VOLUME 9 · ISSUE 03

BALSILLIE PAPERS

Weaponized Interdependence or Shared Resilience? Rethinking Undersea Cable Security in a Fragmenting Order

Brendon J. Cannon

APRIL 28, 2026

Undersea communication cables have historically operated within an interconnected global system characterized by cooperative redundancy and routing agreements, despite episodic geopolitical contestation. Intensifying great power rivalry, however, is driving efforts to reroute cables, exclude vendors and build "trusted corridors." Drawing on recent incidents and policy initiatives, this paper argues that emerging bifurcation threatens to weaken resilience by reducing redundancy, narrowing routing options and increasing incentives for disruption. While verified sabotage remains limited, securitization discourse is reshaping network design in ways that may prove counterproductive. The paper concludes with pragmatic policy options — including minilateral coordination and a scalable regional seas approach — to strengthen cable security while preserving interconnection.

INTRODUCTION

Undersea communication cables are the backbone of the global digital economy. Laid across the seabed in dense, intersecting routes, they carry more than 95 percent of all intercontinental data traffic, enabling everything from financial transactions and cloud services to online meetings and secure communications. As global data demand skyrockets, so too does our reliance on this largely invisible infrastructure.

Undersea cables are fibre-optic cables sheathed in layers of steel wire armouring, copper conductors and a waterproof polyethylene jacket, and about the circumference of a garden hose. They transmit light signals through bundled glass strands at nearly the speed of light. From one end of an ocean to another, they terminate at cable landing stations — onshore facilities located within a state's sovereign jurisdiction. Here, the cables connect to terrestrial fibre, data centres and the broader national communications network.[i]

For decades, the undersea cable ecosystem has proven remarkably resilient, particularly in peacetime and outside moments of major interstate war. Redundant cable connections, reciprocal routing, cost-sharing for repairs, and public–private operating practices have ensured security and reliability.[1]

What follows explains how the increased sabotage and securitization of cables have resulted in fragmentation of the cable ecosystem — and why some responses risk undermining the very resilience that has served the system well.

FROM OBSCURITY TO SECURITIZATION

Interdependence is now at risk for two reasons.

First, instances of cable sabotage, albeit infrequent, are increasing. In the Red Sea, at least four cables were cut in early 2024, amid escalating attacks on international shipping and maritime infrastructure by the Houthi in Yemen. Although the cable cuts were officially attributed to anchor drag, the circumstances and location of the cuts raised suspicions about intentional breakage, especially after two more cables were severed in September 2025 in the Red Sea near Jeddah, Saudi Arabia.[2]

In the Pacific near Taiwan, in early 2023, repeated cable disruptions near the Matsu Islands were initially framed by Taiwan as possible deliberate interference involving Chinese vessels,[3] although no formal sabotage determination was made. More recently, incidents near Penghu — Taiwan's main offshore archipelago — have reinforced concerns about grey-zone pressure on digital infrastructure.[4] While these

[i] For purposes of espionage or sabotage, the easiest place to tap a cable is at a landing site. But cutting a cable at a landing station is also an attack on a state's sovereign territory and would represent an escalation of conflict that is at odds with the grey zone tactics of what some see as recent cable sabotage in the Baltic Sea.

cases have not resulted in sabotage convictions under international law, they have nevertheless shaped threat perceptions, policy planning and defensive postures. On the other side of Eurasia, two separate cable systems were damaged in the Baltic Sea in late 2023 — one linking Finland to Estonia, the other connecting Sweden and Estonia.[5] The following year, in November, the C-Lion1 cable connecting Finland and Germany was severed.[6] Almost at the same time, and also in the Baltic, the BCS East–West Interlink cable running between Lithuania and Sweden was also cut.[7] This affected only these two states, with Lithuania the more affected because the cable supplies one-third of its internet bandwidth. Several governments and security analysts have publicly framed these incidents as sabotage linked to hybrid operations.[8]

Second, as great power rivalry intensifies, a growing number of states and technology companies are rethinking how and where cables should be laid and how best to secure them against sabotage and espionage.[9] This strategic decoupling — part of wider efforts by Canada, the European Union, Japan, the United States and others to de-risk from China — signals a shift toward bifurcation that leads away from the existing interconnected, global undersea cable ecosystem. This shift is engendered by the growing distrust between rivals in the international system and the quest by certain states (Australia, Japan, the United Kingdom and the United States) and groups of states (such as the European Union and the Quad — Australia, India, Japan and the United States) to improve the security of critical infrastructure.

