IMPLEMENTASI KERANGKA KERJA REGULASI KEAMANAN SIBER UNTUK KAPAL OTONOM (MASS) GUNA MENGANTISIPASI RISIKO ANCAMAN HIBRIDA DI ERA PELAYARAN MASA DEPAN DALAM PERTAHANAN NEGARA DI LAUT

Arif Badrudin
Kepala Staf Komando Armada I
arif.badrudin11379@gmail.com
http://doi.org/10.52307/jmi.v912.203

Abstrak

Kemajuan teknologi **Kap kapal Permukaan Otonom Maritim** (MASS) bukan hanya pilihan, tetapi suatu kepastian yang akan mengubah industri maritim global. Namun, meski menawarkan efisiensi, MASS juga menghadapi kerentanan keamanan serius karena ketergantungannya pada sistem digital yang rumit, menjadikannya rentan terhadap ancaman hibrida. Serangan siber dapat menyebabkan kerusakan fisik, kekacauan ekonomi, dan mengancam kedaulatan negara.

Analisis menunjukkan bahwa kerangka regulasi maritim saat ini tidak memadai untuk menangani tantangan ini. Oleh karena itu, Indonesia perlu membangun model regulasi keamanan siber berdasarkan empat pilar: (1) standardisasi teknologi aman dari tahap desain; (2) peraturan operasional dan pengembangan kompetensi sumber daya manusia; (3) kolaborasi dalam berbagi informasi ancaman; dan (4) langkah penegakan hukum yang memberikan efek jera.

Implementasi kerangka ini tidak hanya bersifat teknis, tetapi juga strategis, untuk memastikan Indonesia dapat memanfaatkan teknologi otonom tanpa mengorbankan keamanan dan kedaulatan sebagai Poros Maritim Dunia. Menghadapi perkembangan ancaman siber yang terus berubah, Indonesia dapat bertransformasi dari peserta reaktif menjadi pelopor dalam operasi maritim otonom yang aman dan tangguh.

Kata Kunci:ancaman hibrida, regulasi maritim, regulasi keamanan siber,operasi maritim otonom

Abstract

The advancement of Maritime Autonomous Surface Ships (MASS) technology is not merely an option but a certainty that will transform the global maritime industry. However, despite offering efficiency, MASS also faces serious security vulnerabilities due to its reliance on complex digital systems, making it susceptible to hybrid threats. Cyberattacks can result in physical damage, economic disruption, and pose a threat to national sovereignty.

Analysis indicates that the existing maritime regulatory framework is insufficient to address these challenges. Therefore, Indonesia needs to develop a cybersecurity regulatory model based on four pillars: (1) standardization of secure technology from the design stage; (2) operational regulations and human resource competency development; (3) collaboration in threat information sharing; and (4) law enforcement measures that create a deterrent effect.

The implementation of this framework is not only technical but also strategic, aimed at ensuring that Indonesia can leverage autonomous technologies without compromising its security and sovereignty as the World Maritime Axis. By confronting the evolving landscape of cyber threats, Indonesia can transform from a reactive participant into a pioneer in secure and resilient autonomous maritime operations.

***Keywords**: hybrid threats, maritime regulation, cybersecurity regulation, autonomous maritime operations.*

A. PENDAHULUAN

Sebagai negara kepulauan terkemuka secara global, Indonesia memprioritaskan keamanan maritim sebagai landasan kedaulatan dan kemajuan ekonominya. Visi pemerintah untuk membentuk Poros Maritim Dunia menegaskan kembali dedikasinya terhadap pengelolaan dan pengamanan domain maritim sebagai saluran penting bagi perdagangan dan konektivitas nasional (Pemerintah Indonesia, 2017). Namun demikian, di tengah upaya untuk mengaktualisasikan visi ini, lanskap ancaman maritim mengalami transformasi yang mendalam. Ancaman telah melampaui perselisihan dan konflik teritorial konvensional, berkembang menjadi ancaman hibrida yang lebih rumit, ditandai dengan serangan terkoordinasi yang menggabungkan elemen cyber, fisik, dan disinformasi untuk memenuhi tujuan strategis (NATO, 2021). Bahkan, kartel Narkoba (Narkotika dan Obat-obatan Terlarang) diyakini telah memiliki unit-unit hacker yang dapat melakukan penetrasi siber terhadap system digital penegak hukum (UNODC, 2024).

