



## Improving Indo-Pacific Cable Security and Resilience: Investment, Licensing, and Repair

*By Justin Sherman*

### Abstract

The Indo-Pacific region is an important zone for undersea cables across investments, development, maintenance, and technological innovation. Through case studies of Japan, Indonesia, Singapore, and India, this article examines the actors who are investing in Indo-Pacific cable infrastructure, how Indo-Pacific countries are approaching security issues in cable licensing, and whether actors are investing resources or developing specific policies around cable repairs. It finds that, across these four countries, many types of actors are involved in cable investment, including telecommunications firms, investment banks, and internet companies. However, there is considerable variation in how these countries are addressing security and repair issues. The article concludes by recommending that Indo-Pacific countries remember to balance investment screening and security issues with international collaboration on cables, improve cable outage and repair tracking, consider government-led or government-subsidized cable repair ship programs, and integrate security and resilience assessments into licensing processes.

## INTRODUCTION

Undersea cables carry over 95 percent—by some estimates, even upwards of 99 percent—of intercontinental internet traffic around the world. These hundreds of cables, laid across the ocean floor, are vital to the functioning of the modern-day internet and the transmission of video calls and emails, e-commerce and business transactions, medical and scientific research, and government and military communications. Yet, they remain underappreciated by policymakers around the world. As policymakers, pundits, and media focus increasingly on the digital elements of cybersecurity, such as malicious code or digital espionage, the risk of forgetting the importance of underlying, physical internet infrastructure grows.

The Indo-Pacific region is an important zone for undersea cables across investments, development, maintenance, and technological innovation. Data centers and cloud infrastructure in the region additionally increase these cables' importance to surrounding countries and the globe. Dozens of new cables have become ready for service or will soon be ready for service across the Indo-Pacific. Further, geopolitical tensions increase the need to ground policy assessments in the reality of cable deployment, maintenance, and security in the region. Through case studies of Japan, Indonesia, Singapore, and India, this article examines the actors who are investing in Indo-Pacific cable infrastructure, how Indo-Pacific countries are approaching security issues in cable licensing, and whether actors are investing resources or developing specific policies around cable repairs. It draws on data on undersea cable investments and connectivity as well as public information on cable security, licensing, and repair efforts.

The article finds that, across these four countries, many types of actors are involved in cable investment, including telecommunications

investment banks, and internet companies. However, there is wide variation in how these countries are addressing security issues. For example, on the more developed side, Singapore requires cable license applicants to specify some of their cybersecurity and physical security measures, while on the less developed side, Indonesia is implementing a somewhat ineffective regulatory regime without a strong emphasis on security. In the case of repairs, the article finds that Japan, Singapore, and India have given some attention and/or investment to outage problems, but Indonesia lags behind.

The article concludes by recommending that Indo-Pacific countries remember to balance investment screening and security issues with international collaboration on cables, improve cable outage and repair tracking, consider government-led or government-subsidized cable repair ship programs, and integrate security and resilience assessments into licensing processes.

“These hundreds of cables, laid across the ocean floor, are vital to the functioning of the modern-day internet and the transmission of video calls and emails, e-commerce and business transactions, medical and scientific research, and government and military communications.”

## RECENT TRENDS IN INDO-PACIFIC CABLE INVESTMENT

Building and laying an undersea cable is a complex endeavor. It is logistically intensive, as it involves many companies across the cable supply chain, requires sufficient expertise to lay cables across thousands of miles in the ocean, and typically necessitates engagement with multiple countries' governments. It is also expensive: a single undersea cable can cost hundreds of



millions of dollars to build and lay along the ocean floor. International collaboration to fund, build, lay, operate, and repair undersea cables is a generally necessary feature of the industry.

While there are certainly industry trends and common practices—such as forming consortia of investors across borders—there is no single model that defines how every single undersea cable is owned. Across the world, 65 percent of cables have a single owner, while 33 percent have multiple owners and 2 percent have unclear ownership. 59 percent of undersea cables are privately owned, alongside mixes of state ownership (19 percent), public-private ownership (19 percent), and unclear ownership (3 percent) [1]. Moreover, ownership is not the entire supply chain, which also includes companies building the inner fibers of cables, companies laying cables, and those operating cables.