The motivation to bifurcate and fragment undersea cable interconnectivity and redundancy, however, rests on flawed assumptions. Fragmentation will not only create new vulnerabilities but also undermine the resilience that has made cables largely secure in the first place.

CABLES AS SECURITY INFRASTRUCTURE

For decades, undersea cables operated in relative obscurity, treated as technical infrastructure managed by a mix of private consortia and lightly regulated by national or international regimes such as the 1884 Convention for the Protection of Submarine Telegraph Cables and the 1982 UN Convention on the Law of the Seas. That is no longer the case. As the geopolitical temperature rises, undersea cables are being securitized by state actors,[ii] recast not just as data pipelines but as critical and strategic infrastructure whose control, protection or disruption can do serious damage to the national security of a state or group of states.[10]

[ii] Securitization is the process by which influential actors — such as presidents, monarchs and policymakers — elevate issues to security concerns by declaring, often through public statements, that a particular entity or infrastructure faces an existential threat. In doing so, they convince an audience (whether the general public or a specific segment) that extraordinary measures are necessary to counter this danger. For more on securitization and the theory behind it, see Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis* (Lynne Rienner Publishers, 1998).

In recent years, governments have begun integrating cable protection into broader frameworks of economic and national security.[11] In the United States, for instance, cable vulnerabilities are now discussed in the context of strategic competition with China alongside semiconductor chips, deep-sea mining and rare earth minerals.[12] Accordingly, in 2020, the United States launched the Clean Network initiative, which asked countries and companies to abide by a set of shared principles in technology adoption, data privacy and security practices.[13] It also built on previous efforts by Washington to encourage states to choose cable operators and builders that were non-Chinese.

In practical terms, this has steered new consortia away from Chinese vendors and jurisdictions perceived as high risk. In September 2025, the US House of Representatives passed legislation to tighten US control over critical fibre optic undersea cable equipment, in an attempt to prevent rivals such as China from acquiring technologies used in undersea cables.[14]

Parallel developments have occurred within multilateral and minilateral frameworks. In May 2023, the Quad Partnership for Cable Connectivity was announced. This was meant to underscore the strategic importance of secure, diversified digital infrastructure across the Indo-Pacific. Framed as a regional development priority, the initiative also reflected a growing perception of cables as potential targets of coercion and disruption and further embedded them within the broader context of strategic competition, rivalry and shifting distributions of global power.[15]

Taking the lead in the Quad's effort, Australia stood up a Cable Connectivity and Resilience Centre to share best practices and provide technical assistance across the Indo-Pacific.[16] Japan, meanwhile, has elevated cables within its economic security agenda, backing budget measures to diversify routes and landing stations, as well as, more recently, considering subsidies for cable-laying ships to secure national capacity in deployment and repair.[17]

In Europe, NATO has launched the Critical Undersea Infrastructure Network and established the Maritime Centre for Security of Critical Undersea Infrastructure to coordinate efforts across allies. In the Baltic region, a memorandum of understanding signed by NATO members and the European Union commits to enhanced cooperation in defending undersea infrastructure.[18]

By elevating cables within national and minilateral security agendas, states have increased the political salience of the network — raising the stakes of disruption even as protection efforts expand. But these efforts to secure cables have also extended into elite policy discourse and academic commentary that explicitly securitizes cables as objects under threat that need securing. Policy and scholarly debates[19] increasingly invoke Henry Farrell and Abraham Newman's "weaponized interdependence" framework[20] to interpret cable exposure — especially the risks of monitoring (panopticon) and denial (chokepoint) associated with dependence on rival-linked infrastructure. Academics, while offering more nuance, nevertheless draw on the logic of weaponized interdependence to argue that states should decouple from infrastructure tied to strategic competitors.[21] A similar logic of avoiding exposure and reducing risk — no

matter the cost — has begun to surface in policy circles pushing bifurcation of cable routes. In practice, this has encouraged "trusted route" planning that skirts contested waters and rival jurisdictions.

