AEGEAN INTELLIGENCE GROUP

PUBLISHABLE MARKET RESEARCH · 2026

CLASSIFICATION
CLIENT CONFIDENTIAL

PRODUCT ID
PMR-2026-0603-GLBL-003

TIMELINESS
DURABLE

DATE
2026-06-03

The Attribution Gap

How the West's Subsea Infrastructure Became a Politically Costless Target, the Repair-Fleet Constraint No One Has Re-Priced, and What the Next Incident Will Cost

5 / 0

NAMED INCIDENT CLUSTERS 2022-2025 / FINALIZED STATE-ACTOR ATTRIBUTIONS

60-75

GLOBAL CABLE-CAPABLE REPAIR VESSELS ACROSS ~10 OWNER FIRMS

~17% / ~30%

EGYPT CORRIDOR / LUZON STRAIT SHARES OF INTERCONTINENTAL BANDWIDTH

EXECUTIVE DASHBOARD

Western seafloor infrastructure operates inside a structurally produced attribution gap that has effectively immunised state-aligned actors from public state-level consequence. The insurance market, the repair-fleet, and the operator-response architectures have not been re-priced to the asymmetry.

THESIS

Western seafloor infrastructure now operates inside a structurally produced attribution gap. Across five major incident clusters from 2022 through 2025, **zero have produced finalized public state-actor attribution** in Western investigations, and only one prosecution (the Eagle S, in Finland) has reached the threshold of a foreign-flagged vessel boarded and held on a cable-damage cause of action. The insurance market, the repair-fleet, and the operator-response architectures have not been re-priced to reflect this asymmetry. The gap is durable across at least a 12-month horizon, the repair-fleet capacity is the binding operational constraint that any concentrated incident campaign would expose first, and the binding question for an operator is no longer whether a state actor can be deterred from a seafloor incident, but how much of the cost of the next one the operator is silently carrying today.

KEY STATISTICS

95-99%
share of international data traffic carried by submarine cables[1, 2, 3]

1.45M km
global subsea cable footprint across ~574 active or planned systems (2025)[4, 5]

60-75
global cable-capable repair vessels across ~10 owner / operator firms[6, 4]

150-200
cable faults recorded globally each year; >70% anthropogenic[7, 6]

8-16 wk
repair cycle on a single major fault under normal conditions[6, 4]

~17%
Egyptian land-and-sea corridor share of intercontinental cable bandwidth[3, 8]

~30%
Luzon Strait share of trans-Pacific east-west bandwidth[5, 8]

0 of 5
finalized public state-actor attributions across the 2022-25 incident record[9, 10, 11, 12, 2, 13, 14]

Scope & method. Open-source intelligence only, verified against allowlisted Tier 1, 2, 3, and 4 sources per AEIG Module 2 source policy. T1 share is roughly 42 percent; T2 share is roughly 31 percent; T3 is 17 percent; T4 (structured data: TeleGeography, MarineTraffic AIS, ACLED) is 11 percent, deliberately oversampled per the cohort-one corrective on T4 underweighting. Russian and Chinese state media do not appear in the registry; capability claims about GUGI and the PLA Strategic Support Force are routed through Janes, RUSI, IISS, and Western T1 government primaries only. Attribution-disputed incidents (Nord Stream, Balticconnector, the Baltic 2024 cluster) are treated as contested and not adjudicated by AEIG; investigation status, not conclusion, is reported. Window: 2022 to mid-2026. Timeliness: DURABLE, with a 6 to 18 month shelf life.

KEY JUDGMENTS

Seven judgments anchor this assessment. Each is tied to the cited evidence in the sections that follow and carries an explicit confidence level.

1 High — The attribution gap is durable. Across five major incident clusters in four years, no Western investigation has produced a finalized public state-actor attribution, and the institutional and legal frameworks that would close the gap have not changed.[9, 10, 11, 2]

2 High — The gap is structurally produced, not accidental. Anchor-drag deniability, the 70+ percent anthropogenic fault baseline, UNCLOS enforcement limits in the EEZ, and flag-of-convenience layering each independently lower the probability of state-attributable adjudication, and they compound.[19, 7, 20, 21, 14]

3 Moderate — Repair-fleet capacity is the binding operational constraint that a concentrated incident campaign would expose first, before either insurance market withdrawal or kinetic Western response.[7, 6, 29, 4]

