Ponder the Improbable since 1996

ENHANCING THE SECURITY OF SINGAPORE'S SUBMARINE CABLES: STRENGTHS, CHALLENGES, AND OPPORTUNITIES

Robert Beckman
Asha Hemrajani
Tara Davenport
Sean Tan

Policy Report
May 2024

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Policy Report

ENHANCING THE SECURITY OF SINGAPORE'S SUBMARINE CABLES: STRENGTHS, CHALLENGES, AND OPPORTUNITIES

Robert Beckman
Asha Hemrajani
Tara Davenport
Sean Tan

May 2024

TABLE OF CONTENTS

Executive Summary

Submarine cables carry over 99 per cent of Singapore's international telecommunications traffic. These submarine cables are critical to Singapore's connectivity and play a pivotal role in fostering economic stability and upholding national security. Singapore is also one of the leading submarine cable hubs in the world. While most incidents of damage to submarine cables are accidental, recent developments such as the severance of cables serving the Matsu Islands off the coast of Taiwan as well as the cables under the Baltic Sea connecting Estonia to Finland and Sweden were suspected by some to have been deliberate, and thus have highlighted the potential for intentional acts of sabotage by state and non-state actors. There is also increasing awareness of the possibilities of cyberattacks against the network management systems that manage submarine cable systems. The importance of securing submarine cables and its associated infrastructure has risen for two key reasons: (i) the significance of Singapore's role as a hub for communications for other regions, and (ii) the political, economic, and security ramifications should there be a disruption of communications via submarine cables.

This policy report examines Singapore's approach to safeguarding submarine cables to mitigate potential damages or interference that may disrupt communications. It first highlights the strengths of Singapore's current approaches and strategies to protecting this critical infrastructure. The subsequent section offers recommendations regarding specific measures that Singapore could undertake to bolster the security of submarine cables. These include strengthening criminal penalties for damage to submarine cables, explicitly designating submarine cables as critical infrastructure, enhancing cooperation and coordination between relevant government agencies, enhancing public-private partnerships, and taking the lead in driving regional cooperation on this issue.

Figure 1. Submarine cables landing in Singapore. Extracted from *Telegeography 2024 Submarine Cable Map*, TeleGeography and Submarine Cable Map. Accessed 7 May 2024, www2.telegeography.com/; www.submarinecablemap.com/.

Introduction

Over 99 per cent of Singapore's international telecommunications traffic is carried via submarine cables (with the rest via other means such as satellite). [1] Singapore is one of the leading submarine cable hubs in the world, with twenty-six cables connecting to seven cable landing stations in Singapore.[2] An announcement in June 2023 by Singapore's Ministry for Communications and Information outlined Singapore's ambition to double its capacity for international subsea cable landings within the next ten years, entrenching its global status as a leading network hub as well as improving the reliability of its network by increasing the diversification of cable routes.[3] These submarine cables, which facilitate services that depend on the Internet, are critical to Singapore's connectivity, and are consequently crucial for its economy and national security. Moreover, Singapore is a vital transit hub that facilitates data transmission between various regions, including other parts of Asia, the Persian Gulf, the Mediterranean, and Europe.

Considering the significance of submarine cables to Singapore and its role as a hub for communications for other regions, the protection of submarine cables and cable landing sites has gained increased importance. Interruptions to transmission of data and loss of connectivity can have grave ramifications, including serious economic losses. While most cable faults are accidental (for example, by ships dragging their anchors or by fishing equipment), recent developments have also highlighted the possibility of deliberate acts of sabotage or interference against cables and related infrastructure by state and non-state actors, including as part of grey zone activities or to destabilise states in times of armed conflict.[4] The deliberate attacks against the NordStream pipelines in October 2022 also highlighted

---

[1] Infocomm Media Development Authority, "Statistics on Capacity & Bandwidth Services, 2019–2022," IMDA, www.imda.gov.sg/about-imda/research-and-statistics/telecommunications/statistics-on-capacity-bandwidth-services/statistics-on-capacity-bandwidth-services-2019-2022.

[2] Telegeography, "Submarine Cable Map - Singapore," www.submarinecablemap.com/country/singapore.