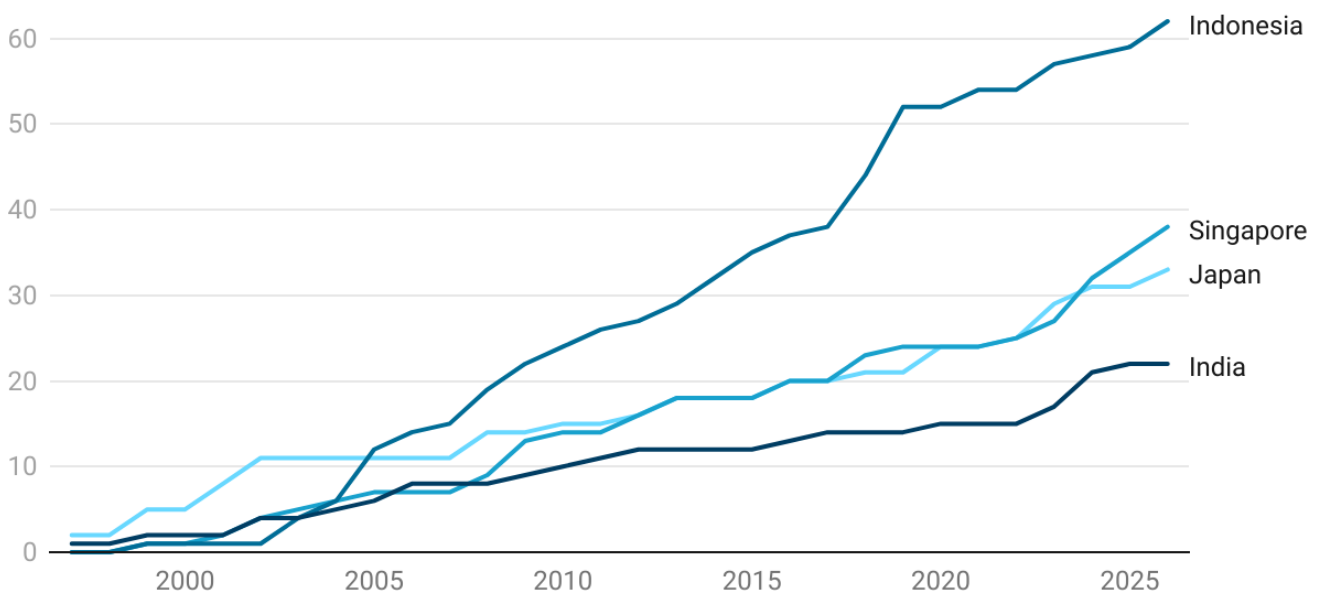
Investment trends in Indo-Pacific cable development are similar in some ways to the US and elsewhere, as internet companies such as Alphabet (Google), Meta (Facebook), Microsoft, and Amazon play a greater role in recent years in

cable development and ownership. In other ways, there are differences—such as the persistent role of traditional telecoms in Indo-Pacific cable investment (e.g., Reliance Jio in India, NTT in Japan) alongside other internet companies and investment firms focused on building out the cable network.

To analyze some of the undersea cable investment and development trends in the Indo-Pacific, this section reviews cable development and investments in four case study countries: Japan, Indonesia, Singapore, and India. It demonstrates that the Indo-Pacific is an important, active zone of cable investment and that a wide variety of players—not just traditional telecoms or a few tech companies—are involved in cable development in the Indo-Pacific.

Figure 1 shows the total number of international cables in each country. Importantly, the number of cables connected to a single country is not the only indicator of a country’s cable connectivity. For instance, some cables may have much lower bandwidth and therefore carry

Figure 1. Number of Domestic and International Cables (1997–2026) [2]



Created with Datawrapper

little traffic. Some countries have numerous undersea cables that connect domestic regions but fewer cables that connect to international locations. The data points in Figure 1 are therefore not the only ones available but are included as one way of capturing the overall trends in cable financing and development in the Indo-Pacific over the last several years.

