



Integrasi Arsitektur C6ISR Dalam Strategi Antisipatif Deteksi Aktivitas Mencurigakan pada Infrastruktur Kabel Bawah Laut Indonesia: Kajian Strategis 2024–2026

Shanty Damayanti Hartatianti¹ David Frederyc Koynja² Pujo Widodo³

Departemen Peperangan Asimetris, Universitas Pertahanan Republik Indonesia^{1,2,3}

Email: shanty.hartatianti@sp.idu.ac.id¹ david.koynja@sp.idu.ac.id² pujowidodo78@gmail.com

Abstrak

Infrastruktur kabel bawah laut merupakan komponen kritis ekonomi digital global dan menjadi elemen penting dalam keamanan maritim selama periode 2024–2026. Geografi Indonesia sebagai negara kepulauan menempatkan jalur kabel, stasiun pendaratan, dan koridor maritim tertentu dalam lingkungan operasi yang kompleks, di mana kerusakan tidak disengaja, aktivitas kriminal, pemaksaan geopolitik, dan gangguan disengaja sulit dibedakan secara waktu nyata. Penelitian ini mengkaji bagaimana arsitektur C6ISR terintegrasi dapat memperkuat deteksi, penilaian atribusi, ketahanan, dan pengambilan keputusan atas insiden kabel bawah laut. C6ISR dalam penelitian ini digunakan sebagai konstruksi analitis khusus yang mengintegrasikan command, control, communications, computers, cyber defence, combat/intervention, intelligence, surveillance, dan reconnaissance; istilah ini tidak dimaksudkan sebagai klaim bahwa C6ISR merupakan akronim doktrinal tunggal yang telah terstandardisasi secara universal. Penelitian menggunakan telaah dokumen dan studi kasus komparatif terhadap insiden Yi Peng 3 dan Eagle S di Laut Baltik, sistem Pukpuk 1 yang diresmikan pada 2026, inisiatif internasional ketahanan kabel, serta kerangka UNCLOS. Hasil analisis menunjukkan bahwa deteksi dan atribusi membutuhkan fusi multi-sumber; ketentuan UNCLOS relevan tetapi tidak memberikan kewenangan penegakan universal yang sederhana bagi negara pantai di EEZ; dan ketahanan bergantung pada kombinasi sensing, koordinasi kelembagaan, diversifikasi rute, kesiapan perbaikan, keamanan stasiun pendaratan, serta kesiapan hukum. Artikel ini mengembangkan arsitektur C6ISR berlapis yang menghubungkan sensing, fusi data, penilaian hukum, keputusan komando, respons, dan pemulihan dalam satu siklus keputusan. Artikel tidak menyimpulkan bahwa insiden tertentu merupakan operasi terselubung yang disponsori negara tanpa temuan otoritatif; kasus digunakan untuk menguji tantangan deteksi, atribusi, dan yurisdiksi.

Kata Kunci: C6ISR; Kabel Bawah Laut; Keamanan Maritim; Operasi Zona Abu-Abu; Ketahanan Infrastruktur Kritis; UNCLOS; Kedaulatan Digital

Abstract

Submarine cable infrastructure is a critical component of the global digital economy and an essential element of maritime security during the 2024–2026 period. Indonesia's archipelagic geography places cable routes, landing stations, and specific maritime corridors within a complex operational environment in which accidental damage, criminal activities, geopolitical coercion, and deliberate disruption are difficult to distinguish in real time. This study examines how an integrated C6ISR architecture can strengthen the detection, attribution assessment, resilience, and decision-making processes associated with submarine cable incidents. In this study, C6ISR is employed as a specialized analytical construct integrating command, control, communications, computers, cyber defence, combat/intervention, intelligence, surveillance, and reconnaissance. The term is not intended to imply that C6ISR constitutes a universally standardized doctrinal acronym. The study employs document analysis and comparative case studies of the Yi Peng 3 and Eagle S incidents in the Baltic Sea, the Pukpuk 1 system commissioned in 2026, international cable resilience initiatives, and the legal framework established under the United Nations Convention on the Law of the Sea (UNCLOS). The analysis indicates that detection and attribution require multi-source information fusion; although UNCLOS provides relevant legal provisions, it does not establish a simple, universally applicable enforcement authority for coastal states within their exclusive economic zones (EEZs). Furthermore, resilience depends on a combination of sensing capabilities, institutional coordination, route diversification, repair readiness, landing station security, and legal preparedness. This article develops a layered C6ISR architecture that connects sensing, data fusion, legal assessment, command decisions, response, and recovery within a unified decision-making cycle. The study does not



conclude that any particular incident constitutes a covert state-sponsored operation in the absence of authoritative findings; instead, the cases are used to examine the challenges of detection, attribution, and jurisdiction.