Accordingly, governments and companies have begun proposing and funding new cable routes that avoid landfall on the sovereign territories of strategic competitors. The Echo and Apricot cable systems, jointly backed by Google and Meta, are designed to avoid landfall in China and routing through parts of the South China Sea.[22] More broadly, big tech firms such as Google, Meta, Microsoft and Amazon have become the dominant financiers of new cable deployments, driven by escalating demand for data capacity, control and security.[23] They have also been pressured by the US government to avoid using Chinese-made technologies in undersea cables.[24] This matters because the infrastructure at stake is predominantly privately owned and operated; as Lars Gjesvik shows,[25] contemporary network coercion often works through private corporate infrastructure and the regulation of firms, rather than through direct state ownership of the underlying networks.

SECURITIZATION AND THE BIFURCATION TRAP

This turn to route avoidance and trusted corridors is often justified through the logic of weaponized interdependence: policymakers increasingly presume that undersea cables will generate the familiar effects associated with network power — namely, chokepoint leverage, heightened exposure to coercion or denial, and strategic vulnerability through dependence on rival-linked infrastructure. These concerns are not unfounded: espionage risks associated with telecommunications infrastructure are well documented, and competition over cable supply chains reflects broader efforts by states to manage dependency, influence standards and limit exposure to rival-linked firms. For submarine cables, however, those effects are frequently overstated in peacetime conditions, because dense redundancy, cooperative routing arrangements and the boomerang costs of disruption make the system difficult to weaponize without wide collateral impact. It is this extension of network power logic — rather than the operational characteristics of cables themselves — that has encouraged bifurcation.

The cumulative effect of these efforts and the securitization of cables is paradoxical. While intended to insulate networks from coercion, the building of corridors that avoid connections and landfall with certain countries risks hardening the system into rival blocs. Bifurcation is likely to undermine the system's core resilience, which has long derived from interdependence, such as route diversity, reciprocal restoration and an interlinking architecture that cushions shocks and keeps data flowing. More specifically, bifurcation does not refer to a single process but to a layered reconfiguration of the undersea communication cable ecosystem. It encompasses the fragmentation of cable routes to avoid specific jurisdictions, the exclusion of certain vendors and suppliers, the segmentation of financing and ownership structures, and the emergence of parallel governance and security frameworks.

These shifts are costly. Building parallel routes, excluding suppliers and maintaining duplicated landing infrastructure raises capital and operational expenditures, lengthens deployment timelines, and reduces

economies of scale. For private firms — which finance most new cable systems — these costs translate into higher prices, constrained redundancy, or delayed upgrades, particularly outside core markets.[26] Cost pressures also matter for security outcomes. Expensive, politically constrained networks tend to be thinner, more brittle and slower to repair, especially in regions with limited traffic volumes. In this sense, bifurcation risks trading perceived geopolitical insulation for reduced operational resilience.

The temptation to "nationalize" data routes is not new. It harks back to the old imperial cable networks built by imperial powers over a century ago. Russia's announcement of efforts to establish a sovereign internet — routing domestic traffic through state-controlled exchanges and limiting foreign linkages — illustrates the short-sightedness of such strategies. Rather than insulating the system from external risk, such strategies create smaller, bounded networks that transmit less data and are easier to tap, sabotage and isolate.[27] The same holds true for undersea cables: a bounded cable system sacrifices redundancy in the name of security and thereby heightens vulnerability to sabotage because potential adversaries will no longer share any blowback effect. In short, fragmentation narrows options and magnifies shocks; interconnection distributes risk and dampens escalation incentives.

Available evidence and experience suggest that the current, interconnected system can, under peacetime conditions, reduce incentives for deliberate disruption, insofar as interference risks widespread collateral effects across multiple states and commercial actors. This can include, in some cases, the initiator.[28] Severing one system can degrade bandwidth and increase latency not only for an intended rival, but for multiple third parties, including, in some cases, the saboteur itself. The resulting boomerang effect acts as a deterrent against deliberate sabotage, particularly in peacetime. Conversely, when networks are segmented into "ours" and "theirs," the anticipated blowback diminishes, making disruption comparatively more attractive.

