The Impacts of China's SEA-H2X Submarine Cable: A Telecommunications Regulatory Study Under the NBTC Framework[1]

Thasan Kheokao [2]

Kulapalee Tantivong

Office of the National Broadcasting and Telecommunications Commission, Bangkok, Thailand

Abstract

Subsea cables carry over 99% of international data traffic and underpin the global digital economy. The Chinese-financed SEA-H2X cable supports Thailand's digital hub ambitions, yet critical vulnerabilities persist, including anchor damage and natural hazards. Although the NBTC regulates telecommunications through compliance measures, it lacks authority to protect physical subsea cable infrastructure. To address this interagency governance gap, this study investigates both the strategic economic impacts of the SEA-H2X cable and the structural vulnerabilities within Thailand's current regulatory framework. The research utilizes a qualitative document analysis guided by a dual Open Systems Interconnection (OSI) framework. Economically, the study evaluates OSI Layers 4–7 to understand how hyperscale platforms, cloud infrastructure, and cross-border trade leverage subsea capacity to drive Thailand's 5.6 trillion-baht digital economy. Regulatorily, the study translates OSI

[1] APA7th Citation: Kheokao, T. & Tantivong, K. (2026). The Impacts of China's SEA-H2X Submarine Cable: A Telecommunications Regulatory Study Under the NBTC Framework. In *Proceedings of the ICA Regional Hub Thailand 2026: Official Concurrent Event of the 76th Annual Conference of the International Communication Association (ICA)* (pp. 401–431). Faculty of Communication Arts, Chulalongkorn University.

[2] Correspondence concerning this article should be addressed to Thasan Kheokao at Office of the National Broadcasting and Telecommunications Commission, 87 Samsen Nai, Phayathai, 10400 Bangkok, Thailand or by email at: tkheokao@gmail.com

International Communication Association
Chula Chulalongkorn University
76TH ANNUAL ICA REGIONAL HUB THAILAND 2026
6–7 June 2026 • Bangkok • Chulalongkorn University
Where Thailand-Mekong-Asian Region
Bridges Divides and Amplifies Voices

Layers 1–3 into a Three-Dimensional (3D) Governance Model to assess logical, physical, and hybrid jurisdictional powers. Thailand's domestic approach is then benchmarked against advanced Indo-Pacific jurisdictions, including Australia, New Zealand, the Philippines, and Singapore. The comparative benchmarking reveals that Thailand currently operates on a reactive bureaucratic model, which contrasts sharply with international best practices. Significant identified vulnerabilities include fragmented interagency coordination, slow repair-permitting processes due to strict customs and cabotage laws, and a lack of active spatial protection zones. To mitigate these risks and support resilient digital circulation, this study proposes critical policy reforms. Thailand must transition from compliance-driven regulation to an all-hazards risk management approach. Key recommendations include integrating SEA-H2X coordinates into live ship tracking systems for proactive geofencing, classifying foreign cable repair ships as professional equipment to expedite emergency entry, and creating a unified cyber-physical command structure bridging the NBTC and maritime enforcement agencies. Furthermore, adopting enhanced ASEAN guidelines is vital for securing transnational subsea infrastructure.

Keywords: *submarine cables, SEA-H2X, telecommunications regulation, National Broadcasting and Telecommunications Commission (NBTC), digital economy, 3D Governance Model, OSI Framework, maritime security, critical infrastructure resilience*

Subsea, or submarine, cables are the physical backbone of the global digital economy, carrying over 99% of international data traffic (Jorge & Namara, 2024). These fiber-optic systems operate at OSI Layer 1 and connect land-based stations across oceans through insulated cables protected by steel

armoring, copper power tubing, and polyethylene sheathing. These cables enable cross-border internet connectivity for trade, communications, and digital services. Because application-layer revenues depend on reliable physical infrastructure, major technology hyperscalers and telecommunications firms are investing in proprietary subsea networks (Bashfield & Strating, 2026; Jorge & Namara, 2024). Chinese telecommunications, cloud, social media, and e-commerce firms have also expanded internationally, making systems such as the SEA-H2X cable important for regional connectivity and online trade in Southeast Asia. Thailand's digital hub ambitions therefore depend on reliable domestic telecommunications infrastructure that supports banking, digital consumption, hospitality services, and e-commerce.

Problem Statement

Although the SEA-H2X cable offers economic benefits, Thailand's digital dependence remains exposed to physical and logistical risks. Subsea cables can be disabled in shallow waters by anchors, bottom-trawling nets, natural hazards, or deliberate sabotage (Chow, 2026; Jacob, 2024). Damage at OSI Layer 1 can disrupt connectivity and affect services operating at OSI Layers 4–7. The NBTC regulates internet service providers through logical compliance tools, including the "30-Minute Trigger" outage fine. However, this approach does not address physical seabed risks, which fall outside the NBTC's direct jurisdiction. Securing subsea cables therefore requires coordination among telecommunications regulators, naval enforcement, marine authorities, and customs agencies. Delays in repair-ship approvals can prolong outages, making cross-agency coordination central to Thailand's digital resilience. Existing literature focuses mainly on logical network protection. This study addresses the gap by linking technical network layers with maritime security and infrastructure governance.

Research Questions

To systematically address this governance gap, this study is guided by the following two research questions:

RQ1: How does the deployment of the Chinese-financed SEA-H2X submarine cable alter the higher-layer (OSI Layers 4–7) digital economy circulation architecture and network centrality dynamics within Thailand?

RQ2: What specific structural and jurisdictional vulnerabilities emerge when benchmarking the National Broadcasting and Telecommunications Commission (NBTC) logical regulatory framework against the physical maritime protection standards of advanced Indo-Pacific jurisdictions?

Objectives of the Study

1. To examine the strategic and economic impacts of the SEA-H2X submarine cable by analyzing how this infrastructure supports digital economy circulation, hyperscale platform integration, and cross-border trade between Thailand, China, and Southeast Asia.

2. To evaluate the NBTC regulatory framework governing domestic telecommunications, identifying structural gaps in how the state transitions from logical network regulation to the physical maritime protection of subsea cables against human and environmental hazards.

Scope of the Study

This study defines its scope through geographical and analytical boundaries:

1. Geographical Scope: The study compares Thailand with the Philippines, Singapore, Australia, and New Zealand to identify governance gaps and best practices.

2. Analytical and Theoretical Scope**:** The study uses the OSI framework and the Three-Dimensional (3D) Governance Model to evaluate economic and regulatory issues.