Organisasi kriminal perdagangan narkoba (DTO) saat ini tidak hanya berfungsi dalam domain fisik, tetapi juga meningkatkan kehadiran operasional mereka di domain digital (Martin, 2014). Sifat ancaman yang dihadapi oleh gugus tugas penyelundupan narkoba adalah hibridisasi, menggabungkan metodologi tradisional dengan strategi perang dunia maya. Eskalasi inisiatif penegakan hukum global telah memaksa DTO untuk mengembangkan atau memperoleh kemampuan cyber yang mahir untuk mempertahankan perusahaan terlarang mereka (UNODC, 2024). Berbeda dengan kolektif peretasan yang disponsori negara, kelompok peretas yang dibiayai kartel biasanya berfungsi sebagai penyedia layanan kejahatan dunia maya (Cyber Cartel Services) atau beroperasi sebagai unit internal yang sangat klandestin. Penilaian intelijen dunia maya telah mengakui entitas seperti grup “CyberCartel” di Amerika Latin, yang menargetkan layanan perbankan dan pemerintah, menunjukkan adanya infrastruktur cyber yang terjalin yang digunakan oleh berbagai organisasi kriminal (Darktrace, 2024). Kartel

terkemuka, termasuk Kartel Sinaloa, dilaporkan mempekerjakan peretas untuk mengeksploitasi perangkat seluler dan sistem elektronik yang terkait dengan badan penegak hukum, termasuk akuisisi data geolokasi (AFCEA International, 2025). Ini mendukung pernyataan bahwa DTO memiliki sumber daya keuangan dan motivasi untuk mendapatkan intelijen cyber yang sangat terspesialisasi. Los Zetas, misalnya, adalah salah satu DTO awal yang konon membanggakan kemampuan teknologi paling canggih, menyiratkan bahwa integrasi kemampuan cyber mewakili kemajuan historis dalam DTO (Hesterman, 2013, di Valencia, 2015).

Terkait dengan kemampuan OKN dalam membiayai berbagai aktifitas illegal dan beradaptas dengan evolusi teknologi, OKN dapat memiliki kemampuan untuk revolusi teknologi dalam sektor maritim, khususnya inovasi Kapal Permukaan Otonom Maritim (MASS). Teknologi ini secara paradoks telah menimbulkan kerentanan keamanan baru yang substansif. Kesulitan ini dikaitkan dengan ketergantungan mendalam arsitektur MASS pada ekosistem digital multifaset, yang mencakup sensor (LiDAR, RADAR), sistem navigasi (GNSS, AIS), aktuator, kecerdasan buatan (AI), dan konektivitas berkelanjutan ke hub kendali jarak jauh yang bertugas memonitor dan mengendalikan operasi MASS melalui jaringan satelit (IMO, 2021a). Setiap titik dalam kontinum digital ini menyajikan vektor serangan yang dapat dieksploitasi oleh aktor negara dan non-negara. Insiden cyber global yang terkenal, seperti serangan ransomware NotPetya pada tahun 2017 yang melumpuhkan raksasa pengiriman Maersk dan mengalami kerugian yang diperkirakan mencapai $300 juta, dengan jelas menggambarkan kerentanan sektor maritim terhadap serangan cyber, bahkan sebelum munculnya otonomi komprehensif (Greenberg, 2018). Serangan semacam itu pada armada MASS dapat memicu dampak bencana yang sangat besar, mulai dari pembajakan kapal dari jarak jauh dan manipulasi data kargo hingga pemanfaatan kapal sebagai instrumen untuk bertabrakan dengan infrastruktur penting, seperti pelabuhan atau platform lepas pantai.

Dengan demikian, kemunculan (MASS) di lingkungan maritim global yang dapat dibangun dan dikendalikan oleh OKN melampaui wacana teoritis belaka. Organisasi Maritim Internasional (IMO) memproyeksikan bahwa kerangka peraturan untuk kapal otonom dapat dilembagakan pada tahun 2028 (IMO, 2023), sehingga berkembang menjadi keniscayaan teknologi yang memerlukan antisipasi strategis. Perbedaan antara kemajuan pesat inovasi teknologi MASS dan adaptasi lamban dari kerangka peraturan keamanan maritim yang ada menimbulkan “kesenjangan kerentanan”

yang berbahaya. Pada tulisan ini menemukan bahwa, dengan tidak adanya kerangka peraturan keamanan siber yang proaktif, komprehensif, dan dibuat dengan cermat yang disesuaikan untuk MASS, aspirasi Indonesia untuk keamanan dan keunggulan maritim secara fundamental akan terancam.