Keywords: C6ISR; Submarine Cables; Maritime Security; Grey-Zone Operations; Critical Infrastructure Resilience; UNCLOS; Digital Sovereignty



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

PENDAHULUAN

Kabel telekomunikasi bawah laut merupakan infrastruktur yang menopang konektivitas digital lintas negara. International Telecommunication Union (ITU) menyatakan bahwa kabel telekomunikasi bawah laut membawa lebih dari 99 persen lalu lintas data global dan menempatkan paparan fisik, konsentrasi geografis, serta waktu pemulihan sebagai isu utama ketahanan (International Telecommunication Union [ITU], 2026a, 2026b). Literatur terbaru juga menunjukkan bahwa keamanan kabel tidak dapat dipisahkan dari tata kelola infrastruktur kritis, kedaulatan digital, dan dinamika geoekonomi (Ganz et al., 2024; Govella, 2025). Relevansi isu tersebut semakin tinggi di Indo-Pasifik. Cannon (2025) menunjukkan bahwa keamanan kabel telah berkembang menjadi agenda kerja sama di antara negara-negara Indo-Pasifik, sementara Davenport (2025) menekankan perlunya kerja sama regional Asia Tenggara yang melampaui fasilitasi pembangunan dan perbaikan menuju pemantauan, pencegahan, respons, berbagi informasi, dan penguatan hukum nasional. Penelitian terbaru lainnya memperlihatkan bahwa risiko bersifat lokasi-spesifik dan dipengaruhi antara lain oleh batimetri, pengawasan, kedekatan strategis, karakteristik sistem, dan tingkat redundansi (Cannon et al., 2026). Bagi Indonesia, persoalan tersebut diperbesar oleh karakter geografis sebagai negara kepulauan yang berada pada persilangan Samudra Hindia dan Pasifik, dengan lalu lintas maritim yang padat dan jaringan konektivitas domestik serta internasional yang tersebar. Stasiun pendaratan dan koridor maritim tertentu dapat berfungsi sebagai node kritis; gangguan pada satu segmen karena itu dapat menghasilkan konsekuensi yang melampaui lokasi kerusakan. Risiko juga tidak terbatas pada pemotongan kabel, tetapi mencakup kerusakan akibat jangkar dan alat tangkap, pekerjaan konstruksi atau pengerukan, bahaya alam, kompromi siber-fisik pada fasilitas darat, serta risiko rantai pasok (Zhang et al., 2026).

Tantangan paling sulit bukan sekadar mendeteksi objek, tetapi membangun dasar pembuktian yang cukup untuk menghubungkan aktivitas maritim dengan kerusakan kabel tanpa melompat dari anomali ke atribusi. Kapal yang berada dekat kabel dapat melakukan kegiatan yang sah, termasuk pelayaran, penangkapan ikan, survei, atau perbaikan. Sebaliknya, gangguan yang disengaja dapat dirancang agar tampak seperti kecelakaan. Literatur mengenai ancaman hibrida di bawah permukaan laut menekankan pentingnya situational awareness dan koordinasi lintas organisasi, tetapi juga memperlihatkan bahwa ketidakpastian dan atribusi merupakan bagian inheren dari masalah (Loik, 2024; Ban, 2025). Dalam konteks ini, penelitian menggunakan istilah “Deterrence by Detection” sebagai proposisi analitis, bukan sebagai doktrin yang telah ditetapkan secara universal. Logikanya adalah bahwa deteksi yang persisten, dokumentasi yang kredibel, atribusi berbasis bukti, dan kemampuan merespons secara sah dapat mengubah manfaat yang diperkirakan dari suatu aktivitas mencurigakan. Namun, efek tersebut hanya mungkin apabila deteksi terhubung dengan kewenangan, bukti, dan ketahanan pemulihan. Literatur yang ada dapat dikelompokkan ke dalam sedikitnya tiga arus. Pertama, kajian mengenai kedaulatan digital dan tata kelola kabel menekankan persoalan kepemilikan, ketergantungan lintas yurisdiksi, dan keterbatasan kapasitas negara untuk mengendalikan infrastruktur yang secara ekonomi strategis (Ganz et al., 2024). Kedua, kajian

keamanan maritim dan kerja sama regional membahas perlindungan, deteksi, pencegahan, serta koordinasi perbaikan pada tingkat kawasan (Cannon, 2025; Davenport, 2025). Ketiga, kajian teknis menitikberatkan pada instalasi, pemantauan kondisi, fault localization, dan maintenance sebagai fondasi keandalan sistem (Zhang et al., 2026). Celah analitis yang diidentifikasi penelitian ini terletak pada belum terintegrasinya secara eksplisit empat fungsi yang sering dibahas secara terpisah: sensing maritim dan bawah laut; fusi serta preservasi bukti; penilaian hukum dan yurisdiksi; dan keputusan respons serta pemulihan. Penelitian ini menawarkan kebaruan berupa arsitektur C6ISR yang disusun secara khusus untuk konteks pertahanan kabel bawah laut Indonesia, dengan mempertahankan perbedaan antara deteksi, kausalitas, niat, atribusi, dan adjudikasi hukum. Dengan demikian, kontribusi penelitian bukan pada klaim adanya teknologi baru, melainkan pada integrasi fungsi-fungsi keputusan ke dalam satu kerangka analitis.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan desain analisis strategis berbasis telaah dokumen dan studi kasus komparatif. Periode analisis mencakup Januari 2024 sampai September 2026. Unit analisis utama terdiri atas (a) kerangka tata kelola dan hukum kabel bawah laut; (b) arsitektur fungsi C6ISR yang relevan untuk deteksi dan respons; dan (c) kasus publik yang memungkinkan penelusuran hubungan antara aktivitas maritim, kerusakan infrastruktur, pembuktian, dan proses hukum. Sumber data diprioritaskan dalam urutan: bahan hukum primer; dokumen dan pernyataan resmi lembaga pemerintah atau organisasi internasional; catatan pengadilan dan penegak hukum; publikasi ilmiah yang ditelaah sejawat; serta sumber teknis sekunder yang digunakan hanya untuk melengkapi informasi yang tidak tersedia pada sumber primer. Sumber utama meliputi UNCLOS 1982, ITU, NATO, otoritas Swedia dan Finlandia, PT Telkom Indonesia/Telin, catatan legislasi Amerika Serikat, serta artikel ilmiah mengenai ketahanan, keamanan maritim, dan hukum kabel bawah laut.