This does not imply that interdependence guarantees restraint, nor that actors will always avoid self-harm; rather, it indicates that under conditions of dense redundancy and shared routing, undersea cables are less readily weaponized as instruments of denial than is often assumed. Adding to this, empirical evidence of legally verified sabotage against undersea communication cables, to date, remains limited. Most cable cuts still result from routine causes — anchoring, fishing gear or natural events — rather than hostile acts.[29] At the same time, several recent incidents — particularly in the Baltic Sea and around Taiwan — have been politically framed as potential acts of deliberate interference, even where definitive attribution has proven elusive. This ambiguity is not incidental: the depth, remoteness and technical complexity of cable systems make conclusive forensic determination exceptionally difficult. As a result, undersea cable incidents increasingly operate in a grey zone, where suspicion, securitization and strategic signalling matter as much as legal proof.

Nevertheless, in open, highly networked systems such as the North Sea, Mediterranean or the western Pacific, the impact of any single cable break is limited. While damage can cause temporary latency and service degradation, redundancy and routing agreements among operators generally ensure continuity of

data flow. Importantly, data does not flow automatically through the network: rerouting during disruptions depends on pre-existing commercial agreements, capacity and interoperability among operators, rather than on physical connectivity alone. Recent Baltic disruptions, for instance, also prompted data rerouting with limited functional impact. This underscored cable operators' and the ecosystem's adaptive capacities without minimizing the risks of multiple, simultaneous incidents.[30] The same interdependence that securitization discourse now frames as vulnerability has, in practice, functioned as resilience.[31]

Rather than pursuing fragmentation, a more effective response would preserve and enhance interconnection, geographic dispersion and cooperative governance. These factors remain the strongest bulwarks against sabotage, systemic failure and strategic miscalculation.

AVOIDING FRAGMENTATION; MAINTAINING RESILIENCE

Dense, redundant networks enable rerouting and limit disruption. Connectivity — not bifurcation — underwrites resilience, while fragmentation risks brittleness. The policy prescriptions below outline pragmatic steps to strengthen cable security without sacrificing interconnection.

1. **National actor mapping and points of contact**: Identify who does what in cable security — from regulators and navies to private operators and repair contractors — to ensure rapid coordination during outages.

2. **Region-specific repair and monitoring protocols**: Catalogue the locations, capacities and mobilization times of cable repair ships and formalize response frameworks between operators and governments.

3. **Minilateral cooperation frameworks**: Encourage small, like-minded groupings (e.g., the Quad) to harmonize standards, share intelligence and coordinate repair logistics.

4. **Regional seas approach as a scalable governance model**: Maritime security is spatially variant and thus regionally anchored security strategies across multiple maritime scales — coastal, zone, basin — are optimal.[32] If we segment the seas into zones, actors can coordinate in contextually meaningful maritime zones. This "regional seas" approach — treating maritime security as basin-specific, coordinating states and operators within contextually meaningful sea spaces to manage cable protection, monitoring and response in ways that complement global governance — requires creativity and could include accepted basins such as the Baltic Sea or the Sea of Japan.[33] Alternatively, regional seas could be conceptualized around existing undersea cable routes — such as a Pacific loop linking Hawaii, Guam, Japan, Taiwan and the Philippines. This would offer a geographically bounded governance framework, but one that also fits into global governance frameworks.

CONCLUSION

Undersea cables have moved from invisibility to the centre of geopolitical discourse, encouraging trusted corridor policies that risk hardening the system into rival blocs. A safer path is to strengthen interdependence while improving protection through mapped points of contact, repair capacity, minilateral coordination and a scalable regional seas approach.

END NOTES

[1] Georgia Bafoutsou, Maria Papaphilippou and Marnix Dekker, "Subsea Cables — What is at Stake?," European Union Agency for Cybersecurity (ENISA), 2023, https://ec.europa.eu/newsroom/cipr/redirection/item/806206/en/2357.