Japan is currently or will soon be connected to 33 undersea cables. There was some cable development in Japan in the early 2000s, with five new cables becoming ready for service in the 1990s and another six in 2001 and 2002. After some additional cables became ready for service in the 2010s, there have been 12 Japan-connected cables either deployed or planned to be deployed since 2020. This recent spike in construction resulted from a new Japanese government push to establish more international landing stations in Japan (described further below) and Japan's importance in the Asia-Pacific as a place for data storage and transmission, as more companies and governments look to do business in the region without putting their data in China. Many of Japan's cables are connected to other countries [3].

Indonesia is currently or will soon be connected to 62 undersea cables. Cable connectivity to Indonesia was slower to progress compared to some other countries in the 1990s and early 2000s. This slowness was part of broader challenges in expanding the country's internet connectivity, due to a "lack of fixed-line [cables on land], the low dispersal of personal computers, the extremely high (monopolistic) price of leased lines and international bandwidth, and the narrow coverage and inadequate capacity or limited bandwidth of terrestrial backbone infrastructure" [4]. However, Indonesia's undersea cable numbers changed quickly in the mid and late 2000s, with 28 cables newly ready for service between 2003 and 2013

“ There has been a recent spike in undersea cable connectivity to India, in significant part because of the Indian government's strong push to grow India's data storage and processing sector and several Indian companies' push to make strategic undersea cable investments. ”

and another 16 coming online between 2018 and 2021. At least eight additional Indonesia-connected cables are or will be ready for service from 2023 to 2026. Unlike Japan, where many undersea cables connect to foreign countries, most of Indonesia's cables connect one part of Indonesia to another part of Indonesia; it only has four international landing stations [5].

Singapore is a growing global data center hub, which means more and more data is flowing into and out of the country, and it is currently or will soon be connected to 38 undersea cables. Singapore had a few undersea cables become ready for service in the late 1990s and early 2000s. From 2008 to 2018, 16 new Singapore-connected undersea cables became ready for service. From 2019 through 2026, 15 new cables have or will become ready for service. The country is home to many international landing stations and has cable connectivity to many other parts of the world, including other parts of Asia, Europe, Africa, Australia, and the US [6].

India is another important country in the undersea cable space due to its growing investments as well as the fact that a major global technology player is becoming more involved in the cable space. There are 22 undersea cables currently or soon-to-be connected to India. There has been a recent spike in undersea cable connectivity to India, in significant part because of the Indian government's strong push to grow India's data storage and processing sector and several Indian companies' push to make strategic

undersea cable investments [7]. From 2020 to 2025, 8 new cables are ready or planned to be ready for service. In 2021, commenting on the India-Asia-Xpress (IAX) and India-Europe-Xpress (IEX) cables in which it was investing, Reliance Jio stated that this was the “first time in the history of fiber optic undersea telecommunications” where a system of this kind placed India at the center of the international network [8]. India also has several international landing stations, and many of its cables make India an important data stopping point between countries in the Indo-Pacific region and beyond [9].

### INDO-PACIFIC CABLE DEVELOPMENT IN GLOBAL CONTEXT

How do trends in the Indo-Pacific compare to trends elsewhere in the world? In the US, undersea cable investments were historically led by traditional telecommunications companies such as AT&T and Verizon, but they are now led by Alphabet (Google), Amazon, Meta (Facebook), and Microsoft. This has been a notable shift in recent years. All of these US internet companies operate major data centers, and three of these companies (Alphabet, Amazon, and Microsoft) are the “hyperscalers” that dominate the global cloud computing market.

Among the four countries examined in this article, there is some similarity to the US, in that increased investments in undersea cables by Google, Meta, and others are seen in Singapore, for instance. However, traditional Indo-Pacific telecommunications companies still invest more in cables presently than their US telecom counterparts. Likely factors in this reality are that US internet companies have come to dominate the US technology market overall as US telecoms have stepped back from undersea cable ownership—and Indo-Pacific telecom companies have retained their focus on physical internet infrastructure investments.

For example, Reliance Jio (India) is a growing

cable investor in India and the region, and Singtel (Singapore) remains an active investor in cables linked to Singapore. Additionally, Chinese state-owned telecommunications companies China Mobile, China Telecom, and China Unicom have greatly increased their investments in undersea cables around the world in the last five to six years [10]. In some countries, the scenario appears mixed. In Japan, a combination of tech conglomerates (e.g., Rakuten), investment firms (e.g., Softbank), and telecom providers (e.g., NTT) all still play a role in cable investment and development. Overall, these countries have a much more diversified investment environment in terms of types of involved companies than in the US. Diversification may or may not benefit security but has likely benefits for competition in the undersea cable development space.