Analisis dilakukan melalui tiga tahap. Tahap pertama adalah ekstraksi bukti berdasarkan tema: ancaman fisik, sensing, fusi data, atribusi, yurisdiksi, pemulihan, dan ketahanan rantai pasok. Tahap kedua adalah triangulasi antar-sumber untuk menguji kesesuaian fakta, tanggal, status hukum, dan tingkat kepastian. Tahap ketiga adalah sintesis untuk menyusun arsitektur C6ISR dan matriks keputusan yang dapat digunakan sebagai model konseptual. Penelitian tidak menggunakan data intelijen rahasia, telemetry proprietary, atau dataset pelacakan kapal yang dibatasi; karena itu, penelitian tidak mengklaim dapat membuktikan operasi rahasia negara dari open-source indicators semata. Keandalan analisis dijaga melalui prinsip evidence-to-claim: setiap klaim faktual penting ditautkan pada sumber yang dapat diverifikasi; interpretasi hukum dibedakan dari isi norma; dan konsep yang masih berupa usulan atau hipotesis diberi label sebagai demikian. Kewarganegaraan kapal, anomali AIS, kedekatan geografis, atau kepemilikan komersial tidak diperlakukan sebagai bukti mandiri mengenai niat bermusuhan atau sponsor negara.

HASIL PENELITIAN DAN PEMBAHASAN

Kabel Bawah Laut sebagai Infrastruktur Strategis dan Risiko Sistemik

Analisis menunjukkan bahwa perlindungan kabel harus diletakkan pada tingkat sistem. Konsentrasi jalur di sekitar landing station, keterbatasan fasilitas perbaikan, kebutuhan kapal khusus, ketergantungan energi dan backhaul, serta karakteristik geografis dasar laut dapat membentuk single points of failure. Kajian ITU menempatkan konsentrasi geografis dan waktu perbaikan sebagai faktor penting ketahanan, sementara studi teknis menunjukkan pentingnya monitoring kondisi, fault localization, dan proses pemulihan yang terintegrasi (ITU, 2026a,

2026b; Zhang et al., 2026). Karena itu, keamanan kabel tidak dapat direduksi menjadi penjagaan fisik segmen kabel. Sistem nasional perlu menghubungkan wet plant monitoring, keamanan landing station, maritime domain awareness, operasi jaringan, keamanan siber, kewenangan hukum, kanal diplomatik, dan logistik perbaikan. Resiliensi merupakan atribut emergen dari keseluruhan sistem, bukan hasil dari satu sensor atau satu lembaga.

Model Ancaman

- Ancaman fisik: kerusakan akibat jangkar dan alat tangkap, pekerjaan konstruksi atau pengerukan, aktivitas dasar laut tanpa kewenangan, serta kemungkinan gangguan disengaja pada segmen yang rentan.
- Ancaman alam: gempa bumi, longsor bawah laut, dan proses geologi/vulkanik yang dapat merusak atau mengganggu sistem kabel.
- Ancaman siber-fisik dan terrestrial: kompromi IT/OT landing station, akses istimewa, manipulasi pemantauan, kompromi rantai pasok, dan gangguan fisik-siber yang saling menguatkan.
- Pengumpulan intelijen: pemetaan jalur, observasi pola perbaikan, pengukuran waktu respons, dan pengumpulan informasi mengenai ketergantungan jaringan. Motif atau pelaku tidak boleh ditetapkan tanpa bukti independen.