[3] Ministry of Communications and Information, "Singapore's Digital Connectivity Blueprint," 6 June 2023, www.imda.gov.sg/-/media/imda/files/programme/digital-connectivity-blueprint/digital-connectivity-blueprint-report.pdf.

[4] Christian Bueger, Tobias Liebetrau, and Jonas Franken, "Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU", In-Depth Analysis for the European Parliament, June 2022 https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

the vulnerabilities of submarine infrastructure.[5] There have also been several reports of damage to submarine cables, where the possibility that it was deliberate was raised or speculated.[6] It is also important to note that hostile actors are more likely to sabotage a nation's communications cables at locations far from the country's shores and territorial waters.

Exacerbating these concerns is the fact that cables can be physically damaged with remarkable ease, for example, by civilian vessels equipped with cutting devices or dredging equipment, which renders assessments on whether such damage is accidental or deliberate more challenging.[7] More sophisticated methods involve the placement of undersea explosives that can be remotely triggered or deliberate cutting by submarines or autonomous vehicles.[8] Communications can also be disrupted by cyberattacks against the remote network management systems (NMS) that manage submarine cable systems.[9]

With this context in mind, this policy report examines Singapore's approach to the safeguarding of cables from damage or interference. It first highlights the strengths of Singapore's current approaches and strategies in protecting this critical infrastructure. It then makes recommendations on further measures Singapore can take to improve the security of submarine cables.

---

[5] See, for example, "EU-NATO Task Force on the Resilience of Critical Infrastructure" https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf, June 2023 (n 4), 5.

[6] Severin Carrell, "Shetland loses telephone and internet services after subsea cable cut," The Guardian, 20 October 2022; "Fibre optical cable sabotage causes global internet slowdown," *The Brussels Times*, 25 October 2022; Niels Nagelhus et al, "The subsea cable cut at Svalbard January 2022: What happened, what were the consequences, and how they were managed?' *Norwegian Institute of International Affairs Policy Brief 1 (2023)*; Huizhong Wu and Johnson Lai, "Taiwan suspects Chinese ships cut islands' internet cables" *AP News*, 18 April 2023; "The damage to a Baltic undersea cable was purposeful, Swedish leader says but gives no details," *AP News*, 24 October 2023.

[7] Bueger, Liebetrau and Franken (n 4), 29 - 30.

[8] Bueger, Liebetrau and Franken (n 4), 29 - 30.

[9] Bueger, Liebetrau and Franken (n 4), 30.

Strengths of Singapore's Approach

Singapore has taken significant steps to ensure the resilience of submarine cables. In 2010, it worked together with the International Cable Protection Committee (ICPC), a non-governmental organisation consisting of both cable industry and governments, to get the critical nature of submarine cables recognised in the United Nations Omnibus Resolution on the Oceans.[10] Singapore has also implemented several of the best practices for governments on the protection of submarine cables recommended by the ICPC.[11] The following sections outline the key strengths of Singapore's approach.

Establishing a Single Point of Contact

Given that submarine cable deployment, installation, operation, and repair involve the mandate of several regulatory agencies including telecommunications, maritime and shipping, and environment, the ICPC has recommended that "states establish a single point of contact for submarine cables and not just for permitting purposes, but also for any issues arising with respect to installation, repair and protection."[12] Singapore designated its telecoms regulator, the Infocomm Media Development Authority (IMDA), "as the point of contact for submarine cables, even if other government bodies have ultimate responsibility for a particular issue."[13] This has helped considerably with the streamlining of processes.

Enhancing Transparency in Cable Deployment and Cable Damage Reporting Incidents

The IMDA has issued two guidelines: (i) Submarine Cable Deployment Guidelines, and (ii) Management of Submarine Cable Incidents.[14] The Deployment Guidelines address the installation and repair of submarine cables in Singapore waters and have streamlined requirements, enabling

---

[10] Ministry of Foreign Affairs Singapore, Statement by Ambassador Vanu Gopala Menon on Agenda Item 74 (A): Oceans and the Law of the Sea, 7 December 2010, www.mfa.gov.sg/Overseas-Mission/New-York/Mission-Updates/Plenary/2010/12/press_201012.

