to Provide for the Regulations of Activities in the Zone and on the Continental Shelf and Fo" (1984), https://maritimeindex.org/legal-document/malaysia_s-exclusive-economic-zone-act-1984-adopted-from-un-treaty-series/.

146 Parliament of Malaysia, "Territorial Sea Act 2012. Laws of Malaysia." (2012), http://www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Act 15.pdf.

147 "Malaysian Statutes-Merchant Shipping Ordinance 1952," Malaysian Statutes, Compilation by Dr Arun Kasi, 2022, https://arunkasico.com/wp-content/uploads/2022/09/MSO-1952-amended-2017.pdf.

148 Malaysia Digital Economy Cooperation, "Malaysia International Connectivity" (Malaysia Digital Economy Cooperation, n.d.), https://soyacincau.com/wp-content/uploads/2021/04/Cabotage-Law-and-Impact-of-Submarine-Cables-v4.pdf.

149 Tay Chester, "Shipowners' Association Says Blaming It for Delay in Undersea Submarine Cable Repairs an 'Oversimplification,'" *The Edge Malaysia,* January 16, 2023, https://theedgemalaysia.com/node/651932.

150 Malaysia Digital Economy Cooperation, "Malaysia International Connectivity."

151 Sulok Tawie, "Sarawak Transport Minister Explains Why State Govt Requested Putrajaya to Reinstate Cabotage Policy," Malay Mail, March 2, 2024, https://www.malaymail.com/news/malaysia/2024/03/02/sarawak-transport-minister-explains-why-state-govt-requested-putrajaya-to-reinstate-cabotage-policy/121048.

152 Ibid.

153 Academic Reports on Submarine Cables, *Regulation and Protection of Submarine Cables in ASEAN*.

154 Government of Malaysia, "Penal Code Section 431A – Laws of Malaysia: Act 574. Mischief by Injury to Telegraph Cable, Wire, Etc." (2009), https://www.burgielaw.com/resources/act?act_title=Penal+Code&section=431A.

155 Malaysian Communication and Multimedia Commission, "Shaping the Digital Landscape," 2018, https://mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-2018_ENG.pdf.

156 Academic Reports on Submarine Cables, *Regulation and Protection of Submarine Cables in ASEAN*.

157 Sumit Kumar, "Challenges Lie Ahead for Quad States – Taipei Times," *Taipei Times,* October 17, 2024, https://www.taipeitimes.com/News/editorials/archives/2024/10/17/2003825417.

158 David Brewster and Simon Bateman, "Maritime Domain Awareness 3.0," 2024, ANU College of Law, Governance and Policy, https://nsc.anu.edu.au/content-centre/research/maritime-domain-awareness-30

159 Dr (Cdr) Arnab Das, "Underwater Domain Awareness (UDA) Framework " (Pune, January 2024), https://maritimeresearchcenter.com/wp-content/uploads/2024/04/Underwater-Domain-Awareness.pdf.

160 Mark B Salter, "Introduction: Circuits and Motion," in *Making Things International 1*, ed. Mark B. Salter (University of Minnesota Press, 2015), vii–xxii.

IMAGE CREDIT

Cover Credit: Korn Srirawan https://www.shutterstock.com/catalog/collections/3565527791237596460

Page 4 Credit: FunF.Sudio https://www.shutterstock.com/image-vector/southeast-asia-map-world-mash-line-2165658387

Page 6 Credit: T.Schneider https://www.shutterstock.com/image-photo/stuttgart-germany-09052021-person-holding-mobile-2091405193

Page 12 Credit: Tawin Mukdharakosa https://www.shutterstock.com/image-photo/thailand-circa-1983-stamp-print-show-152142740

Page 16 Credit Igor Grochev https://www.shutterstock.com/image-photo/penang-malaysia-may-01-2017-cable-692563894

Page 19 Credit: Igor Grochec https://www.shutterstock.com/image-photo/penang-malaysia-nov-23-2017-cable-1030957684

Page 26 Credit: Korn Srirawan https://www.shutterstock.com/image-photo/submarine-cable-inspection-vessel-696994828

Page 28 Credit: Igor Grochev https://www.shutterstock.com/image-photo/penang-malaysia-dec-21-2017-cable-1023480022


BLUE
SECURITY