- Economic Evaluation Scope (Digital Economy): To evaluate the strategic and economic impacts of the SEA-H2X cable (Objective 1), the study focuses on OSI Layers 4 through 7 (Transport, Session, Presentation, and Application layers). This limits the economic analysis to how hyperscalers, cloud infrastructure, and cross-border e-commerce use subsea capacity to support digital trade.
- Regulatory Evaluation Scope (State Governance): To evaluate the NBTC framework and maritime security (Objective 2), the study focuses on the foundational transport architecture of OSI Layers 1 through 3 (Physical, Data Link, and Network layers). Because governing these physical layers requires cross-jurisdictional coordination, the study translates OSI Layers 1–3 into the Three-Dimensional (3D) Governance Model. This framework categorizes state agencies into Logical (data routing), Physical (seabed and maritime enforcement), and Hybrid (dual cyber-physical) dimensions.

Expected Outcomes

The expected outcomes of this research are twofold, reflecting the dual analytical models of the study:

1. Economic and Strategic Insights**:** By evaluating the SEA-H2X cable through the upper network layers (OSI Layers 4–7), the study provide an understanding of how this infrastructure supports digital economy circulation, hyperscale platform integration, and cross-border trade between Thailand, China, and the broader Southeast Asian region.
2. Regulatory and Policy Blueprint**:** The study identifies NBTC framework gaps and proposes measures linking telecommunications regulation with maritime enforcement.

International Communication Association
Chula Chulalongkorn University
76TH ANNUAL ICA REGIONAL HUB THAILAND 2026
6–7 June 2026 • Bangkok • Chulalongkorn University
Where Thailand-Mekong-Asian Region
Bridges Divides and Amplifies Voices

Table 1

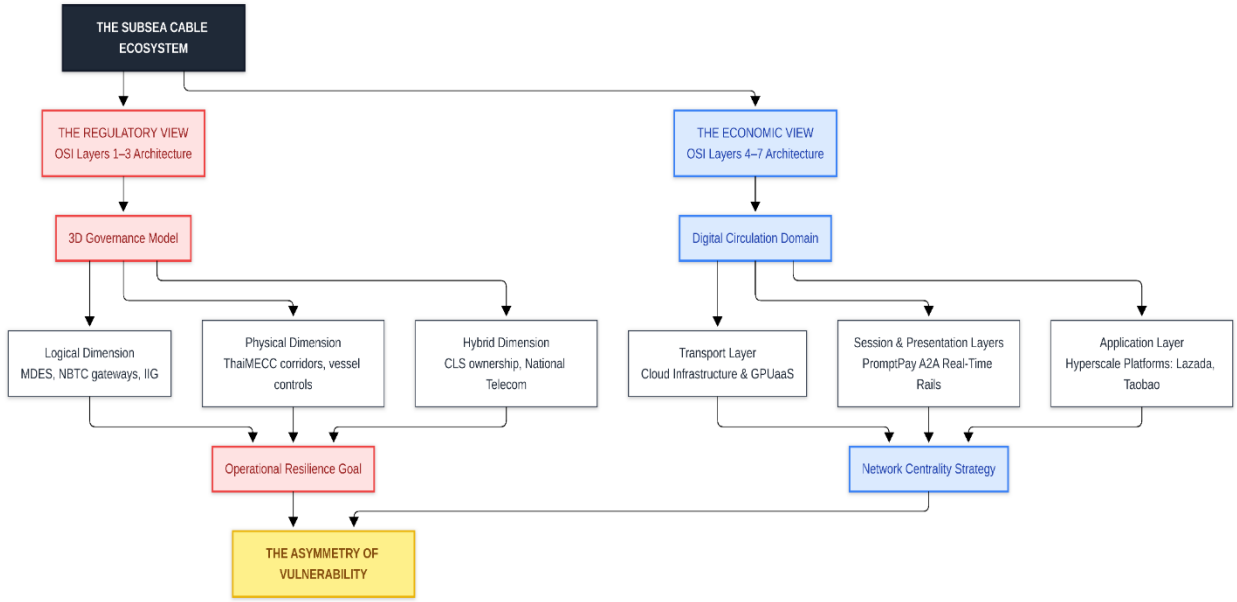
Dual OSI Analytical Framework

Analytical Lens	OSI Layers	Core Focus	Primary Variables Evaluated	Application to SEA-H2X Cable
The Regulatory Model *(3D Governance)*	Layers 1–3 (Physical, Data Link, Network)	State power, administrative law, and maritime enforcement.	Jurisdictional boundaries, spatial protection, and repair permitting speed.	Evaluating how the NBTC and ThaiMECC protect the physical hardware from anchor-dragging and sabotage.
The Economic Model *(Digital Economy)*	Layers 4–7 (Transport, Session, Application)	Macroeconomics, hyperscale platforms, and digital trade.	E-commerce integration, latency reduction, and network centrality.	Evaluating how the physical cable capacity drives Thailand's 5.6 trillion baht digital economy and cloud infrastructure.

Note. OSI = Open Systems Interconnection; SEA-H2X = Southeast Asia-Hong Kong-Hainan Express submarine cable. The framework was developed for this study to organize economic and regulatory analysis.

Figure 1

Conceptual Diagram of the Dual OSI and 3D



Literature Review and Theoretical Framework

The Open Systems Interconnection (OSI) Framework and the Subsea Ecosystem

To analyze physical infrastructure, state regulation, and international data exchange, this study combines the Open Systems Interconnection (OSI) model with the Political Economy of Communication (PEC). The OSI model separates network communications into seven layers, while PEC highlights how subsea cables shape capital concentration, digital gatekeeping, and power relations in the global digital economy. This framework creates two linked analytical lenses: the technical and regulatory view of Layers 1–3, which maps hardware, routing rules, and state authority, and the communication and political economy view of Layers 4–7, which maps platforms, transactions, and the economic influence of infrastructure ownership.

Subsea Infrastructure and the Political Economy of Communication

Subsea cables are material instruments of structural power. By controlling Layer 1 infrastructure, states and multinational firms influence regional data sovereignty, security boundaries, and production networks. The SEA-H2X cable can therefore be understood as both an engineering asset and a means of achieving network centrality: control over the material pathways of digital communication.