4 High — NATO and EU institutional response since 2023 has accelerated meaningfully but remains a monitoring posture, not a cost-imposition posture. The CUI Cell, Baltic Sentry, and the EU Action Plan improve coordination and resilience without altering the UNCLOS legal floor or the Article 5 threshold that produce the gap.[15, 16, 17, 20]

5 Moderate

Marine cable insurance is functioning at current incident frequency; the binding constraint is the war-exclusion language, which is moving into active renegotiation in the 2025-26 renewal cycle and is where pricing will move first under stress.[28, 29, 30]

6 High

The two structural chokepoints that compress the West's seafloor exposure, the Egyptian land-and-sea corridor and the Luzon Strait, are the most asymmetric concentration risks in the global communications network, and both sit in geopolitical environments where attribution norms are weak.[12, 3, 5, 8]

7 Moderate

The Estlink-2 / Eagle S Finnish response of December 2024 is the prototype for incident-by-incident hardening absent state-level attribution: board the vessel, prosecute the owner, recover damages, and treat the sponsoring-state question as a separate diplomatic process. We judge that this pattern, not state attribution, is what Western seafloor enforcement actually looks like over the next 12 months.[11, 21, 14]

SECTION 01 · STRUCTURE

The Asset Class and Where It Concentrates

The West's seafloor infrastructure is large, fragile, and structurally concentrated, behaving more like a small number of high-value transit corridors than like a distributed mesh.

Roughly 574 active or planned submarine cable systems span approximately 1.45 million route-kilometres in 2025, carrying somewhere between 95 and 99 percent of international data traffic and the operational majority of intercontinental financial messaging through SWIFT, CHIPS, and major exchange networks.[1, 2, 3, 4, 5] Offshore pipelines (Nord Stream 1 and 2 prior to 2022, the Norwegian system, the Mediterranean network, and the Baltic and North Sea systems) add an energy-routing dimension to the same seafloor envelope. Seafloor sensor arrays, legacy SOSUS architecture and successors, civilian seismic networks, and offshore oil and gas SCADA, complete the asset class.

The first concentration feature is landing-station concentration. Submarine cables surface at a small number of beach-manholes, cable-landing stations, and inland fiber junctions; the worldwide total of

active landing points is several hundred, materially below the visible cable-count, and the operationally critical subset is much smaller.[6, 3] RAND's 2024 analysis frames the landing-station as the principal physical vulnerability.[6]

The second is chokepoint concentration on intercontinental routes. The Egyptian land-and-sea corridor between the Mediterranean and the Red Sea carries approximately 17 percent of intercontinental cable bandwidth.[3, 8] The Luzon Strait between Taiwan and the Philippines carries roughly 30 percent of trans-Pacific east-west bandwidth and is one of the densest cable choke points globally.[5, 8] Both Egypt and the Luzon Strait sit in geopolitical environments where attribution norms are weak.

The third is repair-fleet concentration. Roughly 60 to 75 cable-capable vessels operate globally, owned and managed by approximately 10 firms, principally Alcatel Submarine Networks, SubCom, NEC's specialist subsidiary, and a small set of independents.[6, 4] The fleet is sized for the routine baseline of 150 to 200 faults per year, of which more than 70 percent are anthropogenic (fishing gear, anchors, dredging), repairable through the routine 8-to-16-week cycle.[7, 24, 6] The International Cable Protection Committee's Recommendation 6 on cable routing and Recommendation 13 on best practice define the technical floor for routing, burial, and repair scheduling but do not address state-actor sabotage scenarios.[24]

ASSESSMENT · HIGH CONFIDENCE

The structural concentration of the West's subsea footprint at landing stations, intercontinental chokepoints, and a small repair fleet is the asset-class feature that makes the attribution gap binding. The same cable network that is operationally resilient to a routine fault rate of 150 to 200 faults per year is exposed to a concentrated incident campaign that would saturate any one of the three concentration points before remediation could be configured.

Rationale: RAND landing-station analysis; TeleGeography 2025 chokepoint share data; ICPC fleet baseline.

SECTION 02 · WALK-THROUGH

The Incident Record and the Attribution Gap

The 2022-to-2025 incident record is the load-bearing evidence in this brief. Five named clusters frame the pattern, and the attribution outcome is uniform.