[2] Eleanor Watson, "Ship sunk by Houthis likely responsible for damaging 3 telecommunications cables under Red Sea," *CBS News*, March 6, 2024, https://www.cbsnews.com/news/houthis-ship-cutting-red-sea-telecommunications-cables; see also Cody Combs and John Dennehy, "Cuts to Red Sea internet cables were probably accidental, experts say," *The National*, September 10, 2025, https://www.thenationalnews.com/future/technology/2025/09/09/red-sea-internet-cables-cut-outage.

[3] Wayne Chang, "Taiwan detains Chinese-crewed ship suspected of cutting undersea cable," CNN, February 26, 2025, https://edition.cnn.com/2025/02/25/asia/taiwan-detains-ship-undersea-cable-intl-hnk/index.html.

[4] Ibid.

[5] Andrius Sytas and Anne Kauranen, "Three Baltic pipe and cable incidents 'are related', Estonia says," *Reuters*, October 27, 2023, https://www.reuters.com/world/europe/three-baltic-pipe-cable-incidents-are-related-estonia-says-2023-10-27.

[6] Johan Ahlander, Essi Lehto and Andrius Sytas, "Two undersea cables in Baltic Sea cut, Germany and Finland fear sabotage," *Reuters*, November 19, 2024, https://www.reuters.com/business/media-telecom/telecoms-cable-linking-finland-germany-likely-severed-owner-says-2024-11-18.

[7] Elisabeth Braw, "How the Baltic Sea nations have tackled suspicious cable cuts," Atlantic Council, November 26, 2025, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-baltic-sea-nations-have-tackled-suspicious-cable-cuts.

[8] Klaudia Maciata, "Fortifying the Baltic Sea — NATO's defence and deterrence strategy for hybrid threats," *NATO Review*, May 5, 2025, https://www.nato.int/docu/review/articles/2025/05/05/fortifying-the-baltic-sea-natos-defence-and-deterrence-strategy-for-hybrid-threats/index.html.

[9] Sophia Besch, Jane Munga, Elina Noor and Erik Brown, "How Different Regions Are Rethinking Their Approaches to Subsea Cables," *Carnegie Emissary*, June 5, 2025, https://carnegieendowment.org/emissary/2025/06/subsea-cable-approaches-lessons-europe-africa-southeast-asia.

[10] Brendon J. Cannon, "Building and deconstructing three levels of undersea cable security in a rivalrous world," Rabdan Security and Defence Institute, January 21, 2025, https://rsdi.ae/en/publications/building-and-deconstructing-three-levels-of-undersea-cable-security-in-a-rivalrous-world.

[11] See, for example, Sophia Besch and Erik Brown, "Securing Europe's Subsea Data Cables," Carnegie Endowment for International Peace, 2024, 1–38; Samuel Bashfield, "Defending Seabed Lines of Communication," *Australian Journal of Maritime & Ocean Affairs*, July 2024: 1–13, https://doi.org/10.1080/18366503.2024.2363607.

[12] See, for example, National Economic Council and National Security Council, 2021–2024 *Quadrennial Supply Chain Review*, The White House: 1–383.

[13] Keith Krach and Meg Rithmire, "How the Clean Network Changed the Future of Global Technology Competition," *HBR* (*Cold Call*, Episode 158), October 5, 2021, https://hbr.org/podcast/2021/10/how-the-clean-network-changed-the-future-of-global-technology-competition.

[14] Jericho Casper, "House Approves Undersea Cable Control Act," *Submarine Telecoms Forum*, September 3, 2025, https://subtelforum.com/house-approves-undersea-cable-control-act.

[15] Brendon J. Cannon, "Undersea cable security in the Indo-Pacific: Enhancing the Quad's collaborative approach," *Marine Policy* 171 (January 2025): 106415, https://doi.org/10.1016/j.marpol.2024.106415.

[16] Samuel Bashfield and Anthony Bergin, "Options for Safeguarding Undersea Critical Infrastructure: Australia and Indo-Pacific Submarine Cables," Australian National University, National Security College, Policy Options Paper no. 25, June 14, 2022, https://nsc.anu.edu.au/content-centre/research/options-safeguarding-undersea-critical-infrastructure-australia-and-indo.