Arsitektur Sensing dan Fusi Data

Lapisan sensing yang relevan mencakup AIS, citra satelit, radar pantai, electro-optical/infrared observation, aset patroli, data lingkungan dan dasar laut, serta—jika layak secara teknis dan hukum—sensing akustik atau berbasis serat optik. NATO Baltic Sentry menunjukkan nilai penggabungan unsur permukaan, udara, sistem nirawak, dan aset pengawasan nasional untuk memperkuat maritime situational awareness (NATO, 2025). Distributed Acoustic Sensing (DAS) dapat dipertimbangkan sebagai salah satu sumber sensor. Literatur teknis menempatkan distributed sensing sebagai bagian dari perkembangan monitoring kabel, tetapi sinyal sensor tidak boleh dianggap sebagai mekanisme atribusi mandiri (Zhang et al., 2026). Kinerja DAS juga bergantung pada konfigurasi sistem, kebisingan lingkungan, lalu lintas kapal, dan karakteristik dasar laut. Untuk Indonesia, implementasi seharusnya dimulai dari pilot project terkontrol dengan pengukuran false positive, false negative, dan kemampuan deteksi sebelum menetapkan target operasional. Nilai tambah utama C6ISR terletak pada fusi. Sistem perlu mengorelasikan posisi dan riwayat kapal, lokasi kabel, data satelit, event akustik, cuaca-laut, kunjungan pelabuhan, pekerjaan dasar laut, jadwal perbaikan, dan indikator siber. Setiap observasi sebaiknya memuat provenance, timestamp, tingkat keyakinan, serta penjelasan atas ketidakpastian. Pendekatan ini mencegah kegagalan analitis ketika satu indikator anomali diperlakukan sebagai bukti konklusif.

Penilaian Atribusi dan Deterrence by Detection

Atribusi perlu diperlakukan sebagai proses bertingkat. Tingkat pertama adalah pencatatan perilaku yang teramati; tingkat kedua adalah hubungan kausal atau fisik dengan aset yang rusak; tingkat ketiga adalah penilaian niat; dan tingkat keempat adalah penilaian hubungan organisasi atau negara. Struktur tersebut konsisten dengan kebutuhan untuk memisahkan observable behavior dari intent dan state attribution. Kesulitan pembuktian merupakan persoalan sentral dalam literatur hukum kabel bawah laut (Zhang & Li, 2025). Dalam kerangka tersebut, “Deterrence by Detection” lebih tepat dipahami sebagai hipotesis strategis. Deteksi yang kredibel dapat memiliki nilai penangkalan hanya apabila informasi dapat dipreservasi, dibawa ke proses hukum atau diplomatik yang sah, dan didukung oleh

ketahanan pemulihan. Dengan kata lain, detection bukan tujuan akhir; nilai strategisnya bergantung pada linkage antara sensing, evidence management, authorized response, dan recovery.

Hukum Laut dan Yurisdiksi

UNCLOS menyediakan beberapa dasar hukum yang relevan. Pasal 79 mengatur kabel dan pipa bawah laut di landas kontinen; Pasal 58 mempertahankan hak dan kewajiban negara lain di EEZ, termasuk kebebasan navigasi dan pemasangan kabel dengan tunduk pada Konvensi; sedangkan Pasal 113 mengatur kewajiban negara untuk menetapkan ketentuan hukum atas kerusakan tertentu terhadap kabel yang dilakukan dengan sengaja atau karena kelalaian yang dapat dipersalahkan dalam kondisi yang ditentukan Konvensi (United Nations, 1982; Division for Ocean Affairs and the Law of the Sea [DOALOS], 2026). Implikasinya adalah bahwa UNCLOS tidak tepat digambarkan sebagai “enforcement vacuum” yang sederhana, tetapi juga tidak memberikan kewenangan otomatis dan umum kepada negara pantai untuk menaiki, menangkap, atau menyita kapal asing di EEZ hanya karena adanya kecurigaan gangguan kabel. Dasar penegakan bergantung pada lokasi, jenis tindakan, hubungan yurisdiksional, hukum domestik, perjanjian yang berlaku, dan keadaan insiden (Davenport, 2025; Zhang & Li, 2025). Perkara Eagle S memperjelas bahwa isu yurisdiksi dapat menjadi pusat sengketa bahkan ketika aparat nasional telah melakukan investigasi dan proses penuntutan. Pada 3 Oktober 2025, Pengadilan Distrik Helsinki tidak memeriksa dakwaan dengan alasan hukum pidana Finlandia tidak dapat diterapkan pada perkara tersebut. Pada 27 Agustus 2026, Pengadilan Banding Helsinki membatalkan keputusan itu dan mengembalikan perkara ke pengadilan tingkat pertama; keputusan banding tersebut sendiri belum berkekuatan hukum tetap (Helsinki District Court, 2025; Helsinki Court of Appeal, 2026). Dengan demikian, koordinasi hukum harus masuk pada tahap awal C6ISR, bukan setelah bukti operasional dikumpulkan. Setiap respons perlu dimulai dengan klasifikasi lokasi, identifikasi rezim hukum, pencatatan kewenangan, dan preservasi bukti yang memperhitungkan kemungkinan penggunaan dalam proses hukum.

