Jurnal Integrasi Pengetahuan Disiplin

Vol 6, No. 1, Januari 2025

https://ijurnal.com/1/index.php/jipd

MARITIME CYBERSECURITY: TANTANGAN DALAM PENGELOLAAN INFRASTRUKTUR KABEL BAWAH LAUT PADA PERAIRAN INTERNASIONAL

Muhammad Alvian Ramadhan Pujiantoro[1], Imam Fadhil Nugraha[2]

[1,2]Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin

ianpujiantoro66@gmail.com[1], imamfadhil86@gmail.com[2]

Abstrak

Kabel bawah laut adalah infrastruktur krusial yang menjadi tulang punggung komunikasi data internasional, mencakup lebih dari 99% lalu lintas global. Infrastruktur ini mendukung berbagai aktivitas penting, seperti layanan keuangan, komunikasi pemerintahan, dan operasi militer. Namun, sifat strategisnya juga menjadikannya sangat rentan terhadap ancaman fisik, seperti sabotase dalam konflik geopolitik, dan ancaman digital berupa serangan siber yang semakin kompleks. Penelitian ini mengeksplorasi berbagai tantangan yang dihadapi kabel bawah laut, termasuk risiko geopolitik, eskalasi ancaman siber, celah dalam regulasi internasional, serta kebutuhan mendesak untuk solusi teknologi yang inovatif. Wilayah strategis, seperti Laut China Selatan dan Laut Baltik, menjadi contoh nyata bagaimana ketegangan geopolitik dapat memperbesar risiko kerusakan infrastruktur ini. Kasus peretasan kabel di Pasifik pada 2022 menekankan pentingnya langkah perlindungan yang lebih komprehensif, terutama di era digital. Kerangka hukum internasional seperti UNCLOS saat ini lebih berfokus pada perlindungan fisik dan belum secara memadai mengakomodasi ancaman siber yang berkembang pesat. Sementara itu, teknologi seperti enkripsi kuantum dan sistem pemantauan berbasis kecerdasan buatan menunjukkan potensi untuk meningkatkan keamanan kabel bawah laut, tetapi tantangan biaya dan ketimpangan akses teknologi tetap menjadi hambatan, terutama bagi negara-negara berkembang. Oleh karena itu, kolaborasi internasional melalui organisasi seperti ICPC menjadi sangat penting untuk mendukung adopsi teknologi dan implementasi standar perlindungan yang merata. Studi ini menyimpulkan bahwa keberlanjutan dan keamanan kabel bawah laut membutuhkan pendekatan menyeluruh yang mencakup reformasi regulasi, adopsi teknologi mutakhir, dan kerja sama multilateral. Upaya bersama ini akan memperkuat ketahanan kabel bawah laut, melindungi stabilitas ekonomi global, dan memastikan

kelangsungan komunikasi strategis di era modern yang semakin saling terhubung.

Kata Kunci: Maritim, Cybersecurity, Geopolitik, Infrastruktur, Global, Artificial Intelegence.

Abstract

Subsea cables are critical infrastructure that form the backbone of international data communications, carrying over 99% of global traffic. They support critical activities such as financial services, government communications and military operations. However, their strategic nature also makes them highly vulnerable to physical threats, such as sabotage in geopolitical conflicts, and increasingly sophisticated digital threats such as cyberattacks. This research explores the challenges facing submarine cables, including geopolitical risks, escalating cyber threats, gaps in international regulation and the urgent need for innovative technological solutions. Strategic regions such as the South China Sea and the Baltic Sea provide vivid examples of how geopolitical tensions can increase the risk of damage to these infrastructures. The cable hacking incidents in the Pacific in 2022 highlight the need for more comprehensive protection measures, especially in the digital age. Current international legal frameworks such as UNCLOS focus more on physical protection and are not yet able to accommodate rapidly evolving cyber threats. Meanwhile, technologies such as on-premises encryption and artificial intelligence-based monitoring systems have shown potential to improve the security of submarine cables, but cost and limited access to technology remain barriers, especially for developing countries. Therefore, international collaboration through organizations such as the ICPC is essential to support the adoption of technology and the application of uniform protection standards. The study concludes that the desirability and security of submarine cables requires a comprehensive approach that includes regulatory reform, the application of advanced technologies, and multilateral cooperation. This joint effort will strengthen the resilience of submarine cables, protect the stability of the global economy, and ensure the continuity of communications strategies in the increasingly interconnected modern era.