Layers 1–3: Physical Foundations and Infrastructure Risks (The Regulatory Model)

The foundational transport architecture of the digital economy sits in OSI Layers 1–3: the physical cable, landing stations, optical systems, and routing protocols. This architecture carries approximately 99% of global internet traffic but remains exposed to two major risk categories (Jorge & Namara, 2024):

- *Human Activity* (70–75% of incidents): Most physical damage occurs in relatively shallow coastal waters due to commercial shipping and fishing. Drifting vessels dragging

massive anchors in heavy weather can easily snag or snap cables, while bottom-trawling commercial fishing boats frequently sever them (Chow, 2026; Jacob, 2024).

- *Natural Hazards* (10–20% of incidents): Earthquakes, turbidity currents, seabed scouring, and irregular seabed topography can damage or expose cables (Chow, 2026; Jacob, 2024).

Layers 4–7: The SEA-H2X Cable and Digital Economy Circulation (The Economic Model)

While regulators focus on OSI Layers 1–3, much of the digital economy's value is generated at OSI Layers 4–7. By early 2026, Thailand's digital economy was valued at 5.6 trillion baht, supported by 67.8 million internet users and 59 million active smartphone devices (Simpson, 2026). Application-layer services depend on bandwidth, low latency, and reliable underlying physical networks. Infrastructure such as the SEA-H2X submarine cable can therefore support hyperscale digital commerce across the region.

- *Layer 4* (The Transport Layer) – Cloud Infrastructure and Data Center Growth: Cloud infrastructure and Content Delivery Networks (CDNs) serve as primary components of this network tier. The rapid advancement of Layer 4 within Thailand is demonstrated by the Board of Investment's approval of 38 data center projects valued at nearly 460 billion baht (Simpson, 2026). In total, approximately USD 2.7 billion in committed capital is being directed toward expanding data center capacity and artificial intelligence training infrastructure through 2027 (Simpson, 2026). This growth is supported by Chinese cloud providers, including Huawei, Tencent, and Alibaba Cloud. Alibaba Cloud is a leading Asia-Pacific provider and is projected to hold 36% of China's cloud infrastructure services market, with 27% of Asia-Pacific organizations expecting to deploy it (Alibaba Cloud, 2026). Direct SEA-H2X capacity can help these platforms cache data closer to Thai users and reduce reliance on older transit routes.

- *Layers 5 and 6 (Session and Presentation)* – Cross-Border Ecosystems and Encrypted Transactions: Thailand's digital economy increasingly relies on secure online payments. Cash

transactions fell from 68% of point-of-sale transactions in 2019 to 31% in 2024, while PromptPay integration with systems such as Singapore's PayNow supports cross-border transfers (Simpson, 2026). A2A real-time transfers now account for 44% of domestic e-commerce transaction value, exceeding mobile wallets (30%) and cash-on-delivery (7%) (2C2P, 2026; Simpson, 2026). These payment flows require reliable regional bandwidth.

- *Layer 7 (The Application Layer)* – Network Centrality and Vertical Integration: Thailand's e-commerce sector is consolidating around platforms such as Shopee, Lazada, and TikTok Shop. By late 2024, 69.2% of Thai internet users made online purchases weekly, contributing to a 1.1 trillion baht e-commerce market by 2025 (DHL, 2026; Simpson, 2026). Shopee Thailand recorded 49.96 billion baht in revenue by 2024, followed by Lazada Thailand at 28.29 billion baht (Simpson, 2026). Layer 7 analysis shows why application-layer firms increasingly seek direct access to Layer 1 capacity. Alibaba Group, for example, recorded 996.35 billion yuan (USD 137.3 billion) in annual revenue and 983 million monthly active users on Taobao, while China's cross-border export B2B e-commerce market was projected to reach 6.9 trillion yuan by 2025 (Alibaba Group, 2026; Thomas, 2026). Because these flows require reliable capacity, hyperscalers increasingly finance or own subsea infrastructure, deepening Thailand's integration with regional e-commerce ecosystems.

Thailand's Regulatory Governance and the Interagency 3D Matrix

Thailand's subsea cable governance is divided across logical, physical, and hybrid dimensions.

- *Dimension 1 (Logical Layer):* MDES sets digital policy, while the NBTC licenses IIG and ISP operators and enforces outage compliance. The NCSA designates telecommunications backbones as Critical Information Infrastructure (Cybersecurity Act B.E. 2562, 2019; Telecommunications Business Act B.E. 2544, 2001).

- *Dimension 2 (Physical Layer):* ThaiMECC coordinates maritime protection, while the Marine Department manages navigation and repair-ship permissions and DMCR oversees coastal environmental protection (Maritime National Interests Protection Act B.E. 2562, 2019).
- *Dimension 3 (Hybrid Layer):* The NBTC grants rights-of-way and Type Three Telecommunications Licenses for Cable Landing Stations, while National Telecom operates gateways and secures landing sites.

Table 2

Thailand's Interagency 3D Matrix for Subsea Cables

Governance Dimension	Target of Regulation	Primary Thai Agencies	Core Regulatory Mechanisms
Dimension 1: Logical Layer	Data routing, cloud, cyber defense, and ISP compliance.	MDES, NBTC, NCSA	Issues International Internet Gateway (IIG) licenses and enforces the "30-Minute Trigger" outage fine.
Dimension 2: Physical Layer	Seabed protection, vessel routing, anchor control.	ThaiMECC, Marine Dept., DMCR	Enforces maritime laws, processes repair ship entry, and manages environmental protection zones.
Dimension 3: Hybrid Layer	Cable Landing Stations (CLS) and bridging physical/cyber gaps.	NBTC, National Telecom (NT)	Grants physical rights-of-way for onshore stations; operates network gateways while securing physical landing sites.

Note. The table summarizes Thailand's interagency governance dimensions for subsea cable regulation. CLS = Cable Landing Station; DMCR = Department of Marine and Coastal Resources; IIG = International Internet Gateway; ISP = Internet Service Provider; MDES = Ministry of Digital Economy and Society; NBTC = National Broadcasting and Telecommunications Commission; NCSA = National Cyber Security Agency; NT = National Telecom; ThaiMECC = Thai Maritime Enforcement Command Center.

International Best Practices and Legislative Benchmarking

Because subsea cables cross jurisdictions, Thailand's framework is benchmarked against selected Indo-Pacific models.