Studi Kasus I: Yi Peng 3

Dua kabel data di Laut Baltik rusak pada 17–18 November 2024. Swedish Accident Investigation Authority mengidentifikasi Yi Peng 3, kapal berbendera Tiongkok, sebagai kapal yang relevan bagi penyelidikan. Otoritas Swedia melaporkan bahwa kapal tersebut menyeret jangkar dalam jarak yang panjang, tetapi penyelidikan tidak menghasilkan bukti konklusif bahwa kerusakan dilakukan dengan sengaja. Karena kapal berada di perairan internasional, Swedia juga menghadapi batasan yurisdiksi dalam melakukan tindakan investigatif tertentu; penyidik Tiongkok kemudian terlibat dalam proses di atas kapal (Swedish Accident Investigation Authority, 2024, 2025). Kasus ini penting bukan karena menetapkan pelaku, melainkan karena menunjukkan batas inferensi dari satu set indikator. AIS yang tidak lengkap atau perilaku kapal yang tidak lazim dapat memperkuat kebutuhan observasi, tetapi tidak otomatis membuktikan niat, kausalitas, atau sponsor negara. Bagi C6ISR, lesson learned utamanya adalah menjaga chain of reasoning dari observasi menuju atribusi tanpa menggabungkan seluruh tahap menjadi satu kesimpulan.

Studi Kasus II: Eagle S

Pada 25 Desember 2024, Eagle S, kapal tanker berbendera Kepulauan Cook, diselidiki setelah insiden di Teluk Finlandia. Otoritas Finlandia menyatakan penyelidikan kriminal terhadap kerusakan kabel telah selesai pada Juni 2025 dan menyebut tiga perwira senior

sebagai tersangka. Pada Agustus 2025, jaksa mengajukan dakwaan berkaitan dengan kerusakan berat dan gangguan komunikasi, sementara pihak terdakwa membantah kesalahan dan mempertanyakan yurisdiksi (Finnish National Bureau of Investigation, 2025; Finnish Prosecution Service, 2025). Perkembangan selanjutnya menunjukkan pentingnya dinamika yurisdiksi. Pengadilan Distrik Helsinki pada Oktober 2025 menyatakan dakwaan dan tuntutan ganti rugi tidak dapat diperiksa berdasarkan hukum pidana Finlandia. Pada 27 Agustus 2026, Pengadilan Banding Helsinki membatalkan keputusan tersebut dan mengembalikan perkara untuk pemeriksaan lebih lanjut. Pengadilan banding menyatakan bahwa otoritas Finlandia memiliki kompetensi untuk memeriksa dakwaan dengan mempertimbangkan prinsip teritorial dan konsekuensi tindak pidana di Finlandia; keputusan tersebut belum final (Helsinki District Court, 2025; Helsinki Court of Appeal, 2026). Pelajaran operasional bagi Indonesia adalah bahwa evidence architecture harus dibangun sejak detik awal: identifikasi kapal, lokasi hukum, preservasi jejak dasar laut, dokumentasi keadaan kapal sejauh diperoleh secara sah, chain of custody, dan konsultasi hukum. Dengan demikian, C6ISR bukan hanya sistem sensor, tetapi juga sistem produksi bukti yang dapat dipertanggungjawabkan.

Studi Kasus III: Pukpuk 1 dan Diversifikasi Rute

PT Telkom Indonesia melalui Telin meresmikan sistem kabel bawah laut Pukpuk pada 8 Mei 2026 di Jayapura. Informasi resmi Telkom mendeskripsikan Pukpuk sebagai sistem lintas batas Indonesia–Papua Nugini, dengan stasiun pendaratan Jayapura berfungsi sebagai gateway menuju jaringan Kumul Papua Nugini. Deskripsi teknis sekunder menggambarkan konektivitas lanjutan melalui jaringan yang sudah ada menuju arah Pasifik dan Amerika Serikat (PT Telkom Indonesia, 2026; Submarine Networks, 2026). Pukpuk penting bagi kajian ini bukan karena menjadi “kabel langsung Jayapura–Amerika Serikat”, melainkan karena menunjukkan nilai route diversification. Diversifikasi dapat mengurangi ketergantungan pada satu jalur, tetapi tidak menghapus risiko jika landing station, backhaul darat, akses perbaikan, energi, atau sistem pengelolaan jaringan tetap terkonsentrasi. Karena itu, pengembangan ketahanan harus menggabungkan route diversity dengan node diversity dan recovery diversity.

Keamanan Rantai Pasok dan Landing Station

Keamanan rantai pasok perlu didasarkan pada risk management yang dapat diaudit, bukan pada kewarganegaraan vendor semata. Kontrol yang relevan meliputi secure procurement requirements, software and firmware provenance, independent testing, cryptographic integrity, privileged-access control, maintenance logging, dan incident disclosure. Klaim mengenai backdoor vendor tidak boleh digunakan tanpa bukti teknis atau temuan otoritatif. Landing station harus diperlakukan sebagai infrastruktur kritis siber-fisik karena menghubungkan lapisan bawah laut dengan jaringan terrestrial. Physical access control, personnel security, network segmentation, secure remote maintenance, redundant power, tamper detection, dan recovery procedures perlu dipertimbangkan sebagai bagian dari common operational picture. Kerentanan pada fasilitas darat dapat menurunkan nilai investasi pada perlindungan wet plant jika kedua lapisan tidak dikendalikan secara terintegrasi.