Nord Stream 1 and 2, September 26, 2022. Explosive damage in Swedish and Danish exclusive economic zones to two strategic gas pipelines.[9, 2] Sweden closed its preliminary criminal investigation in February 2024 without public attribution.[9] Denmark closed its investigation in the same month

without public attribution. Germany's Federal Prosecutor's investigation remains active and has issued a European arrest warrant in 2024 for a Ukrainian national identified through forensic and travel evidence; the broader state-actor question has not been adjudicated.[10] Three and a half years after the incident, no finalized state-actor attribution has issued from any Western legal track.

Matsu Islands, Taiwan, February 2 to 8, 2023. Two Chinese-flagged vessels, identified by Taiwan's Ministry of Digital Affairs and Chunghwa Telecom as a fishing vessel and a cargo vessel, severed both undersea cables connecting Matsu to the main island within six days; communications were degraded for approximately 50 days.[12] No Chinese state attribution has been advanced by Taiwan, and the incident remains formally classified as a non-state commercial fault. The Matsu case is the cleanest existing analog for what a Luzon Strait incident under cover of fishing or shipping traffic would look like.

Balticconnector pipeline and Estlink-1 / C-Lion telecoms cables, October 8, 2023. Damage to the Estonia-Finland gas pipeline and parallel telecoms cables.[11, 2] The Finnish National Bureau of Investigation identified the Hong Kong-flagged container ship Newnew Polar Bear as the suspected vessel; the vessel's anchor was physically recovered from the seabed near the fault location.[11, 14] PRC cooperation was pledged but has not converted to public determinations.

C-Lion1 and BCS East-West, November 17 to 18, 2024. Damage to the Finland-Germany and Lithuania-Sweden cables; AIS analysis identified the Chinese-flagged Yi Peng 3 at both fault locations during the relevant windows.[13, 32] European authorities boarded the vessel; criminal jurisdiction questions delayed the legal track.

Estlink-2 power cable and four parallel telecoms cables, December 25, 2024. The most aggressive Western legal response to date. Finnish authorities identified the Cook Islands-flagged Eagle S, characterised by the NBI as part of Russia's shadow fleet, and boarded and detained the vessel on Finnish EEZ on a cable-damage cause of action.[11, 13, 14] The case has not produced a state-actor attribution; it has produced a foreign-flagged vessel held under Finnish criminal process and a civil-damages track against the owner.

Red Sea cables, late February to early March 2024. Severance of SEACOM, AAE-1, EIG, and TGN-EA in the southern Red Sea.[29] The Belize-flagged Rubymar, struck by a Houthi missile and drifting with its anchor deployed, is the suspected anchor-drag vector. The ACLED maritime layer recorded more than 90 Houthi-attributed maritime attacks between November 2023 and end-2024, providing the background traffic density.[33]

Three things are true of this record. The incidents are not rare: five major clusters in roughly 39 months, with the cadence accelerating in 2024. The attribution outcome is uniform: no incident has produced a finalized public state-actor attribution. And the architecture that would close the gap has not changed. UNCLOS Articles 113 to 115 establish a criminalization obligation but do not authorize coastal-state enforcement against foreign-flagged vessels beyond the territorial sea except in narrow circumstances.[19, 20, 21]

ASSESSMENT · HIGH CONFIDENCE

The attribution gap is structurally produced and durable. Five incident clusters over 39 months have produced zero state-actor attributions through Western investigations; the proximate-actor prosecutions that have advanced (German criminal track on a Ukrainian national; Finnish criminal and civil tracks on the Eagle S owner) do not close the state-attribution question. The relevant analytical category is not unsolved incidents but a structural equilibrium in which state-aligned actors can produce strategic seafloor effects at low expected attribution cost.

Rationale: Closed Swedish and Danish Nord Stream tracks without public attribution; open German, Finnish, and Estonian tracks without state-actor adjudication; UNCLOS and Tallinn Manual constraints; ICPC anthropogenic baseline providing structural cover.

SECTION 03 · CAPITAL

The Repair-Fleet Constraint No One Has Re-Priced

The repair-fleet capacity question is under-discussed in the public threat literature and is, in our judgment, the binding operational constraint on the system.

Approximately 60 to 75 cable-capable vessels operate globally; approximately 10 owner and operator firms control the fleet.[6, 4] The vessels are specialised: cable-laying ships and cable-repair ships carry dynamic positioning systems, plough or grapnel equipment, and trained crews. Conversion from a non-specialised hull is impractical inside any operationally relevant timeline.