Australia:

Australia uses Cable Protection Zones and all-hazards security obligations, although responsibilities remain distributed across agencies (Bashfield et al., 2025; Telecommunications Act 1997, 1997; United Nations Convention on the Law of the Sea, 1982):

- **The Australian Communications and Media Authority (ACMA):** Acting under *Schedule 3A of the Telecommunications Act 1997*, ACMA is the civilian regulator with the authority to declare Cable Protection Zones (CPZs) where high-risk activities are banned. However, the establishment of new CPZs has been limited because carriers must pay a $161,251 fee to ACMA; no new zones have been established since 2007 (Jacob, 2024).
- **The Australian Federal Police (AFP):** The AFP holds the statutory mandate to criminally prosecute individuals for negligent cable damage, but functions strictly as a reactive agency that only investigates *after* a cable has been severed.
- **Maritime Border Command (MBC):** A joint task force of the Navy and Australian Border Force that conducts general marine patrols, though it currently lacks automated integration with ACMA's CPZ coordinates to proactively stop ships before they drag anchors.
- **Department of Home Affairs & DFAT:** To address these operational gaps, Home Affairs enforces the *Security of Critical Infrastructure Act 2018 (SOCI Act)*, requiring telecom providers to implement cyber and physical risk programs. Meanwhile, the Department of Foreign Affairs and Trade (DFAT) operates the Cable Connectivity and Resilience Centre (CCRC) to assist Indo-Pacific nations in upgrading regulatory resilience (Bezzina, 2026; Wong, 2024).

New Zealand:

New Zealand emphasizes statutory deterrence and Cable Protection Areas, supported by maritime monitoring and designated protection authority (Department of the Prime Minister and Cabinet, 2026):

- **Ministry of Transport (Te Manatū Waka):** As the chief administrator of the *Submarine Cables and Pipelines Protection Act 1996*, this ministry creates and maintains Cable Protection Areas (CPAs). It applies a strict enforcement policy in which the evidentiary burden of proof is reversed onto the vessel master if fishing gear is found in the water, carrying fines up to $250,000 NZD and vessel forfeiture (Submarine Cables and Pipelines Protection Act 1996, 1996).
- **Maritime New Zealand:** The agency responsible for actively tracking commercial ship traffic via Automatic Identification Systems (AIS) and issuing formal exemptions for specialized cable repair vessels.
- **Transpower New Zealand Limited:** A state-owned enterprise representing the hybrid layer. Transpower physically funds 24-hour sea and air patrols using legally designated "Protection Officers" with statutory power to seize illegal maritime gear, while logically managing the electrical and telecom grid.

The Philippines:

The Philippines combines foreign ownership reform with repair-permitting measures to reduce bottlenecks (Bureau of Customs, 2026; Republic Act No. 11659, 2022):

- **DICT and NTC:** The Department of Information and Communications Technology and the National Telecommunications Commission handle logical licensing, open-access mandates, and anti-monopoly regulations.
- **National Maritime Council (NMC) & Philippine Coast Guard (PCG):** The NMC designs spatial Cable Protection Zones, while the PCG and the Navy physically patrol high-risk

chokepoints and utilize AIS tracking to intercept ships illegally dropping anchors near cable routes.

- **Bureau of Customs (BOC):** The BOC addressed a significant repair-permitting bottleneck by enacting *Customs Administrative Order (CAO) No. 02-2026*. This order grants duty and tax relief to foreign International Cable-Laying and Repair Vessels (ICLRVs), classifying them as "professional equipment" to bypass strict cabotage laws and support emergency repair operations (Bureau of Customs, 2026).
- **National Security Council (NSC):** Following *Republic Act No. 11659*, which allowed 100% foreign ownership of subsea cables, the NSC conducts geopolitical vetting to assess risks associated with foreign state-owned enterprises and data streams at Philippine landing hubs (Republic Act No. 11659, 2022).

Singapore:

Singapore uses coordinated telecommunications, maritime, cybersecurity, and land-use governance to manage dense cable and port infrastructure (Murphy & Bryja, 2025):

- **Infocomm Media Development Authority (IMDA):** Operating as the overarching coordinator and single-window clearinghouse, IMDA issues telecom licenses and enforces the *Guidelines on the Management of Submarine Cable Damage Incidents*. During a cable cut, IMDA coordinates with private operators to use historical AIS data to trace and penalize responsible ships (Infocomm Media Development Authority, 2019).
- **Maritime and Port Authority of Singapore (MPA):** Managing the physical “wet plant,” the MPA mandates that cables within port limits be trenched and buried 4 to 12 meters deep into the seabed to withstand anchor drops from Very Large Crude Carriers (Maritime and Port Authority of Singapore Act 1996, 1996).

- **Cyber Security Agency of Singapore (CSA):** Acting as the hybrid defender under the *Cybersecurity Act 2018*, the CSA designates cables and Cable Landing Stations as Critical Information Infrastructure (CII). It enforces logical software safeguards against hacking and physical access controls at landing facilities (Cybersecurity Act 2018, 2018).
- **SLA and URA:** The Singapore Land Authority and Urban Redevelopment Authority manage state seabed property leases and confine landing paths to specific zoned areas to avoid conflicts with port expansions.

Summary of Literature Review

The benchmarking shows that cable resilience requires more than telecommunications licensing. It depends on coordinated legal authority for repair permitting, maritime enforcement, and cyber-physical protection. Chapter 3 explains how these documents were analyzed through the 3D Governance Model.

Table 3

Comparative Benchmarking of Indo-Pacific Subsea Cable Resilience

Resilience Metric	Thailand (NBTC & ThaiMECC)	The Philippines (DICT & BOC)	Singapore (IMDA & MPA)	Australia (ACMA)	New Zealand (Maritime NZ)
Operational Philosophy	**Reactive Bureaucratic:** Focuses on paperwork and post-fault administrative fines.	**Regulatory Reform:** Fast-tracking rules to attract hyperscale investments.	**Preventive Regional Coordination:** Focuses on prevention, tracking, and regional hubs.	**All-Hazards Defense:** Focuses on holistic risk and national significance.	**Strict Statutory Deterrence:** Significant statutory penalties for zone incursions.
Repair Permitting (Layer 1)	**Lengthy:** Complex approvals across Customs and Marine Dept.	**Facilitated:** CAO No. 02-2026 grants tax/duty relief and waives cabotage for repair ships.	**Streamlined:** IMDA acts as a single-window coordinator for rapid entry.	**Moderate:** Relies on standardized visa and maritime protocols.	**Rapid:** Coordinated through regional standby agreements (SPMMA).
Spatial Protection (Seabed)	**Limited:** No active, real-time geofencing or dedicated protection zones.	**In Progress:** Transitioning corridors to the National Maritime Council.	**Developed:** Mandatory deep-trenching; live AIS ship tracking to prevent anchor drag.	**Limited Expansion:** Schedule 3A has Cable Protection Zones, but $161k fees limit new zones.	**Strict:** Cable Protection Areas with sea/air patrols and a reversed burden of proof.