“Overall, these countries have a much more diversified investment environment in terms of types of involved companies than in the US.”

Other factors influencing Indo-Pacific cable investment and development include business factors such as: responding to continued demand for new undersea cables and bandwidth, enhancing cloud and data processing opportunities, and responding to the increased transfer of data within Asia; policy and political factors such as engaging in regional capacity-building, promoting one’s country as a global data hub, and pushing back against the influence of Western, particularly American, internet companies; and geopolitical factors such as state-to-state competition [11]. Many of these factors also cross-cut these categories, such as the fact



that Chinese state-owned telecoms have greatly increased their investments in undersea cables in the last five or so years; this likely has a mix of business, policy, political, and geopolitical motivations. The same goes for Reliance Jio's interest in building out more undersea cables connected to India.

### **CABLE SECURITY AND RESILIENCE REVIEW CAPACITY IN THE INDO-PACIFIC**

How are countries in the Indo-Pacific planning for, assessing, and managing cable security and resilience issues? Doing so includes reviewing and bolstering cables' physical security, such as protecting subsea line terminating equipment (SLTE) and undersea cable landing stations. It also includes addressing cybersecurity, such as protecting the internet-connected, remote network management systems increasingly used to manage complex cable networks. In addition, it includes addressing resilience, such as ensuring fast repairs in the event of accidental or intentional damage. Though most cable damage stems from accidents and natural weather events, countries have also expressed national security worries about the potential intentional destruction of or damage to cables during conflict.

This section examines some recent cable security policy, licensing review, and repair developments in Japan, Indonesia, Singapore, and India. Singapore has some of the more detailed requirements for cable license applicants to

“

Though most cable damage stems from accidents and natural weather events, countries have also expressed national security worries about the potential intentional destruction of or damage to cables during conflict.

”

submit some information about cybersecurity and physical security. India has some requirements, although it is more focused on use of cables for domestic security. Japan is more focused on strategic security risks and cooperation with foreign partners on detecting outages. Indonesia lacks effective cable protection policies.

### **Japan**

Japan's efforts around geopolitical conflict, international competition, and national security generally have focused more explicitly on China in recent years. Its 2022 National Security Strategy stated that “China's current external stance, military activities, and other activities have become a matter of serious concern for Japan and the international community” that presents “the greatest strategic challenge in ensuring the peace and security of Japan and the peace and stability of the international community” [12].

Some scholars have suggested that Japan can tie its undersea cable investments and security activities into broader geopolitical efforts around China and in furtherance of Japan's Free and Open Indo-Pacific initiative [13]. In June 2023, Japan's Ministry of Internal Affairs and Communications and the European Commission signed a memorandum of cooperation on “undersea cables for secure, resilient, and sustainable global connectivity,” following the May 2022 launch of the Japan-EU Digital Partnership [14]. It laid out the goals of “securing and sustainable connectivity,” focused on improving communication speed, quality, safety, and redundancy in routes; exploring how Arctic cable routes “may reduce latency and stimulate data flows between Japan and the EU, as well as between Europe and Asia”; building out a joint system for detecting and reporting undersea cable outages; and exploring how undersea

cable technology could be used for “monitoring disaster symptoms, climate change, and the environment” [15].

This followed an announcement by the Japanese government in 2022 that it would invest \$440 million in a more decentralized undersea cable network touching Japan for a combination of economic and security reasons [16]. Among those security reasons, recent cable cuts to Taiwan (with debates continuing about Beijing’s involvement) and earthquakes were at the top of the list [17].

### Indonesia

Indonesia is a growing cable hub, though many of its cables are purely domestically connected, and the government is building out several new processes for licensing and monitoring undersea cables connected to the country. Its Ministry of Communication and Informatics imposed new regulations in 2021 that required all cables crossing Indonesian waters to have an Indonesian telecom, with at least five years of relevant experience, own at least five percent stake [18]. The 2021 regulations and subsequent ones issued in 2022 collectively require the government to conduct surveys of the cable network—which may be delayed due to insufficient data and visibility into where exactly cables are located—and give overlapping authorities to multiple agencies.