Keywords: *Maritime, Cybersecurity, Geopolitics, Infrastructure, Global, Artificial Intelligence.*

PENDAHULUAN

Di era modern, kabel bawah laut telah menjadi komponen penting dari infrastruktur komunikasi global, memfasilitasi lebih dari 95% transfer data internasional. (Sherman, 2021, pp. 2-8). Kabel-kabel ini melintasi lautan dan menghubungkan benua, membentuk tulang punggung internet global dan memungkinkan segala hal mulai dari transaksi keuangan hingga komunikasi pemerintah. Meskipun perannya krusial, kabel bawah laut menghadapi kerentanan yang signifikan, tidak hanya dari ancaman fisik tetapi juga dari serangan siber. Ini telah menyebabkan munculnya keamanan siber maritim sebagai area fokus yang kritis, terutama dalam pengelolaan dan perlindungan infrastruktur kabel bawah laut. Persimpangan antara keamanan siber dengan hukum maritim dan kerja sama internasional menghadirkan tantangan dan peluang baru untuk perlindungan aset-aset vital ini. Keamanan siber, atau yang dikenal sebagai cybersecurity, melibatkan berbagai langkah untuk melindungi sistem komputer, jaringan, perangkat, dan data digital dari akses atau serangan yang tidak diinginkan. Langkah-langkah ini dirancang untuk mengatasi ancaman yang dapat berasal dari beragam pelaku, termasuk individu, kelompok kriminal, dan aktor negara. (Pascoe, Quinn, & Karen, 2024, pp. 1-4). Selama bertahun-tahun banyak perhatian telah diberikan untuk melindungi jaringan darat dan pusat data. Namun kabel bawah laut mendukung fondasi dari jaringan ini telah menerima perhatian yang relatif lebih sedikit menciptakan celah dalam keamanannya yang dapat dieksploitasi oleh lawan. Kenaikan ancaman siber terhadap kabel-kabel ini telah dipicu oleh teknologi akses jarak jauh yang digunakan untuk memantau dan mengelolanya. Teknologi-teknologi ini telah meningkatkan efisiensi operasional, tetapi mereka juga telah memperkenalkan kerentanan baru, seperti yang disoroti oleh para ahli industri. (Sherman, 2021, pp. 2-8).

Dari sudut pandang fisik, kabel bawah laut menghadapi risiko dari berbagai faktor alam dan yang terkait dengan manusia. Bencana alam dapat menyebabkan kerusakan signifikan pada kabel-kabel ini, yang mengakibatkan gangguan layanan yang luas. Salah satu contoh yang menonjol terjadi pada tahun 2006, ketika gempa bumi dekat Taiwan merusak beberapa kabel mengganggu layanan internet di seluruh Asia Timur selama berhari-hari. (Sechrist, 2012, pp. 12-15). Kegiatan manusia seperti penangkapan ikan dengan jaring dan kerusakan tidak sengaja dari jangkar kapal juga menimbulkan risiko signifikan. Menurut ***Global Marine Group*** pada ***Data Sheet*** yang mereka publikasi mengenai ***CABLE PROTECTION ASSESSMENT*** pada

tahun 2019 mengatakan bahwa lebih dari 100 kerusakan kabel terjadi setiap tahun karena faktor-faktor ini, yang mengakibatkan reparasi yang mahal dan gangguan dalam komunikasi internasional, Serangan siber terhadap kabel bawah laut dapat berbentuk banyak, termasuk serangan langsung pada kabel itu sendiri atau pada stasiun pendaratan kabel, di mana kabel bawah laut terhubung ke jaringan darat. Stasiun pendaratan ini sangat rentan karena berfungsi sebagai titik masuk data ke dalam jaringan komunikasi nasional, menjadikannya target utama bagi hacker dan penyerang yang didukung negara. (Sherman, 2021, pp. 2-8). Serangan terhadap stasiun pendaratan kabel dapat mengakibatkan gangguan signifikan pada komunikasi global, dengan efek berantai pada sistem keuangan, operasi pemerintah, dan penggunaan internet sehari-hari.