Tujuan Penulisan

Secara praktis, makalah ini diantisipasi untuk menghasilkan manfaat dalam domain berikut:

a. Untuk Pemerintah dan Regulator: Untuk memberikan landasan konseptual dan rekomendasi kebijakan konkret untuk penyusunan awal peraturan nasional mengenai keamanan siber MASS.

b. Untuk Angkatan Laut: Untuk memberikan wawasan strategis untuk integrasi keamanan siber maritim ke dalam doktrin pertahanan dan strategi operasional, serta untuk meningkatkan postur pertahanan untuk mengantisipasi era baru peperangan.

c. Untuk Industri Maritim: Untuk menawarkan panduan untuk integrasi teknologi otonom yang aman dan untuk meningkatkan kesadaran mengenai pentingnya investasi dalam ketahanan dunia maya.

d. Untuk Akademisi: Untuk berfungsi sebagai referensi dan katalis untuk penyelidikan ilmiah lebih lanjut dalam bidang hukum, teknologi, dan keamanan maritim di era digital. Rumusan Masalah

Gambaran Umum.

Dengan melihat pada uraian diatas, penelitian ini mengartikulasikan beberapa Ggambaran umum:

a. Sejauh mana karakteristik ancaman hibrida kontemporer dapat mengeksploitasi kerentanan tertentu yang tertanam dalam arsitektur teknologi Kapal Otomatis (MASS)?

b. Seberapa komprehensifkah kerangka peraturan keamanan maritim internasional yang ada, seperti SOLAS dan Kode ISPS, dalam memastikan keamanan siber dalam operasi MASS?

c. Bagaimana model kerangka kerja peraturan keamanan siber yang komprehensif dan dapat ditindaklanjuti untuk MASS dapat diterapkan secara efektif di Indonesia, sambil secara bersamaan mempertimbangkan keseimbangan antara keamanan, inovasi, dan kelayakan komersial?

B. METODE PENELITIAN

Tulisan ini disusun menggunakan metode penelitian hukum normatif-analitis (normative-analytical legal research) yang diperkaya dengan pendekatan analisis risiko hibrida (*hybrid risk analysis approach*). Pendekatan yang

dilakukan adalah normatif-analitis dengan fokus utama penelitian adalah menganalisis kekosongan dan ketidakcukupan regulasi maritim internasional yang ada saat ini (seperti ISPS Code dan SOLAS) dalam menghadapi ancaman siber dan otonom. Hal ini dilakukan melalui analisis kualitatif terhadap bahan hukum primer (konvensi internasional, peraturan IMO, seperti *Guidelines on Maritime Cyber Risk Management* dan bahan hukum sekunder

C. PEMBAHASAN

Keberhasilan TNI AL dalam menggagalkan berbagai penyelundupan Narkoba beberapa waktu terakhir, dapat mendorong retaliasi dari OKN dengan jalan meretas system digital TNI AL. Karenanya, kemampuan pertahanan siber TNI AL harus dipersiapkan dengan memadai agar mampu mencegah peretasan yang dapat merusak jaring komando yang telah terbangun di berbagai platform. Ancaman hibrida dalam domain maritim merupakan manifestasi strategis dari permusuhan yang mengaburkan demarkasi antara perang dan kegiatan masa damai, menggunakan penggabungan terkoordinasi dari beragam instrumen paksaan yang mencakup sarana militer dan non-militer, untuk memenuhi tujuan tanpa harus melanggar ambang batas menjadi konflik terbuka.

Berbeda dengan ancaman konvensional, yang mudah diidentifikasi, ancaman hibrida menunjukkan tingkat ambiguitas yang signifikan, sering dieksekusi oleh entitas proksi atau aktor yang atribusinya tetap menantang, dan mereka secara khusus menargetkan kerentanan sistemik suatu negara, termasuk kerangka kerja infrastruktur ekonomi, sosial, dan kritis (Hoffman, 2007). Di laut, fenomena ini dapat dioperasionalkan melalui sintesis penyebaran kapal milisi maritim, serangan siber terhadap infrastruktur pelabuhan, penyebaran disinformasi mengenai insiden maritim, dan pengerahan tekanan ekonomi pada perusahaan pelayaran. Ilustrasi yang menonjol dari metodologi ini adalah penggunaan *spoofing* GPS di Laut Hitam pada tahun 2017, yang melibatkan lebih dari 20 kapal melaporkan posisi GPS yang salah yang menunjukkan kedekatan dengan bandara terestrial, sebuah insiden yang secara luas dianggap sebagai demonstrasi awal perang elektronik oleh negara-bangsa (Coker et al., 2017).