Already, Indonesia’s regulatory processes have resulted in some cable developers facing unanticipated delays in implementing approved projects and others receiving inaccurate information from the state about where they are permitted to lay cables [19]. It is unclear how much the government considers such factors as the physical security of landing stations and other equipment, the cybersecurity of cable management technology, and overall network resilience when making licensing decisions.

“Already, Indonesia’s regulatory processes have resulted in some cable developers facing unanticipated delays in implementing approved projects and others receiving inaccurate information from the state about where they are permitted to lay cables.”

### Singapore

Singapore has a relatively comprehensive regulatory regime governing telecommunications systems in the country, including undersea cables, which already considers some security issues. The government requires that undersea cable developers apply for a Facilities-Based Operations (FBO) license, for which applicants must provide corporate ownership information, business plans and finances, and network plans [20].

Singapore is clear, though, that the two main factors considered for new undersea cable applications are the project’s financial viability and economic benefit to the country as well as the project’s efficient use of land resources and sea corridor. Companies applying for cable approval must conduct an environmental impact assessment, for example, which is certainly important, but they are not required to conduct a cybersecurity risk assessment or submit a cable repair plan [21].

When damage to a cable does occur, however, Singapore requires that companies notify the Infocomm Media Development Authority (IMDA) and also seek approval to obtain information about vessels nearby the cable that may have damaged it. Companies that want to repair cables must apply for approval to do so, which includes submitting a description of systems to be repaired, intended operations and operation areas, details of the repair craft and other vehicles, communication and reporting plans,

work schedules, repair methodology, safety of navigation procedures, contingency plans for the craft, and information on personnel [22].

### India

India, by contrast, has long placed more controls around undersea cable security and is having more conversations about cable resilience and repair. In January 2002, the Indian government opened undersea cable management opportunities to private Indian companies, who were required to apply for an International Long Distance (ILD) service license to set up cable landing stations and lay undersea cables in the country. The state also established numerous other requirements as part of the licensing application process, including that applicants would provide equal access to bottleneck facilities for international bandwidth and meet certain design specifications for traffic transmission.

India also implemented several security-related requirements, such as prohibiting companies from building landing stations in “security sensitive areas”; requiring that companies provide physical security and access control measures for landing station offices; requiring companies to comply as necessary with government efforts “to counteract espionage, subversive act[s], sabotage, or any other unlawful activity”; mandating that foreign personnel building and managing the cable were security-cleared by the Ministry of Home Affairs; requiring privacy-protective measures to prevent “unauthorized” interception of traffic; and preventing companies from operating cables until they installed monitoring equipment and had it inspected by security authorities [23]. Notably, few of these requirements—reflective of the state of world affairs in 2002—pertained to cybersecurity. Some of these measures may also be framed as security but relate more to state control per se.

The government made changes to these licensing requirements in the following years, such as when it issued regulations in 2007 clarifying definitions, procedures, and many other details; it was firm that its security requirements remained in place [24]. Most recently, the Indian Department of Telecommunications noted that consortia of investors were building India-connected undersea cables but were going through Indian companies to apply for licenses, where the Indian companies were slated to manage the landing station but did not have ownership in the consortia [25]. The government then issued updated cable licensing guidelines in June 2023, clarifying that the Indian companies have to demonstrate ownership of the cable landing station and other equipment in Indian territory—as well as updating its categorization of cable landing stations to reflect new generations of undersea cable systems [26]. Significantly, another element of the Indian government’s announcement is the Department of Commerce forming a committee to study the “different financial viability models” for designated Indian cable repair vessels, with potential financial incentives from the government [27].

### RECOMMENDATIONS

In light of the developments described in the previous sections around cable investments, security reviews in licensing, and repairs, this article offers the following recommendations:

**Remember the importance of international and collaborative investments.** Indo-Pacific countries are continuing to invest in undersea cable infrastructure while there is also growing scrutiny of tech investments from certain countries. Investment security reviews are indeed an important consideration for countries looking to understand the risks of malicious actors potentially influencing cable development. However, countries pursuing investment security

policies for cables should remember that collaboration among many companies and organizations from around the world has enabled the large investments necessary to plan, build, lay, and operate undersea internet infrastructure. Significantly undermining that with too much emphasis on potential investment risks and national security would undermine network resilience by constraining important cable development opportunities.

**Improve cable outage and repair tracking.**

As Indo-Pacific countries continue to invest more in undersea cables, as described above, they should work with the international community's shared interest in maintaining a robust and resilient undersea cable network and in ensuring that outages are tracked and that damages are repaired as quickly as possible. Japan and the EU plan to build out a system to better track undersea cable outages. The US already does some tracking of these outages but has many areas to improve. New memorandums of cooperation between governments, working within broader international coalitions, would minimize duplicated costs of setting up numerous, bilateral digital channels through which to share information about outages.

**Consider government-led or government-subsidized cable repair ship programs.** Once governments and companies identify undersea cable outages, they must fix the problem. While many companies already invest money in repairing damaged undersea cables, these investments may be insufficient, and governments may have security and economic interests in accelerating the speed of those repairs. Undersea cable repairs can also be delayed for a variety of reasons, ranging from international legal issues to the tactical challenges of coordinating repairs in multiple languages. The recently established US Cable Ship Security Program, and the discussions underway

in India, provide two potential examples for a government-led or government-subsidized program to ensure there are cable repair ships on standby. The other Indo-Pacific countries examined in this article would benefit from these kinds of programs, especially for countries where many of their cables are internationally connected (e.g., Singapore, Japan).

**Integrate security and resilience assessments into licensing processes.** Cable developers do not have sufficient incentives to consider the security and resilience issues of their cable systems. Many undersea cable landing stations, for instance, are left overly exposed to natural disaster events or lack the most basic physical security measures [28]. Governments often insufficiently screen for these issues as well. The licensing process is one place to implement these risk assessments, focused on physical security, cybersecurity, and network resilience and reliability. Some Indo-Pacific governments, such as India, already have some security requirements around cable licensing. Singapore requires license applicants to disclose physical security and cybersecurity measures. But, as borne out in the review of cable licensing processes in Japan and Indonesia, not every country has these mechanisms in place. Singapore's list of network protection disclosures could serve as one starting point for other countries, as can the US, which is arguably one of the most sophisticated countries when it comes to cable security reviews because of its executive branch "Team Telecom" committee that screens proposed cable projects of national security risks. This includes countries considering where regulatory regimes may be too onerous and in fact undermine quick cable repairs [29].

The continued growth of cloud computing services, implementation of technologies like 5G telecommunications, and regional and state-specific efforts to make the Indo-Pacific a global



data hub will only keep the region’s undersea activity going. While some countries have devoted more attention and resources to cable security and resilience issues—such as Singapore’s licensing requirements around security or India’s recent decision to look into cable repair ships—there is still much to be done to continue enhancing regional capacity. Ultimately, the most effective solutions will lie in understanding both industry and government perspectives, forging cooperation between states, and balancing the need to impose security requirements on some elements of the supply chain with the need to facilitate an open, international, collaborative environment for cable investment and growth.

---

*Justin Sherman is the founder and CEO of Global Cyber Strategies and a Nonresident Fellow at the Atlantic Council.*

*This publication is part of a project on “Undersea Cables, Geoeconomics, and Security in the Indo-Pacific: Risks and Resilience” that was made possible by a grant from the Japan Foundation.*

*The views expressed in this publication are those of the author and do not necessarily reflect the position of the Center for Indo-Pacific Affairs or any organization with which the author is affiliated.*

© 2024 University of Hawai‘i at Mānoa Center for Indo-Pacific Affairs. All rights reserved.