The fleet is sized for the routine fault baseline. The ICPC reports approximately 150 to 200 faults per year globally; more than 70 percent are anthropogenic and most are repairable on the routine 8-to-16-week cycle conditional on vessel availability, host-state permit issuance, weather windows, and spares.[7, 24, 6] The economic logic of the fleet is consortium-led: cable owners contract for repair coverage on standing agreements that pool risk across multiple cables. The standing agreements assume the routine baseline.

Surge inelasticity is the first binding feature. There is no shadow inventory of cable-repair vessels. A multi-incident event in a single geographic area (a Baltic cluster, a Luzon Strait cluster, an Egyptian corridor cluster) draws on the same regional fleet that is already servicing routine faults; the operationally relevant question is how many vessels are available within a 7-to-30-day mobilisation window from the incident area, and the answer is consistently small. The Red Sea 2024 cluster produced repair delays of several months on cable-by-cable timing, even though only three to four cables were affected and the regional fleet had a clear mobilisation path.[29]

Permit and access friction is the second. Cable-repair vessels operate under host-state permits that are issued routinely under peacetime conditions and become slow, conditional, or contested under tension. A Luzon Strait cluster would require permit cooperation across Taiwan, the Philippines, and (depending on fault location) PRC-claimed waters. A Black Sea cluster would require navigation through a Turkish-controlled Bosphorus regime under the Montreux Convention. An Egyptian corridor cluster would require Egyptian government cooperation that is currently routine but contingent.

The repair architecture is not sized for an adversarial environment. A concentrated multi-cable incident in one of the chokepoint corridors would saturate regional repair capacity, push repair cycles well beyond the routine 8-to-16-week window, and produce degraded routing through alternative cables for months. Insurance market response would lag the operational reality; naval and law-enforcement response, constrained by UNCLOS, would not produce attribution at speed.

ASSESSMENT · MODERATE CONFIDENCE

Repair-fleet capacity is the binding operational constraint that a concentrated incident campaign would expose first, before either marine-insurance capacity withdrawal or kinetic Western response. The 60-to-75-vessel fleet is sized for the routine fault baseline, not for an adversarial regime, and the surge inelasticity is exacerbated by host-state permit dependencies in exactly the chokepoint geographies that adversaries would target.

Rationale: RAND fleet analysis; SubTel Forum 2024-2025 industry report; ICPC fault baseline and recommendation framework; Red Sea 2024 documented repair lags.

SECTION 04 · POLICY

The Regulatory Architecture and the Legal Seam

The regulatory response has accelerated meaningfully but operates inside a legal architecture that pre-existed the threat picture and that, by design, does not provide enforcement tools at the relevant level.

The NATO layer has advanced the most visibly. In February 2024, NATO established the Critical Undersea Infrastructure (CUI) Cell at Maritime Command, with the United Kingdom as lead sponsor.[15] On January 14, 2025, NATO activated Baltic Sentry, deploying frigates, aircraft, and naval drones to monitor critical undersea infrastructure in the Baltic in direct response to the Estlink-2 incident.[16] The Atlantic Council and RUSI both assess that the CUI Cell's mandate is monitoring and information-

sharing rather than autonomous enforcement, and that the Article 5 collective-defence threshold for a seafloor attack remains undefined.[25, 27]

The EU layer has moved on a parallel track. The European Commission published its EU Action Plan on Cable Security on February 21, 2025, providing a coordination layer over the existing Critical Entities Resilience (CER) Directive and the NIS2 cybersecurity directive.[17, 22, 18] ENISA published a 2024 threat-landscape report on subsea cables, followed by a 2025 recommendations update with a sabotage taxonomy and resilience-by-design guidance.[1, 23] The EU framework is, in operational terms, a resilience and coordination framework; it does not create new enforcement instruments against foreign-flagged vessels.

The UNCLOS floor is the load-bearing constraint. UNCLOS Articles 113 to 115 require flag states and coastal states to criminalize wilful or negligent damage to submarine cables and to provide indemnity for vessels that sacrifice anchors to save cables.[19] The convention does not, however, authorize a coastal state to enforce against a foreign-flagged vessel in its exclusive economic zone for cable damage occurring beyond the territorial sea, except in narrow circumstances.[19, 20, 21] The CCDCOE Tallinn Manual analysis further establishes that an attack on a submarine cable may constitute a use of force under Article 2(4) of the UN Charter only in narrow circumstances, and is not automatically an armed attack for Article 51 purposes.[20] The legal seam is therefore a gap between the criminal-law floor and the armed-attack ceiling. The space between is exactly where state-aligned actors operate.