Table 3

Comparative Benchmarking of Indo-Pacific Subsea Cable Resilience (Cont.)

Resilience Metric	Thailand (NBTC & ThaiMECC)	The Philippines (DICT & BOC)	Singapore (IMDA & MPA)	Australia (ACMA)	New Zealand (Maritime NZ)
Logical/Cyber Resilience	**Compliance-Driven:** 20,000 Baht/day fine for outages greater than 30 mins.	**Investment-Driven:** Allows 100% foreign ownership to boost infrastructure.	**CII-Based:** Cybersecurity Act designates landing stations as Critical Information Infrastructure.	**Comprehensive:** SOCI Act mandates annual Risk Management Programs.	**Security-Oriented:** GCSB enforces anti-interception via TICSA laws.

Note. ACMA = Australian Communications and Media Authority; AIS = Automatic Identification System; BOC = Bureau of Customs; CAO = Customs Administrative Order; CII = Critical Information Infrastructure; DICT = Department of Information and Communications Technology; GCSB = Government Communications Security Bureau; IMDA = Infocomm Media Development Authority; MPA = Maritime and Port Authority of Singapore; NZ = New Zealand; SOCI = Security of Critical Infrastructure; SPMMA = South Pacific Marine Maintenance Agreement; TICSA = Telecommunications (Interception Capability and Security) Act. The comparison synthesizes legal and policy frameworks discussed in the text.

Methodology

This chapter outlines the qualitative document analysis used to assess the SEA-H2X cable's economic significance and benchmark Thailand's NBTC framework against selected Indo-Pacific jurisdictions. The study analyzes legal texts, policy frameworks, administrative orders, macroeconomic reports, and geopolitical analyses to examine digital economic activities across OSI Layers 4–7 and governance responsibilities across OSI Layers 1–3. Primary interviews were excluded because the analysis focuses on statutory authority, finalized policy documents, and published market data.

Research Design: Qualitative Document Analysis

The study applies qualitative document analysis to identify recurring legal, regulatory, and economic patterns across selected jurisdictions. This approach is appropriate because the research questions concern formal rules, institutional mandates, and publicly documented policy practices rather than participant perceptions.

The Analytical Framework: The Dual OSI Approach

The methodology applies two analytical lenses derived from the OSI model. OSI Layers 4–7 are used to assess how SEA-H2X capacity supports hyperscale digital commerce, cloud delivery networks, e-commerce, and network centrality. OSI Layers 1–3 identify the physical, data link, and network layers managed by telecommunications regulators. Because the OSI model is technical rather than legal, this study translates these layers into the 3D Governance Model.

Translating OSI Layers 1–3 Into the 3D Governance Model

The 3D Governance Model categorizes state authority into three dimensions:

Dimension 1: The Logical Layer (Data & Telecommunications): Translating OSI Layers 2 and 3, this dimension governs everything traveling inside the cable. Documents coded under this layer

include policies dictating IP routing, bandwidth allocations, ISP licensing, and cyber-defense mandates.

Dimension 2: The Physical Layer (Seabed & Maritime Enforcement): Translating the "wet plant" of OSI Layer 1, this dimension governs the external marine environment. Documents coded under this layer include statutes defining Cable Protection Zones (CPZs), seabed trenching permits, and naval enforcement against anchor-dragging and commercial bottom-trawling.

Dimension 3: The Hybrid Layer (Convergence of Cyber and Physical): This dimension captures the entities and laws that bridge digital data with physical asset safety. Documents coded here include laws designating physical Cable Landing Stations (CLS) as Critical Information Infrastructure (CII), bridging the gap between raw hardware (Layer 1) and network routing (Layer 3).

Document Sampling Criteria

A purposive sampling strategy selected Thailand, the Philippines, Singapore, Australia, and New Zealand because they represent different subsea cable governance models within the Indo-Pacific. Data collection was limited to primary legal statutes, verified government policy frameworks, published administrative orders, international treaties, macroeconomic reports, and geopolitical analyses relevant to OSI Layers 1–7.

Data Sources and Sampled Literature

International and Regional Treaties

- United Nations Convention on the Law of the Sea (UNCLOS) 1982: Articles 21, 58, 79, 112, 113, 114, and 115 were reviewed. These articles guarantee the freedom to lay cables

while requiring states to criminalize willful or negligent damage to subsea infrastructure (United Nations Convention on the Law of the Sea, 1982).

- Enhanced ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables (2026): Evaluated for directives on expedited repair permits, cabotage exemptions, and single points of contact during cross-border infrastructure emergencies (ASEAN Digital Ministers Meeting, 2026).
- The Global Underwater Infrastructure Defence Effort (GUIDE): Analyzed as a cross-regional framework established in 2026 to foster civilian-led, defense-supported intelligence sharing and incident response coordination (Qiu, 2026; The Straits Times, 2026).

Thailand (Domestic Baseline)

- Telecommunications Business Act, B.E. 2544 (2001) and amendments: Analyzed for Type Three Telecommunications License requirements governing physical rights-of-way for Cable Landing Stations (Telecommunications Business Act B.E. 2544, 2001).
- Maritime National Interests Protection Act, B.E. 2562 (2019): Examined as the core physical protection statute that empowers the Thai Maritime Enforcement Command Center (ThaiMECC) to police the seas and classify subsea cables as a protected maritime national interest (Maritime National Interests Protection Act B.E. 2562, 2019).
- Cybersecurity Act, B.E. 2562 (2019): Reviewed for its designation of telecommunications backbones and subsea gateways as Critical Information Infrastructure requiring vulnerability audits (Cybersecurity Act B.E. 2562, 2019).
- Act on Navigation in Thai Waters, B.E. 2456 (1913) and the Royal Ordinance on Fisheries, B.E. 2558 (2015): Assessed for rules governing shipping channels, commercial trawling bans within coastal waters, and the mandatory use of Vessel Monitoring Systems

(VMS) (Act on Navigation in Thai Waters B.E. 2456, 1913; Royal Ordinance on Fisheries B.E. 2558, 2015).