[11] International Cable Protection Committee, "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables." 18 November 2022, www.ICPC-Gov't-Best-Practices-for-Cable-Protection--Resilience-Version-1.2-(English).pdf.

[12] Ibid

[13] Ibid

[14] Infocomm Media Development Authority, "Deployment and Repair of Submarine Cable Systems," www.imda.gov.sg/regulations-and-licensing-listing/deployment-and-repair-of-submarine-cable-systems.

damage to cables to be quickly repaired. The Incident Guidelines "provide licensees with an overview of the management of cable damage incidents in Singapore Port Limits and the Traffic Separation Scheme (TSS) zone."[15] It describes how cable operators may approach the Maritime and Port Authority of Singapore (MPA) to obtain information on vessels in the vicinity of the cable incidents.

Managing Competing Activities

The Incident Guidelines aim to prevent "cable damage incidents arising from anchoring and fishing activities".[16] Cable operators are strongly encouraged to put in place measures such as burying to better protect their cables. Singapore has established minimum spatial gaps between existing cables and other marine and coastal activities and when necessary, has established no-anchorage zones.[17] It also consistently updates its nautical charts to reflect cable locations.

Increasing Capacity and Geographic Diversity

Singapore has focused its efforts on increasing capacity and promoting geographic diversity in cable routes to ensure continued connectivity in the event of interruptions to data traffic, another best practice recommended by the ICPC. This promotes network resilience and reduces the risk of losses from a single event, "whether an earthquake, tsunami, a vessel anchor, fishing gear or terrorist attack."[18] This is why Singapore's goal to intensify the use of available space and landing resources to enable further diversification of submarine cable networks by operators is critical.[19]

---

[15] Ibid

[16] Ibid

[17] Further reading: Port Marine Circular No. 03 of 2017: Prohibition of Anchoring in the Straits of Malacca and Singapore, www.mpa.gov.sg/media-centre/details/prohibition-of-anchoring-in-the-straits-of-malacca-and-singapore

[18] International Cable Protection Committee, "Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables", 7.

[19] Ministry of Communications and Information, "Singapore's Digital Connectivity Blueprint", (n 3).

Challenges

Singapore has taken a proactive and practical approach to ensuring the protection of its cables. However, it faces two challenges. First, it is a geographically disadvantaged state that is unable to claim to full suite of maritime zones afforded to it under the 1982 UN Convention on the Law of the Sea (UNCLOS) due to proximity with its neighbours, Indonesia and Malaysia. In reality, there are few cable breaks in Singapore waters due to the small maritime space and the requirements that cables be buried. Moreover, there remain undelimited maritime areas with both Malaysia and Indonesia which limits what Singapore can do within these areas.[20]

Second, the multijurisdictional nature of cables poses considerable obstacles to the adoption of truly robust and effective measures to protect them from damage or interference. A significant risk to cables serving Singapore is from damage that occurs in spaces that are under the sovereignty or jurisdiction of other states or in areas beyond national jurisdiction. If other states that are connected to Singapore by submarine cables do not take effective measures to protect the cable segments that land in their territory or are located within their territorial waters or maritime zones under its national jurisdiction, there is realistically little that Singapore can do. Effective protection of cables requires both regional and international cooperation and cannot be done by Singapore alone.

Notwithstanding the need for multilateral cooperation, there are steps that Singapore can take as a starting point to strengthen both the physical and cybersecurity of submarine cables that link it to the rest of the world.

[20] For example, the east bound section of the TSS is in Indonesian waters, and parts of the west bound section of the TSS are in Malaysian waters. There may also be a small part of the TSS is waters that are contested.