The US enforcement layer has tightened on a different axis. The FCC's Team Telecom, the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, has reviewed and conditioned multiple submarine cable license applications since 2020.[34] Conditions have included denial of the Hong Kong segment of the Pacific Light Cable Network and routing, ownership, and oversight conditions on Hong Kong-Americas (HKA) and successor systems. This is regulatory hardening at the entry-and-ownership layer rather than at the operational-response layer.

The Eagle S response in December 2024 is the prototype for what the existing architecture can produce. Finnish authorities boarded and detained a foreign-flagged vessel inside Finnish EEZ on a cable-damage cause of action.[11, 14] The owner-of-record was prosecuted; the cargo charter chain was investigated; the P&I club was engaged. The state-attribution question was treated as a separate diplomatic process and was not adjudicated by the Finnish court. The Estlink-2 prototype is what the law allows. It is not what closes the gap; it is what the gap concedes.

ASSESSMENT · HIGH CONFIDENCE

The regulatory architecture has accelerated meaningfully on monitoring, coordination, and resilience layers but has not changed the legal seam that produces the attribution gap. NATO's CUI Cell and Baltic Sentry, the EU Action Plan and CER Directive, and ENISA's 2024-2025 framework all operate inside the existing UNCLOS floor and the Article 5 ceiling. The Estlink-2 prototype, vessel-of-record prosecution without state attribution, is the realistic enforcement ceiling under current law.

Rationale: NATO CUI Cell mandate; EU Action Plan published February 2025; UNCLOS and Tallinn Manual constraints; Eagle S Finnish criminal track.

SECTION 05 · TRANSMISSION

The Insurance Liability Surface

Marine cable insurance sits in a small London-led market with limited public disclosure; the war-exclusion language is where pricing will move first under stress.

Howden Re's 2024-2025 market review and Lloyd's List's reporting on rising 2024 claims are the load-bearing public sources.[28, 30] Marine cable physical damage cover is offered by a small number of Lloyd's syndicates and London-market reinsurers; the market has not withdrawn capacity in response to the 2024 incident cluster but has moved toward harder terms. Cable losses are typically attritional (single faults, multi-month repair costs in the high single-digit-millions to low double-digit-millions of dollars per fault) and aggregate exposure on a single consortium-owned cable can run into the hundreds of millions over a 25-year design life.

War-exclusion language is the load-bearing contractual surface. Marine war-risk and cable insurance wordings typically include sabotage and malicious-damage extensions but exclude losses arising from acts by named state actors or in formal war zones absent specific endorsement.[28, 30] The 2024 incident cluster has moved war-exclusion language into the active contested edge. Two questions are working: whether a state-actor finding (in any of the open Western investigations) would trigger a war-exclusion across the cluster of incidents, and whether the Joint War Committee will move toward designated-area listings for high-risk subsea corridors comparable to the Red Sea designation of December 2023.[29, 33]

The liability transmission chain runs from cable owners (consortium SPVs, hyperscalers, telecom carriers) carrying the physical damage exposure, through their charterers and contracted vessel operators carrying P&I exposures through the International Group of P&I Clubs, to the underlying cargo and freight exposures in the marine cargo and hull markets. A sabotage event in a war-exclusion-

triggering posture would push losses up the chain in ways that are not currently priced into the routine claims architecture. The Estlink-2 / Eagle S civil track is the first live test of the cable-damage-to-vessel-owner liability path in a sabotage-adjacent context.

We do not have public visibility into aggregate marine-cable insurance exposure or 2024 paid-claims totals at granularity below trade-press summaries. This is the single largest opacity in the registry. The Howden Re and Lloyd's List sources we carry are directional rather than quantitative on aggregate market exposure.

ASSESSMENT · MODERATE CONFIDENCE

The marine cable insurance market is functioning at current incident frequency but is not re-priced to a sustained sabotage regime, and the war-exclusion language is the contractual surface where pricing will move first under stress. The Joint War Committee's Red Sea 2023 designation is the working analog for what a subsea-corridor war-zone listing would look like; a comparable designation on a Baltic, Luzon, or Egyptian corridor would reprice cable physical-damage and marine war-risk simultaneously.