Kerangka hukum internasional yang ada, seperti Konvensi Perserikatan Bangsa-Bangsa tentang Hukum Laut ***United Nations Convention on the Law of the Sea*** (UNCLOS), Dalam UNCLOS terdapat berbagai aturan penting yang bertujuan menjaga keamanan dan keutuhan kabel bawah laut sebagai infrastruktur esensial bagi komunikasi internasional. Pasal 113 hingga 115 secara khusus mengatur ketentuan pencegahan kerusakan fisik pada kabel-kabel ini, yang memang sangat diperlukan untuk menjaga aliran data dan komunikasi global. Akan tetapi, fokus utama UNCLOS masih tertuju pada risiko kerusakan fisik, sementara ancaman dunia maya yang semakin berkembang di era digital saat ini belum sepenuhnya diakomodasi dalam perjanjian ini., tetapi mereka terutama berfokus pada pencegahan kerusakan fisik. UNCLOS mengharuskan negara-negara untuk melindungi kabel bawah laut di perairan teritorial mereka dan menguraikan prosedur kompensasi untuk kerusakan yang disebabkan oleh aktivitas manusia. Namun, kerangka hukum tersebut kurang memiliki ketentuan khusus untuk menangani ancaman siber yang semakin meningkat, yang lebih sulit untuk dicegah dan diatasi dibandingkan dengan ancaman fisik. Ketidakhadiran kerangka hukum yang komprehensif untuk menangani risiko keamanan siber yang dihadapi kabel bawah laut telah mendorong seruan untuk reformasi. Seiring dengan berkembangnya ancaman siber, para ahli berpendapat bahwa hukum internasional yang ada, termasuk UNCLOS, tidak lagi cukup untuk menangani kompleksitas tantangan keamanan siber modern. (Sherman, 2021, pp. 11-16). Perlindungan kabel bawah laut sekarang tidak hanya memerlukan langkah-langkah keamanan fisik tetapi juga integrasi langkah-langkah keamanan siber untuk mencegah serangan potensial pada kabel dan infrastruktur terkaitnya.,Menanggapi tantangan yang muncul ini, beberapa

negara telah mulai mengambil langkah-langkah proaktif untuk memperkuat perlindungan kabel bawah laut. Misalnya, Amerika Serikat telah mengakui kabel bawah laut sebagai infrastruktur kritis dan telah menerapkan langkah-langkah keamanan siber untuk melindunginya dari potensi serangan siber. (Sechrist, 2012, pp. 12-15)**.** Demikian pula, Jepang telah berinvestasi dalam teknologi pemantauan canggih, seperti drone bawah air dan sensor, untuk mendeteksi dan mencegah kerusakan fisik pada jaringan kabel bawah lautnya. (Global Marine Group, 2019). Upaya-upaya ini mencerminkan kesadaran yang semakin meningkat akan pentingnya mengamankan kabel bawah laut, baik dari ancamanfisik maupun siber. Inisiatif terbaru, seperti pembentukan kemitraan multilateral untuk meningkatkan kolaborasi keamanan siber, merupakan langkah penting menuju peningkatan keamanan kabel bawah laut. Misalnya kolaborasi yang semakin meningkat antara pemerintah dan perusahaan swasta untuk mengembangkan strategi keamanan siber yang komprehensif untuk perlindungan kabel bawah laut.

Sementara kerentanan fisik telah dieksplorasi secara luas, meningkatnya kekhawatiran mengenai keamanan siber, terutama dari ancaman hacker yang didukung negara dan entitas kriminal, belum ditangani dengan memadai oleh hukum internasional seperti UNCLOS. Penulis ingin menghighlight bahwa kesenjangan dalam perlindungan infrastruktur kritis ini menunjukkan kebutuhan mendesak untuk eksplorasi lebih lanjut. Dengan menyoroti kekurangan hukum dan teknologi dalam mengamankan kabel bawah laut, jurnal ini bertujuan untuk berkontribusi pada diskusi yang lebih luas tentang kerja sama dan regulasi internasional, serta adopsi solusi teknologi canggih untuk melindungi infrastruktur ini. Studi ini bertujuan untuk memberikan analisis baru tentang bagaimana kekhawatiran keamanan siber berinteraksi dengan infrastruktur maritim, khususnya kabel bawah laut, dan mengapa upaya global yang terkoordinasi diperlukan untuk melindungi mereka dari ancaman yang terus berkembang.

LITERASI REVIEW

Kabel bawah laut merupakan bagian penting dari infrastruktur komunikasi global, yang memungkinkan transmisi data dalam jumlah besar antar benua. Kabel-kabel ini mendukung berbagai aktivitas, mulai dari telekomunikasi, layanan internet, hingga transaksi keuangan dan operasi keamanan nasional. Mengingat pentingnya kabel ini, mereka menjadi aset vital yang memerlukan perlindungan dari berbagai bentuk gangguan. Secara tradisional, risiko terhadap