Opportunities – Legal And Policy Recommendations

Strengthening Criminal Penalties for Damage to Submarine Cables

UNCLOS places certain rights and obligations on States Parties pertaining to the protection of submarine cables. Article 113 of UNCLOS obliges States Parties to adopt laws and regulations to provide that the breaking or injury of a submarine cable beneath the high seas or Exclusive Economic Zone (EEZ) either willfully or negligently by vessels registered in that State or persons subject to its jurisdiction are punishable offences. Article 113 provides a clear legal basis for Singapore to extend its criminal legislation to damage to cables that occur in the EEZ of other States and the high seas that are caused by Singapore-registered vessels and Singapore nationals. Examples of such national legislation can be found in Australia's Submarine Cables and Pipelines Protection Act 1963 and New Zealand's Submarine Cables and Pipelines Protection Act 1996.[21] Singapore should also consider implementing Article 113 of UNCLOS in its national legislation, as called for in the General Assembly resolution on oceans and law of the sea.[22]

In internal waters and territorial seas subject to coastal state sovereignty, coastal states may adopt laws and regulations to protect submarine cables pursuant to its sovereignty over these areas under UNCLOS and may also adopt laws and regulations relating to innocent passage of vessels in the territorial sea to protect submarine cables.[23]

Singapore has adopted legislation under its Telecommunications Act which makes damage of any cable used for telecommunications or interference with a system of public telecommunication licensee an offence punishable with a fine not exceeding $50,000 or imprisonment of not more than three years.[24] Similarly, under the Penal Code, acts of mischief that causes or is likely to cause a disruption to the provision of a key service which includes the provision of telecommunications is punishable with an imprisonment term of

[21] Further reading: Australia, Submarine Cables and Pipelines Protection Act, section 7, https://www.legislation.gov.au/C1963A00061/2005-09-20/text; New Zealand, Submarine Cables and Pipelines Protection Act 1996, section 11, https://www.legislation.govt.nz/act/public/1996/0022/latest/whole.html.

[22] United Nations, "General Assembly Resolution A/Res/77/248," 9 January 2023, para 190, documents.un.org/doc/undoc/gen/n23/004/78/pdf/n2300478.pdf?token=Qo3XgsUpeCV8fxQhzr&fe=true

[23] United Nations Convention on the Law of the Sea (UNCLOS), arts 2; 21 (c), https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

[24] Singapore, "Telecommunications Act," sections 61 and 68, https://sso.agc.gov.sg/Act/TA1999.

up to 10 years, or with a fine, or both.[25] These offences apply to acts within Singapore's territory and waters under its territorial sovereignty.

The question is whether such offences would also apply to acts of damage to cables that result in a disruption to telecommunications committed outside of Singapore. As illustrated by the recent high court decision of Ng Kok Wai v. Public Prosecutor, the Penal Code will only apply to offences committed outside of Singapore (including in the EEZ or high seas) if: (i) there is an applicable statutory provision that renders an act committed by an accused person outside of Singapore an offence under Singapore law, and (ii) there is an applicable statutory provision that confers authority on Singapore courts to try the accused person for the offence in question.[26] Whether Parliament intended the offences on disruption to telecommunications under the Penal Code to have extraterritorial effect and apply to acts outside of Singapore is ultimately a question of statutory interpretation.[27]

To remove all uncertainty, Singapore ought to deliberate the potential benefits of instituting legislation that criminalises damage to submarine cables that lands in Singapore, irrespective of the offender's nationality or the location of the incident, particularly if such damage leads to the disruption of telecommunications services to Singapore.

The extension of criminal legislation to the acts of foreign nationals or its own citizens outside its territory would be justified under the "effects doctrine" in international law which allows states to extend its criminal law to acts committed outside its territory if the "effects" of the acts are felt in its territory. There are several examples of Singaporean legislation that apply to acts that occur outside of Singapore, including the Computer Misuse Act, the Prevention of Corruption Act, and certain offences under the Penal Code. Making deliberate damage or interference with submarine cables that land in Singapore an offence regardless of where it occurs will go some way to deterring such acts and reiterate Singapore's commitment to the protection of submarine cables.

Designating Submarine Cable Infrastructure as Critical Infrastructure

Singapore should also designate cable landing stations and submarine cables as critical information infrastructure, as recommended by the ICPC. Singapore already has tools available under the Cybersecurity

[25] Singapore, "Penal Code," section 427, https://sso.agc.gov.sg/act/pc1871.
[26] Ng Kok Wai v. Public Prosecutor [2023] SGHC 306, para. 16, elitigation.sg/gd/s/2023_SGHC_306.
[27] Ibid, para 30.