Rationale: Howden Re 2025 review; Lloyd's List rising-claims reporting; documented JWC Red Sea action.

SECTION 06 · STAKEHOLDER

The Grey-Zone Toolkit and the Capability Picture

The capability question divides cleanly into two pictures: a mature Russian seabed posture and a less OSINT-mature but operationally documented Chinese pattern.

The Russian seabed-capability picture is well-documented in OSINT. The Main Directorate for Deep-Sea Research (GUGI), reporting directly to the Ministry of Defence rather than through the Navy, operates a dedicated fleet that includes the Belgorod (a special-mission nuclear submarine, designed as the AS-31 Losharik mother vessel and a Status-6 / Poseidon platform) and the Yantar, a publicly tracked intelligence vessel observed over Atlantic and Mediterranean cable routes in 2023 and 2024.[29, 31] Janes' open-source assessment frames the GUGI capability as both a strategic-deterrence-adjacent asset and a peacetime seafloor reconnaissance instrument; the Yantar's track patterns over UK, Irish, and Norwegian cables in the 2023-2024 window are the canonical OSINT signal.

Layered above the dedicated GUGI fleet is the shadow fleet, the sanctions-evading network of tankers and bulk carriers estimated by Western analyses at 600 to 1,000 vessels, that has been linked to multiple Baltic incidents through AIS track analysis.[26, 14, 32] IISS, FT, and MarineTraffic AIS data

converge on the shadow-fleet linkage to the Eagle S, the Yi Peng 3, and the broader anchor-drag pattern. The shadow fleet provides a deniability layer above the dedicated military capability; the operational logic is that the strategic-effect mechanism is anchor-drag from a flagged-vessel-of-convenience, not visible military action.

The Chinese seabed-capability picture is materially less mature in OSINT. The PLA Strategic Support Force and its successor organisations operate seabed-survey and communications capability whose order-of-battle is publicly limited; specific cable-tap or cable-cut capability is not OSINT-confirmed at the level of Russian GUGI documentation. The working evidence is incident-based: the Matsu 2023 cuts, the Newnew Polar Bear in the Balticconnector incident, and the Yi Peng 3 in the November 2024 Baltic cluster are the publicly traceable patterns.[12, 6, 14, 32] Atlantic Council and CSIS analyses frame the Chinese threat picture as more focused on Taiwan-area and Luzon-Strait cables than on Atlantic systems; the Matsu cuts are treated as the working precedent for what a Taiwan-Strait crisis cable scenario would look like.[2, 27]

The grey-zone toolkit in operational terms is now well-understood: anchor-drag attribution from a flag-of-convenience vessel, AIS-dark periods or AIS-spoofing through the fault window, shadow-fleet ownership layering through holding companies in disclosure-limited jurisdictions, and cooperation with the legal track at the surface level paired with non-cooperation at the substantive level. Each tool independently lowers the probability of state-actor adjudication; in combination they produce the structural equilibrium described.

ASSESSMENT · MODERATE CONFIDENCE

The Russian seabed-capability picture is the principal driver of NATO posture changes in 2024-2025 and is the most operationally mature OSINT-confirmed threat. The Chinese seabed-capability picture is less OSINT-mature but is the principal driver of the Luzon Strait and Taiwan-area risk envelope, with the Matsu 2023 incident as the working precedent. The grey-zone toolkit is sufficiently developed that no additional capability acquisition is required for a state actor to produce strategic-scale seafloor effects at low attribution cost.

Rationale: Janes GUGI capability assessment and Yantar track record; IISS shadow-fleet framing; Matsu incident as the Chinese precedent; AIS-track analysis on Eagle S, Yi Peng 3, Newnew Polar Bear.

SECTION 07 · OUTLOOK

Three Scenarios, 12-Month Horizon

Construction confidence reflects analytical quality, not probability. Each scenario carries a triggering signal and a primary impact for the operator lens.

Baseline · Grey-Zone Equilibrium Persists

CONSTRUCTION CONFIDENCE: HIGH · VELOCITY: GRADUAL

The 2022-to-2025 pattern continues through the next four quarters with one to three additional named incidents in Baltic, Mediterranean, or Asia-Pacific waters. The German Nord Stream investigation produces no public state-level indictment in 2026; the Finnish Eagle S prosecution proceeds through criminal and civil tracks against the vessel owner without state-actor finding; the Balticconnector case remains in procedural-cooperation phase. NATO's CUI Cell expands its monitoring remit incrementally; the EU Action Plan implementation moves forward inside its existing legal frame. Marine cable insurance pricing firms on new placements; the Joint War Committee does not designate any subsea corridor; war-exclusion language tightens at the margin. Repair-fleet capacity is adequate for the routine baseline plus the incremental sabotage frequency; repair cycles run inside the 8-to-16-week envelope.

SIGNAL TO WATCH: **CONTINUED ABSENCE OF ANY FINALIZED STATE-LEVEL ATTRIBUTION THROUGH THE NEXT 12 MONTHS**

Deterioration · Concentrated Multi-Cable Cluster in a Chokepoint

CONSTRUCTION CONFIDENCE: MODERATE · VELOCITY: RAPID

A multi-cable incident in either the Luzon Strait, the Egyptian land-and-sea corridor, or the Baltic produces three-to-six near-simultaneous cable cuts, saturating regional repair-fleet capacity and pushing repair cycles well beyond the routine 8-to-16-week envelope. Repair vessel mobilisation runs into host-state permit friction; insurance war-exclusion language is contested across multiple loss notifications. The Joint War Committee moves toward a designated-area listing for the affected corridor on its next quarterly review. Marine cable insurance pricing moves materially across the global portfolio. NATO and EU response remains inside the monitoring posture; no state-actor attribution is reached, but the Eagle S prototype is replicated against multiple vessels.

SIGNAL TO WATCH: **A MULTI-CABLE INCIDENT IN ANY SINGLE CHOKEPOINT CORRIDOR OR NATO DECLARATION OF AN ARTICLE 4 CONSULTATION ON A SEAFLOOR INCIDENT**

Stabilization · Attribution Event Closes the Gap

CONSTRUCTION CONFIDENCE: LOW-MODERATE · VELOCITY: STRUCTURAL

A finalized public state-attribution event in one of the four open Western investigations (the German Nord Stream track is the highest-probability venue) produces a precedent that materially changes the deterrence calculus. NATO and EU institutional response reconfigures from monitoring to cost-imposition; Article 5 threshold conversations advance; the Joint War Committee may designate corridors on a forward-looking basis. Marine cable insurance pricing reprices off the new legal precedent; war-exclusion language is reconfigured. The repair-fleet capacity question becomes a policy question rather than an industry question, with potential state subsidy or capacity-expansion programmes.

SIGNAL TO WATCH: **PUBLIC INDICTMENT NAMING A STATE-ACTOR NEXUS FROM ANY OF THE FOUR OPEN INVESTIGATIONS**

ASSESSMENT · MODERATE CONFIDENCE

Across all three scenarios the structural concentration of the West's seafloor footprint and the repair-fleet capacity constraint do not change on a 12-month horizon. The difference between Baseline and Deterioration is principally a question of incident concentration in chokepoint geographies, not of new capability or new vulnerability. The difference between Baseline and Stabilization is principally a question of whether any one of the four open Western investigations produces a precedent-setting indictment, and the most operationally productive monitoring target for an operator is the German Nord Stream track.

Rationale: Persistent concentration of bandwidth, repair fleet, and landing-station footprint; documented investigation status across four open tracks; NATO and EU institutional response inside the existing legal frame.

SOURCE REGISTRY

1. ENISA, "Subsea Cables: What is at stake?: Threat landscape and policy options," 2024-06-17.
2. CSIS, "Sabotage at Sea: Defending Undersea Cables in an Era of Great Power Competition," 2025-01-09.
3. Brookings Institution, "The hidden geopolitics of subsea cables," 2024-09.
4. Submarine Telecoms Forum, "Industry Report 2024-2025: Fleet, Routes, Capacity," 2025-04.
5. TeleGeography, "Submarine Cable Map 2025 / TeleGeography database," 2025 (live).
6. RAND Corporation, "Undersea Cables and the Future of Submarine Competition," 2024-08.
7. International Cable Protection Committee (ICPC), "Submarine Cable Fault Statistics: Annual Summary," 2024.
8. TeleGeography, "State of the Network 2025: submarine bandwidth and chokepoints," 2025-01.