Lawfare sebagai Arena Debat Hukum dan Diplomati

Istilah lawfare digunakan secara terbatas untuk menggambarkan kontestasi interpretasi hukum, pilihan litigasi, pengembangan aturan domestik, dan diplomasi mengenai perlindungan kabel. Kerangka UNCLOS tetap menjadi landasan penting; pada saat yang sama, literatur kontemporer menunjukkan adanya perdebatan mengenai keterbatasan yurisdiksi, standar pembuktian, dan mekanisme tanggung jawab atas kerusakan yang disengaja atau karena

kelalaian yang dapat dipersalahkan (Davenport, 2025; Zhang & Li, 2025). Contoh lain adalah Strategic Subsea Cables Act S.3249 di Amerika Serikat. Rancangan tersebut diperkenalkan pada 20 November 2025 dan pada Juni 2026 ditempatkan pada Senate Legislative Calendar. Status tersebut berarti rancangan masih merupakan proses legislasi dan tidak boleh disebut sebagai undang-undang yang telah berlaku (U.S. Congress, 2025; U.S. Senate, 2026). Bagi Indonesia, implikasinya adalah perlunya strategi berbasis standar, evidence sharing, kerja sama perbaikan, serta klarifikasi hukum regional, bukan asumsi bahwa satu reinterpretasi hukum akan menyelesaikan semua persoalan yurisdiksi.

Tabel 1. Pembelajaran Analitis dari Studi Kasus

Kasus	Fakta yang terverifikasi	Batas inferensi	Implikasi C6ISR
Yi Peng 3	Dua kabel data rusak; Yi Peng 3 relevan dalam penyelidikan; investigasi Swedia tidak menetapkan niat disengaja secara konklusif.	Tidak cukup untuk menyimpulkan sabotase atau sponsor negara hanya dari pergerakan kapal/AIS.	Pisahkan observasi, kausalitas, niat, dan atribusi.
Eagle S	Investigasi, dakwaan, putusan yurisdiksi 2025, dan pembalikan putusan pada tingkat banding 27 Agustus 2026.	Proses belum menghasilkan putusan pidana final yang menentukan tanggung jawab para terdakwa.	Klasifikasi lokasi dan konsultasi hukum harus dimulai sejak awal respons.
Pukpuk 1	Sistem lintas batas Indonesia-Papua Nugini diresmikan 8 Mei 2026 dan memperkuat konektivitas Jayapura.	Data publik yang ditinjau tidak menetapkan kapasitas/latensi tertentu atau klaim manfaat C6ISR kuantitatif.	Gunakan sebagai contoh diversifikasi rute, bukan sebagai bukti penghapusan risiko.

Matriks Keputusan C6ISR yang Diusulkan

Sintesis studi dokumen dan kasus menghasilkan matriks keputusan yang menempatkan bukti, kewenangan, dan pemulihan dalam satu rantai keputusan. Matriks ini merupakan keluaran konseptual penelitian, bukan prosedur operasional yang saat ini diklaim telah diterapkan secara nasional.

Tabel 2. Matriks Keputusan C6ISR Indonesia yang Diusulkan

Tahap	Pertanyaan inti	Bukti utama	Keluaran keputusan	Kontrol
Deteksi	Apakah terdapat anomali?	AIS, satelit, radar, DAS/akustik, alert operator	Observasi/alert	Tidak ada atribusi dari satu indikator
Korelasi	Apakah anomali beririsan dengan infrastruktur kritis?	GIS kabel, jejak kapal, data lingkungan	Skor risiko/keyakinan	Provenance dan ketidakpastian dicatat
Penilaian	Apakah kerusakan/aktivitas telah terkonfirmasi?	Inspeksi, citra, bukti dasar laut, log	Klasifikasi insiden	Chain of custody
Atribusi	Apa yang dapat dikaitkan dengan peristiwa?	Forensik, bukti awak/peralatan, intelijen	Penilaian atribusi	Niat dipisahkan dari kewarganegaraan
Keputusan	Tindakan apa yang sah dan proporsional?	Lokasi, hukum, kewenangan	Perintah/respons	Kajian hukum sebelum tindakan koersif
Pemulihan	Bagaimana layanan dipulihkan?	Telemetri, reroute, data perbaikan	Rencana pemulihan	Lesson learned dan pembaruan risiko

Model Ketahanan Strategis Indonesia

Berdasarkan temuan, ketahanan dapat dibangun melalui lima lapisan. Pertama, diversifikasi rute dan node dengan memodelkan jaringan sebagai graf yang memuat landing station, backhaul, ketergantungan energi, pusat data, titik interkoneksi, dan akses perbaikan. Kedua, maritime awareness persisten yang menggabungkan AIS dengan sumber independen

dan tidak menggunakan istilah “kapal gelap” sebagai sinonim aktivitas bermusuhan. Ketiga, atribusi berbasis tangga bukti dengan preservasi evidence. Keempat, koordinasi hukum-operasional sejak tahap awal. Kelima, preparedness untuk repair dan continuity melalui kontrak, kabel cadangan, jalur perizinan cepat, rerouting, dan latihan bersama. Pendekatan berlapis ini sejalan dengan literatur yang menempatkan resilience sebagai kombinasi physical protection, governance, surveillance, redundancy, dan repair capacity (Cannon et al., 2026; Davenport, 2025; ITU, 2026a).

KESIMPULAN

Keamanan kabel bawah laut merupakan persoalan ketahanan maritim siber-fisik yang menghubungkan infrastruktur digital, keamanan laut, hukum internasional, dan kontinuitas ekonomi. Analisis 2024–2026 menunjukkan bahwa masalah utama bukan sekadar kemampuan mendeteksi keberadaan kapal, tetapi kemampuan negara untuk menggabungkan observasi heterogen, mempertahankan ketidakpastian secara disiplin, membangun penilaian atribusi berbasis bukti, menjalankan kewenangan yang sah, dan memulihkan konektivitas secara cepat. Kasus Yi Peng 3 memperlihatkan bahwa indikator maritim penting belum tentu cukup untuk membuktikan niat atau sponsor negara. Perkara Eagle S menunjukkan bahwa investigasi nasional yang substantif tetap berinteraksi dengan pertanyaan yurisdiksi. Pukpuk 1 menunjukkan nilai route diversification bagi Indonesia Timur, tetapi sekaligus menegaskan bahwa redundansi rute perlu diikuti diversifikasi node, backhaul, dan kapasitas pemulihan. Temuan tersebut memperkuat relevansi model C6ISR yang menempatkan sensing, fusi, hukum, komando, respons, dan recovery sebagai satu siklus. Kontribusi penelitian bukan klaim bahwa C6ISR atau “Deterrence by Detection” telah menjadi doktrin nasional. Keduanya digunakan sebagai perangkat analitis untuk merancang arsitektur keputusan yang lebih terintegrasi. Bagi Indonesia, ketahanan strategis akan lebih kuat ketika deteksi persisten, evidence preservation, legal preparedness, route diversification, landing-station security, dan repair readiness dirancang sebagai satu ekosistem. Pendekatan ini mendukung kedaulatan digital sekaligus mempertahankan disiplin analitis dan kesesuaian dengan hukum internasional.

Kebaruan (novelty) penelitian ini terletak pada pengembangan arsitektur analitis C6ISR yang terintegrasi untuk memperkuat deteksi dini, penilaian atribusi, pengambilan keputusan strategis, dan pemulihan terhadap potensi gangguan pada infrastruktur kabel bawah laut Indonesia dalam konteks ancaman maritim dan operasi zona abu-abu periode 2024–2026. Berbeda dari kajian terdahulu yang cenderung membahas keamanan kabel bawah laut melalui perspektif teknis, hukum laut internasional, atau ketahanan infrastruktur secara terpisah, penelitian ini mengintegrasikan fungsi komando dan kendali, komunikasi, komputasi, pertahanan siber, intervensi, intelijen, pengawasan, dan pengintaian ke dalam suatu siklus keputusan yang menghubungkan deteksi anomali, fusi informasi multi-sumber, evaluasi hukum, respons operasional, dan pemulihan infrastruktur. Kebaruan konseptual penelitian ini juga terletak pada penempatan atribusi insiden dan penentuan kewenangan hukum sebagai komponen yang saling berkaitan dalam arsitektur C6ISR, sehingga indikasi teknis mengenai aktivitas mencurigakan tidak secara otomatis ditafsirkan sebagai bukti sabotase atau tindakan yang disponsori negara, melainkan harus diuji melalui verifikasi intelijen, konteks operasional, dan ketentuan hukum yang relevan, termasuk United Nations Convention on the Law of the Sea (UNCLOS). Melalui studi kasus komparatif insiden Yi Peng 3 dan Eagle S di Laut Baltik, analisis sistem kabel bawah laut Pukpuk 1, serta telaah inisiatif internasional mengenai ketahanan kabel, penelitian ini menghubungkan pembelajaran lintas kawasan dengan kebutuhan strategis Indonesia sebagai negara kepulauan yang memiliki kompleksitas geografis, kelembagaan, dan yurisdiksi maritim. Kontribusi utama penelitian ini adalah perumusan kerangka C6ISR berlapis



yang tidak hanya berorientasi pada deteksi ancaman, tetapi juga mengintegrasikan validasi informasi, batas kewenangan hukum, koordinasi antarlembaga, kesiapan intervensi, redundansi jaringan, dan kemampuan perbaikan sebagai elemen ketahanan infrastruktur kritis. Dengan demikian, penelitian ini berpotensi memperluas kajian keamanan maritim dan perlindungan infrastruktur digital melalui pendekatan sosio-teknis dan strategis yang menghubungkan kapabilitas intelijen, tata kelola hukum, dan resiliensi operasional dalam satu kerangka analisis yang kontekstual bagi Indonesia.