Act[28] that, if explicitly stated to be applicable to cable landing stations and submarine cables that land in Singapore, would considerably strengthen the protection of cables.

The 2018 Cybersecurity Act is a comprehensive law that establishes a legal framework for managing and responding to cybersecurity threats. It specifies requirements for critical information infrastructure (CII) operators to implement cybersecurity measures and report security incidents. It also empowers the Cyber Security Agency (CSA) of Singapore to investigate and take action against cyberthreats, including the ability to compel CII operators to report cybersecurity incidents.

If a CII operator fails to comply with the requirements under the Act, they may face penalties that include fines, imprisonment, or the suspension/ revocation of licence to operate. The first schedule of the Cybersecurity Act includes a list of essential services provided by specific systems as listed in the Annex.

However, the specific systems that provide the essential services listed, while known to the authorities, are not identified in the Act and the identities of the specific CII operators has not been made public.

However, given the growing awareness worldwide about the need to further protect submarine cables and their associated landing stations, Singapore could consider explicitly designating:

1. Submarine cables and related landing stations as critical infrastructure;
2. Companies who operate submarine cables and landing stations as CII service providers and impose similar restrictions and requirements as applied to other CII operators in Singapore. In particular, the requirement to notify the relevant authority upon any break in service due to deliberate vandalism, an act of war, or accidental damage is key.

It is important to note the European Union (EU) has done just that. In December 2022, the EU issued the updated NIS2 Directive, whose objective is to strengthen the security and robustness of critical infrastructure. Submarine cables are highlighted in two parts of the Directive. Clause 97 stipulates that “incidents affecting undersea communications cables should be reported to the Computer Security Incident Response Team or, where

[28] Singapore, “Cybersecurity Act 2018,” sso.agc.gov.sg/Acts-Supp/9-2018/.

applicable, the competent authority"[29] and that "the national cybersecurity strategy should, where relevant, take into account the cybersecurity of undersea communications cables and include a mapping of potential cybersecurity risks and mitigation measures to secure the highest level of their protection."[30] In the same Directive, there is an exhortation to Member States of the EU that as part of their national cybersecurity strategy, they should adopt policies "related to sustaining the general availability, integrity and confidentiality of the public core of the open internet, including, where relevant, the cybersecurity of undersea communications cables."[31] These developments reflect the importance of the nexus between cybersecurity and the physical infrastructure that underpin cyberspace and is an important consideration as Singapore continues to strengthen its policies on the protection of submarine cables.

Enhancing Inter-Agency Cooperation

The protection of submarine cables requires a whole-of-government (WoG) approach that involves several government agencies, including the Ministry of Communications and Information, IMDA, MPA, Attorney-General's Chambers, Ministry of Defence, Cyber Security Agency, and Ministry of Home Affairs. Inter-agency cooperation could include developing common policies, information sharing, establishing coordination mechanisms in cases of serious disruptions to the transmission of data with assigned roles and responsibilities, and conducting joint exercises and training.

Enhancing Public-Private Partnerships

As nearly all submarine cables globally are owned and/or operated by companies, collaboration between cable owners/operators and governments to protect cables is critical. While collaboration can take a multitude of forms, the following recommendations represent an important starting point.

First, as observed by other commentators, government and industry must work together to define and agree upon approaches to manage and mitigate the risk to submarine cables.[32] To initiate comprehensive cable protection efforts, an initial dialogue involving all relevant stakeholders is recommended. This should involve all relevant stakeholders, including all government agencies that have a mandate for protecting cables.

---

[29] European Union, "Directive (EU) 2022/2555 of 14 December 2022," eur-lex.europa.eu/eli/dir/2022/2555.

[30] Ibid

[31] Ibid, article 7, clause (d).

[32] Joseph Keller, "The Disconnect on Undersea Cable Security," Lawfare, 7 May 2023, www.lawfareblog.com/disconnect-undersea-cable-security.

Second, another area of collaboration is the facilitation of annual tabletop exercises for operators to improve their readiness. A tabletop exercise is a simulated scenario that closely resembles a genuine event that can negatively affect a country's or an entity's business or operational continuity. Tabletop exercises are best run with a multitude of stakeholders to raise awareness of the importance of readiness. A simulated incident of damage to cables or landing stations or cyberattacks against the NMS could be run to test the responses of the stakeholders involved, including the cable operators, relevant government agencies, submarine cable repair companies etc.