## REFERENCES

- [1] Justin Sherman, Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security, Atlantic Council, September 2021, 7, 9.
- [2] Telegeography, Submarine Cable Map, accessed December 19, 2023.
- [3] Submarine Cable Networks, “Japan,” accessed December 19, 2023.
- [4] Haryo Aswicahyono and Deni Friawan, “Infrastructure Development in Indonesia,” in Nagesh Kumar (ed.), International Infrastructure Development in East Asia — Towards Balanced Regional Development and Integration, ERIA Research Project Report, 2007, 136.
- [5] Submarine Cable Networks, “Indonesia,” accessed December 19, 2023.
- [6] Submarine Cable Networks, “Singapore,” accessed December 19, 2023.
- [7] See for example, Gagandeep Kaur, “In-Depth: Why Are So Many Submarine Cables Landing in India?” Economic Times, April 18, 2023.
- [8] Niharika Sharma, “Why is Mukesh Ambani Building an International Undersea Cable System?” Quartz, June 2, 2021.
- [9] Submarine Cable Networks, “India,” accessed December 19, 2023.
- [10] Sherman, Cyber Defense Across the Ocean Floor, 12.
- [11] Max Parry and Tony Leung, “3 Trends Leading to a New Digital Silk Road in Asia-Pacific,” Equinix, August 24, 2022; Business Line, “Editorial: With the Right Policies, India Can Become the World’s Data Hub,” November 25, 2022; Lok Sabha, Indian Government, Report of the Joint Committee on the Personal Data Protection Bill, 2019, December 2021; Joe Brock, “Exclusive: China Plans \$500 million Subsea Internet Cable to Rival US-Backed Project,” Reuters, April 6, 2023; Laura Zhou, “China Builds Undersea Cable Cases Amid Digital Infrastructure Rivalry,” South China Morning Post, December 12, 2021.
- [12] Cabinet Secretariat, Japan, National Security Strategy of Japan, December 2022, 9.
- [13] Geoffrey F. Gresh and Hotaka Nakamura, “Japan: New Lord of the Subsea?” The Diplomat, May 18, 2023.
- [14] European Commission, “EU and Japan Boost Strategic Cooperation on Digital and on Critical Raw Materials Supply Chains,” July 13, 2023.
- [15] Ministry of Internal Affairs and Communications of Japan, Memorandum of Cooperation on Submarine Cables for Secure, Resilient, and Sustainable Global Connectivity—Between the Ministry of Internal Affairs and Communications of Japan and the European Commission on Behalf of the European Union, July 13, 2023, 1-2.
- [16] Robert Clark, “Japan’s \$440M Plan to Ensure Subsea Cable, Data Center Diversity,” Light Reading, January 26, 2022.
- [17] Huizhong Wu and Johnson Lai, “Taiwan Suspects Chinese Ships Cut Islands’ Internet Cables,” Associated Press, April 18, 2023; Clark, “Japan’s \$440M Plan to Ensure Subsea Cable, Data Center Diversity.”
- [18] William Yuen Yee, “Indonesia Isn’t Ready to Become Asia’s Submarine Cable Hub,” Foreign Policy, August 31, 2023.
- [19] Trissia Wijaya, “Regulatory Risks Key Barrier to Investment in Submarine Cables,” Center for Indonesian Policy Studies, June 28, 2023.
- [20] Infocomm Media Development Authority, Singapore, “Facilities-Based Operations (FBO) License,” accessed October 15, 2023; Infocomm Media Development Authority, Singapore, Guidelines on Submission of Application for Facilities-Based Operations License, June 28, 2021. Annex 1: 1-3.
- [21] Infocomm Media Development Authority, Singapore, Guidelines on Deployment of Submarine Cables into Singapore, October 1, 2016.
- [22] Infocomm Media Development Authority, Singapore, Guidelines on the Management of Submarine Cable Damage Incidents in Singapore Port Limits and the Traffic Separation Scheme Zone, October 6, 2020.
- [23] Ministry of Communications & Information Technology, India, Guidelines for Issue of License for International Long Distance Service, January 15, 2002.
- [24] Telecom Regulatory Authority of India, International Telecommunication Access to Essential Facilities at Cable Landing Stations Regulations, 2007 (5 of 2007), June 7, 2007.

[25] Telecom Regulatory Authority of India, Recommendations on Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India, June 19, 2023, 3.

[26] Ministry of Communications, India, “TRAI Releases Recommendations on ‘Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India,’” June 20, 2023.

[27] Ibid.

[28] Lane Burdette, “Leveraging Submarine Cables for Political Gain: U.S. Responses to Chinese Strategy.” *Journal of Public & International Affairs*, May 5, 2021.

[29] See for example, Yee, “Indonesia Isn’t Ready to Become Asia’s Submarine Cable Hub.”