The Philippines

- Customs Administrative Order (CAO) No. 02-2026: Analyzed for its mechanism to grant duty relief, tax relief, and cabotage bypass for foreign International Cable-Laying and Repair Vessels (Bureau of Customs, 2026).
- Republic Act No. 11659 (Amended Public Service Act): Analyzed for allowing up to 100% foreign ownership of telecommunications infrastructure and shifting protection toward National Security Council audits (Republic Act No. 11659, 2022).
- Republic Act No. 10844 (The DICT Act of 2015) and the National Cybersecurity Plan 2023–2028: Examined for risk-based infrastructure vulnerability protection protocols (National Cybersecurity Plan 2023–2028, 2024; Republic Act No. 10844, 2016).

Singapore

- IMDA Guidelines on the Management of Submarine Cable Damage Incidents: Reviewed for protocols requiring cable operators to submit route position lists to the Maritime and Port Authority for vessel tracking after anchor-dragging incidents (Infocomm Media Development Authority, 2019).
- Code of Practice for Telecommunication Service Resiliency (CPTSR): Assessed for mandatory route diversification and network uptime baselines, including penalties of up to $1 million SGD for widespread outages (Infocomm Media Development Authority, 2008).
- Maritime and Port Authority of Singapore Act 1996: Analyzed for physical mandates, including cable burial requirements to withstand anchor drops from Very Large Crude Carriers (Maritime and Port Authority of Singapore Act 1996, 1996).

Australia

- Telecommunications Act 1997 (Cth), Schedule 3A: Analyzed as a key Australian physical cable protection framework for its mechanisms empowering ACMA to declare Cable Protection Zones (CPZs), shift the evidentiary burden of proof, and criminalize negligent cable damage (Telecommunications Act 1997, 1997).
- Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act): Evaluated for its classification of subsea cables as Critical Telecommunications Assets requiring rigorous Positive Security Obligations (PSOs) and 12-to-72-hour incident reporting mandates (Security of Critical Infrastructure Act 2018, 2018).

New Zealand

- Submarine Cables and Pipelines Protection Act 1996: Analyzed for Cable Protection Areas, reversed evidentiary burden, statutory fines, and vessel forfeiture for illegal anchoring or fishing (Submarine Cables and Pipelines Protection Act 1996, 1996).
- Telecommunications (Interception Capability and Security) Act 2013 (TICSA): Reviewed for logical layer security, requiring operators to cooperate with intelligence agencies to prevent foreign cyber espionage (Telecommunications [Interception Capability and Security] Act 2013, 2013).

Digital Economy and Geopolitical-Economic Strategy Reports (OSI Layers 4–7)

The study also sampled 2026 macroeconomic reports, telecommunications data, and geopolitical analyses to evaluate OSI Layers 4–7:

- ***Macroeconomic and Digital Inclusion Reports:*** *Used* to extract data on Thailand's digital economy, payment integration, cloud investment, mobile connectivity, and e-commerce trends (DHL, 2026; Okeleke et al., 2026; Simpson, 2026).

- ***Strategic Analyses of Network Centrality and the Digital Silk Road:*** Used to assess how Chinese cloud and e-commerce platforms secure application-layer revenues through infrastructure expansion (Alibaba Group, 2026; Comms8, 2026).

Data Analysis Strategy: Dual Coding and Comparative Benchmarking

Phase 1: Economic and Strategic Coding (OSI Layers 4–7)

Phase 1 coded macroeconomic and geopolitical documents across OSI Layers 4–7 to track hyperscaler expansion, e-commerce integration, latency optimization, and data center investment (Simpson, 2026).

Phase 2: Structural Regulatory Coding (The 3D Governance Model). Phase 2 coded legal and policy documents through the 3D Governance Model, distinguishing logical, physical, and hybrid jurisdictional authority.

Phase 3: Comparative Benchmarking and Gap Analysis. Once the statutes were structurally categorized, a comparative benchmarking analysis was performed. This step contrasted Thailand's domestic compliance mechanisms against the specialized operational resilience protocols of Australia, New Zealand, the Philippines, and Singapore. The analysis evaluated variables such as "Repair Permitting Speed," "Spatial Protection Enforcement," and "Interagency Command Structures."

This comparison identified gaps between Thailand’s reactive compliance model and international practices such as repair-vessel tax relief, AIS monitoring, and integrated cyber-physical risk management.

Table 4

Exemplar Coding Protocol and Data-to-Node Abstraction Matrix

Governance Dimension	Target of Regulation	Sampled Primary Source Document	Initial Open Code (Extracted Operational Concept)	Assigned Analytical Node / Structural Category
Dimension 1: Logical Layer	Data routing, cloud compliance, and ISP data continuity	*NBTC Framework Regulatory Guidelines* (Thailand)	"Operational resilience framework centered around a mandatory '30-Minute Trigger' for outages"	**Reactive Administrative Enforcement Mechanisms**
Dimension 2: Physical Layer	Seabed topography protection and maritime threat mitigation	*Maritime National Interests Protection Act B.E. 2562* (Thailand)	"Empowers ThaiMECC... to track, surveil, and defend subsea routing corridors"	**Spatial Seabed Geofencing and Active Patrol Powers**
Dimension 2: Physical Layer	Bureaucratic agility, repair permitting speed, and cabotage	*Customs Administrative Order (CAO) No. 02-2026* (The Philippines)	"Classifying [repair vessels] as professional equipment to bypass strict cabotage laws"	**Streamlined Multi-Port Emergency Repair Clearances**
Dimension 3: Hybrid Layer	Converged protection of onshore physical gateway nodes	*Cybersecurity Act B.E. 2562 / Cybersecurity Act 2018* (Singapore)	"Formally designates cables and Cable Landing Stations as Critical Information Infrastructure"	**Dual Cyber-Physical Security System Integration**

Note. The table illustrates how selected primary source documents were coded into governance dimensions and analytical nodes. CAO = Customs Administrative Order; CII = Critical Information Infrastructure; CLS = Cable Landing Station; ISP = Internet Service Provider; NBTC = National Broadcasting and Telecommunications Commission; ThaiMECC = Thai Maritime Enforcement Command Center.

Policy Recommendations and Conclusion

Introduction and Summary of the Gap Analysis

The SEA-H2X submarine cable supports Thailand's OSI Layers 4–7 digital economy, including e-commerce, digital payments, and cloud infrastructure investment. However, the analysis shows that Thailand's physical transport layer remains exposed to maritime risks. The NBTC regulates logical compliance, but physical protection requires stronger coordination with maritime and customs authorities.

Strategic Economic Recommendations: Securing OSI Layers 4–7

Thailand should use SEA-H2X capacity to support application-layer growth while reducing overreliance on single foreign ecosystems. This can be advanced by attracting domestic data center investment and integrating cross-border digital supply chains.