Third, collaboration should also include timely sharing of information. For example, cable companies should report all observed malicious activity along with details of their response (e.g., repair damage and restore services) to the IMDA. As the lead agency, IMDA would then be responsible for disseminating the information to other relevant agencies.

Fourth, government and industry should also explore the possibility of collaboration on specialised research and development in the areas of submarine cable protection, detection of faults, and repair.

Enhancing Regional Cooperation

Regional co-operation is crucial to protecting submarine cables effectively. Singapore, being a global submarine cable hub, is well-placed to drive this effort by working with other Southeast Asian states that have convergent interests in enhancing digital connectivity and the concomitant benefits that such connectivity brings to their populations. Singapore can leverage existing regional mechanisms to encourage cooperation on submarine cables.

ASEAN Cooperation

Since 2013, ASEAN has, through the Digital Ministers Meetings (ADGMIN), recognised the significance of submarine cables to regional and global connectivity and agreed to intensify regional cooperation to protect submarine cables from man-made and natural disasters.[33] To date, ADGMIN initiatives have focused on expediting the restoration of telecommunications by reducing regulatory requirements for repair, which is undoubtedly a critical component of the security of submarine cables. For example, in 2019, the

[33] Infocomm Media Development Authority, "Singapore Declaration: Connecting Communities, Co-Creating Possibilities 13th TELMIN", para. 9, 14-15 November 2013, www.imda.gov.sg/-/media/imda/files/inner/about-us/newsroom/media-releases/2013/1511_jointrelease/singaporedeclaration.pdf.

ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables were adopted to simplify the permit application process for the repair of submarine cables in ASEAN countries.[34] The ASEAN Digital Masterplan 2025 also notes the same and suggests that "ASEAN may consider commissioning a project to identify best practices and agreement to a pan-ASEAN set of processes and rights" to facilitate the repair of submarine cables.[35]

No actions have been taken at the ASEAN level regarding the protection of submarine cables from damage or interference, most likely because it is unclear which agency is responsible for the protection of cables in individual ASEAN member states. ADGMIN falls under the purview of the ASEAN Economic Pillar, whereas security issues are addressed through the efforts of the Ministers of Defence, Foreign Affairs, or Home Affairs, that operate under the auspices of the Political-Security Pillar. However, as is the case within governments, ensuring the resilience of submarine cable systems requires coordination amongst different sectoral bodies in ASEAN. Such cross-sectoral coordination within ASEAN has the potential to considerably strengthen the security of submarine cables holistically, including ensuring expeditious repair of cables as well as other measures aimed at information sharing on possible incidents or the possibility of patrols around key submarine cable routes.

Information Fusion Centre

Another possible area for regional cooperation is through information gathering and sharing on submarine cable issues through the International Fusion Centre (IFC), a regional Maritime Security (MARSEC) centre. The IFC's role is to ensure "safe and secure seas through timely and comprehensive information sharing with our partners."[36] The IFC has "been at the forefront of providing actionable information to cue responses by regional and international navies, coast guards and other maritime agencies to deal with the full range of MARSEC threats and incidents."[37]

Although these threats and incidents include conventional ones such as armed robbery and piracy, the IFC is well placed to expand this role to include the collection and processing of cable incident reporting. In recent

---

[34] ASEAN, "ASEAN Guidelines for Strengthening Resilience and Repair of Submarine Cables in the ASEAN Region," https://asean.org/wp-content/uploads/2012/05/ASEAN-Guidelines-for-Strengthening-Resilience-and-Repair-of-Submarine-Ca....pdf

[35] ASEAN, "ASEAN Digital Masterplan 2025," asean.org/wp-content/uploads/2021/09/ASEAN-Digital-Masterplan-EDITED.pdf.

[36] Information Fusion Centre, "About IFC", https://www.ifc.org.sg/ifc2web/app_pages/User/commonv2/aboutusMain.cshtml

[37] Ibid

years, the IFC has widened its "range of partnerships to include military and enforcement agencies as well as shipping companies."[38] In addition to the IFC's traditional role of providing assistance to ships in distress, their function as facilitators can further enhance the coordination of information sharing and timely responses to damage to cables.

