THREAT ANALYSIS

Recorded Future®

By Insikt Group®

July 17, 2025

Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity

Geopolitical tensions, particularly Russia's war against Ukraine and China's coercive activity targeting Taiwan, are very likely driving sabotage threats to submarine cable infrastructure.

Lack of redundancy in cable networks, lack of diversity of cable routes, and limited global repair capacity very likely increase the risk of significant outages from cable damages.

Public-private partnerships improving repair capabilities, monitoring and security measures, and cable system resilience are critical to preventing major connectivity disruptions from cable damages.

Executive Summary

Events over the last eighteen months indicate that the risk environment for submarine cables has very likely escalated, and the threat of state-sponsored malicious activity targeting submarine cable infrastructure is likely to rise further amid heightened geopolitical tensions. Insikt Group's assessment of the current risk environment for submarine cables aligns with the findings of our 2023 assessment, which highlighted the convergence of geopolitical, physical, and cyber threats. Based on an analysis of 44 publicly reported cable damages occurring in 32 distinct groupings in 2024 and 2025 (**Appendix A**), Insikt Group assesses that three factors in the submarine cable ecosystem — lack of redundancy in cable networks, lack of diversity of cable routes, and limited global repair capacity — very likely increase the likelihood of significant outages from damages. Regions with low redundancy, such as parts of West and Central Africa, isolated Pacific islands, and certain secondary European routes, are more likely to suffer disproportionate impact from cable damage, especially when geopolitical tensions coincide with infrastructure constraints.

While accidents will very likely continue to cause the majority of day-to-day interruptions, recent incidents in the Baltic Sea and around Taiwan indicate that submarine cable systems remain vulnerable to threats such as anchor dragging, which states can use as a low-sophistication tactic to target adversaries' critical infrastructure while maintaining plausible deniability. Insikt Group identified four incidents involving eight distinct cable damages in the Baltic Sea and five incidents involving five distinct cable damages around Taiwan in 2024 and 2025. At least five of these nine incidents were attributed to ships dragging their anchors, including four Russia- or China-linked vessels operating under suspicious circumstances or with opaque ownership structures, although the resulting investigations have highlighted the difficulty of attributing cable cuts to state-sponsored sabotage. Such campaigns attributed to Russia in the North Atlantic–Baltic region and China in the western Pacific are likely to increase in frequency as tensions rise, leveraging deniable tactics in both shallow and deep water to apply political pressure without overt escalation.

Without a significant expansion of dedicated repair vessels, repair capacity is very likely to lag behind demand, pushing median restoration times beyond the current 40-day benchmark. National permitting delays and conflict zone access restrictions will likely extend repair times further, making streamlined diplomatic clearance processes an increasingly critical element of submarine cable resilience. Satellite and microwave links will almost certainly remain partial stop-gaps, restoring only a fraction of lost bandwidth during major outages. To mitigate these challenges, joint public-private partnerships investing in repair and maintenance capabilities, improving real-time monitoring and security measures around submarine cable infrastructure, and conducting comprehensive stress tests are critical to improving resilience and guarding against a low-probability but high-impact event in which damages to multiple cables cause prolonged connectivity issues.

Key Findings

- Insikt Group identified a total of 44 publicly reported cable damages in 2024 and 2025 occurring in 32 distinct groupings. Unknown causes accounted for the largest number of damages (31%), followed by anchor dragging (25%) and seismic activity or other natural phenomena (16%).
- Of the identified cable damages, three caused significant and prolonged outages. These cases indicate that three factors — lack of redundancy, lack of diversity of cable routes, and limited repair capacity — very likely raise the risk of severe impact from damages to submarine cables.
- Insikt Group identified four incidents in the Baltic Sea involving eight distinct submarine cable damages and five incidents around Taiwan involving five distinct submarine cable damages in 2024 and 2025, four of which involved China- or Russia-linked vessels with opaque ownership or suspicious maneuvers near the damaged cables.
- Geopolitical tensions — namely, Russia's war against Ukraine and China's coercive actions toward Taiwan — very likely remain the primary drivers of state-linked sabotage activity targeting submarine cables.
- Joint public-private partnerships promoting investment in cable repair and maintenance capabilities, enhancing security and surveillance of critical submarine infrastructure, and improving resilience in current and future cable networks will be critical to addressing rising threats to cable infrastructure.

Background

There are currently 597 subsea cables in operation or under construction as of April 2025, compared to 559 subsea cables in 2024. These cables account for an estimated 99% of international data traffic, representing critical infrastructure underpinning global telecommunications and financial flows. In 2024, 24 new cable systems came online, according to the Submarine Telecoms Forum (SubTel Forum) — eight in the Europe-Middle East-Africa region, six in Oceania, four in the Indian Ocean, four in the Americas, and two transpacific systems.

Among commercial suppliers of cable systems, three companies — France's Alcatel, the US's SubCom, and Japan's NEC — lead in the number of systems delivered, kilometers of cable produced, and future systems planned, although China's HMN Technologies (Hengtong) is playing an increasing role. Between 2020 and 2024, Alcatel delivered 23 systems, SubCom delivered thirteen, NEC ten, and HMN seven. Alcatel, the largest player, is also involved in nine planned future cable systems, representing 39% of future projects, while NEC is involved in four (17%) and SubCom two (9%).

There are approximately 80 vessels globally dedicated to maintaining and expanding submarine cable infrastructure, with the United Kingdom's (UK) Global Marine Systems (13%), France's Orange Marine (13%), SubCom (11.6%), Alcatel Submarine Networks (ASN) (10%) and Malaysia's Optic Marine Services (10%) owning the most vessels.

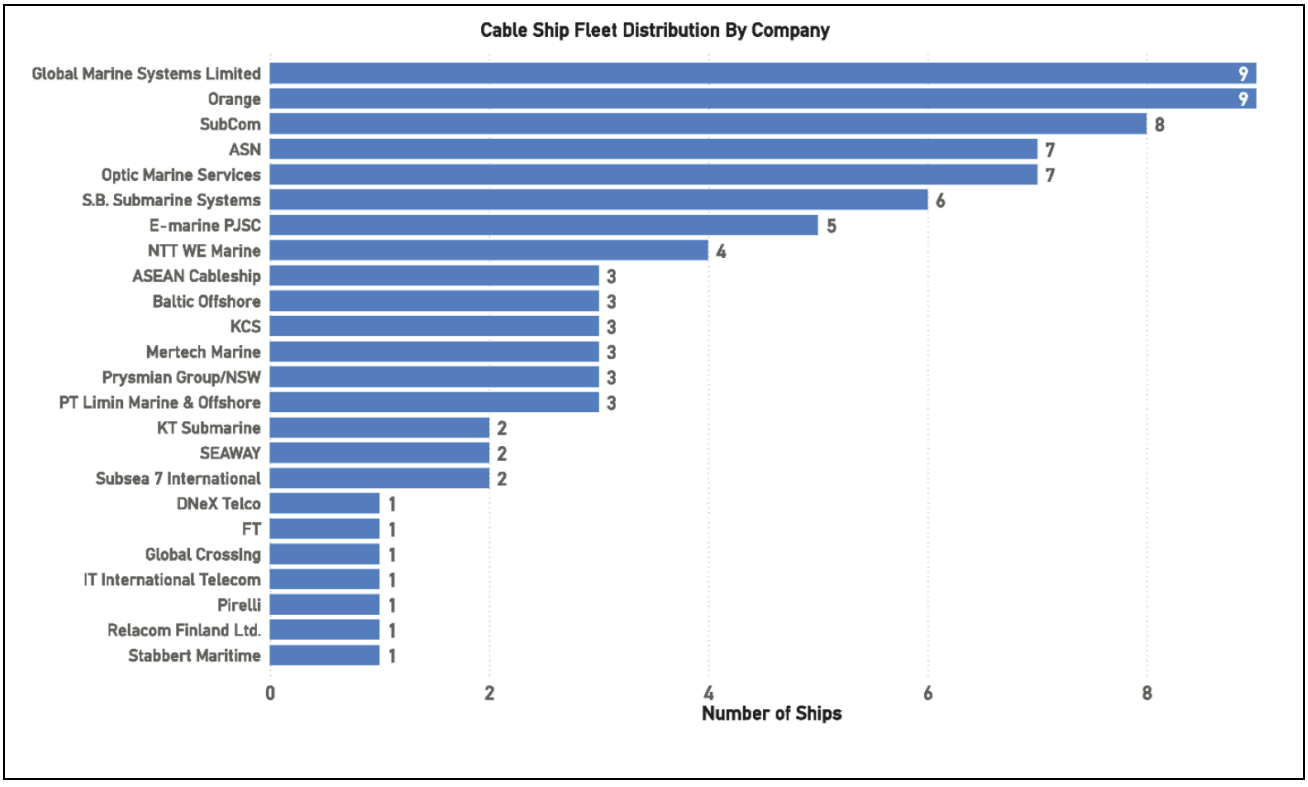


Figure 1: *Cable ship fleet distribution by company*
(Source: Submarine Telecoms Forum Industry Report 2024–2025: Issue 13)

Damage to submarine cables is not uncommon, with an average of 150 to 200 faults occurring globally each year, according to the International Cable Protection Committee (ICPC). Most of these faults never reach the threshold of public reporting, since the majority do not cause detectable issues due to the availability of alternate routes for traffic. From 2015 to 2024, SubTel Forum identified a total of 237 publicized cable fault incidents globally — likely a fraction of the total cable faults — the vast majority of which were attributable to human activities, namely fishing and anchor dragging. Regionally, the "AustralAsia" region accounted for 36.3% of all reported faults during this period, making it the most fault-prone area, followed by Europe, the Middle East, and Africa (28.7%) and the Americas (20.3%) The ICPC reports that the most common cause of cable damage is a ship anchor or fishing equipment contacting a cable in depths of less than 200 meters. Undersea abrasion and natural phenomena — such as underwater rockslides and seismic activity — account for approximately 10% of faults.

While cable faults are relatively common, they require significant resources to repair; the ICPC reports that cable repairs average between $1 and $3 million, require "specialized cable ships with highly trained crews," and can take months to complete.

Submarine Cable Risk Environment

Submarine cable systems very likely continue to face an escalating risk environment, driven in part by increasing geopolitical tensions — aligning with our July 2023 assessment. In 2024, SubTel Forum — a leading industry platform for submarine cable analysis and reporting — reported 46 incidents, the highest figure since it began publishing data on subsea cable faults in 2013 and a sharp uptick from the fifteen reported in 2023. This corresponds to heightened public awareness of submarine cable vulnerabilities amid several recent high-profile damages and related concerns about intentional malicious actions, such as sabotage — although the increase may be partially attributable to increased reporting on subsea cable faults, as opposed to strictly reflecting an increase in incidents. However, most recent incidents have not resulted in prolonged connectivity disruptions.

An assessment of the three most impactful damages in 2024 and 2025 — located in the Red Sea, West Africa, and South Africa — indicates that the greatest threat to submarine cables is almost certainly where damages occur in areas with limited redundancy and repair capacity, regardless of whether the result of malicious targeting driven by geopolitical interests, unintentional human activity, or natural phenomena.

Most Impactful Cable Damages of 2024–2025

Insikt Group identified 44 publicly reported submarine cable damages occurring in 32 groupings in 2024 and 2025 (**Appendix A**). Of these, three cases caused damage to multiple submarine internet cables resulting in substantial and prolonged disruption to internet and telecommunications traffic. In each case, disruption to services resulted from damages to multiple submarine cables at once, with the most impacted countries lacking reliable alternative routes for traffic, exacerbated by limited repair capabilities and permitting issues that prolonged repair timelines.

- In February 2024, a UK-owned vessel struck by a Houthi-fired missile sank in the Red Sea, damaging the Asia Africa Europe-1 (AAE-1), Europe India Gateway (EIG), and SEACOM cables and disrupting 25% of traffic between Asia, Europe, and the Middle East. According to Hong Kong telecommunications company HGC Global Communications, the damage caused "a significant impact on communication networks in the Middle East."
- In March 2024, an underwater rock slide damaged four submarine cables off West Africa: the West African Cable System (WACS), Africa Coast to Europe (ACE), MainOne, and SAT-3 cables. NetBlocks reported disruptions to internet connections in at least sixteen Central and West African countries, with disruptions to mobile payments and cloud applications for several days. CloudFlare reported a significant impact on a total of thirteen countries. In Liberia, disruptions lasted more than twelve hours. The outage also left multiple Nigerian banks offline, severely impacted connectivity in Ghana, and incurred estimated repair costs of $8 million.
- In May 2024, damage to two cables off the coast of South Africa — SEACOM and the Eastern Africa Submarine System (EASSy) — significantly reduced connectivity between East and South Africa, and caused internet outages for Kenya and several other East African countries. According to Netblocks, the cut disrupted internet services in twelve countries, with Tanzania, Mozambique, and Malawi particularly affected.

Risk Factors for Submarine Cable Systems

Three primary factors — lack of redundancy, lack of diversity of cable routes, and limited repair capacity — very likely raise the likelihood of severe outages caused by damage to submarine cables. Additionally, permitting issues stemming from different regulatory environments and geopolitical tensions can extend the timeline for cable repairs, as can kinetic conflicts in the vicinity of cable breaks.

Lack of Redundancy

Jurisdictions with limited alternate options to reroute traffic are most vulnerable to prolonged or significant disruptions. Following the May 2024 damages to SEACOM and EASSy, Kenya rerouted traffic to the TEAMS cable, with Safaricom and Airtel reporting they had activated alternative connectivity, but Tanzania experienced greater disruption due to its fewer connectivity options (**Figure 2**). In this case, the earlier February 2024 Red Sea damages further limited alternate options for connectivity, with Microsoft stating that the two incidents together "had reduced the total network capacity for most of Africa's regions." By contrast, Cloudflare reported that two cable cuts in November 2024 in the Baltic Sea — the BCS East-West Interlink connecting Sweden and Lithuania, and the C-Lion1 cable connecting Finland and Germany — "resulted in little-to-no observable impact to the affected countries … in large part because of the significant redundancy and resilience of Internet infrastructure in Europe." Highlighting the importance of redundancy measures, the European Commission reported in 2024 that "many islands in the Union, including the three island Member States [Cyprus, Ireland, and Malta], as well as the EU outermost regions and overseas countries and territories, are almost entirely dependent on such submarine cables for intra-Union communications," indicating a likely higher level of vulnerability.

Infrastructure Disruptions: All, 2024-05-11 to 2024-05-12

location	incident_impact	incident_auto_classification	low_pct ▲	curr_pct
Tanzania, TZ	⚠ HIGH	internet outage	29%	33%
Mayotte, YT	⚠ HIGH	internet outage	33%	65%
Mozambique, MZ	! MEDIUM	internet outage	60%	58%
Malawi, MW	! MEDIUM	internet outage	69%	87%
Sierra Leone, SL	LOW	internet outage	71%	85%
Burundi, BI	LOW	internet outage	74%	80%
Madagascar, MG	LOW	internet outage	76%	72%
Comoros, KM	LOW	internet outage	81%	88%
Rwanda, RW	LOW	internet outage	81%	80%
Uganda, UG	LOW	internet outage	83%	86%
Somalia, SO	LOW	internet outage	84%	84%
Kenya, KE	✅ RESTORED	internet outage	89%	96%

Figure 2: *Impact of May 2024 SEACOM and EASSy cable outages in East Africa (Source: NetBlocks)*

While satellites provide edge connectivity and connect locations that do not have easy access to physical infrastructure, they account for a small amount of overall global capacity and typically cannot replace fiber-optic submarine cables, which also move large amounts of data faster and more cheaply. TeleGeography reports that "cables can carry far more data at far less cost than satellites," and only a small percentage of intercontinental data traffic is transmitted via satellite, according to Cloudflare. For example, the US Federal Communications Commission (FCC) reports that satellites account for just 0.37% of all US international capacity. According to the ICPC, "a trans-pacific fibre-optic call need only travel about 5,000 miles point-to-point," compared to a satellite call, which must travel 22,235 miles from the Earth to a satellite and then another 22,235 back. Illustrating this, a backup microwave system was activated following damages to two submarine cables connecting Taiwan and the Matsu Islands in February 2023, but only restored an estimated 5% of the bandwidth that the cables had provided, with full internet access not restored until April 2023.

Lack of Diversity of Cable Routes

Deploying submarine cables along similar geographic routes very likely increases systemic risk by creating single points of failure. Countries with multiple submarine cables routed along varying geographic routes are more insulated from major connectivity losses; conversely, those with fewer connecting cables, placed in close proximity to each other, are almost certainly more susceptible to multiple cable damages and associated disruptions. Recent incidents of damage to multiple cables at once indicate that threat actors could attempt to exploit the concentration of cables along similar routes in an effort to cause prolonged outages across a geographic area. For example, the Red Sea cable cuts in February 2024, detailed above, illustrated the importance of route diversity. The March 2024 damages to four cables off West Africa, which all occurred due to an underwater landslide in the "Le

Trou Sans Fond" canyon off of Côte d'Ivoire, illustrated how a concentration of cables at one point can make multiple cables susceptible to human-made threats or, as in this case, natural phenomena (**Figure 3**). Similarly, Egypt is a critical internet chokepoint through which multiple submarine cables connecting Europe, Africa, and Asia run; the vulnerabilities associated with this arrangement were apparent following June 2022 damages to both the AAE-1 and the SeaMeWe-5 cables. In December 2024, the US Department of Homeland Security noted that "while incidents in geographic chokepoints are relatively rare, each one brings much-needed attention to the vulnerability of similarly concentrated cables around the world."

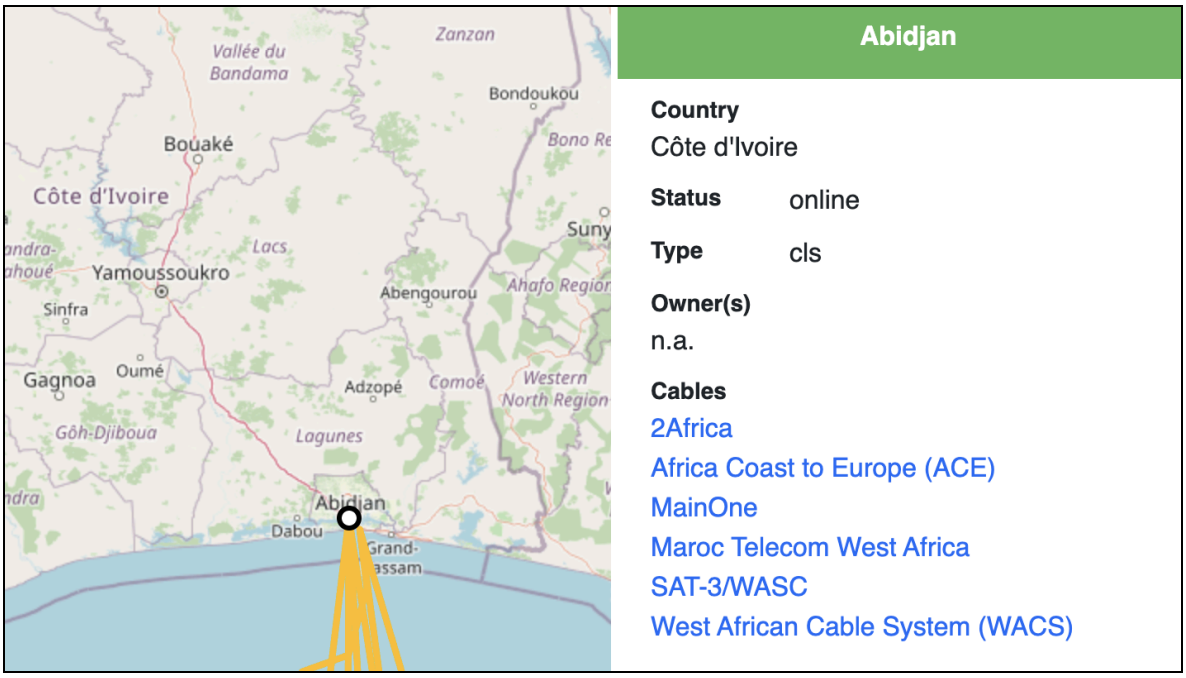


Figure 3: *Multiple cables convene at Abidjan, Côte d'Ivoire (Source: Fiber Atlantic)*

The concentration of submarine cables at a single cable landing station increases the likelihood that damage to or near a landing site will impact multiple cables. These stations provide multiple functions, including supplying power to the cable and connecting it to terrestrial networks, and their locations are often chosen based on access to existing infrastructure or regulatory factors, rather than because they offer particularly high protection from natural disasters or physical threats, such as sabotage or surveillance. As a result, cables frequently cluster around or at the same landing site — raising the threat that sabotage or espionage operations could impact multiple cables at once by targeting landing stations. For example, according to the US FCC, landing sites on the southeastern US coast are clustered in three primary locations in Florida, with nearly all landing sites developed to support multiple submarine cables. In October 2022, cybersecurity company Zscaler warned that cuts to multiple cables at landing stations in Marseille linking the city to Milan, Barcelona, and Lyon "impacted major cables with connectivity to Asia, Europe, US and potentially other parts of the world." In August 2023, the European Union Agency for Cybersecurity (ENISA) reported that landing stations represent a weak point in the ecosystem due to their vulnerability to "espionage attacks, deliberate power cuts, sabotage attacks with explosives, or even missile attacks in the case of a military conflict."

Limited Repair Capacity Poses Long-Term Problem

Repair capacity, which continues to lag behind the expansion of submarine cable networks, almost certainly represents an underappreciated point of vulnerability in the submarine cable ecosystem. As cable systems have expanded dramatically, investment in ships that can service these cables has lagged behind, resulting in the growth of cable systems outpacing repair capacity. Most of these vessels are therefore focused on laying new cable systems, constraining their ability to respond immediately to cable faults. According to ENISA, given the complex nature of repairs and limited repair capacity, "a coordinated attack against multiple subsea cables could have a major impact on global internet connectivity." For example, the Léon Thévenin, a cable repair ship docked in Cape Town, South Africa, was the only vessel dedicated to serving Africa at the time of the March 2024 cable outages, extending the repair timeline. In February 2023, all five of Vietnam's operational undersea cables suffered partial or total damage at the same time, resulting in the loss of 75% of its data transmission capacity. With nearby ships busy, repairs on all cables were not fully completed until late November 2023, and telecommunications firms were forced to purchase spare terrestrial capacity to help stabilize connections. Reflecting concerns regarding the limited availability of repair vessels, the US established the Cable Security Fleet in 2020 with two dedicated US-flagged cable repair ships (the CS Dependable and CS Decisive) to speed repairs to submarine cables relevant to US national security.

Unless significant investments are made in streamlining repair processes and expanding cable ship repair capacity, repair times are likely to continue trending upward. According to SubTel Forum, the average repair time for the restoration of cable faults has risen from 2015 to 2024, with the average repair time in 2023 consisting of 40 days. Vietnam's five submarine cable systems, which account for most of its international bandwidth, experience an average of fifteen incidents annually; prior to 2022, repairs lasted one to two months per incident, but have recently lasted longer, extending disruptions. This is almost certainly a result of the increasing gap in the rates of subsea cable infrastructure expansion and stagnating repair capabilities.

Regulatory Factors, Conflict, and Territorial Disputes Likely to Prolong Repair Timelines

Regulatory hurdles, such as complex and lengthy permitting processes for repair ships that vary by national territory, likely prolong repair timelines, exacerbating the impact of limited repair capacity. Cable damage in areas subject to territorial disputes and ongoing kinetic conflicts almost certainly increases the prospect of prolonged outages due to the denial of access to repair vessels. The International Institute for Strategic Studies reports that repairs in the Asia-Pacific region take up to 30 days on average from notification of an incident, compared to fifteen in North America, due to more stringent permitting requirements. For example, repairs to April 2024 damages to the SeaMeWe-5 cable in Indonesian waters, which reduced Bangladesh's internet capacity by a third, were not completed until June 28, 2024, as Jakarta's cabotage policy delayed repairs for several weeks. In March 2024, telecommunications provider SEACOM reported that it would likely take longer than expected to repair three cables in the Red Sea damaged by a ship hit by Houthi strikes since permitting could take up to eight weeks to obtain. The Yemeni government refused to grant permission to initiate repairs of the damaged AAE-1 cable to the cable's operating consortium, which includes telecommunications firm

TeleYemen, as one of the firm's two branches is under the control of the Houthi group. An investigation of the consortium reportedly delayed repairs of the AAE-1 until July 2024. Further, SubTel Forum reported that ongoing threats posed by the Houthi group likely limited companies that agreed to carry out repairs and incurred high premiums.

Additionally, amid ongoing territorial disputes between China and the Philippines in the South China Sea, the China Coast Guard (the CCG) has attempted to block Philippine resupply operations to vessels at the Second Thomas Shoal, Scarborough Shoal, and Sabina Shoal. In addition to harassing Philippine vessels, the CCG and other Chinese forces have for decades interfered with vessels from other claimants in the South China Sea, as well as vessels operated by outside powers like the United States. These incidents suggest that Beijing could take similar action to block repair vessels from accessing damaged submarine infrastructure in the event of a potential escalation of tension or outbreak of hostilities around Taiwan.

Geopolitical Conflicts Likely Driving Submarine Cable Sabotage

Throughout 2024 and 2025, high-profile damages of cables in the Baltic Sea and around Taiwan have contributed to growing concerns about malicious targeting of submarine cables, particularly state-sponsored sabotage, driven by geopolitical conflicts. Insikt Group identified four incidents of cable damages impacting eight cables in the Baltic Sea (**Figure 4**) and five incidents of damages to five cables around Taiwan (**Figure 5**) in 2024 and 2025, representing 30% of all cable damages globally publicly reported during this period (available in **Appendix A**).

Baltic Sea

Since late 2023, approximately eleven internet cables in the Baltic Sea have been damaged, according to European officials, although several US and European intelligence services have stated that the damages were likely the result of maritime accidents, rather than state-directed sabotage — very likely reflecting the difficulty of definitively determining whether an incident was intentional and malicious. Coinciding with submarine cable damages, Russia has almost certainly increased hybrid warfare operations targeting European countries, including sabotage of critical infrastructure, since its full-scale invasion of Ukraine in February 2022, as it seeks to destabilize NATO member states and reduce support for Ukraine. Insikt Group identified the following damages to submarine cables in the Baltic Sea in 2024 and 2025:

- In February 2025, Swedish police began investigating the suspected sabotage of the C-Lion1 cable connecting Rostock, Germany, and Helsinki, Finland, in Sweden's exclusive economic zone (EEZ); Finnish telecom operator Cinia reported it was the third damage to the cable in recent months, although there was no impact to data traffic.
- On January 26, 2025, Latvia reported that an undersea cable connecting Latvia and Sweden was damaged along the Gotland-Ventspils segment in Sweden's EEZ. Swedish prosecutors subsequently attributed the damage to accidental anchor-dragging by the Malta-flagged Vezhen cargo ship; there were no reported interruptions to communications.

- In December 2024, Finnish authorities boarded and seized the Cook Islands-flagged Eagle S ship on suspicion of damaging the Estlink-2 power cable, three fiber-optic cables between Finland and Estonia (likely the FEC-1, FEC-2, and Baltic Sea Submarine Cable), and one cable between Finland and Germany (likely the C-Lion1). Repairs to the cable were complete by January 6, 2025, with full power cable restoration expected by mid-2025.
- In November 2024, two submarine cables in the Baltic Sea — the C-Lion1 and the BCS East-West Interlink between Lithuania and Sweden — were damaged within approximately 100 kilometers of each other during a period of several hours. Swedish, Finnish, and Lithuanian investigations concluded that the Chinese vessel Yi Peng 3 had severed the cables by dragging its anchor. According to RIPE Labs, only 20–30% of paths measured had relatively minor latency increases and no visible packet loss, indicating sufficient backup capacity and alternative routes to prevent connectivity issues.

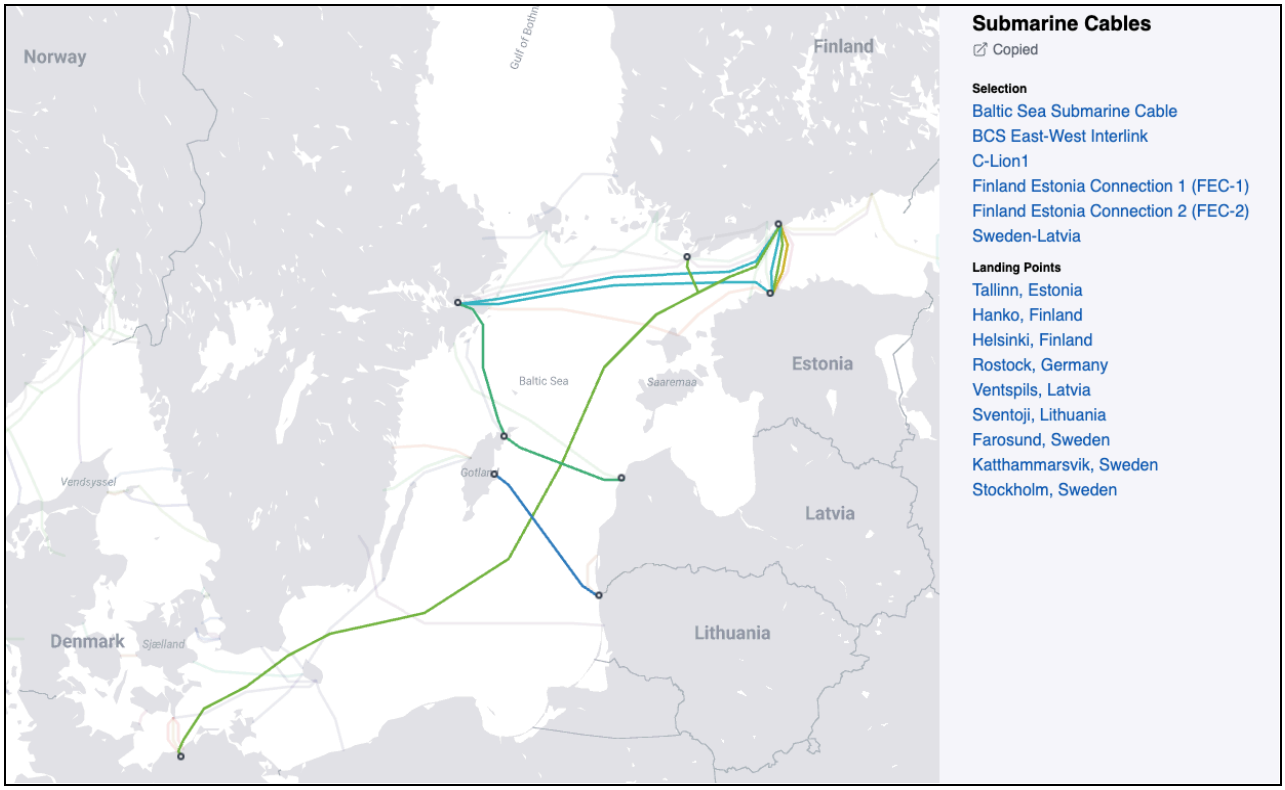


Figure 4: *Baltic Sea cables damaged in 2024–2025 (Source: TeleGeography)*

Taiwan

In an August 2024 report, Taiwan's National Audit Office noted that there were "36 cases of damage [to submarine cables] caused by external forces" from 2019 to 2023, with an average of seven cable failures per year — primarily caused by anchoring or dredging from vessels. Taiwan has reported five cases of submarine cable malfunctions in 2025, and three each in 2024 and 2023, according to Reuters, citing Taiwan's Ministry of Digital Affairs. These damages, while often not directly attributable to Chinese state-directed sabotage, have coincided with an increase in Chinese coercive efforts toward

Taiwan, including major military exercises, incursions into maritime and air spaces near Taiwan, destructive and disruptive cyberattacks against Taiwanese critical infrastructure, and use of "lawfare" measures. Insikt Group identified the following damages to submarine cables around Taiwan in 2024 and 2025:

- On February 25, 2025, Taiwan's Coast Guard detained the Togo-flagged, Chinese-crewed freighter Hong Tai 58, after the severing of the No. 3 undersea cable linking Taiwan and the Penghu Islands. The ship, which used the alternate name Hong Tai 168, reportedly dragged its anchor between February 22 and 25 while maneuvering in a zig-zag pattern over the cable.
- In February 2025, the No. 2 submarine cable between Taiwan's main island and the Matsu Islands experienced a "complete disruption" due to damages at multiple points. Chunghwa Telecom stated that communications were automatically rerouted through microwave backup.
- In January 2025, the No. 2 and No. 3 cables connecting Taiwan and the Matsu Islands broke one week apart, which Taiwan's Ministry of Digital Affairs attributed to "natural deterioration."
- In early January 2025, Taiwan's Coast Guard Administration announced that a cable operated by Chunghwa Telecom, part of the Trans-Pacific Express Cable System connecting Taiwan and the US, was damaged, likely by Cameroon-flagged and Chinese-owned cargo ship Shun Xing 39. According to MarineTraffic, the vessel was suspiciously drifting for over a month around Taiwan's north coast without loading or discharging cargo, and Lloyd's List linked it to two additional identities — Tanzania-flagged Xing Shun 39 and Cameroon-flagged Xing Shun 39 — likely indicating deliberate efforts to prevent identification.

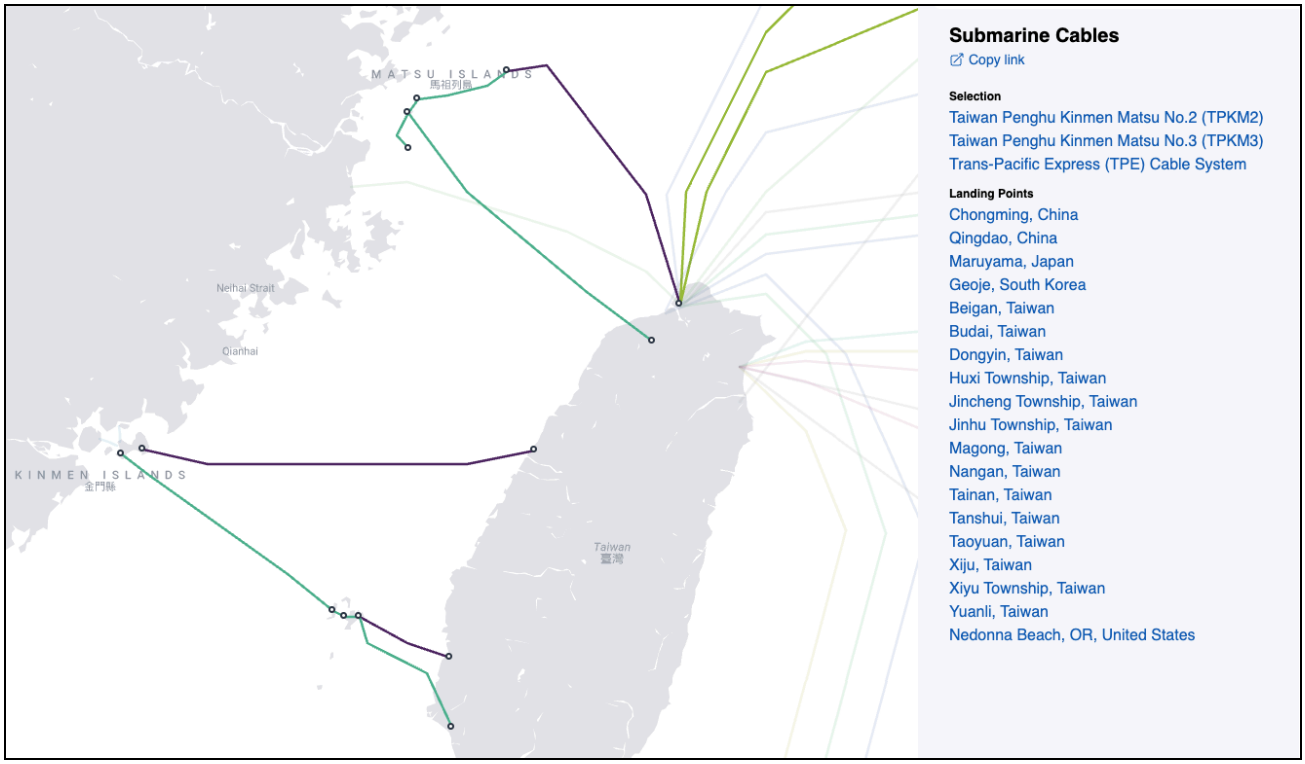


Figure 5: *Cables damaged around Taiwan in 2024–2025 (Source: TeleGeography)*

Nation-State Threats

Aligning with our 2023 analysis of threats to submarine cables, Insikt Group continues to assess that Russia's full-scale invasion of Ukraine in February 2022 and China's increasing coercive activity against Taiwan almost certainly remain the primary geopolitical drivers of sabotage threats to submarine cables. State actors continue to be the most likely to possess the specialized expertise and equipment needed to identify and covertly sever deepwater cables, compared to lower-sophistication operations in shallower waters that are easier to conduct but also less impactful and simpler to repair. While it is difficult to definitively attribute recent incidents in the Baltic Sea and around Taiwan to state-sponsored sabotage, such operations align with both Russia and China's strategic objectives, recently observed activities, and current deep-sea capabilities.

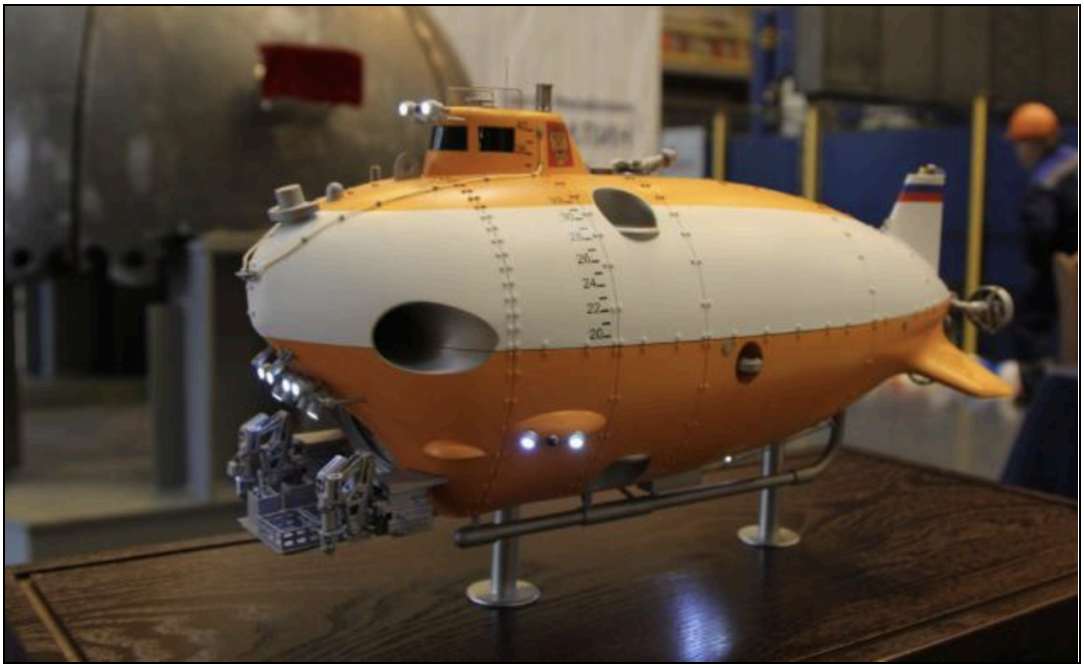
Russia

The act of targeting submarine cables with commercial vessels aligns with Russian hybrid warfare doctrine, which prioritizes disruptive actions to destabilize adversaries below the threshold of kinetic warfare. Since the Soviet era, Russia has viewed the ability to target Western critical infrastructure, including submarine cables, as an imperative. In this, Russia's strategy of "escalate to deescalate" involves the ability to inflict economic damage — here, to subsea cables — as a method of deterring undesirable actions by an adversary (NATO countries). In May 2025, NATO reported that "the vulnerability of subsea infrastructure, including cables, pipelines, and energy assets, has become a central concern for NATO and Allies … demonstrating how hybrid attacks can cause strategic disruption without overt military confrontation." In November 2024, Insikt Group assessed that Russia is very likely intensifying its sabotage operations across Europe targeting critical infrastructure as part of its broader hybrid warfare strategy, which augments conventional military operations in Ukraine with deniable and subversive actions against Ukraine's allies. Notably, Russian Deputy Chairman of the Security Council and former Russian President Dmitry Medvedev stated in June 2023 that "if we proceed from the proven complicity of Western countries in blowing up the Nord Streams, then we have no constraints — even moral — left to prevent us from destroying the ocean floor cable communications of our enemies."

Recent maritime surveillance activity associated with the Russian government very likely indicates efforts to identify and monitor European critical infrastructure. In April 2025, The Sunday Times reported that the UK had identified several Russian sensors suspected of attempting to collect intelligence on UK nuclear submarines and other underwater critical infrastructure, including deep-sea communication cables. In January 2025, reports emerged that the Jazz tanker, suspected of being part of Russia's shadow fleet, had three purported engine failures directly above submarine cables in the North Sea. Lloyd's List reported that Eagle S carried spying equipment to monitor naval activity, prompting concerns of Russia-directed sabotage after the December 2024 damages to the Estlink-2. In November 2024, the Irish navy escorted Russia's Yantar surveillance ship out of the Irish Sea after it sailed near cables carrying data for Google and Microsoft. Reflecting concerns over such activity, in May 2024, NATO held the first meeting of its Critical Undersea Infrastructure Network, focused on

enhancing undersea cable security, including the use of AI, drones, and new sensors to detect suspicious activity.

Moscow's efforts to develop its deep-sea exploration and submarine capabilities very likely support its ability to conduct undersea sabotage. Within the Russian military and intelligence apparatus, both the Main Directorate of Deep Sea Research (GUGI) and the Intelligence Directorate of the Main Staff of the Russian Navy have almost certainly played a role in Russia-directed submarine sabotage operations. Specifically, GUGI operates at least eight specialized nuclear-powered submarines, and its Yantar surveillance vessel is equipped with two Konsul class deep-sea mini-submarines (the AS-37 Rus and AS-39 Konsul) that can access waters at depths of 6,000 meters, enabling the identification, mapping, and surveillance of submarine infrastructure, as well as very likely facilitating sabotage or tapping of cables.[1] In March 2024, TASS (a Russian state-owned news agency) reported that special purpose submarine "Losharik" (AS-31), which is operated by GUGI and was damaged in 2019, would undergo tests including diving to its maximum depth of 6,000 meters in June 2024 after the completion of lengthy repairs.[2] Also in March 2024, Russia's Ministry of Defense introduced a new autonomous mini-submarine named "Sergei Bavilin," which it claimed can dive to 11,000 meters and which will be operated by GUGI.[3] In July 2023, a new oceanographic research vessel, the "Evgenii Gorigledzhan," which was reportedly built for the use of GUGI, joined the Russian Navy; it can reportedly take on underwater vehicles, carry out underwater technical work, and conduct oceanographic surveys.[4] [5]



[1] *https://theins.ru/en/news/277940*
[2] *https://tass[.]ru/armiya-i-opk/20278493*
[3] *https://submarinersclub.ru/news?id=3594*
[4] *https://topwar[.]ru/224971-postroennoe-dlja-gugi-mo-okeanograficheskoe-issledovatelskoe-sudno-evgenij-gorigledzhan-voshlo-v-sostav-flota.html*
[5] *https://www.aoosk[.]ru/press-center/news/ois-evgeniy-gorigledzhan-gotov-voyti-v-sostav-voenno-morskogo-flota-rossii/*

Figure 6: *Model of the Sergei Bavilin mini-sub (Source: JSC United Shipbuilding Corporation[6])*

In addition to maritime assets directly controlled by and developed for Russian government and military entities, Western officials have recently expressed concern that Moscow can deploy its so-called "shadow fleet" — vessels Russia has almost certainly used to circumvent the G7 price cap on its oil exports — to target submarine cable infrastructure. In January 2025, the European Parliament debated measures to "detect and counter sabotage by the Russian shadow fleet, primarily in the Baltic Sea," citing increasing incidents of ships damaging undersea infrastructure.

China

In January 2025, Taiwan's National Security Bureau (NSB) assessed that the cutting of submarine cables has become a new threat from foreign hostile forces in the past three years, very likely reflecting heightened concerns regarding potential China-directed threats to critical infrastructure as part of its coercive activities toward Taiwan. Since 2017, the Matsu Islands' cables have reportedly been damaged at least 30 times, and approximately one-third of those cases involved Chinese vessels. On June 26, 2025, the Tainan District Court sentenced the Chinese captain of the Hong Tai 58 to three years in prison for the February 2025 damages to the cable between Penghu and Taiwan; according to an April 2025 indictment, the captain allegedly ordered the crew to release the anchor and drag it along the seafloor, maneuvering the ship to sever the cable. On March 12, 2025, the Taiwanese Coast Guard intercepted a Chinese research vessel, the Yan Ping 2, entering restricted waters and directed it out of the area after reportedly observing crew members drop unspecified detection equipment into the water. In January 2025, the Taiwanese Coast Guard announced it was "monitoring 52 suspicious Chinese-owned ships flying flags of convenience from Mongolia, Cameroon, Tanzania, Togo, and Sierra Leone," underscoring fears of efforts to target submarine infrastructure while hindering attribution. Reflecting these concerns, Taiwan has reportedly invested an estimated $18 million to construct 700 satellite stations as a contingency for cable disruptions.

China's development of deep-sea capabilities also very likely supports its ability to conduct targeted operations toward submarine infrastructure. In January 2025, Insikt Group reported that a Chinese university, a Chinese company, and independent individuals in China had filed patents for submarine cable-cutting devices in 2020, 2013, and 2009, respectively. Additionally, in 2023, Insikt Group assessed that the expanding role of Chinese companies in deploying, owning, and operating submarine cables increases the threat of espionage for the countries and companies that use them. Specifically, China's preparations for a potential military incursion into Taiwan and the deterioration of US-China bilateral relations very likely incentivize physical attacks and intelligence collection efforts targeting the submarine cable system to undermine the economic, diplomatic, and security objectives of the US and its allies.

[6] *https://www.aoosk[.]ru/press-center/news/v-osk-zalozhili-avtonomnyy-glubokovodnyy-apparat/*

Mitigations

Given the critical role submarine cables play in global communications, financial flows, and the security of data transmission, public and private sector entities should consider the following strategies to ensure the security and resilience of these systems:

- **Designating submarine cable protection zones:** Establishing zones within certain fixed areas prohibiting specific activities posing risks to submarine cables, such as fishing, anchoring, and dredging, can help avoid cable damages from commercial activities.
- **Deterrence via penalties for damage**: Substantial penalties for damaging submarine cables and increased enforcement of cable protection laws would likely incentivize vessels to take greater care to avoid causing accidental damage, and may make it more difficult for states to conduct sabotage operations in a plausibly deniable manner by deterring individuals from assisting with such efforts.
- **Periodic threat assessments of specific submarine cable systems:** Owners and operators should conduct regular security assessments to identify vulnerabilities and dependencies of submarine cable systems, which may vary by region and as geopolitical tensions shift.
- **Regular stress tests of submarine critical infrastructure systems, including cables:** Both public and private organizations should conduct regular stress tests for submarine cable systems to assess resilience in varying scenarios, such as malicious targeting or underwater avalanches. This should also account for interactions with other critical infrastructure, such as telecommunications.
- **Improving surveillance and monitoring of threats to submarine cable infrastructure:** Initiatives such as NATO's "Baltic Sentry" operation to protect cables in the Baltic Sea from intentional sabotage or NATO's Critical Undersea Infrastructure Network, established in 2023, can help proactively identify threats and deter adversaries from conducting intentional sabotage. For cable operators and owners, implementing automated early warning systems to identify potentially harmful events, such as systems for monitoring seismic activity or threat intelligence platforms enabling tracking of high-risk vessels near cables, can also reduce delays in the detection of cable damage.
- **Enhanced security measures around submarine cable landing stations:** Cable landing stations very likely represent more accessible targets for sabotage compared to deep-water cables, which only a small number of countries likely have the advanced capabilities required to access. Reflecting the importance of protecting these sites, in April 2025, Liberia announced it would relocate the landing station for the Africa Coast to Europe (ACE) cable — its sole source of international internet bandwidth — after nearby construction caused repeated outages from August 2024.
- **Increasing regional intelligence sharing:** Where feasible, increased intelligence sharing of suspicious activity around regionally critical submarine cable systems among military, intelligence, and law enforcement agencies can enable rapid identification of threats to these systems. Where appropriate, this may also include the publication of declassified information on

impending threats to such infrastructure, a strategy Western intelligence agencies deployed prior to Russia's full-scale invasion of Ukraine in February 2022.

- **Joint public-private investment in cable repair and maintenance capacity:** Increasing repair capacity will be crucial as demand for subsea cables rises globally — particularly in the Asia Pacific, where demand continues to rapidly expand. From the government side, this can include dedicating new or additional funding to augment the industrial base for cable deployment, repair, and maintenance — such as the US-funded Cable Security Fleet. Public-private investment in this area should account for the impact of geopolitical tensions on submarine cable threats and prioritize bolstering cable repair capabilities for regions likely at the greatest risk of state-sponsored malicious activity, such as the Baltic Sea or Taiwan.
- **Prioritizing redundancy and geographic diversity of new cable systems:** For example, to improve the resilience of Taiwan's communications infrastructure amid multiple recent cable breaks, the Taiwan government will subsidize the construction of a No. 4 Taiwan-Matsu cable, expected to be completed by mid-2026. When considering routes for new cable systems, providers should prioritize the protection of cables from natural or human-made hazards, including considering alternative routes to reduce chokepoints.

Additionally, organizations can use the following indicators to identify likely state-sponsored threats to submarine cable infrastructure. While none of the factors alone is likely sufficient to definitively confirm a state's intent to target multiple submarine cables, the presence of multiple indicators very likely entails a higher risk.

- Unscheduled loitering of survey or repair cable ships over key submarine cable routes
- Observed erratic geolocation data or indications that a vessel has repeatedly turned off tracking, such as Automatic Identification System (AIS) transponders, near submarine cables
- An uptick in observed physical or cyber-espionage targeting landing station facilities or personnel, not exclusively limited to state actors or individuals directly affiliated with intelligence services
- Efforts to rapidly augment a nation's submarine or deep-sea capabilities, such as an uptick in state-affiliated entities filing patent applications for these purposes
- Adversary official or state media narratives alleging planned sabotage or espionage of cable systems by likely target countries, such as Russian officials and state media alleging NATO member country efforts to target submarine cables
- Indications of preparation for kinetic conflict by an adversary country, which would likely entail a shift from low-level, plausibly deniable sabotage to more destructive actions intended to hamper military communications, such as targeting deep-water cables

Outlook

The simultaneous physical sabotage of multiple critical submarine cables in a way that causes a prolonged outage is unlikely for most countries, but not impossible. Such an event could severely degrade communications, including military channels; disrupt access to emergency and financial services; interrupt business operations on a large scale; and incur significant economic losses — highlighting the importance of developing indicators to signal the potential occurrence of such a low-probability but high-impact scenario. For example, according to an August 2024 report from Taiwan's National Audit Office, damages to the country's ten domestic submarine cables would severely affect communications between Taiwan's primary island and Penghu, Kinmen, and Lienchiang (Matsu Islands) counties.

The risk environment facing submarine cables — and other submarine critical infrastructure, such as pipelines — will very likely continue to increase as geopolitical conflicts and tensions rise. Recent damages to submarine cables in the Baltic Sea and around Taiwan, suspected to be sabotage, have often involved anchor dragging by commercial vessels — complicating the determination of malicious intent and attribution to a state actor — and occurred at shallower depths where repairs are relatively easier. By contrast, Insikt Group assesses that successful sabotage of multiple high-capacity submarine cables resulting in greater damage and prolonged outages would very likely occur in deeper waters, which would very likely involve state-sponsored threat actors, due to the difficulty of accessing these sites. Such an operation would very likely be intended to disrupt the military communications and stability of the targeted nation or region immediately preceding the outbreak of kinetic conflict, whereas lower-sophistication sabotage operations are intended to signal the vulnerability of critical submarine infrastructure while maintaining plausible deniability.

Nevertheless, in addition to the threat of large-scale malicious activity targeting submarine cables, lower-level sabotage targeting individual cables can still cause temporary connectivity issues, which — while under the threshold of a complete internet outage — can undermine the flow of information and inflict psychological damage on the population of a target country. As such, we assess that Russian and Chinese state-sponsored sabotage of submarine cables via commercial vessels will likely remain an attractive option for targeting perceived adversaries' critical infrastructure below the threshold of kinetic conflict as geopolitical tensions rise, aligning with both Moscow's and Beijing's observed "hybrid warfare" and "gray zone" tactics. In this context, initiatives for the monitoring and protection of submarine critical infrastructure, such as NATO's Baltic Sentry, are likely critical to deterring these threats.

Appendix A: Publicly Reported Submarine Cable Damages (2024–2025)

Cable Name(s)	Location	Date	Cause	Impact
West African Cable System (WACS)	South Africa	**June 1, 2025**	Faulty branching unit	The damage caused slow internet speeds in South Africa, particularly in the south, where most connections run over WACS. Maintenance began June 1 and is scheduled to be completed by June 16.
Africa Coast to Europe (ACE)	Liberia	**April 2, 2025**	The Liberia Telecommunications Authority (LTA) and Cable Consortium of Liberia (CCL) initiated repair and rerouting operations after nearby construction damaged the cable's landing site.	The damage had reportedly caused intermittent outages since August 2024, with operators stating that further damage to the landing site risked a complete internet outage. A repair vessel arrived in Liberia on April 22, with repairs expected to cause intermittent disruptions to service from April 23 to 30.
Pakistan and East Africa Connecting Europe (PEACE)	East Coast of Africa/Red Sea (Zafarana area)	**March 4, 2025**	Unknown	Repairs could reportedly take months due to limited repair capacity. Internet traffic was shifted to older cable routes, but previous

				damages to the AAE-1 cable in the Red Sea restricted alternate routes.
ACS Alaska-Oregon Network (AKORN)	Southeast Alaska	**February 28, 2025**	Unknown	Operator Alaska Communications began investigating network disruptions in Juneau on February 28, secured emergency capacity on March 1, and restored most service by March 2.
Taiwan Penghu Kinmen Matsu No. 3 (TPKM3)	Taiwan-Penghu County	**February 25, 2025**	On April 11, Taiwan prosecutors indicted the captain of the Togo-flagged Hong Tail 58 (also reported as Hongtai 168) for intentionally damaging the cable by directing the crew to drag the anchor between February 22 and 25 while maneuvering in a zig-zag pattern.	Chunghwa Telecom stated that no disruption in service occurred, with data transmitted via alternative cables and microwave technologies.
Taiwan Penghu Kinmen Matsu No. 2 (TPKM2)	Taiwan-Matsu Islands	**February 16, 2025**	This incident followed damage to the No. 2 cable in January 2025, which Taiwan's Ministry of Digital Affairs attributed to "natural deterioration."	Chunghwa Telecom reported a "complete disconnection," but connectivity in the Matsu Islands was restored using a microwave backup system. Repairs were completed as of March 14.

C-Lion1	Swedish EEZ	**January 26, 2025**	Initially reported on February 20, the damage was confirmed as a shunt fault on March 4, in the same area where damage to the Sweden-Latvia cable occurred.	Finnish operator Cinia stated that data traffic was not impacted; the cable repair vessel Cable Vigilance arrived at the fault site on March 10 and completed repairs by March 14.
Sweden-Latvia (Gotland-Ventspils segment)	Swedish EEZ	**January 26, 2025**	According to operator LVRTC, the damage occurred at a depth of 100 meters. On February 3, Swedish prosecutors attributed the damages to anchor dragging by the Maltese-flagged, Bulgaria-owned Vezhen cargo ship and ruled out sabotage.	LVRTC reported that cable repair operations began on February 19 and were completed with service fully restored by February 28; there were no reported interruptions to communications.
Taiwan Penghu Kinmen Matsu No. 2 (TPKM2)	Taiwan-Matsu Islands	**January 22, 2025**	Taiwan's Ministry of Digital Affairs attributed the damages to "natural deterioration."	Chunghwa Telecom activated microwave backup systems within one hour of the No. 2 cable failure, which followed the No. 3 cable failure the week prior.
Quintillion Subsea Cable Network	Northwest Alaska	**January 18, 2025**	Operator Quintillion attributed the outage to submarine sea ice activity in the Beaufort Sea.	On January 18, Quintillion stated that sea ice would prevent repair vessels from accessing the area until late summer. Back-up services were deployed to

				restore connectivity in phases from February 17 to April 14.
Taiwan Penghu Kinmen Matsu No. 3 (TPKM3)	Taiwan-Matsu Islands	**January 15, 2025**	Taiwan's Ministry of Digital Affairs attributed the damages to "natural deterioration."	Chunghwa Telecom reported that repairs to the No. 3 cable were completed on March 2, but traffic had already been rerouted through other cables and microwave backups, so traffic was unaffected.
Trans-Pacific Express (TPE) Cable System	Near Keelung, Taiwan	**January 4, 2025**	Taiwan's Coast Guard Administration stated that the Shunxing39 (or Xing Shun 39), a Chinese-controlled Tanzanian-flagged cargo ship, was suspected to be responsible. According to MarineTraffic, the vessel was suspiciously drifting for over a month around Taiwan's north coast without loading or discharging cargo.	Chunghwa Telecom reported that only four fibers were impacted and that connections were immediately restored by rerouting data to other cables.
TATA TGN Intra-Asia (TGN-IA)	Vietnam	**December 26, 2024**	Unknown	A fault on the IA branch S1, connecting Vietnam to Singapore, resulted in a complete loss of connectivity between Vietnam, Hong Kong, and

				Singapore. Repairs were completed by February 2025.
Four unspecified internet lines (likely the Finland Estonia Connection 1 [FEC-1]; Finland Estonia Connection 2 [FEC-2] or E-FINEST; the Baltic Sea Submarine Cable; and C-Lion1)	Baltic Sea	**December 25, 2024**	On December 26, Finnish authorities seized the Cook Islands-flagged Eagle S ship and later confirmed extensive anchor drag marks on the seabed. Finland released the ship on March 2.	The incident reportedly damaged two fiber-optic cables owned by Elisa (likely the FEC-1 and FEC-2), a third link owned by Chinese Citic (likely the Baltic Sea Submarine Cable), and a fourth cable between Finland and Germany, owned by Cinia (likely the C-Lion1). However, repairs were completed by January 6, with no impact on services in Finland or Estonia. The anchor also damaged the Estlink-2 submarine power cable between Estonia and Finland; repairs started in May and full service was recovered on July 15.
Interchange Cable Network 1 (ICN1)	Vanuatu	**December 16, 2024**	An earthquake reportedly caused a fire at the cable landing station.	Internet connectivity was severely disrupted, and services were fully restored ten days later.

Asia Pacific Gateway (APG)	Vietnam	**November 29, 2024**	Unknown	The failure interrupted all international connections along the route, with repair completed by May 1. Compounding the damages, a fault on the S1H5 section of the AAE-1 cable, which connects Vietnam to Singapore, delayed the full restoration of that system multiple times from May to December 2024.
C-Lion1, BCS East-West Interlink	Baltic Sea	**November 17, 2024**	Swedish investigations concluded that the Yi Peng 3 vessel severed the two cables by dragging its anchor for about 100 miles along the seabed.	The damage reduced approximately one-third of Lithuania's internet capacity, but connections were restored by bypassing the failure. There were no significant interruptions to connectivity from either damaged cable. Repairs on the BCS East-West Interlink and C-Lion1 were completed by November 28.
FALCON	Kuwait	**September 25, 2024**	Unknown	The Communication and Information Technology

				Regulatory Authority (CITRA) engaged local ISPs to redirect traffic, and by September 26, 30% of service was restored through alternatives. Traffic returned to normal by September 29 under an emergency plan for diverting traffic.
(Likely) Asia-America Gateway (AAG)	Malaysia	**September 20, 2024**	Unknown	Service provider Unifi stated that internet services were disrupted, but traffic was rerouted through alternative connections and recovery was expected by the end of the same day.
Alaska United Southeast (AU-SE)	Southeast Alaska (Sitka)	**August 29, 2024**	Unknown	Most internet and cellular services in Sitka were down until approximately September 3, when some services were restored via a mix of satellite and microwave technology. Repairs began on September 8 and finished on September 16.
Asia Africa Europe-1 (AAE-1)	Pakistan	**August 28, 2024**	Users in Pakistan reported internet disruptions throughout 2024, which ISPs and	In November 2024, PTA confirmed SMW-4 was fully repaired. Repairs began on the AAE-1

			observers warned could be due to government censorship and monitoring. However, the Pakistan Telecommunication Authority (PTA) attributed slowdowns to faults in the SMW4 and AAE-1 cables, two of seven cables connecting Pakistan.	cable on January 2, according to the PTA, and were completed by January 16.
Tonga Domestic Cable Extension (TDCE)	Tonga	**August 26, 2024**	An earthquake near Ha'apai damaged Tonga's only inter-island domestic submarine cable, one and a half weeks after repairs to June 2024 damage were completed.	Cable communications to Vava'u and Ha'apai were cut. Repairs reportedly concluded the first week of September 2024.
Eastern Africa Submarine System (EASSy)	South Africa	**August 20, 2024**	Several links on EASSy went offline due to a shunt fault.	Traffic to the Middle East and Central and Eastern Europe reportedly saw increased latency, but there were no major disruptions. The initial repair was estimated to be completed by August 25 but was delayed by several days.
Tonga Domestic Cable Extension (TDCE)	Tonga	**June 29, 2024**	An earthquake caused underwater rockslides, damaging the cable in two places.	Vava'u and Ha'apai experienced severe disruptions to telephone and internet services for several weeks, with

				limited services restored via backup satellites on June 30. Repairs began on August 16 after the repair ship was delayed due to mechanical issues.
TATA TGN-Intra Asia (TGN-IA), Asia Pacific Gateway (APG), and Asia Africa Europe-1 (AAE-1)	Vietnam	**June 15, 2024**	Unknown	Three of five cables connecting Vietnam went down, significantly affecting internet connections.
SEACOM/Tata TGN-Eurasia, Eastern Africa Submarine System (EASSy)	East Africa	**May 12, 2024**	Suspected anchor dragging	The damages significantly reduced connectivity between East and South Africa. Kenya's Safaricom announced the restoration of services on May 16, and Airtel Uganda reported internet service as "near normal." All cables were repaired by June 3.
Bahamas Domestic Submarine Network (BDSNi)	Bahamas	**April 27, 2024**	The Bahamas Telecommunications Company (BTC) sued a yacht it claimed had damaged the cable after trying to anchor off Cable Beach.	The BTC rerouted traffic via an "unstable" alternate connection.

South Africa Far East (SAFE)	Mauritius, Réunion	**April 26, 2024**	Unknown	The damage impacted service on Mauritius and Réunion. Mauritius Telecom reported that repairs were completed the same day, but caused temporary disruptions to SBM Bank.
Quintillion Subsea Cable Network	Northern Alaska	**April 23, 2024**	Quintillion reported that the break occurred in an area with oil and gas operations due to "environmental conditions."	Customers reported slow internet and connectivity issues in North Slope, although providers transitioned to backup infrastructure and temporarily restored most service the same day.
SeaMeWe-5	Bangladesh	**April 19, 2024**	Unknown	The damages caused a loss of 1.7 terabits per second (Tbps) of international capacity, resulting in slow internet speeds, although bandwidth was shifted to the SeaMeWe-4 cable. However, repairs were delayed due to permitting timelines and were not completed until June 28.
West African Cable System (WACS), Africa Coast to Europe	West Africa	**March 14, 2024**	Seismic activity caused damage to all four cables in the Le Trou Sans Fond Canyon.	NetBlocks reported intensifying telecom outages and banking service disruptions across West Africa.

(ACE), MainOne, SAT-3/WASC				MainOne initially said on March 15 that repairs would take one to two weeks, but on March 25 said it would be six to eight weeks due to the number of cables damaged. All four cables were repaired between April 6 and May 14.
Asia Africa Europe-1 (AAE-1), Europe India Gateway (EIG), SEACOM/Tata TGN-Eurasia	Red Sea	**February 24, 2024**	US officials reported the cuts were caused by the anchor of the sinking Belize-flagged, UK-owned Rubymar, which was struck by a Houthi-fired missile on February 18.	The damages disrupted traffic from East Africa to Southeast Asia, impacting an estimated 25% of regional traffic. SEACOM estimated that permits could take eight weeks to obtain. Repairs experienced delays after the Yemeni government launched an investigation into the AAE-1 consortium, but began on all cables in July 2024.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com