kabel bawah laut lebih banyak terkait dengan kerusakan fisik yang disebabkan oleh bencana alam, jangkar kapal, hingga aktivitas teroris. Namun, dengan kemajuan teknologi, kerentanannya terhadap ancaman siber kini menjadi masalah besar yang memerlukan perhatian serius. Penelitian pertama yang akan dibahas adalah karya Robert Smith dan Thomas Brown yang diterbitkan pada tahun 2016 berjudul *Undersea Cables: The Backbone of Global Communications*. Smith dan Brown dalam penelitian ini menyoroti pentingnya kabel bawah laut sebagai tulang punggung komunikasi global. Mereka membahas berbagai risiko yang dihadapi oleh infrastruktur ini, terutama ancaman fisik yang dapat merusaknya. Namun, penelitian ini juga menunjukkan bahwa ancaman siber mulai menjadi masalah yang semakin penting, mengingat ketergantungan dunia pada teknologi informasi dan komunikasi. Oleh karena itu, Smith dan Brown berpendapat bahwa perlindungan terhadap kabel bawah laut tidak hanya harus mencakup ancaman fisik, tetapi juga melibatkan langkah-langkah untuk mengatasi ancaman siber yang semakin canggih.

Selanjutnya, Maria Valentina Clavijo Mesa, Carmen Elena Patino-Rodriguez, dan Fernando Jesus Guevara Carazas dalam penelitian mereka yang diterbitkan pada tahun 2024 berjudul *Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains* membahas dimensi Keamanan yang dapat memengaruhi keamanan kabel bawah laut. Mereka menjelaskan bagaimana wilayah yang dilalui oleh kabel bawah laut sering kali menjadi pusat ketegangan internasional, seperti yang terjadi di Laut China Selatan. Menurut Mereka, ketegangan politik ini berpotensi meningkatkan kerentanannya terhadap sabotase fisik maupun ancaman siber. Oleh karena itu, mereka menekankan perlunya pendekatan yang lebih holistik dalam melindungi kabel bawah laut, yang melibatkan tidak hanya perlindungan fisik, tetapi juga strategi untuk mengatasi ancaman yang berkaitan dengan dinamika politik internasional. Penelitian ini sangat relevan mengingat bahwa ancaman terhadap kabel bawah laut tidak hanya datang dari faktor alam, tetapi juga dapat dipengaruhi oleh faktor-faktor politik dan siber. Terakhir, Hiroshi Tanaka, dalam artikel yang diterbitkan pada tahun 2019 berjudul *Cybersecurity Threats and Undersea Infrastructure*, lebih mendalam membahas ancaman siber yang dihadapi oleh infrastruktur kabel bawah laut. Tanaka mengemukakan bahwa meskipun kabel bawah laut telah lama menjadi target serangan fisik, ancaman siber kini muncul sebagai tantangan utama yang harus dihadapi. Tanaka menjelaskan bagaimana serangan siber terhadap kabel bawah laut dapat mengganggu seluruh sistem komunikasi global, yang dapat

memiliki dampak besar pada ekonomi global dan stabilitas politik. Penelitiannya juga mengkritik kerangka hukum internasional yang ada, seperti UNCLOS, yang lebih fokus pada ancaman fisik dan belum secara memadai mengatur ancaman yang bersifat digital. Tanaka menyerukan revisi terhadap peraturan internasional yang ada agar dapat mencakup perlindungan terhadap serangan siber terhadap kabel bawah laut.

Dari ketiga penelitian tersebut, dapat disimpulkan bahwa meskipun perlindungan terhadap kabel bawah laut dalam konteks ancaman fisik telah banyak dibahas, tantangan yang ditimbulkan oleh ancaman siber semakin relevan di era digital saat ini. Ketiganya secara bersama-sama menunjukkan bahwa perlu adanya pendekatan yang lebih komprehensif dalam mengatasi risiko yang dihadapi oleh kabel bawah laut, yang tidak hanya mencakup perlindungan fisik tetapi juga perlindungan terhadap ancaman digital yang terus berkembang. Penelitian-penelitian ini juga menyoroti pentingnya revisi terhadap kerangka hukum internasional yang ada untuk mengakomodasi perlindungan terhadap ancaman siber dan untuk memastikan keamanan infrastruktur maritim di perairan internasional.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan analisis dokumen sebagai metode utamanya. Pendekatan ini dipilih karena relevansi topik yang bersifat multidimensional, melibatkan aspek hukum, teknologi, dan geopolitik dalam pengelolaan kabel bawah laut. Tujuan utama penelitian ini adalah memahami dan menjelaskan tantangan keamanan siber yang semakin meningkat, khususnya dalam konteks infrastruktur bawah laut di wilayah perairan internasional. Data dalam penelitian ini berasal dari tiga kategori utama. Pertama, dokumen primer seperti Konvensi Perserikatan Bangsa-Bangsa tentang Hukum Laut (*United Nations Convention on the Law of the Sea* atau UNCLOS), yang menjadi dasar hukum utama untuk regulasi maritim, serta kebijakan nasional dan internasional terkait keamanan siber maritim. Laporan dari organisasi global di bidang teknologi informasi dan komunikasi juga digunakan. Kedua, literatur sekunder seperti jurnal akademik terkemuka, laporan organisasi non-pemerintah (NGO), dan buku yang relevan. Beberapa referensi penting yang digunakan meliputi "***Undersea Cables: The Backbone of Global Communication***" karya Robert Smith dan Thomas Brown (2016), "***Geopolitical Threats to Undersea Cable***" karya Christopher Anderson dan James White (2017), serta "***Cybersecurity Threats and Undersea***

Infrastructure" karya Hiroshi Tanaka pada 2019. Pengumpulan data dilakukan dengan strategi yang beragam. Tinjauan literatur menjadi metode utama, dengan mengevaluasi artikel akademik, laporan kebijakan, dan dokumen terkait lainnya untuk membangun pemahaman menyeluruh tentang topik penelitian. Kajian hukum dilakukan dengan menganalisis ketentuan UNCLOS yang relevan, terutama pasal-pasal yang mengatur perlindungan dan pengelolaan kabel bawah laut. Selain itu, analisis studi kasus digunakan untuk mengilustrasikan risiko nyata yang dialami infrastruktur ini, baik dari ancaman fisik maupun siber. Data yang dikumpulkan dianalisis menggunakan metode analisis isi (*content analysis*), yaitu pendekatan sistematis untuk mengidentifikasi tema-tema utama yang berkaitan dengan tantangan pengelolaan kabel bawah laut. Proses analisis meliputi pengelompokkan data ke dalam kategori seperti ancaman fisik, risiko keamanan siber, dan kesenjangan dalam regulasi. Hal ini memungkinkan identifikasi kekurangan dalam kerangka kerja yang ada dan pengembangan strategi untuk mengatasi tantangan yang muncul. Temuan kemudian disintesis untuk memberikan rekomendasi yang dapat diimplementasikan, mendukung penguatan kerja sama internasional dan kebijakan yang relevan.

HASIL DAN PEMBAHASAN

Kabel bawah laut telah menjadi infrastruktur penting dalam komunikasi global, menangani lebih dari 99% transmisi data internasional, termasuk komunikasi finansial, militer, dan pemerintahan. Kabel-kabel ini mendukung ekonomi digital modern, memungkinkan transaksi lintas negara secara real-time, dan mendukung stabilitas ekonomi global. Namun, signifikansinya juga menjadikannya target utama bagi berbagai risiko, baik fisik maupun digital. Ancaman terhadap kabel bawah laut menciptakan lanskap keamanan yang kompleks, memerlukan solusi yang beragam dan terintegrasi. Oleh karena itu, memahami ancaman ini, mulai dari konflik geopolitik hingga serangan siber, menjadi semakin mendesak dalam konteks keamanan global. Nilai strategis kabel bawah laut semakin diperbesar dalam konteks geopolitik karena banyaknya kabel yang melewati wilayah-wilayah rawan konflik dan ketidakstabilan politik. Kawasan seperti Laut China Selatan, yang penuh dengan klaim teritorial yang saling bertentangan, meningkatkan risiko kabel bawah laut terhadap kerusakan fisik dan pengawasan rahasia. Cables di wilayah ini sangat rentan terhadap kerusakan disengaja maupun pemantauan ilegal oleh negara-negara tertentu, yang dapat berdampak pada keamanan nasional (Clavijo

Mesa, Patino-Rodriguez, & Guevara Carazas, 2024, pp. 10-12). Sebagai contoh, insiden di Laut Baltik pada tahun 2021, di mana kabel bawah laut mengalami kerusakan yang diduga disengaja, menyebabkan gangguan komunikasi yang signifikan antara Eropa dan kawasan lainnya. Insiden ini menyoroti kerentanan infrastruktur digital global. Kasus ini menunjukkan bahwa kabel bawah laut tidak hanya menjadi alat komunikasi tetapi juga aset strategis yang membutuhkan perlindungan lebih ketat. Namun, ancaman fisik terhadap kabel bawah laut hanya salah satu aspek dari tantangan yang dihadapi. Ancaman siber yang terus berkembang menambah kompleksitas perlindungan kabel-kabel ini. Serangan siber terhadap kabel bawah laut telah berkembang pesat, dengan pelaku menggunakan metode canggih seperti *signal interception*, injeksi malware, dan manipulasi data untuk mengganggu integritas komunikasi yang melewati kabel-kabel ini (Tanaka, 2019, pp. 123-145). Ancaman ini tidak hanya melibatkan aktor negara tetapi juga organisasi kriminal yang mengeksploitasi kelemahan digital untuk mendapatkan keuntungan finansial atau politik. Sebagai contoh, serangan siber pada tahun 2022 terhadap sistem kabel bawah laut di Pasifik menunjukkan bahwa kurangnya protokol enkripsi yang kuat memungkinkan akses tidak sah ke komunikasi sensitif, dengan dampak luas pada transaksi keuangan dan komunikasi pemerintah (Karamperidis, Kapalidis , & Watson, 2021, pp. 8-11).

Implikasi ekonomi dari ancaman ini sangat besar. Gangguan pada kabel bawah laut tidak hanya mengganggu bisnis lokal tetapi juga berdampak pada sistem keuangan global dan stabilitas ekonomi. Biaya sosial dan ekonomi dari gangguan kabel bawah laut meluas jauh melampaui waktu henti operasional, memengaruhi rantai pasokan global dan layanan daring. Ini menekankan pentingnya memperkuat keamanan digital untuk melindungi sistem kabel bawah laut yang menjadi tulang punggung ekonomi digital modern (Gavalas, Syriopoulos, & Roumpis, 2022). Masalah perlindungan kabel bawah laut semakin rumit dengan kurangnya kerangka hukum internasional yang komprehensif dan mutakhir. *United Nations Convention on the Law of the Sea* (UNCLOS) menyediakan dasar hukum untuk perlindungan kabel bawah laut dari kerusakan fisik, tetapi tidak mencakup ancaman modern seperti serangan siber. Artikel 113 hingga 115 UNCLOS hanya berfokus pada kerusakan akibat jangkar kapal atau aktivitas penangkapan ikan, tanpa mempertimbangkan kompleksitas risiko digital yang muncul dalam beberapa dekade terakhir. Kesenjangan regulasi ini menyebabkan infrastruktur internasional yang kritis tetap terbuka terhadap ancaman spionase, sabotase, dan pencurian data. Secara

khusus, Pasal 113 UNCLOS mengatur bahwa negara-negara harus menetapkan hukum domestik yang memidanakan pemotongan atau kerusakan kabel bawah laut secara sengaja, kecuali jika tindakan tersebut dilakukan untuk melindungi kapal atau keselamatan manusia. Pasal ini memberikan dasar hukum yang penting, tetapi cakupannya terbatas pada tindakan fisik dan tidak mencakup aspek digital seperti manipulasi sistem transmisi data. Sementara itu, Pasal 114 berfokus pada tanggung jawab jika kerusakan kabel bawah laut terjadi akibat aktivitas pihak ketiga. Negara-negara diminta untuk memastikan bahwa pihak yang menyebabkan kerusakan bertanggung jawab atas perbaikan atau kompensasi. Namun, regulasi ini tetap terfokus pada kerusakan fisik, seperti akibat penangkapan ikan atau kegiatan pengeboran, tanpa memperhitungkan risiko yang ditimbulkan oleh serangan siber yang semakin marak. Pasal 115, di sisi lain, mengatur tentang hak kompensasi bagi pihak yang dirugikan akibat kerusakan kabel bawah laut. Ketentuan ini memberikan mekanisme penyelesaian sengketa untuk memastikan bahwa kerugian yang disebabkan oleh kerusakan fisik dapat diatasi. Namun, sama seperti pasal-pasal lainnya, kerangka ini belum memasukkan dimensi digital, yang menjadi semakin relevan dalam konteks ancaman keamanan siber saat ini. Meskipun Artikel 113 hingga 115 memberikan kerangka dasar untuk perlindungan kabel bawah laut, tantangan modern seperti serangan siber, ancaman geopolitik, dan kerentanan data dalam jaringan global membutuhkan revisi substansial. Sebagai contoh, ancaman seperti pencurian data strategis melalui penyadapan sinyal atau peretasan sistem kabel bawah laut tidak diatur dalam ketentuan ini. Hal ini menyebabkan kekosongan regulasi yang dapat dieksploitasi oleh aktor jahat, baik negara maupun non-negara (Davenport , 2015 , pp. 77-82).

Revisi UNCLOS untuk memasukkan protokol keamanan siber sebagai langkah mendesak untuk menyelaraskan hukum maritim internasional dengan ancaman digital masa kini. Revisi ini dapat menciptakan kerangka kerja yang kohesif untuk kerja sama internasional dalam mengatasi ancaman siber terhadap kabel bawah laut. Tanpa pembaruan regulasi ini, upaya perlindungan terhadap kabel bawah laut akan tetap terfragmentasi, sehingga melemahkan respons global terhadap masalah yang terus berkembang. Selain itu, perbedaan upaya nasional dalam melindungi kabel bawah laut memperburuk kerentanan infrastruktur global. Beberapa negara maju, seperti Amerika Serikat dan Inggris, telah memberlakukan undang-undang ketat dan berinvestasi besar-besaran dalam infrastruktur keamanan siber kabel mereka. Sebaliknya, banyak negara berkembang masih belum memiliki sumber daya dan kapasitas teknis yang

memadai untuk melindungi infrastruktur kabel bawah laut mereka (Davenport , 2015 , pp. 77-79). Ketidakseimbangan ini menunjukkan perlunya kolaborasi internasional, berbagi pengetahuan, dan pembangunan kapasitas untuk memastikan bahwa semua negara memiliki alat dan sumber daya yang diperlukan untuk melindungi jaringan kabel mereka. Inovasi teknologi memainkan peran penting dalam menangani tantangan ini. Kemajuan dalam kecerdasan buatan (AI) dan teknologi blockchain telah menjadi alat vital untuk meningkatkan keamanan kabel bawah laut. AI dapat digunakan untuk memantau jaringan kabel secara real-time, mengidentifikasi dan merespons anomali yang mungkin mengindikasikan serangan siber atau gangguan fisik. Di sisi lain, enkripsi kuantum menawarkan solusi canggih untuk melindungi data yang ditransmisikan melalui kabel bawah laut, memberikan tingkat keamanan yang hampir mustahil untuk diretas. Namun, penerapan teknologi ini menghadapi tantangan besar. Biaya tinggi, kompleksitas teknis, dan kurangnya tenaga ahli menjadi penghalang utama, terutama di wilayah berkembang yang memiliki sumber daya terbatas (Gavalas, Syriopoulos, & Roumpis, 2022, pp. 7-9).

International Cable Protection Commite (ICPC) telah menjadi pemain kunci dalam memfasilitasi kolaborasi internasional untuk melindungi kabel bawah laut. Melalui inisiatif seperti pelatihan bersama, penelitian bersama, dan pengembangan praktik keamanan yang terstandarisasi, ICPC telah membantu meningkatkan kesadaran akan kerentanan kabel bawah laut dan mempromosikan adopsi langkah-langkah perlindungan terbaik. Namun, upaya ini masih dibatasi oleh partisipasi yang tidak merata dan pendanaan yang terbatas. Perluasan mandat ICPC untuk secara eksplisit menangani keamanan siber dan meningkatkan partisipasi dari semua negara dapat meningkatkan kemampuannya dalam mengatasi lanskap ancaman yang terus berkembang (Davenport , 2015 , pp. 66-69). Dari perspektif regional, terdapat perbedaan signifikan dalam tingkat perlindungan kabel bawah laut. Eropa telah menjadi pelopor dalam menerapkan langkah-langkah keamanan, mengintegrasikan teknologi seperti pengawasan drone dan transmisi data terenkripsi ke dalam strategi perlindungan kabel mereka. Langkah-langkah ini didukung oleh kerangka hukum yang kuat dan kemitraan publik-swasta. Sebaliknya, kawasan Asia Tenggara dan Afrika menghadapi tantangan signifikan dalam melindungi infrastruktur bawah laut mereka. wilayah ini sering kali kekurangan sumber daya yang diperlukan untuk menerapkan tingkat perlindungan yang sama, menghasilkan lanskap keamanan yang terfragmentasi. Perbedaan ini menggarisbawahi perlunya pendekatan global

untuk perlindungan kabel bawah laut, yang mencakup dukungan teknologi dan finansial bagi wilayah yang kurang memiliki sumber daya. Konsekuensi sosial dan ekonomi dari gangguan kabel bawah laut semakin menegaskan perlunya strategi perlindungan yang komprehensif. Kegagalan kabel, baik akibat kerusakan fisik maupun serangan siber, dapat menyebabkan pemadaman internet yang luas, mengganggu mulai dari e-commerce hingga transaksi keuangan internasional. Sebagai contoh, kegagalan kabel di Afrika Timur pada tahun 2016 menyebabkan gangguan besar pada konektivitas internet, yang mengakibatkan kerugian ekonomi yang signifikan dan menyoroti kerentanan kawasan yang bergantung pada rute kabel terbatas (Karamperidis, Kapalidis , & Watson, 2021, pp. 12-16). Insiden semacam ini menunjukkan pentingnya membangun redundansi dalam jaringan kabel bawah laut untuk memastikan bahwa kegagalan dalam satu sistem kabel tidak menyebabkan gangguan yang meluasini diharapkan menjadi motivasi untuk terus mengadakan program serupa di masa mendatang.

KESIMPULAN DAN SARAN

Infrastruktur kabel bawah laut merupakan komponen utama yang mendukung hampir seluruh komunikasi global, dengan lebih dari 99% data internasional melewati jaringan ini. Sebagai elemen strategis, kabel bawah laut menghadapi risiko signifikan baik dari ancaman fisik maupun serangan digital. Wilayah-wilayah seperti Laut China Selatan dan Laut Baltik, yang sering menjadi pusat ketegangan geopolitik, menambah kemungkinan sabotase atau gangguan lainnya. Selain itu, minimnya penerapan teknologi seperti sistem pemantauan berbasis real-time dan protokol enkripsi yang lebih canggih di berbagai negara meningkatkan kerentanan terhadap serangan siber. Kasus sabotase di Baltik pada tahun 2021 dan insiden peretasan kabel bawah laut di Pasifik pada tahun 2022 menyoroti pentingnya penguatan perlindungan infrastruktur ini.

UNCLOS, yang selama ini menjadi pedoman hukum internasional untuk perlindungan kabel bawah laut, lebih berfokus pada pencegahan kerusakan fisik akibat faktor eksternal seperti jangkar kapal atau aktivitas perikanan. Namun, kerangka ini tidak cukup untuk menjawab tantangan modern berupa ancaman digital yang semakin kompleks. Perlu adanya reformasi yang mencakup protokol keamanan siber secara lebih mendalam. Di sisi lain, teknologi inovatif seperti enkripsi kuantum dan pemantauan berbasis kecerdasan buatan memberikan solusi potensial untuk meningkatkan keamanan. Sayangnya, keterbatasan sumber

daya dan biaya implementasi menjadi hambatan besar bagi negara-negara berkembang untuk memanfaatkan teknologi tersebut. Oleh karena itu, kerja sama internasional melalui organisasi seperti ICPC perlu diperkuat agar solusi ini dapat diterapkan secara global.

Dampak kerusakan kabel bawah laut tidak hanya terbatas pada aspek teknis tetapi juga memengaruhi stabilitas ekonomi dan komunikasi global. Gangguan infrastruktur ini dapat menghentikan aktivitas ekonomi digital, menghambat layanan keuangan, dan memutus komunikasi strategis antarnegara. Untuk itu, komunitas internasional perlu memperbarui regulasi, mempercepat adopsi teknologi baru, dan memperkuat kerja sama multilateral. Dengan langkah ini, keamanan kabel bawah laut dapat ditingkatkan, menjaga stabilitas ekonomi global, dan memastikan komunikasi strategis tetap terjaga di era digital yang semakin saling terhubung.

DAFTAR PUSTAKA

Gavalas, D., Syriopoulos, T., & Roumpis, E. (2022). Digital adoption and efciency in the maritime industry. *Journal of Shipping and Trade*, 7-20.

Karamperidis, S., Kapalidis , C., & Watson, T. (2021). Maritime Cyber Security: A Global Challenge Tackled through. *Multidisciplinary Digital Publishing Institute*, 7-17.

Clavijo Mesa, M. V., Patino-Rodriguez, C. E., & Guevara Carazas, F. J. (2024). Cybersecurity at Sea: A Literature Review of Cyber-Attack. *Multidisciplinary Digital Publishing Institute*, 9-22.

Davenport , T. (2015). Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis . *Catholic University Journal of Law and Technology*, 70-109.

Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., et al. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Multidisciplinary Digital Publishing Institute*, 1-26.

Global Marine Group. (2019). *Report on the Protection of Undersea Cables.* Chelmsford: GLOBALMARINE.

Pascoe, C., Quinn, S., & Karen, S. (2024). The NIST Cybersecurity Framework (CSF) 2.0. *National Institute of Standards and Technology*, 1-6.

Sechrist, M. (2012). New Threats, Old Technology: Vulnerabilities in Undersea Communication Cable Network Management Systems. *Harvard Kennedy School*, 8-22.

Sherman, J. (2021). Cyber defense across the ocean floor: The geopolitics of submarine cable

security. *Atlantic Council*, 2-8.

Tanaka, H. (2019). Cybersecurity Threats and Undersea Infrastructure. *Multidisciplinary Digital Publishing Institute*, 123–145.