[17] Erin L. Murphy and Thomas Bryja, "The Strategic Future of Subsea Cables: Japan Case Study," Center for Strategic and International Studies, August 26, 2025, https://www.csis.org/analysis/strategic-future-subsea-cables-japan-case-study.

[18] Klaudia Maciata, "Fortifying the Baltic Sea — NATO's defence and deterrence strategy for hybrid threats," *NATO Review*, May 5, 2025, https://www.nato.int/docu/review/articles/2025/05/05/fortifying-the-baltic-sea-natos-defence-and-deterrence-strategy-for-hybrid-threats/index.html.

[19] Daniel F. Runde, Erin L. Murphy and Thomas Bryja, "Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition," Center for Strategic and International Studies, August 16, 2024, https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition.

[20] Henry Farrell and Abraham L. Newman, "Weaponized interdependence: How global economic networks shape state coercion," *International Security* 44, no. 1 (2019): 42–79.

[21] See Segal's critique of Huawei and 5G networks. Adam Segal, 2021, "Huawei, 5G, and Weaponized Interdependence," in *The Uses and Abuses of Weaponized Interdependence*, eds. Daniel W. Drezner, Henry Farrell and Abraham L. Newman (Brookings Institution Press, 2025), 149–166.

[22] Murphy and Bryja, "The Strategic Future of Subsea Cables."

[23] Christopher Mims, "Google, Amazon, Meta and Microsoft Weave a Fiber-Optic Web of Power," *The Wall Street Journal*, January 15, 2022, https://www.wsj.com/business/telecom/google-amazon-meta-and-microsoft-weave-a-fiber-optic-web-of-power-11642222824.

[24] Anna Ribeiro, "Congress presses Google, Meta, Microsoft, Amazon over Chinese tech in US bound subsea cables," *Industrial Cyber*, July 22, 2025, https://industrialcyber.co/critical-infrastructure/congress-presses-google-meta-microsoft-amazon-over-chinese-tech-in-us-bound-subsea-cables.

[25] Lars Gjesvik, "Private infrastructure in weaponized interdependence," *Review of International Political Economy* 30, no. 2 (2023), 722–746.

[26] Magdalena Petrova, "Underwater cables are a vital piece of the AI buildout and internet — investment is booming," *CNBC*, November 8, 2025, https://www.cnbc.com/2025/11/08/big-tech-ai-underwater-cables.html.

[27] Cannon, "Building and deconstructing three levels of undersea cable."

[28] Brendon J. Cannon, Kazuki Matsuo and Moeri Matsuda, "Mapping undersea cable risk from bathymetry to geopolitics: Evidence-based rankings and tailored resilience strategies," *Marine Policy* 186 (April 2026): 107012.

[29] Kristi Govella, "Undersea cables, geoeconomics, and security in the Indo-Pacific: Risks and resilience," *Marine Policy* 180 (October 2025): 106809, https://doi.org/10.1016/j.marpol.2025.106809.

[30] Emile Aben, "Does the Internet Route Around Damage? Baltic Sea Cable Cuts," *RIPE Labs*, November 20, 2024, https://labs.ripe.net/author/emileaben/does-the-internet-route-around-damage-baltic-sea-cable-cuts.

[31] Christian Bueger and Tobias Liebetrau, "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network," *Contemporary Security Policy* 42, no. 3 (2021): 391–413, https://doi.org/10.1080/13523260.2021.1907129.

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

[33] Cannon, Matsuo and Matsuda, "Mapping undersea cable risk from bathymetry to geopolitics."

Brendon J. Cannon is an academic with expertise in international security, geopolitics, and the Indo-Pacific, with a particular focus on global power distributions, regional security dynamics, and the interplay between security and emerging technologies. His research examines great power rivalry, security alignments, and classical geopolitics across the Euro-Atlantic and Indo-Pacific regions. His current research explores transformative technologies, most notably the security and governance of the global undersea cable network that underpins our knowledge economy, to include AI. Cannon is a Fellow at the Balsillie School of International Affairs and was most recently a Balsillie Scholar (June-July 2025).

BALSILLIE PAPERS

ISSN 2563-674X • doi:10.51644/BAP93

balsilliepapers.ca