- **Leverage Network Centrality for Data Center Investment:** Thailand should encourage hyperscalers to host data centers domestically through targeted regulatory flexibility. Localized Layer 4 infrastructure can support data residency, reduce latency, and retain more digital value domestically.
- **Integrate Cross-Border Digital Supply Chains:** MDES should link domestic digital infrastructure, including PromptPay, with regional payment and e-commerce systems to lower cross-border transaction costs.

The Regulatory Blueprint: Upgrading the 3D Governance Model (OSI Layers 1–3)

Securing the foundational capacity required by the digital economy requires coordinated reform of Thailand's state architecture, including logical regulation, physical maritime protection, and hybrid cyber-physical coordination.

Reforming the Logical Dimension (NBTC and Cyber)

- **Recommendation: Transition to All-Hazards Risk Management.** The NBTC should require Type 3 submarine cable operators to submit annual Critical Infrastructure Risk Management Programs covering cyber, physical, personnel, and supply-chain risks (Bezzina, 2026; Vocus, 2025).

Empowering the Physical Dimension (ThaiMECC and Customs)

- **Recommendation 1: Proactive Spatial Protection and AIS Geofencing.** ThaiMECC should establish Cable Protection Zones and integrate SEA-H2X coordinates into live AIS tracking to detect anchor-dragging risks (Infocomm Media Development Authority, 2019; Maritime National Interests Protection Act B.E. 2562, 2019; Murphy & Bryja, 2025).
- **Recommendation 2: Improve Repair-Ship Permitting Based on the BOC Model.** Thailand should consider adapting the Philippines' CAO No. 02-2026 to grant conditional duty relief, cabotage flexibility, and faster entry for cable repair vessels (Bureau of Customs, 2026).

Fostering Hybrid Convergence (Bridging NBTC and ThaiMECC)

- **Recommendation: Establish a Single-Window Command Structure.** Thailand should reduce separation between the NBTC and ThaiMECC by creating a hybrid task force for cable landing stations, physical defense, and network continuity (Maritime National Interests Protection Act B.E. 2562, 2019).

Advancing Multilateral and Regional Diplomacy

Because the SEA-H2X cable is a transnational asset, Thailand cannot secure it in isolation; regional permit coordination, nautical-chart sharing, repair-crew facilitation, and joint monitoring are necessary parts of cable resilience.

- **Adopt and Operationalize the Enhanced ASEAN Guidelines:** Thailand should establish a single-window national contact point for permits, nautical-chart sharing, and repair-crew customs coordination (ASEAN Digital Ministers Meeting, 2026).
- **Engage in International Defense Frameworks:** Thailand should participate in regional and cross-regional frameworks such as GUIDE to support joint training, intelligence exchange, and infrastructure monitoring (Qiu, 2026; The Straits Times, 2026).

Conclusion

Thailand's subsea cable resilience requires more than telecommunications licensing and outage fines. The NBTC's logical compliance role must be connected with ThaiMECC's maritime enforcement and customs repair procedures. Spatial protection zones, faster repair permitting, and ASEAN cooperation would strengthen SEA-H2X resilience and support Thailand's regional digital hub strategy.

Table 5

Strategic Recommendations for the SEA-H2X Cable Ecosystem

Identified Vulnerability	Governing Dimension	Proposed Policy Recommendation	International Benchmark Applied
Focus on reactive outage fines rather than preventative cyber-physical security.	Dimension 1 (Logical)	Shift to mandatory, all-hazards Critical Infrastructure Risk Management Programs (CIRMPs) for telecom operators.	Australia: Security of Critical Infrastructure (SOCI) Act.
Cables left exposed to anchor-dragging in shallow territorial waters.	Dimension 2 (Physical)	Integrate Subsea Cable coordinates into live AIS tracking to create automated geofences triggering Naval/Coast Guard warnings.	Singapore: IMDA & Information Fusion Center (IFC) real-time AIS monitoring.

Table 5

Strategic Recommendations for the SEA-H2X Cable Ecosystem (Contd.)

Identified Vulnerability	Governing Dimension	Proposed Policy Recommendation	International Benchmark Applied
Repair ships delayed by complex customs duties and strict cabotage laws.	Dimension 2 (Physical)	Classify foreign cable repair ships as "professional equipment" to grant temporary tax relief and rapid multi-port entry.	The Philippines: Customs Administrative Order (CAO) No. 02-2026.
Fragmented command between the NBTC (Telecom) and ThaiMECC (Maritime).	Dimension 3 (Hybrid)	Empower hybrid "Protection Officers" within state enterprises to coordinate physical defense and logical continuity simultaneously.	New Zealand: Transpower statutory Protection Officers.
Regional repair protocols remain highly disjointed.	Multilateral	Adopt non-binding frameworks to create a single-window national contact point for sharing nautical charts and permits.	ASEAN: Enhanced ASEAN Guidelines for Submarine Cables.

Note. The recommendations synthesize the comparative benchmarking analysis presented in Table 3 and the coding framework presented in Table 4. AIS = Automatic Identification System; CAO = Customs Administrative Order; CIRMPs = Critical Infrastructure Risk Management Programs; IFC = Information Fusion Center; NBTC = National Broadcasting and Telecommunications Commission; SOCI = Security of Critical Infrastructure; ThaiMECC = Thai Maritime Enforcement Command Center.

References

2C2P. (2026). *Popular payment methods in Thailand: What consumers want*. https://2c2p.com/articles/thailand-payment-methods/

Act on Navigation in Thai Waters B.E. 2456. (1913). (Thail.). https://faolex.fao.org/docs/pdf/tha218661.pdf

Alibaba Cloud. (2026). *Alibaba maintains leading position by revenue as Asia Pacific's largest cloud provider with growing market share*. https://www.thaipr.net/en/it_en/3716862

Alibaba Group. (2026, June 14). *Alibaba Group announces March quarter 2026 and fiscal year 2026 results*. *The National Law Review*. https://natlawreview.com/

Cybersecurity Act B.E. 2562. (2019). (Thail.). https://www.ncsa.or.th/assets/documents/%E0%B8%81%E0%B8%8E%E0%B8%AB%E0%B8%A1%E0%B8%B2%E0%B8%A2/CybersecurityAct-2019-EN.pdf

Cybersecurity Act 2018. (2018). (Sing.). https://sso.agc.gov.sg/Act/CA2018

ASEAN Digital Ministers Meeting. (2026, January 16). *Enhanced ASEAN guidelines for strengthening resilience and repair of submarine cables*. Association of Southeast Asian Nations. https://asean.org/