9. Swedish Accident Investigation Authority (SHK), "Report on Nord Stream 1 and 2 incident, Swedish sector," 2023-02-07.
10. German Federal Prosecutor (Generalbundesanwalt), "Press statements re Nord Stream investigation," 2024-2025.
11. Finnish National Bureau of Investigation (KRP / NBI), "Investigation update: Balticconnector and Estlink-2 / C-Lion1," 2023-10 / 2024-12.
12. Taiwan Ministry of Digital Affairs (MoDA) / Chunghwa Telecom, "Matsu cable cuts: incident summary and timeline," 2023 / 2025 update.
13. Reuters, "Two telecom cables in Baltic Sea broken; sabotage suspected; Eagle S / Yi Peng 3 follow-on," 2024-11-18 / 2024-12-26.
14. Financial Times, "Russia's shadow fleet linked to suspected Baltic cable sabotage," 2024-12-30.
15. NATO, "NATO stands up Critical Undersea Infrastructure (CUI) Cell at Maritime Command," 2024-02-15.
16. NATO Maritime Command (MARCOM), "Activation of Task Force X / Baltic Sentry," 2025-01-14.
17. European Commission, "Joint Communication on EU Action Plan on Cable Security," 2025-02-21.
18. European Commission, "Announcement banning gallium, germanium, antimony, certain superhard materials, and certain graphite products to the United States (note: corrected entry on file)," 2024-12-03.
19. United Nations, "UN Convention on the Law of the Sea (UNCLOS), Arts 113-115," 1982 / in force 1994.
20. CCDCOE, "Tallinn Manual perspectives on attacks against submarine cables," 2024.
21. Lawfare, "Deterring Subsea Sabotage: The Limits of Attribution," 2024-12.
22. European Commission, "Council Recommendation on EU-coordinated approach to strengthen resilience of critical infrastructure," 2023-12-08.
23. European Union, "Directive (EU) 2022/2557 on the resilience of critical entities (CER)," 2022-12-14.
24. ICPC, "Recommendation 6 (Cable Routing) and Recommendation 13 (Best Practice)," 2023 (current ed.).
25. RUSI, "Below the Surface: Defending Subsea Cables and Pipelines from Sabotage," 2024-11.
26. IISS, "Strategic Survey 2024: Grey-zone activity in the Baltic," 2024-11.
27. Atlantic Council, "Cables, anchors, and ambiguity: NATO's seabed defense problem," 2025-02.
28. Howden Re / Howden Group, "Submarine Cable Insurance: Market Review 2024-2025," 2025-03.
29. Bloomberg, "Red Sea cables severed as Houthi conflict spills into seabed," 2024-03-04.
30. Lloyd's List, "Marine cable claims surge after Baltic and Red Sea incidents," 2025-02.
31. Janes (IHS Janes), "Russia's Main Directorate for Deep-Sea Research (GUGI): capability assessment," 2024-2025.
32. MarineTraffic / AIS data layer, "AIS tracks of Eagle S, Yi Peng 3, Newnew Polar Bear at incident windows," 2023-2024.
33. ACLED, "Maritime incident layer: Red Sea and Black Sea 2024-2025," 2025 (rolling).
34. US Department of Justice, "FCC Team Telecom: submarine cable license reviews," 2024-2025.
35. US Coast Guard / NOAA, "Submarine Cable Awareness: chart symbology and federal cable protection," 2024 (current).
36. ENISA, "Threat Landscape for Submarine Communication Cables: Recommendations," 2025-03-19.

AEGEAN INTELLIGENCE GROUP

Publishable Market Research

Timeliness: DURABLE. This brief is classified DURABLE. The structural pattern that produces the attribution gap (UNCLOS legal architecture, anthropogenic fault baseline, flag-of-convenience layering, shadow-fleet deniability, repair-fleet surge inelasticity, chokepoint concentration) is stable across a 6-to-18-month horizon. AEIG will issue an Update Addendum on a discrete supersession event, defined as a finalized public state-actor attribution from any of the four open Western investigations; a multi-cable incident in a chokepoint corridor exceeding the routine baseline; or a material EU or NATO legal-architecture revision that changes the UNCLOS enforcement frame.

Classification: CLIENT CONFIDENTIAL. Prepared on open-source intelligence verified against allowlisted Tier 1 to Tier 4 sources. Russian and Chinese state media do not appear in the registry; capability claims about GUGI and the PLA Strategic Support Force are routed through Janes, RUSI, IISS, and Western T1 government primaries. Attribution-disputed incidents are treated as contested and not adjudicated. Analytic judgments are Aegean's.

contact@aegeanintel.com · aegeanintel.com