Serangan cyber khusus ini, ketika disinergikan dengan manuver fisik kapal tanpa bendera di dalam zona ekonomi eksklusif (ZEE), berpotensi menimbulkan kebingungan, menimbulkan penilaian yang tidak akurat, dan secara bertahap merusak kedaulatan negara atas wilayah maritim. Dengan demikian, memahami bahwa Kapal Permukaan Otonom Maritim (MASS)

dapat berfungsi baik sebagai target dan instrumen dalam kerangka operasional hibrida sangat penting; bayangkan jika terjadi suatu situasi dengan scenario pembajakan kapal tanker otonom untuk ditabrakkan dengan terminal gas alam cair. Maka situasi ini telah melampaui ranah kecelakaan belaka, berkembang menjadi serangan strategis dengan konsekuensi ekonomi dan politik yang dampaknya sangat luas secara domestic maupun global.

Temuan: Teknologi dan Kerentanan

a. Kapal Otonom (MASS)

Saat ini kerangka arsitektur teknologi memungkinkan untuk Pembangunan MASS, yang sangat penting untuk kemanjuran operasionalnya, secara intrinsik menghasilkan permukaan serangan yang luas dan beragam. Hal ini disebabkan oleh integrasi dua domain yang sebelumnya berbeda: teknologi operasional (OT) yang mengatur fungsi fisik kapal (navigasi, propulsi, kemudi) dan teknologi informasi (TI) yang mengawasi manajemen data (kargo, komunikasi, administrasi). Konvergensi dan penggabungan dalam pemanfaatan TI dan OT, bersama dengan konektivitas nirkabel berkelanjutan, memberantas “celah udara” atau pemisahan fisik yang secara tradisional berfungsi sebagai benteng pertahanan untuk sistem OT di atas kapal konvensional (Svilicic et al., 2020). Kerentanan eksplisit dapat dilihat dalam beberapa komponen penting diantaranya.

1) Sistem Navigasi (GNSS & AIS): Sinyal Sistem Satelit Navigasi Global (GNSS) tetap tidak terenkripsi dan rentan terhadap gangguan (penghilangan sinyal) dan *spoofing* (pemalsuan sinyal), yang dapat mengakibatkan penyimpangan navigasi untuk kapal. Sistem Identifikasi Otomatis (AIS), yang dirancang untuk mencegah tabrakan, juga rentan terhadap manipulasi, yang dapat menimbulkan penciptaan “kapal hantu” atau mengaburkan posisi kapal yang sebenarnya (Balduzzi et al., 2014).

2) Sistem Kontrol (ECDIS & Autopilot): *Electronic Chart Display and Information Systems* (ECDIS) yang terinfeksi malware dapat menampilkan grafik navigasi yang salah, sementara infiltrasi yang tidak sah dari sistem autopilot dapat memberikan peretas kendali dan penguasaan penuh atas mekanisme kemudi kapal.

3) Jaringan Komunikasi: Hubungan komunikasi antara kapal dan Pusat Operasi Jarak Jauh melalui *Very Small Aperture Terminal* (VSAT) rentan terhadap intersepsi atau gangguan, yang dapat memutuskan

kontrol operator atau memfasilitasi serangan *man-in-the-middle*.

4) Rantai Pasokan Perangkat Lunak: Malware dapat secara diam-diam diintegrasikan ke dalam sistem kapal selama fase konstruksi, pembaruan, atau pemeliharaan oleh teknisi pihak ketiga, membuat serangan tersebut sangat sulit dideteksi (Kim et al., 2022).

b. Pengendalian operasi anti Penyelundupan Narkoba.

Beberapa kerentanan kritis dalam pengendalian operasi anti penyelundupan Narkoba yang dilakukan oleh TNI AL diantaranya adalah:

1) Komunikasi Terenkripsi: Kartel menggunakan enkripsi tingkat tinggi (Pretty Good Privacy - PGP dan jaringan Tor) yang mempersulit upaya penyadapan (Fox, 2016). Satuan tugas harus mengasumsikan bahwa semua komunikasi internal non-enkripsi dapat disadap.

2) Infiltrasi dan Rekayasa Sosial: Peretas yang didanai kartel akan secara aktif melakukan social engineering untuk menargetkan personel satuan tugas guna mendapatkan akses kredensial ke sistem sensitif.

c. Keterbatasan Peraturan Keamanan Maritim Saat Ini

Landasan kerangka peraturan keamanan maritim internasional yang ada, khususnya Kode Keamanan Fasilitas Kapal dan Pelabuhan Internasional (ISPS), secara intrinsik tidak memadai untuk mengatasi ancaman siber kontemporer, terutama yang ditujukan untuk sistem otonom. Hal ini mengingat ISPS Code dilembagakan setelah insiden teroris 11 September 2001, sehingga penekanan utamanya adalah mencegah akses fisik yang tidak sah ke kapal maritim dan fasilitas pelabuhan (IMO, 2002). Paradigma keamanannya didasarkan pada prinsip-prinsip “pagar, penjaga, dan gerbang,” sedangkan ancaman cyber memiliki kemampuan untuk menghindari pertahanan ini tanpa meninggalkan bukti fisik apa pun.

Sebagai contoh adalah upaya untuk mengintegrasikan manajemen risiko dunia maya dalam kerangka manajemen keselamatan yang ada saat ini masih belum memadai; MASS yang dibangun dengan berorientasi pada penyelesaian misi tertentu, wajib diperlengkapi kemampuan pertahanan terhadap ancaman siber yang berbeda, menjadi sangat penting, sehingga memberikan signifikansi yang kuat untuk keamanan siber dan keselamatan tradisional (Choi & Qi 2023). Selain itu, perjanjian internasional seperti Konvensi untuk Penindasan Tindakan Melawan Keselamatan Navigasi Maritim (Konvensi SUA) memerlukan

amandemen eksplisit untuk mengkriminalisasi serangan siber yang menargetkan kapal, hingga saat ini konsep dan penerapannya masih ambigu secara hukum (Choi & Qi, 2023). Meskipun Organisasi Maritim Internasional (IMO) telah mengumumkan "Pedoman Manajemen Risiko Siber Maritim" (MSC.428 (98)), pedoman ini bersifat rekomendasi dan tidak memiliki karakteristik kekuatan wajib dari Kode ISPS, yang mengakibatkan implementasi yang bervariasi dan seringkali tidak memadai (IMO, 2021b). Akibatnya, ada kekosongan peraturan yang berbahaya: Teknologi MASS telah berkembang pesat, sementara instrumen hukum yang dimaksudkan untuk mengaturnya telah tertinggal secara signifikan. Kesenjangan ini memerlukan perbaikan segera melalui pembentukan kerangka peraturan baru yang berkaitan dengan tantangan yang dihadirkan oleh abad ke-21.

Analisis.

Dengan memperhatikan uraian atas masing-masing kerentanan ini, ketika system autonomous maupun rentang kendali operasi dikuasai oleh peretas untuk eksploitasi, maka kerentanan ini akan memiliki potensi untuk bertindak sebagai katalis dalam konteks ancaman hibrida. Akibatnya, keamanan MASS tidak lagi dapat dipertimbangkan secara eksklusif dari sudut pandang keselamatan pelayaran; sebaliknya, situasi tersebut harus dipandang sebagai elemen integral dari kerangka keamanan siber-fisik yang berkaitan dengan infrastruktur maritim nasional.

Potensi OKN untuk mengeksploitasi MASS dan pengendalian operasi anti narkoba dalam skenario ancaman hibrida jauh melampaui pencurian data belaka; itu mencakup sabotase fisik yang ekstensif dan dikendalikan dari jarak jauh. Mengingat kapasitas untuk memanipulasi operasi fisik kapal secara digital, entitas jahat dapat mengubah aset komersial jutaan dolar menjadi senjata kinetik atau instrumen paksaan ekonomi. Analisis risiko yang efektif harus melampaui metodologi kualitatif konvensional dan merangkul pendekatan hibrida yang menggabungkan evaluasi kuantitatif probabilitas serangan dengan penilaian kualitatif dari konsekuensi strategis mereka (Yuzui & Kaneko, 2023). Beberapa Tindakan yang dapat dilakukan oleh OKN dalam mendanai operasi siber adalah:

a. Spionase Operasional: Meretas sistem digital satuan tugas Anda untuk mendapatkan rencana operasi, daftar informan, rincian aset, atau data pribadi personel, yang semuanya dapat digunakan untuk serangan fisik kepada personel, keluarga maupun institusi.