Bashfield, S., & Strating, R. (2026). 'Friendshoring' the seabed: Securing submarine cables through network centrality. *European Journal of International Security*, *First View*, 1–22. https://doi.org/10.1017/eis.2026.10042

Bashfield, S., Parthasarathy, B., Sridhar, V., & Youlten, O. (2025, November). *Securing Indo-Pacific submarine cable networks: Options for Australia-India cooperation*. Australia India Institute. https://aii.unimelb.edu.au/seabed-program/

Bezzina, M. (2026). *SOCI Act compliance: A leader's roadmap to critical infrastructure resilience*. Agilient. https://www.agilient.com.au/soci-act-compliance-guide/

Bureau of Customs. (2026, May 6). *Customs Administrative Order No. 02-2026: Rules on conditional importation (temporary admission) of international cable-laying and repair vessels*. Department of Finance, Republic of the Philippines. https://customs.gov.ph/

Chow, M. (2026, May 20). *Undersea cable risks: Lessons for Southeast Asia*. Fulcrum, ISEAS–Yusof Ishak Institute. https://fulcrum.sg/undersea-cable-risks-in-hormuz-lessons-for-southeast-asia/

Comms8. (2026). *Live commerce in China 2026: How brands are winning the trillion-yuan livestream market*. https://www.comms8.com/blog/2026/live-commerce-in-china-2026-how-brands-are-winning-the-trillion-yuan-livestream-market

Department of the Prime Minister and Cabinet. (2026). *Proactive release: New Zealand cyber security strategy 2026–2030 and enhancing the cyber security of critical infrastructure*. New Zealand Government. https://www.dpmc.govt.nz/search?f%5B0%5D=issue_status%3A%21%28642%29&f%5B1%5D=pmc_content_owner%3A1079&page=0

DHL. (2026). *2026 e-commerce trends report*. https://www.dhl.com/global-en/home/insights-and-innovation/thought-leadership.html

Infocomm Media Development Authority. (2008). *Code of practice for telecommunication service resiliency 2008 ("Service Resiliency Code")*. Government of Singapore. https://www.imda.gov.sg/regulations-and-licensing-listing/telecommunication-service-resiliency-code

Infocomm Media Development Authority. (2019, April 1). *Guidelines on the management of submarine cable damage incidents in Singapore port limits and the traffic separation scheme zone*. Government of Singapore. https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/Codes-of-Practice-and-Guidelines/Acts-Codes/Guidelines-on-the-Management-of-Submarine-Cable-Damage-Incidents.pdf

Jacob, J. (2024, August 30). Let's take a close look at how we protect our undersea cables. *The Strategist*. Australian Strategic Policy Institute. https://www.aspistrategist.org.au/lets-take-a-close-look-at-how-we-protect-our-undersea-cables/

Jorge, S., & Namara, E. (2024, January). *Good practices for subsea cables policy: Investing in digital inclusion*. Global Digital Inclusion Partnership. https://globaldigitalinclusion.org/2024/01/17/good-practices-for-subsea-cables-policy-investing-in-digital-inclusion/

Maritime and Port Authority of Singapore Act 1996. (1996). (Sing.). https://sso.agc.gov.sg/Act/MPASA1996

Maritime National Interests Protection Act B.E. 2562. (2019). (Thail.). https://www.krisdika.go.th/

Murphy, E. L., & Bryja, T. (2025, September 24). *The strategic future of subsea cables: Singapore case study*. Center for Strategic and International Studies. https://www.csis.org/analysis/strategic-future-subsea-cables-singapore-case-study

National Cybersecurity Plan 2023–2028. (2024). Department of Information and Communications Technology, Republic of the Philippines. https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf

Okeleke, K., Borole, S., Joiner, J., Ballon, H. A., Yuan, C., & Ganawa, S. (2026, March). *The mobile economy 2026*. GSMA Intelligence. https://www.gsma.com/mobileeconomy/

Qiu, W. (2026, June 1). 17 nations launch GUIDE: A cross-regional defence framework for critical underwater infrastructure. *Submarine Networks.* https://www.submarinenetworks.com/

Republic Act No. 10844: Department of Information and Communications Technology Act of 2015. (2016, May 23). Congress of the Philippines. https://cms-cdn.e.gov.ph/DICT/pdf/RA10844_DICT.pdf

Republic Act No. 11659: An act amending Commonwealth Act No. 146, otherwise known as the Public Service Act, as amended. (2022, March 21). Congress of the Philippines. https://www.officialgazette.gov.ph/2022/03/21/republic-act-no-11659/

Simpson, T. (2026). What is the state of Thailand's digital economy in 2026? A comprehensive market overview. *Digital in Asia.* https://digitalinasia.com/

Royal Ordinance on Fisheries B.E. 2558. (2015). (Thail.). https://www4.fisheries.go.th/article_pic/12620770.pdf

Security of Critical Infrastructure Act 2018. (2018). (Austl.). https://www.legislation.gov.au/C2018A00029/latest

Submarine Cables and Pipelines Protection Act 1996. (1996). (N.Z.). https://www.legislation.govt.nz/act/public/1996/0022/latest/dlm375803.html

The Straits Times. (2026, May 30). *17 nations launch effort to protect subsea infrastructure*. SPH Media Limited. https://www.straitstimes.com/

Telecommunications (Interception Capability and Security) Act 2013. (2013). (N.Z.). https://www.legislation.govt.nz/act/public/2013/0091/latest/DLM5177923.html

Telecommunications Business Act B.E. 2544. (2001). (Thail.). https://world.moleg.go.kr/cms/commonDown.do?DLD_CFM_NO=VOOW1ZT8UVUE0GQDEMCO&FL_SEQ=146343

Telecommunications Act 1997, Schedule 3A (1997). (Austl.). https://www.legislation.gov.au/Details/C2017C00284

United Nations Convention on the Law of the Sea. (1982, December 10). United Nations. https://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm

Thomas, T. (2026, March). *Alibaba statistics & facts 2026*. Business Stats. https://businessstats.com/

Vocus. (2025, August 29). *Vocus submission: Developing Horizon 2 of the 2023–2030 Australian cyber security strategy*. Department of Home Affairs. https://www.homeaffairs.gov.au/

Wong, P. (2024, July 29). *Launch of the Cable Connectivity and Resilience Centre*. Australian Minister for Foreign Affairs. https://www.foreignminister.gov.au/minister/penny-wong/media-release/launch-cable-connectivity-and-resilience-centre