DAFTAR PUSTAKA

- Ban, K. J. (2025). 해저케이블 안보와 회색지대 공세 [Undersea cable security and gray zone offensives]. *국가안보와 전략*, 25(1), 157–184.
- Cannon, B. J. (2025). Undersea cable security in the Indo-Pacific: Enhancing the Quad's collaborative approach. *Marine Policy*, 171, 106415. <https://doi.org/10.1016/j.marpol.2024.106415>
- Cannon, B. J., Matsuo, K., & Matsuda, M. (2026). Mapping undersea cable risk from bathymetry to geopolitics: Evidence-based rankings and tailored resilience strategies. *Marine Policy*, 186, 107012. <https://doi.org/10.1016/j.marpol.2025.107012>
- Davenport, T. M. (2025). The protection of submarine cables in Southeast Asia: The security gap and challenges and opportunities for regional cooperation. *Marine Policy*, 171, 106435. <https://doi.org/10.1016/j.marpol.2024.106435>
- Division for Ocean Affairs and the Law of the Sea. (2026). United Nations Convention on the Law of the Sea: Submarine cables and EEZ legal materials. United Nations. https://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm
- Finnish National Bureau of Investigation. (2025, June 13). Criminal investigation by the NBI into cable damage in the Gulf of Finland concluded. <https://poliisi.fi/en/-/criminal-investigation-by-the-nbi-into-cable-damage-in-the-gulf-of-finland-concluded>
- Finnish Prosecution Service. (2025, August 11). Charges have been brought in the case concerning the cutting of submarine cables in the Gulf of Finland during Christmas 2024. <https://www.syyttajalaitos.fi/en/-/charges-have-been-brought-in-the-case-concerning-the-cutting-of-submarine-cables-in-the-gulf-of-finland-during-christmas-2024>
- Ganz, A., Camellini, M., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Submarine cables and the risks to digital sovereignty. *Minds and Machines*, 34(3), Article 31. <https://doi.org/10.1007/s11023-024-09683-z>
- Govella, K. (2025). Undersea cables, geoeconomics, and security in the Indo-Pacific: Risks and resilience. *Marine Policy*, 180, 106809. <https://doi.org/10.1016/j.marpol.2025.106809>
- Helsinki Court of Appeal. (2026, August 27). HelHO:2026:9, R 16/2025/2572: International procedural law, UNCLOS, jurisdiction, and territorial scope of criminal law. <https://www.tuomioistuimet.fi/ajankohtaista/tiedotteet/tiedote-hovioikeuden-paatoksesta-ns-eagle-s-aluksen-asiassa-r-16-2025-2572/>
- Helsinki District Court. (2025, October 3). District Court judgment in the criminal case involving the tanker EAGLE S, R 706/2025/12270.
- International Telecommunication Union. (2026a, July 10). International Advisory Body approves landmark report to strengthen submarine cable resilience. <https://www.itu.int/>
- International Telecommunication Union. (2026b). Submarine cable resilience. ITU Digital Resilience. <https://www.itu.int/en/ITU-D/Pages/Resilience.aspx>



- Loik, R. (2024). Undersea hybrid threats in strategic competition: The emerging domain of NATO–EU defense cooperation. *Journal on Baltic Security*, 10(2), 1–25. https://doi.org/10.57767/jobs_2024_008
- NATO. (2025, January 14). Baltic Sentry to enhance NATO's presence in the Baltic Sea. https://www.nato.int/cps/en/natohq/news_232122.htm
- PT Telkom Indonesia (Persero) Tbk. (2026, May 9). TelkomGroup resmikan kabel laut Pukpuk: Jembatan digital pertama yang menghubungkan Indonesia–Papua Nugini. <https://www.telkom.co.id/>
- Submarine Networks. (2026). Puk-Puk 1: Secondary technical description of the Pukpuk system and connectivity path.
- Swedish Accident Investigation Authority. (2024, December 19). Investigations concerning the Chinese vessel Yi Peng 3 and the Baltic Sea cable damage. <https://www.havkom.se/>
- Swedish Accident Investigation Authority. (2025, April 15). Findings concerning the Yi Peng 3 investigation and Baltic Sea cable damage. <https://www.havkom.se/>
- U.S. Army DEVCOM C5ISR Center. (2026). C5ISR Center: Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance. <https://www.c5isrcenter.devcom.army.mil/>
- U.S. Congress, Government Publishing Office. (2025, November 20). S.3249 — Strategic Subsea Cables Act of 2025. <https://www.congress.gov/bill/119th-congress/senate-bill/3249>
- U.S. Senate. (2026, June 4). S.3249 legislative status: Placed on the Senate Legislative Calendar under General Orders. <https://www.senate.gov/>
- United Nations. (1982). United Nations Convention on the Law of the Sea, Articles 58, 79, and 112–115. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
- Zhang, D., & Li, H. (2025). Research on the international legal regulation of willful or culpably negligent damage to submarine cables. *Marine Development*, 3, Article 19. <https://doi.org/10.1007/s44312-025-00064-3>
- Zhang, D., Guo, Y., Yuan, Q., Ni, Z., Xu, H., Liu, X., & Qiu, H. (2026). Submarine cable systems: A review of installation, monitoring, and maintenance processes and technologies. *Processes*, 14(5), 821. <https://doi.org/10.3390/pr14050821>