Singapore may wish to consider recommending that governments in the region cooperate with the cable industry and with each other through the IFC. While the modalities of such co-operation warrant further research, such cooperation could consist of four elements. First, co-operating states would require cable companies to immediately notify designated government focal points in the landing states when there is a fault in a cable landing in that state, and the approximate location of the fault. Second, the government focal points would notify their representative at the IFC of the time and approximate location of the break. Third, the IFC would use maritime automatic identification system data, satellites, and other mechanisms to identify ships that are present at the location of the cable break. Fourth, if there are grounds for suspecting that the cable may have been intentionally cut, the IFC will notify naval vessels of its member states that are in the area and request them to investigate.

Conclusion

Given the criticality of their purpose and impact on economies, submarine cables must be maintained in a state of continuous functionality to the greatest extent possible. The rising number of cable damage incidents globally, both deliberate and accidental, has made it clear that should there be an incident of damage or interference with critical infrastructure such as cables, responses should be prompt and well coordinated. Singapore has made significant strides in strengthening the robustness of its submarine cables, but there are further opportunities for reinforcing the security of undersea cables as it continues to expand its capacity. These include strengthening criminal penalties for damage to undersea cables, explicitly designating undersea cables as critical infrastructure, enhancing cooperation and coordination between the relevant government agencies, enhancing public-private partnerships, and taking the lead in driving regional cooperation on this issue. These forms of collaboration in working towards ensuring the physical, digital, and economic resilience of the undersea communications cable sector are critical to boosting Singapore's digital security.

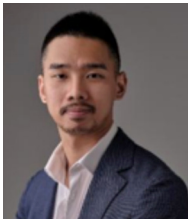
[38] Ibid

About the Authors

Robert Beckman is the Co-Head of the Ocean Law and Policy programme of the Centre for International Law (CIL) and was the founding Director of CIL. He is also an Emeritus Professor at the NUS Faculty of Law, where he taught Ocean Law & Policy for many years. He is also a Senior Advisor to the Maritime Security Programme of the Institute for Defence & Strategic Studies (IDSS) at the S Rajaratnam School of International Studies (RSIS) at Nanyang Technological University (NTU). He has published widely on ocean law and policy issues, including submarine cables.

Asha Hemrajani is Senior Fellow, at the Centre of Excellence for National Security (CENS) at RSIS where her research covers information and data security, telecommunications, critical infrastructure, Artificial Intelligence, and emerging technologies. She has over 20 years of industry experience in tech and was formerly a member of the Board of Directors at ICANN, the global domain names regulator. Asha holds a degree in Electrical Engineering and a ModularMaster in Cybersecurity.

Dr Tara Davenport is an Assistant Professor at the Faculty of Law, National University of Singapore (NUS), Co-Head of the Oceans Law and Policy Programme at the Centre for International Law at NUS, and Deputy Director of the Asian-Pacific Centre for Environmental Law at NUS. She has written on the South China Sea disputes, submarine cables, deep seabed mining and maritime security issues, and is also the co-rapporteur for the International Law Association's Study Committee on Submarine Cables and Pipelines.



Sean Tan is a Senior Analyst at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Prior to joining CENS, he was based at the Centre for Information Integrity and the Internet (IN-cube) at the Wee Kim Wee School of Communications and Information, NTU. In addition to subsea cables, Sean's current areas of research include online harms, disinformation, and foreign interference and hybrid threats.

About the Centre of Excellence for National Security (CENS)

The **S. Rajaratnam School of International Studies (RSIS)** is a global think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education, and networking, it produces research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.

CENS is a research unit of RSIS at the Nanyang Technological University, Singapore. Established on 1 April 2006, CENS *raison d'être* is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues. CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs.

For more details, please visit www.rsis.edu.sg and www.rsis.edu.sg/cens. Join us at our social media channels at www.rsis.edu.sg/rsis-social-media-channels or scan the QR code.

RSiS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University, Singapore

Nanyang Technological University, Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg