WIDYA YURIDIKA: JURNAL HUKUM
P-ISSN: 2615-7586, E-ISSN: 2620-5556
Volume 6, (2), 2023

http://publishing-widyagama.ac.id/ejournal-v2/index.php/yuridika/

Praktik Pemenuhan Kewajiban Kelaiklautan Kapal Kargo Oleh Pengangkut Terhadap Ancaman *Cyberattack*

Stephen Wongso[1], Sinta Dewi Rosadi[2], Purnama Trisnamansyah[3], Fauzi Maulana Hakim[4]

[1] Fakultas Hukum, Universitas Padjadjaran, Indonesia, stphnwongso@gmail.com
[2] Fakultas Hukum, Universitas Padjadjaran, Indonesia
[3] Fakultas Hukum, Universitas Padjadjaran, Indonesia
[4] Fakultas Hukum, Universitas Padjadjaran, Indonesia

ABSTRACT

Cyberattack issue in the shipping industries which was happened through some incidents towards ships, made the protection of cargo owners need to be reviewed. The seaworthiness obligation which interpreted as a means for a vessel to be fit to face the foreseeable perils in a voyage, makes cyberattack create its own discourse. This should not be separated with the cyberattack threat which has not been understood as an ordinary peril of a voyage. Moreover, the regulations in Indonesia which does not adopt the Hague-Visby Rules 1924, makes the industry fully rely on the Indonesian Shipping Law as a legal basis. The normative juridical research method makes the emphasis of the research on the use of library sources. The research specification uses an analytical descriptive that describes a literature study on the obligation of seaworthiness in dealing with the threat of cyberattack both in practice and regulation. The results of this study found that, first, the implementation of due diligence by the carrier in order to fulfil its seaworthiness obligations must also be applied to deal with the threat of cyberattack. The nature of the cyberattack that attacks the ship's information systems and technology, should make this attack predictable in a voyage. Moreover, the carrier's compliance with the cyber risk management guidelines on the ship should make the carrier declared to have fulfilled its seaworthiness obligations. Second, there is a legal vacuum in Indonesian positive law in regulating seaworthiness obligations in the face of cyberattack threats. Moreover, the legal gap between Indonesia's positive law and the 1924 HVR makes it difficult for Indonesian practitioners to follow global standards.

MANUSCRIPT INFO

Manuscript History:
Received:
2022-12-02

Accepted:
2023-05-04

Corresponding Author:
Stephen Wongso,
stphnwongso@gmail.com

***Keywords*:**
Cyberattack; Seaworthiness Obligation; Shipping Industry

Cite this paper Wongso, S., Rosadi, S. D., Trisnamansyah, P., & Hakim, F. M. (2023). Praktik Pemenuhan Kewajiban Kelaiklautan Kapal Kargo Oleh Pengangkut Terhadap Ancaman Cyberattack. *Widya Yuridika: Jurnal Hukum, 6*(2). doi:10.31328/wy.v6i2.4242

Layout Version:
v.6.2023

PENDAHULUAN

Seiring dengan perkembangan teknologi dalam suatu industri, ancaman *cyberattack* akan selalu menjadi ancaman yang nyata dan senantiasa mengancaman industri tersebut. Sejak tahun 2017, setidaknya ada beberapa perusahaan pengangkutan raksasa yang terkena *cyberattack* seperti *Mediterranean Shipping Company* ('MSC'), CMA-CGM S.A., Maersk *Shipping Company*, Hyundai *Merchant Marine* dan COSCO *Shipping Lines*. Beberapa kasus serangan yang terjadi tertuju pada kantor pusat dari perusahaan sebagaimana terjadi

terhadap Maersk *Shipping Company* pada tahun 2017, yang membuat pelayaran tertunda di banyak Pelabuhan.[1] Tidak hanya tertuju pada perusahaan, salah satu insiden yang terjadi pada tahun 2017, serangan langsung tertuju pada kapal. Kapal USS Fitzgerald mengalami tabrakan dengan kapal dagang berbendera Filipina (ACX Crystal), alasan kecelakaan ini disinyalir disebabkan oleh sistem navigasi dari USS Fitzgerald diretas.

Melansir dari temuan yang termuat dalam laporan *Japan Transport Safety Board* atau Badan Keamanan Transportasi Jepang, insiden ini disimpulkan terjadi karena sistem navigasi dari ACX Crystal tidak dapat mendeteksi keberadaan dari USS Fitzgerald yang seharusnya terdeteksi di radar. Terlebih lagi, pada saat terjadinya tabrakan antara kedua kapal tersebut, sistem komunikasi yang seharusnya menjadi alat untuk berkomunikasi antara kapal dengan perusahaan dan/atau Pelabuhan terganggu sehingga percakapan yang terjadi pada saat itu menjadi tidak jelas.[2] Hal ini tentunya menimbulkan pertanyaan mengenai keadaan faktual yang terjadi terhadap teknologi-teknologi yang ada pada kapal pada saat kejadian. Beberapa jurnal yang menyinggung mengenai insiden ini membuka kemungkinan akan terjadinya peretasan terhadap teknologi yang ada di ACX Crystal maupun USS Fitzgerald.[3] Akibatnya, USS Fitzgerald kehilangan kendali penuh atas navigasi kapalnya yang membuat mereka tidak mampu mengantisipasi ACX Crystal yang berada pada jalur yang sama. 10 awak kapal meninggal dalam insiden tersebut. [4] Insiden tersebut menjadi bukti nyata adanya bahaya yang dapat ditimbulkan oleh *cyberattack* dalam pelayaran.

Adanya ancaman nyata yang dapat diakibatkan oleh *cyberattack* diakui oleh dunia internasional. Walaupun belum adanya suatu klaim materiil yang timbul langsung dari kerugian yang diakibatkan oleh *cyberattack*, rentetan serangan yang telah terjadi tentu tidak dapat dipandang sebelah mata. Beberapa organisasi internasional yang menaungi kegiatan pengangkutan kargo laut seperti *International Maritime Organization* ('IMO') dan *Baltic International Maritime Council* ('BIMCO') telah mempublikasikan pedoman bagi industri perkapalan dunia mengenai persiapan terhadap *cyberattack* sebagai suatu tanda peningkatan urgensi global terhadap isu ini. Merujuk kepada Resolusi IMO MSC.428(92) yang menekankan bahwa ancaman *cyberattack* merupakan suatu isu yang penting dan sebaiknya diperhatikan oleh negara guna menunjang pengiriman yang aman. Sebagaimana dikutip langsung dari Resolusi MSC.428(98) yang menyatakan "*recognizing the urgent need to raise awareness on cyber risk threats*" menunjukkan bahwa isu ini merupakan isu yang nyata yang memerlukan perhatian khusus. Hal senada juga dinyatakan oleh BIMCO melalui *Guidelines on Cyber Security Onboard Ships* yang lebih spesifik membahas mengenai persiapan bagi kapal beserta kru kapal untuk menghadapi ancaman dari *cyberattack*.

Dalam konteks hubungan keperdataan dalam suatu kegiatan pengangkutan laut, ancaman *cyberattack* dapat menjadi faktor yang menyebabkan kerugian materiil. Oleh karena itu, langkah-langkah konkret yang sifatnya preventif tentu perlu dilaksanakan oleh pelaku-pelaku pengangkutan, khususnya pengangkut sebagai pihak yang bertanggungjawab dalam keselamatan suatu pelayaran. Dalam praktik pengangkutan global, dikenal suatu kewajiban bagi pengangkut dalam menjalankan suatu pelayaran. Salah satu konvensi internasional yang dijadikan rujukan dalam hal ini *Hague-Visby Rules* 1924 ('HVR 1924') yang mengatur mengenai hubungan antara pengangkut dengan pemilik kargo (*shipper and carrier*). HVR 1924 sendiri menjadi rujukan dalam penelitian ini karena konvensi ini menjadi konvensi yang vital dalam pengangkutan internasional. Hal ini ditunjukkan dari data bahwa HVR 1924 telah diratifikasi lebih dari 80 Negara, dimana beberapa negara diantaranya

[1]Andrew Kinsey, "Cyber Security Threats Challenge International Shipping Industry", 2021, <https://www.maritimeprofessional.com/news/cyber-security-threats-challenge-international-369770 > [diakses pada 8 Februari 2022]

[2] Nobuo Takeda, "Marine Accident Investigation Report", *Japan Transport Safety Board*, hlm.8

[3] Ben Farah, "Cybersecurity in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends", *Maritime Digital Information*, 2022, hlm.6

[4] Ben Farah, *Op.Cit,* hlm.7

termasuk negara-negara yang berhubungan erat dengan perdagangan Indonesia seperti Jepang, Malaysia, Amerika Serikat, Singapura, Australia dan Korea Selatan.[5] Fakta ini didukung juga oleh penggunaan HVR 1924 dalam beberapa kontrak pengangkutan standar seperti ASBAGASVOY dan GENCON 2022 yang merupakan kontrak standar dari BIMCO. Terlebih lagi, jika dibandingkan dengan konvensi serupa seperti Hamburg Rules dan Rotterdam Rules, HVR 1924 masih dinilai konvensi paling relevan untuk digunakan.[6]

Berdasarkan Pasal 3 ayat 1 HVR 1924 untuk memastikan kelaiklautan kapal (*seaworthiness*) pada saat sebelum dan pada saat suatu kapal akan berlayar. Dalam terjemahan aslinya digunakan kalimat:

> "*Carrier must before and at the beginning of a voyage, exercise due diligence to make the ship seaworthy, to properly man, equip and supply the ship and to make the ship cargoworthy*".
>
> (terjemahan bebas penulis: pengangkut wajib sebelum dan pada saat memulai suatu pelayaran, melaksanakan uji kelayakan untuk membuat kapal laiklaut, memastikan kapal diperlengkapi dengan peralatan, perlengkapan serta awak yang baik dan membuat kapal mampu mengangkut kargo sampai dengan tujuan)

Dalam konteks *common law,* kewajiban *due diligence* yang diatur pada Pasal tersebut telah dieksaminasi secara komprehensif dalam berbagai yurisprudensi. Dalam kasus *Cia Sud Americana de Vapores v. Sinochem Tianjin Import & Export Corp* pada tahun 2010 yang menyatakan bahwa kewajiban memastikan kelaiklautan ini berarti pengangkut wajib memastikan kapal telah dilengkapi dengan suatu sistem keamanan yang sewajarnya ditemukan untuk melindungi kargo dari "bahaya biasa" (*ordinary perils of the sea*) yang dapat diperkirakan sebelumnya.[7]

Lebih lanjut, dalam *Great China Metal Industries v. Malaysian International Shipping Corporation Berhad* ditekankan bahwa sebelum suatu kapal berlayar harus laik laut terhadap bahaya-bahaya yang sepatutnya dapat diperkirakan berdasarkan pengetahuan yang sewajarnya (*reasonably foreseeable*).[8] Apabila suatu bahaya tidak dapat dibuktikan sebagai *ordinary perils of the sea*, maka bahaya tersebut dianggap tidak dapat diperkirakan sebelumnya sehingga dikategorikan sebagai *force majeure* atau *overmacht*. Tentu ini merupakan suatu kekosongan hukum yang perlu dijawab oleh regulasi yang

Dalam hukum Indonesia, kewajiban serupa dapat ditemukan dalam Pasal 470 KUHD yang secara implisit menjelaskan tanggung jawab dari pengangkut untuk menanggung kerusakan pada barang yang diangkutnya yang disebabkan oleh kurang baiknya alat pengangkutan atau kurang cakapnya pekerja yang dipakainya. Pasal 470 KUHD ini berkaitan dengan Pasal 1 angka 33 Undang-Undang Nomor 17 Tahun 2008 tentang Pelayaran ('UU Pelayaran') yang menjelaskan kelaiklautan kapal sebagai suatu keadaan kapal yang memenuhi syarat, dimana salah dua syarat yang harus dipenuhi adalah manajemen keamanan kapal untuk berlayar di perairan tertentu serta persyaratan keamanan kapal. Frasa "untuk berlayar di perairan tertentu" dalam Pasal tersebut pada prinsipnya merujuk pada konsep yang sama dengan konsep "*ordinary perils of the sea*" yang dikenal dalam sistem *common law.*

---

[5] Atur Tetty Lubis, "Towards a Reformed Carriage of Goods by Sea Law: Indonesia and Global Practice", *Mulawarman Law Review,* Vol.5 Issue.1, 2020, hlm.71-72

[6] *Ibid.*

[7] *Cia Sud Americana De Vapores v. Sinochem Tianjin Import & Export Corp* ("**The Aconcagua**") [2010] 1 Lloyd's Rep 1 para.367

[8] *Great China Material Industries Co Ltd v. Malaysian International Shipping Corporation Berhad* ("**Bunga Seroja**") [1998] 196 CLR 161, para.92; Kopitoff *v. Wilson* [1876] 1 QBD 377, para.380; *Steel v. State Line Steamship Co* [1877] 3 App Cas 72, para.77,84,88; *Gilroy Sons & Co v. W R Price & Co* [1893] AC 56 para.63; *Virginia Carolina Chemical Co v. Norfolk and North American Steam Shipping Co* [1912] 1 KB 229, para.243-244

Berdasarkan penjabaran di atas, dapat terlihat suatu diskursus hukum mengenai *cyberattack* sepatutnya menjadi suatu bahaya yang dapat diperkirakan terjadi dalam suatu pelayaran. Oleh karena itu, pengangkut sepatutnya perlu mempersiapkan kapalnya untuk menghadapi ancaman *cyberattack*. Hal ini tidak terlepas dari pertanggungjawaban pengangkut hanya akan lahir apabila kerugian terbukti disebabkan oleh kelalaian pengangkut untuk memenuhi kewajiban kelaiklautan. Terlebih lagi, dari perspektif hukum nasional, isu ancaman *cyberattack* terhadap pelayaran nasional terasa masih belum jelas baik dari segi regulasi maupun pedoman teknis. Sebagai negara yang tidak meratifikasi HVR 1924, tinjauan ini juga bermaksud untuk meninjau kesiapan hukum positif Indonesia untuk meregulasi isu ancaman *cyberattack* dalam industri pengangkutan barang melalui laut. Maka dari itu, pokok dari penelitian jurnal ini akan membahas 2 (dua) pokok bahasan, yakni tindakan cakupan tindakan *due diligence* pengangkut dalam memenuhi kewajiban kelaiklautan guna menghadapi ancaman *cyberattack* dan hukum positif Indonesia dalam meregulasi kewajiban kelaiklautan guna menghadapi ancaman *cyberattack*.

Penelitian ini sendiri bertujuan untuk menganalisa penerapan tindakan *due diligence* dari pengangkut untuk memenuhi kewajiban kelaiklautan kapal berdasarkan HvR sebagai respons penyelenggaraan pengangkutan global terhadap ancaman *cyberattack* dan mengkaji kesiapan hukum positif di Indonesia dalam mengatur kewajiban kelaiklautan kapal sebagai respons terhadap ancaman *cyberattack* kepada penyelenggaraan pengangkutan nasional.

METODE

Metode penelitian yang digunakan dalam menyusun jurnal ini adalah menggunakan pendekatan yuridis normatif. Hal ini berarti titik berat dari penelitian adalah penggunaan bahan-bahan dari sumber pustaka atau data sekunder yang mungkin mencakup bahan primer, sekunder dan tersier. Penulisan yang digunakan dalam penelitian ini akan menggunakan metode deskripsitf analisis, yang berarti penelitian akan memberikan gambaran secara rinci, dan komprehensif yang disajikan secara menyeluruh dan sistematis mengenai segala unsur penelitian baik perundang-undangan maupun teori hukum.[9]

Adapun data-data yang akan digunakan dalam jurnal ini dikumpulkan penulis menggunakan studi kepustakaan. Artinya pengumpulan data umumnya didapatkan dari buku, jurnal dan dokumen ilmiah lainnya yang berkaitan dengan hukum pengangkutan laut. Serta, analisis yang digunakan dalam penelitian ini adalah metode yuridis normatif kualitatif. Hal ini berarti penelitian didasarkan pada asas dan norma hukum yang ada dalam peraturan perundang-undangan dan juga yurisprudensi sebagai hukum positif.[10] Penelitian ini juga dilakukan dengan metode analisis kualitatif yang artinya dilakukan dengan memberikan uraian sistematis tentang objek penelitian.

HASIL DAN PEMBAHASAN

Kewajiban Kelaiklautan Berdasarkan Hague-Visby Rules 1924 Sebagai Perlindungan Preventif Kargo Terhadap Ancaman *Cyberattack*

Pasal 3 ayat 1 HVR 1924 memberikan kewajiban bagi pengangkut untuk melaksanakan *due diligence* guna memastikan suatu kapal laik laut. Merujuk pada *state practice* dari negara-negara dengan sistem *common law,* , maka kewajiban yang ada dalam Pasal 3 angka 1 HVR 1924 ini akan terdiri dari 4 (empat) aspek yakni:

[9] Soemitro dan Ronny Hanitijo, *Metodologi Penelitian Hukum dan Jurimetri*, Jakarta: Ghalia Indonesia, 1983, hlm.10

[10] Amiruddin dan Zainal Asikin, *Pengantar Metode Penelitian Hukum*, Jakarta: Raja Grafindo, 2004, hlm.163-167

1. Kapal, awak kapal, dan perlengkapan yang ada di kapal harus mampu untuk menghadapi bahaya yang sekiranya akan ditemukan dalam suatu pelayaran;[11]
2. Kapal harus dalam kondisi yang layak untuk mengangkut kargo sesuai dengan perjanjian;[12]
3. Layak dan mampu untuk melewati bahaya yang mungkin ditemukan dalam pelayaran;[13]
4. Kemampuan dan kelayakan kapal dipenuhi berdasarkan prinsip kehati-hatian oleh pemilik kapal yang mumpuni untuk melaksanakan pelayaran.[14]

Terlihat bahwa pemenuhan kewajiban ini membuat pengangkut wajib memastikan kapal baik secara fisik mampu untuk sampai ke tujuan dengan selamat (*seaworthy*) dan mampu menjaga kargo tetap aman (*cargoworthy*).[15] Mengutip penjelasan dari Simon Baughen, *cargoworthiness* merupakan bagian yang penting dalam *seaworthiness* dan memiliki tolok ukur yang sama seperti kelaiklautan kapal.[16]

Terlebih lagi, aspek penting yang perlu digarisbawahi dalam kewajiban kelaiklautan ini adalah sifatnya yang kasuistik. Hal ini dapat dilihat dalam kasus *the Toledo* tahun 1995, yang mengkorporasikan HVR 1924 dalam perjanjian carternya.[17] Kapal Toledo berangkat dari St. John New Brunswick menuju Denmark melalui Samudera Atlantik pada musim dingin dan mengangkut kalium karbonat. Kapal *Toledo* sendiri sudah memiliki sertifikat kelas dengan perlengkapan barang yang cukup mumpuni pada masanya. Namun, rute yang akan dilewati oleh kapal ini sudah sangat terkenal akan cuaca buruknya pada musim dingin. Terbukti, setelah melewati Samudera Atlantik, bingkai penyimpanan kargo di dalam kapal retak sehingga beberapa kargo menjadi rusak.[18]

Aspek kasuistik dari kewajiban ini juga terlihat dari kasus Bunga Seroja, Suatu kapal kargo yang berlayar dari Sydney menuju Keelung menghadapi cuaca buruk berupa badai yang membuat kargo menjadi rusak. Terhadap permasalahan ini, Hakim Pengadilan Tinggi Australia menginterpretasikan standar bahaya biasa yang ada di HVR 1924 harus diinterpretasikan berdasarkan kemampuan untuk memitigasinya (*foreseen/unforeseen event*).[19] Dalam kasus yang sama, Hakim juga menjelaskan bahwa pemenuhan kewajiban kelaiklautan akan berpokok pada tindakan pengangkut untuk memitigasi segala resiko dengan melaksanakan *due diligence* terhadap kapal.[20] Berdasarkan kasus ini, maka terlihat bahwa tentu suatu pengukuran atau perkiraan yang dilakukan oleh pengangkut dapat meleset. Kemungkinan bahwa cuaca buruk yang ada dalam kasus Bunga Seroja ini dapat terjadi dalam skala yang terlampau besar dan ternyata tidak sesuai dengan prakiraan. Namun, fakta bahwa cuaca buruk mungkin dapat terjadi dalam pengangkutan tersebut membuat pengangkut wajib melaksanakan *due diligence* untuk mempersiapkan kapal agar layak untuk berlaut menghadapi cuaca buruk tersebut.

Kedua kasus di atas memberikan pemahaman mengenai kewajiban kelaiklautan, yakni bahwa kewajiban kelaiklautan berarti pengangkut wajib memastikan kapal memiliki kapasitas untuk menuntaskan suatu pelayaran menghadapi bahaya yang sepatutnya dapat

[11] *Bradley & Sons v. Federal Steam Navigation Co.* [1926] 24 Lloyds Rep 446, para.454 (C.A. per Scruttion L.J.)
[12] *Actis Co.Ltd v. The Sanko Steamship Co.Ltd* ("**The Aquacharm**") [1982] 1 Lloyd's Rep 7, para.11; *Empresa Cubana Importada De Alimentos "Alimport" v. Iasmos Shipping Co. S.A.* ("**The Good Friend**") [1984] 2 Lloyd's Rep 586 para.593
[13] *Kopitoff v. Wilson, Op.Cit*, para.380
[14] *McFadden v. Blue Star Line*, 1 K.B. 697 para.192
[15] Hang Fung v. Mullion [1966] 1 Lloyd's Rep 511; *The Gundulic* [1981] 2 Lloyd's Rep 418; *Queensland National Bank v Peninsular and Oriental SN Co* [1898] 1 QB 567
[16] Simon Baughen, *Shipping Law*, Oxfordshire: Routledge, 2018, hlm.89
[17] *The Toledo* [1995] 1 Lloyd's Rep. 40.
[18] *Ibid.* hlm.45
[19] Ian Davis, "Perils of the Sea: the Bunga Seroja Case", *Maritime Studies Journal 103,* 1998, hlm.31
[20] *Ibid.*

diperkirakan olehnya. Ukuran yang digunakan untuk mengukur persiapan dari pengangkut sangat kasuistik, menyesuaikan dengan bahaya yang sepatutnya akan ditemukan dalam suatu pelayaran spesifik. Artinya, suatu keadaan laik laut tidak akan selalu berlaku untuk pelayaran lainnya. Suatu kapal dapat dikatakan laik laut pada pelayaran A namun dapat menjadi tidak laik laut untuk pelayaran B.

Tentu perkiraan bahaya yang sepatutnya dihadapi dapat meleset. Cuaca buruk yang terjadi dapat memiliki intensitas yang tidak dapat diperkirakan dan tidak biasa terjadi di suatu daerah atau rute pelayaran tertentu. Dalam kasus demikian, merujuk pada Pasal 4 ayat 1 HVR 1924, pengangkut tidak perlu bertanggungjawab terhadap kerusakan kargo apabila berhasil membuktikan bahwa ia telah melaksanakan *due diligence* dengan sepatutnya. Hal ini menunjukkan beban pembuktian dari kewajiban ini tidak terletak pada hasil dari suatu pelayaran sehingga *due diligence* merupakan *obligation of conduct* dan bukan merupakan *obligation of result*. Terlepas dari bahaya yang terjadi kemudian menghasilkan kerugian terhadap kargo atau tidak, apabila pengangkut berhasil membuktikan bahwa *due diligence* yang sepatutnya telah dilaksanakan, maka ia akan tetap terbebas dari tanggung jawab terhadap kargo yang rusak.

Berdasarkan penjelasan di atas, dapat terlihat bahwa kewajiban kelaiklautan adalah langkah preventif yang dapat dilakukan oleh Pengangkut guna memastikan suatu kapal mampu untuk melindungi kargo dan aman untuk menuntaskan suatu pelayaran dari ancaman *Cyberattack*. Kewajiban kelaiklautan sebagai suatu kewajiban yang membuat pengangkut memastikan kapal telah dilengkapi oleh perlengkapan dan awak yang mumpuni untuk menghadapi bahaya yang sepatutnya dapat ditemukan dalam suatu pelayaran, membuat pemenuhan kewajiban ini secara ideal dapat mengurangi dampak *cyberattack* terhadap kapal. Walaupun demikian, perlu dibuktikan bahwa *cyberattack* adalah suatu bahaya yang sepatutnya dapat diperkirakan dalam pelayaran dan tentu ada suatu langkah realistis yang mampu dilaksanakan oleh Pengangkut untuk menyiapkan kapal agar mampu menahan resiko ancaman *cyberattack*.

Ancaman *Cyberattack* Sebagai Bahaya Yang Sepatutnya Dapat Diperkirakan Dalam Suatu Pelayaran

Kewajiban kelaiklautan mewajibkan pengangkut untuk melaksanakan *due diligence* terhadap kapal pada saat akan melaksanakan suatu pelayaran. Artinya, dalam melaksanakan *due diligence*, pengangkut akan menimbang perlengkapan dan peralatan serta awak yang cocok untuk menghadapi bahaya yang sekiranya telah ia perkirakan terjadi dalam pelayaran yang bersangkutan. Merujuk pada contoh kasus *the Toledo*, dalam menghadapi cuaca buruk di Samudera Atlantik, pengangkut dituntut untuk seharusnya memperlengkapi kapal dengan perlengkapan dan awak yang mumpuni untuk menghadapi cuaca buruk di Samudera Atlantik yang cukup ekstrim.

Kasus *Cia Sud Americana de Vapores v. Sinochem Tianjin Import & Export Corp* pada tahun 2010 memberikan tolok ukur untuk kewajiban kelaiklautan wajib memastikan kapal telah dilengkapi dengan suatu sistem keamanan yang sewajarnya ditemukan untuk melindungi kargo dari "bahaya biasa" (*ordinary perils*) yang sekiranya dapat diperkirakan terjadi.[21] Tolok ukur untuk mengukur *ordinary perils* ini wajib diukur dengan pengetahuan yang sewajarnya diketahui oleh pengangkut. Secara tekstual, mengartikan *ordinary perils* dapat merujuk pada *Black's Law Dictionary*, dimana yang dimaksud dengan *ordinary* adalah "*typical, everyday occurrences*" atau diartikan bebas sebagai kejadian sehari-hari.[22] Hal ini membuat tafsiran gramatikal dari standar kelaiklautan yang ditetapkan dalam HVR 1924 adalah bahaya yang sehari-hari terjadi dan sekiranya dapat diperkirakan sebelumnya.

[21] *The Aconcagua,* para.367
[22] Brian Garner, *Black's Law Dictionary*, St. Paul, Thomson Reuters, hlm.142

Apabila merujuk kembali pada aspek kasuistik dalam kasus *Bunga Seroja*, fakta bahwa suatu bahaya **mungkin dapat terjadi** dalam pengangkutan membuat pengangkut wajib mempersiapkan kapal agar layak untuk berlaut menghadapi bahaya tersebut. Hal ini berkaitan juga dengan kunci dari pemenuhan kewajiban kelaiklautan adalah pelaksanaan due diligence atau uji kelayakan. Kewajiban untuk melaksanakan due diligence berarti kewajiban pengangkut hanya terbatas untuk melaksanakan perawatan yang sewajarnya *(take reasonable care*). Kewajiban ini terpenuhi apabila pengangkut telah melaksanakan tindakan pencegahan yang sewajarnya dilaksanakan. Pada konteks yang demikian, dampak dari cyberattack terhadap kargo berpotensi tidak menjadi tanggung jawab dari pengangkut.

Merujuk pada pedoman dari IMO dalam IMO MSC Fal.1/Circ.3 yang juga merupakan dokumen rujukan untuk standarisasi keamanan ISM Code, ada suatu kebutuhan mendesak bagi pengangkut untuk mempersiapkan kapal menghadapi *cyberattack*. Sebenarnya sebagaimana terlihat misalnya dalam insiden USS Fitzgerald bahwa malfungsi dari teknologi yang ada di kapal dapat berakibat sangat fatal.[23] Tabrakan yang terjadi antara USS Fitzgerald dengan Kapal berbendera Filipina tidak seharusnya terjadi apabila teknologi radar dan komunikasi yang ada dapat berfungsi dengan baik. Opsi lainnya sebagai alternatif solusi yang seharusnya dapat menjadi pelajaran bagi industri pengangkutan laut pasca insiden ini adalah memiliki rencana cadangan apabila terjadi malfungsi teknologi sebagaimana terjadi pada insiden USS Fitzgerald.

Tentu *cyberattack* tidak bersifat seperti bajak laut maupun cuaca buruk yang sifatnya situasional. Artinya, akan sangat tergantung dengan rute yang diambil oleh suatu kapal dalam suatu pelayaran. *Cyberattack* menjadi ancaman nyata bukan karena situasi yang akan dilewati oleh kapal, namun karena fakta bahwa setiap kapal diperlengkapi dengan sistem teknologi yang membantu pelaksanaan kapal. Terlebih lagi, sistem teknologi yang ada di kapal mengambil peran vital dalam keberlangsungan kapal. Sama dengan fakta bahwa melewati lautan Somalia membuat kapal akan beresiko bertemu dengan bajak laut, membekali kapal dengan sistem teknologi membuat kapal akan beresiko terhadap *cyberattack*. Hal ini sejalan dengan edaran IMO yang tidak bermaksud untuk menghindarkan kapal dari *cyberattack* namun lebih bermaksud untuk meningkatkan resiliensi (ketahanan) kapal dari dampak *cyberattack*.[24] Hal ini menggambarkan bahwa sebenarnya dampak dari *cyberattack* dapat dimitigasi oleh pengangkut melalui tindakan-tindakan persiapan sebelum pelayaran.

Seharusnya *cyberattack* dapat dipandang sebagai suatu bahaya yang sekiranya dapat terjadi di suatu pelayaran dan peristiwa yang sehari-hari terjadi. Memperlengkapi kapal dengan sistem teknologi seharusnya dipandang sebagai suatu paket yang sama dengan ancaman yang terkandung di dalamnya yakni ancaman *cyberattack*. Sehingga seharusnya suatu kapal hanya akan menjadi laik laut apabila telah diperlengkapi dengan standar peralatan atau sistem pertahanan untuk menghadapi *cyberattack*.

Tindakan *Due Diligence* yang Dapat Dilaksanakan oleh Pengangkut Guna Memenuhi Kewajiban Kelaiklautan

Merujuk pada IMO MSC Fal.1/Circ.3 *Guidelines on Maritime Cyber Risk Management*, ada beberapa fundamental yang harus dikokohkan dalam kegiatan pelayaran guna meningkatkan ketahanan kapal kargo terhadap ancaman *cyberattack*.[25]

1. Identifikasi sistem-sistem yang rawan terhadap cyberattack. Khususnya terhadap sistem-sistem yang ketika terjadi malfungsi dapat memberikan dampak yang signifikan terhadap keberlangsungan kapal kargo. Hal ini juga termasuk

[23] Ben Farah, *Op.Cit*, hlm.6
[24] Annex 1 IMO MSC Fal.1/Circ.3, hlm.3
[25] *Ibid.*

mengidentifikasi peranan dan tanggung jawab dari tiap-tiap personil kapal kargo untuk sistem yang ada pada kapal kargo;
2. Mengimplementasikan proses dan langkah manajemen resiko terhadap kemungkinan-kemungkinan cyberattack. Langkah ini yang kemudian diharapkan dapat memastikan kelangsungan dari pelayaran apabila terjadi cyberattack terhadap kapal kargo;
3. Mensosialisasikan tindakan-tindakan yang membuat awak kapal kargo dapat mendeteksi adanya cyberattack tepat waktu;
4. Mensosialisasikan dan mengembangkan rencana-rencana dalam menghadapi cyberattack. Hal ini dimaksudkan untuk meningkatkan resiliensi kapal kargo dan kemampuan kapal kargo untuk memulihkan kembali sistem yang terganggu akibat dari cyberattack yang terjadi; dan
5. Mengidentifikasi langkah-langkah cadangan yang tepat untuk memulihkan kembali sistem yang ada di kapal kargo pasca terdampak *cyberattack*.

Kelima poin penting ini merupakan fundamental yang wajib diterapkan oleh kapal kargo guna meningkatkan resiliensi kapal kargo terhadap *cyberattack*.

Secara lebih teknis, IMO sebenarnya merujuk pada beberapa panduan teknis untuk menjelaskan langkah konkret dari pedoman yang dimaksud IMO. Salah dua dari beberapa panduan yang dimaksud adalah BIMCO *Guidelines on Cybersecurity Onboard Ships* dan *International Association of Classification Societies* ("**IACS**") *Guidelines on Vessels' Cyber Resilience*.[26] Penulis sendiri merujuk pada dua panduan ini karena kedua panduan ini dipublikasi oleh dua organisasi internasional yang sangat berpengaruh dalam pengangkutan global.

Prinsipnya adalah pengangkut wajib mampu untuk mengidentifikasi tiap-tiap sistem yang digunakannya di kapal kargo, termasuk resiko yang ada apabila pengangkut memilih untuk menggunakan sistem tersebut. Pendekatan manajemen resiko dibutuhkan dalam langkah ini. Pengangkut wajib mengetahui tiap-tiap rincian dari sistem yang digunakan, baik yang berkaitan dengan teknologi informasi maupun teknologi operasional. Pada sebuah simulasi yang dilakukan pada tahun 2018, beberapa bagian penting yang menyusun infrastruktur kapal rentan terhadap serangan siber. Adapun bagian-bagian utama yang membangun suatu infrastruktur kapal adalah:[27]

1. Sistem Manajemen Daya
2. Sistem Komunikasi
3. Sistem Navigasi
4. Sistem Manajemen Kargo; dan
5. Alarm Kapal

Setelah pengangkut mampu untuk melaksanakan identifikasi aset, maka langkah selanjutnya yang dapat dilaksanakan oleh pengangkut adalah penilaian resiko. Beberapa faktor yang direkomendasikan untuk dipertimbangkan adalah kemungkinan terjadinya peretasan yang membuat adanya akses tidak sah dari pihak lain dan kemungkinan adanya hilang koneksi secara keseluruhan oleh kapal kargo. Konektivitas antar sistem seperti sistem navigasi dan komunikasi menjadi pokok perhatian dari kedua panduan ini.[28] Merujuk pada lampiran A panduan IACS, beberapa rekomendasi yang dapat diterapkan oleh pengangkut adalah sebagai berikut:[29]

[26] *Ibid*. hlm.4
[27] Bellsola Olba, "State of the Art of Port Simulation Models for Risk and Capacity Assessment Based on the Vessel Navigational Behaviour Through the Nautical Infrastructure", *Journal of Traffic and Transportation Engineering*, hlm.338
[28] *Ibid*.
[29] Annex A, IACS Recommendation No.166, hlm.15-36

1. Sistem Komunikasi

   Suatu penelitian mengkritisi teknologi komunikasi yang ada di kapal karena rentan terhadap serangan siber seperti pemutusan jalur komunikasi, namun seringkali ditemukan bahwa kapal tidak memiliki rencana cadangan apabila sistem tersebut terganggu.[30]

   Baik pedoman IACS maupun BIMCO merekomendasikan pengangkut untuk memiliki perangkat komunikasi yang terenkripsi. Selain itu, penting untuk setiap awak kapal kargo memahami bahwa pengoperasian sistem dengan otorisasi yang jelas akan sangat penting untuk keamanan sistem komunikasi kapal. Pedoman yang ada juga merekomendasikan bahwa setiap sistem yang ada, termasuk sistem keamanan dari sistem komunikasi ini diuji secara berkala. Pengujian ini bertujuan untuk secara menerus menguji kerentanan dari sistem komunikasi yang ada di kapal.

   Adapun penulis menarik suatu kesimpulan bahwa kunci penting dalam sistem komunikasi kapal yang baik adalah otorisasi akses yang memadai. Pada saat tiap akses terhadap sistem komunikasi membutuhkan otorisasi yang cukup, maka berdasarkan panduan yang ada, cukup untuk meningkatkan resiliensi kapal terhadap *cyberattack*.

2. Sistem Navigasi

   Pengujian terhadap sistem navigasi terbagi menjadi dua jenis dalam pedoman yang ada. Sistem navigasi terbagi menjadi sistem yang ada pada kapal dan sistem yang ada di kantor kapal (*remote access*). Kepemilikan sistem navigasi yang tidak hanya ada pada kapal, namun juga sistem navigasi yang terpantau dari kantor kapal membuat sistem navigasi memiliki cadangan.

   Ketentuan umum untuk persyaratan kualitas sistem ini adalah kemampuan dari sistem untuk mencegah sebaik mungkin kemungkinan teretas. Salah satu skenario yang dipersiapkan adalah perlu adanya sistem cadangan dari kantor kapal apabila sistem navigasi kapal teretas. Hal ini berguna sehingga pada saat adanya akses yang tidak terotorisasi, maka sistem yang ada di kantor kapal perlu mencoba melawan dan mengembalikan kontrol navigasi pada kapal.

3. Jaringan

   Umumnya, kapal akan menggerakan sistemnya menggunakan jaringan internet. Hal ini memang merupakan pilihan yang umum dan paling mudah untuk dilakukan. Permasalahannya adalah penggunaan jaringan internet tanpa enkripsi dan perlindungan tambahan yang digunakan oleh kapal malah akan membuat kapal terpapar pada bahaya peretasan.

   Terhadap hal ini, beberapa langkah yang direkomendasikan oleh pedoman seperti yang dibuat oleh BIMCO dan IACS adalah membuat alamat IP yang terenkripsi khusus untuk sistem kapal. Tentunya hal ini tidak secara mutlak melindungi kapal dari bahaya peretasan, namun secara praktik yang ada sejauh ini, tindakan demikian dapat setidaknya meminimalisir resiko peretasan.

   Bilamana kapal diperlengkapi dengan teknologi *remote access*, maka penting untuk memastikan fitur untuk pengendali dapat mematikan akses pada saat apapun. Hal ini menjadi penting karena serangan terhadap fitur *remote access* dapat menimbulkan dampak yang signifikan pada kemaslahatan kapal.

Melihat langkah-langkah yang dapat ditempuh untuk meningkatkan resiliensi kapal terhadap cyberattack, maka sebenarnya nyata bahwa pengangkut memiliki tanggungjawab untuk memastikan kapal telah sesuai dengan pedoman yang ada. Hal ini mengingat pedoman BIMCO dan IACS telah disesuaikan dengan perkembangan tantangan pengangkutan modern. Walaupun kedua pedoman ini tidak memiliki kekuatan hukum yang mengikat, namun,

[30] Frank Akpan, "Cybersecurity Challenges in the Maritime Sector", *Network Journal Studies*, Vol.2, 2022, hlm.130

praktik terbaik yang telah dikompilasi oleh ahli dalam bidang pengangkutan laut ini menjadi standar yang pantas untuk memenuhi standar kewajiban kelaiklautan berdasarkan HVR 1924.

Hukum Positif Indonesia Dalam Meregulasi Kewajiban Kelaiklautan Guna Menghadapi Ancaman *Cyber Attack*

Sebagaimana dijabarkan pada bagian-bagian sebelumnya, salah satu dasar yang membuat HVR 1924 menjadi aturan yang baik untuk mengatur kewajiban kelaiklautan adalah ukuran yang digunakan sangat dinamis menyesuaikan dengan bahaya yang sekiranya ditemukan dalam pengangkutan. Walaupun demikian, aturan ini sedikit berbeda dengan UU Pelayaran, hubungan hukum yang diatur dalam HVR 1924 bersifat keperdataan antara pengangkut dengan pemilik kargo. Sedangkan, dalam UU Pelayaran, hubungan hukum yang diatur lebih merujuk pada sifat pertanggungjawaban pengangkut terhadap negara. Indonesia sendiri sampai hari ini tidak memiliki suatu aturan terkodifikasi dalam suatu produk hukum yang dapat langsung dibandingkan dengan HVR 1924 mengenai hal ini. Maka dari itu, perlu untuk melihat perspektif hukum positif Indonesia dari cakupan yang lebih luas

Kewajiban kelaiklautan secara keperdataan di Indonesia sebenarnya dapat lahir dari Pasal 470 KUHD yang menyatakan suatu bentuk tanggung jawab dari pengangkut untuk untuk menanggung kerusakan pada barang yang diangkutnya yang disebabkan oleh kurang baiknya alat pengangkutan atau kurang cakapnya pekerja yang dipakainya. Tanggung jawab sebagaimana dimaksud dalam Pasal 470 KUHD ini tentu sangat luas, membutuhkan aturan lain untuk menginterpretasi standar yang akan digunakan untuk menentukan kurang baik dan/atau kurang cakapnya kelengkapan kapal. Untuk itu, Pasal 470 KUHD perlu diinterpretasikan sebagai kewajiban kelaiklautan kapal yang mana adalah kewajiban dari pengangkut untuk memastikan kapal telah diperlengkapi dengan alat dan awak yang baik. Pasal 1 (33) UU Pelayaran menjelaskan kelaiklautan kapal sebagai keadaan kapal yang memenuhi persyaratan-persyaratan tertentu.

Proses suatu kapal dapat dinyatakan laik laut membutuhkan pengangkut untuk memiliki sertifikat-sertifikat yang menjadi persyaratan kelaiklautan. Setelah itu, sertifikat tersebut yang menjadi dasar bagi syahbandar untuk menyatakan suatu kapal telah laik laut. Permasalahannya adalah sertifikat-sertifikat ini tidak mencerminkan suatu kapal laik laut. Salah satu sertifikat yang dibutuhkan adalah sertifikat keselamatan kapal, dimana untuk kapal barang berdasarkan Pasal 22 Peraturan Menteri Perhubungan Nomor PM.57 Tahun 2021 tentang Tata Cara Pemeriksaan, Pengujian dan Sertifikasi Keselamatan Kapal akan berlaku selama 12 bulan. Prosedur pengecekan kelaiklautan yang demikian akan menciptakan suatu tolok ukur yang kaku dan rendah dalam pelayaran internasional. Standar yang dimiliki oleh hukum positif di Indonesia berusaha membuat sistem keselamatan dan keamanan kapal menjadi sistem yang dapat berlaku untuk setiap pelayaran selama lima tahun. Walaupun pada praktiknya memang akan dilakukan pengecekan kembali oleh Syahbandar pada saat sebelum melaksanakan suatu pelayaran, yang akan diuji adalah kepemilikan dan keabsahan dari sertifikat-sertifikat yang dimiliki oleh kapal guna memperoleh *port clearance*.

Pada perspektif privat, jika Pasal 470 KUHD yang mana menjelaskan pengangkut akan bertanggung jawab apabila ada kerusakan yang diakibatkan oleh kurang baiknya alat pengangkutan, menggunakan standarisasi hukum positif Indonesia yang ada dalam UU Pelayaran beserta peraturan turunannya, maka standarisasi Indonesia akan terbelakang jika dibandingkan dengan standar internasional. HVR 1924 sebagai aturan yang digunakan umum secara internasional menetapkan suatu standar yang sifatnya kasuistik yang berarti kelaiklautan wajib diukur untuk setiap keadaan pelayaran. Logika yang penting untuk dipahami dalam kasus ini adalah kegagalan untuk memiliki sertifikat keamanan dan keselamatan kapal tentu adalah pelanggaran terhadap kelaiklautan kapal, baik

menggunakan standar nasional maupun internasional. Namun, jika membandingkan standar yang ada pada HVR 1924 dengan hukum nasional maka akan memandang hal ini pada satu tingkat daripada sekedar pemenuhan sertifikat. Pemenuhan sertifikat keamanan dan keselamatan berdasarkan hukum Indonesia, tidak berarti pemenuhan kewajiban kelaiklautan berdasarkan HVR 1924. Kembali lagi, standar yang lebih faktual pada HVR 1924 membuat hukum nasional tidak dapat mencapai standar tersebut.

Secara lebih teknis, Peraturan Menteri Perhubungan Nomor 51 Tahun 2021 tentang Prosedur dan Tata Cara Pelaksanaan Verifikasi Manajemen Keamanan Kapal dan Fasilitas Pelabuhan ("**Permenhub 51/2021**") sebagai peraturan turunan dari UU Pelayaran menetapkan bahwa standar internasional yang dirujuk untuk verifikasi manajemen keamanan kapal adalah koda ISPS atau ISPS *Code*. Koda ini merupakan suatu koda yang digunakan secara internasional untuk memberikan perintah serta anjuran bagi kapal, Pelabuhan dan pemerintah untuk menciptakan suatu ekosistem pengangkutan yang aman. Sebagaimana merujuk pada Pasal 1 ayat 1 Permenhub 51/2021, proses verifikasi manajemen keamanan kapal akan menilai keefektifan penerapan manajemen keamanan kapal terhadap Koda. Adapun koda yang dimaksud disini adalah ISPS *Code*. Verifikasi sebagaimana dimaksud pada Pasal 1 ayat 1 ini dijelaskan dalam Pasal 2 ayat 2 dilakukan secara berkala sebanyak 3 kali selama 5 tahun.

Aturan teknis ini mengandung 2 permasalahan yang membuat regulasi Indonesia kurang relevan untuk menghadapi ancaman *Cyberattack* dalam industri pengangkutan global. Fakta bahwa IMO MSC-FAL.1 Circ.3 Rev.1, tidak mencantumkan ISPS *Code* sebagai panduan teknis dalam manajemen resiko siber, dan ISPS *Code* sendiri tidak mengatur mengenai persiapan terhadap ancaman *cyberattack* membuat suatu kekosongan hukum dalam isu persiapan terhadap ancaman *cyberattack* ini.

Memang, Indonesia tidak meratifikasi HVR 1924, namun fakta bahwa berbagai negara di Asia bahkan Dunia meratifikasi HVR 1924 membuat Indonesia perlu mempertimbangkan meratifikasi atau mengadopsi aturan ini. Berdasarkan kelemahan yang ada pada hukum positif Indonesia dalam mengatur kelaiklautan kapal secara privat atau keperdataan, membuat hubungan kontraktual pelaku usaha Indonesia dengan pelaku usaha asing pada bidang ini akan terhambat. Mayoritas kontrak pengangkutan baik dalam rupa kontrak pengangkutan maupun konosemen sudah memasukkan HVR 1924 sebagai pilihan hukum.

Pelaku usaha Indonesia yang berperan sebagai pengangkut tentunya akan kesulitan apabila merujuk pada hukum positif di Indonesia semata. Pemenuhan sertifikat-sertifikat kelaiklautan kapal yang ada pada hukum positif Indonesia rasanya kurang mampu untuk menjawab standar tinggi yang diberikan dalam HVR 1924. Walaupun memang praktik global juga menggunakan sertifikat sebagai tanda pemenuhan kewajiban kelaiklautan secara publik, namun standar tersebut rasanya belum cukup untuk pelayaran tertentu khususnya dalam ranah privat.

PENUTUP

Tindakan due diligence pengangkut untuk memenuhi kewajiban kelaiklautan berdasarkan HVR 1924 juga dibutuhkan untuk ancaman cyberattack. Standar kelaiklautan berdasarkan HVR 1924 menetapkan tindakan due diligence pengangkut membuat kapal siap untuk menghadapi bahaya yang sepatutnya dapat diperkirakan dalam suatu pelayaran. Sifat dari cyberattack yang menyerang sistem informasi dari kapal, dan sistem kapal yang mayoritas bergantung pada teknologi informasi membuat serangan ini dapat diperkirakan terjadi dalam suatu pelayaran. Terlebih lagi, kepatuhan pengangkut terhadap pedoman-pedoman teknis seperti BIMCO dan AICS membuat pengangkut dapat dinyatakan telah memenuhi kewajiban kelaiklautan.

Dalam perspektif Indonesia, Hukum positif di Indonesia belum secara eksplisit mengatur kewajiban pengangkut terhadap kelaiklautan kapal untuk menghadapi ancaman cyberattack. UU Pelayaran beserta PP 31/2021 yang menetapkan pemenuhan kewajiban kelaiklautan berdasarkan pemenuhan sertifikasi, tidak cukup kasuistik untuk menentukan kelaiklautan kapal. Terlebih lagi, ISPS Code sebagai standar yang dirujuk Indonesia dalam konteks verifikasi manajemen keamanan dan keselamatan kapal tidak membahas mengenai persiapan kapal terhadap ancaman cyberattack, dan tidak dirujuk oleh IMO sebagai dokumen teknis yang dapat dijadikan pedoman untuk menghadapi ancaman cyberattack membuat Indonesia memiliki kekosongan hukum dalam memberikan standar bagi pengangkut untuk memenuhi kewajiban kelaiklautan menghadapi ancaman cyberattack.

Untuk DPR dan pemerintah sebagai regulator sebaiknya mengadopsi HVR 1924 beserta dengan yurisprudensi yang memberikan interpretasi terhadap penerapan kewajiban kelaiklautan. Standar yang kasuistik membuat aturan yang dibuat pada tahun 1924 ini masih relevan sampai pada saat ini. Revisi UU Pelayaran beserta peraturan turunannya perlu dilaksanakan untuk menyesuaikan standar kelaiklautan yang ada di Indonesia dengan yang digunakan pada praktik internasional berdasarkan HVR 1924. Sementara untuk pengangkut, sebaiknya dapat meningkatkan standar tindakan due diligence yang dilaksanakan guna memenuhi kewajiban kelaiklautan dalam menghadapi ancaman cyberattack. Pemenuhan kewajiban kelaiklautan yang bertitik pada pelaksanaan due diligence sepatutnya dilaksanakan dengan manajemen resiko, Sebagai negara anggota dari IMO, pengangkut dapat merujuk pada pedoman teknis yang disusun oleh IMO. Pelaksanaan due diligence sesuai pedoman yang direkomendasikan oleh IMO, dapat membuat pengangkut telah dianggap melaksanakan kewajiban kelaiklautan.

DAFTAR PUSTAKA

Buku

Brian Garner, *Black's Law Dictionary*, St. Paul, Thomson Reuters

Asikin, Amiruddin dan Zainal. (2014). *Pengantar Metode Penelitian Hukum*. Jakarta: Raja Grafindo

Baughen,Simon. (2018). *Shipping Law*. Oxfordshire: Routledge

Soemitro dan Ronny Hanitijo. (1983). *Metodologi Penelitian Hukum dan Jurimetri*, Jakarta: Ghalia Indonesia,

Artikel Jurnal

Bellsola Olba, "State of the Art of Port Simulation Models for Risk and Capacity Assessment Based on the Vessel Navigational Behaviour Through the Nautical Infrastructure", *Journal of Traffic and Transportation Engineering*

Ben Farah, "Cybersecurity in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends", *Maritime Digital Information*, 2022

Frank Akpan, "Cybersecurity Challenges in the Maritime Sector", *Network Journal Studies*, Vol.2, 2022,

Ian Davis, "Perils of the Sea: the Bunga Seroja Case", *Maritime Studies Journal 103,* 1998

Nobuo Takeda, "Marine Accident Investigation Report", *Japan Transport Safety Board*

Website

Andrew Kinsey. 2021. Cyber Security Threats Challenge International Shipping Industry dari. https://www.maritimeprofessional.com/news/cyber-security-threats-challenge-international-369770

Dokumen Hukum Lainnya

Actis Co.Ltd v. The Sanko Steamship Co.Ltd ("**The Aquacharm**") [1982] 1 Lloyd's Rep 7

Bradley & Sons v. Federal Steam Navigation Co. [1926] 24 Lloyds Rep 446, para.454 (C.A. per Scruttion L.J.)

Cia Sud Americana De Vapores v. Sinochem Tianjin Import & Export Corp ("**The Aconcagua**") [2010] 1 Lloyd's Rep 1

Empresa Cubana Importada De Alimentos "Alimport" v. Iasmos Shipping Co. S.A. ("**The Good Friend**") [1984] 2 Lloyd's Rep 586

G*ilroy Sons & Co v. W R Price & Co* [1893] AC 56

Great China Material Industries Co Ltd v. Malaysian International Shipping Corporation Berhad ("**Bunga Seroja**") [1998] 196 CLR 161

Hang Fung v. Mullion [1966] 1 Lloyd's Rep 511

IACS Recommendation No.166

IMO MSC Fal.1/Circ.3

Kopitoff *v. Wilson* [1876] 1 QBD 377

McFadden v. Blue Star Line, 1 K.B. 697 para.192

Steel v. State Line Steamship Co [1877] 3 App Cas 72

Virginia Carolina Chemical Co v. Norfolk and North American Steam Shipping Co [1912] 1 KB 229