b. Gangguan Rantai Pasokan: Serangan terhadap sistem logistik

pelabuhan atau bandara (key logger di terminal peti kemas) untuk mengubah data pengiriman, memungkinkan kontainer berisi narkoba lolos dari inspeksi (Europol, n.d.).

c. Pencucian Uang Digital: Memanfaatkan peretas untuk membangun dan mengamankan infrastruktur pencucian uang menggunakan mata uang kripto dan layanan Deep Web yang sangat terenkripsi, yang merupakan salah satu aspek terpenting dari keberlanjutan OKN (Singh, 2007; UNODC, 2024).

Untuk dapat membayangkannya secara nyata, berikut ini adalah beberapa skenario ancaman spesifik mencontohkan potensi bahaya seperti pada penjelasan diatas:

a. Kapal "Senjata": Para peretas cyber merebut kendali kapal tanker gas alam cair (LNG) otonom melalui serangan spoofing GPS dan manipulasi ECDIS. Kapal kemudian diarahkan pada kecepatan maksimum dengan tujuan untuk ditabrakkan dengan terminal kontainer di pelabuhan strategis yang signifikan seperti Tanjung Priok. Konsekuensi berikutnya termasuk ledakan dahsyat, ketidakmampuan pelabuhan utama negara, gangguan rantai pasokan nasional yang berkepanjangan, dan kepanikan publik yang meluas. Atribusi serangan semacam itu sangat sulit untuk dapat diantisipasi mengingat waktu yang relative singkat; serangan semacam ini dapat saja dilakukan oleh kelompok teroris, maupun kelompok hacker yang didukung oleh negara atau kelompok tertentu.

b. "Blokade Chokepoint": Sebuah armada sederhana kapal kargo otonom yang berfungsi di dalam Selat Malaka mengalami kehilangan kendali jarak jauh secara simultan melalui serangan pada mekanisme propulsi mereka. Kapal-kapal yang diretas ini diarahkan untuk secara efektif menghalangi salah satu koridor maritim yang paling banyak diperdagangkan di dunia, misalnya di sekitar Selat Singapura pada bagian tersempitnya. Kejadian ini dapat disamarkan sebagai "kegagalan teknis massal," tentu saja akan berdampak langsung terhadap aktifitas pelayaran di selat tersibuk ini dan jika tidak segera diatasi akan memicu lonjakan harga minyak global. Kondisi ini akan berdampak buruk pada ekonomi negara-negara yang bergantung pada rute ini, dan menimbulkan kebingungan bagi pasukan angkatan laut regional dalam melakukan aksi tanggap yang tepat yang akan menghindari eskalasi.

c. Spionase "*Phantom Fleet*": Entitas yang disponsori negara menggunakan data Sistem Identifikasi Otomatis (AIS) yang dimanipulasi untuk membuat armada "kapal hantu" di sekitar zona pelatihan militer Angkatan Laut. Keberadaan kapal fiktif ini memaksa militer AL untuk

memodifikasi atau menunda latihan mereka, sementara kendaraan bawah laut otonom (AUV) yang sebenarnya, yang tidak memancarkan sinyal AIS, melakukan operasi pengumpulan intelijen tanpa deteksi.

Skenario ini menyiratkan bahwa pemodelan ancaman sistematis dan kerangka penilaian risiko yang divalidasi, seperti yang dianjurkan oleh Erbas et al. (2024), sangat penting untuk memahami dan mempersiapkan pertahanan terhadap ancaman yang berbeda secara kualitatif ini. Dengan tidak adanya pemahaman seperti itu, strategi defensif apa pun secara inheren akan reaktif dan tidak memadai.

Proposal Model Kerangka Kerja Peraturan Keamanan Siber untuk MASS

Untuk memperbaiki kekosongan peraturan yang berlaku, Indonesia harus mengambil inisiatif dalam merumuskan kerangka peraturan keamanan siber yang komprehensif dan adaptif untuk MASS yang didasarkan pada empat pilar penting. Kerangka kerja harus melampaui paradigma berorientasi kepatuhan yang kaku, beralih ke kerangka kerja berbasis risiko dan berorientasi pada tujuan yang memfasilitasi inovasi sambil secara bersamaan memastikan standar keamanan yang tinggi. Ini sejalan dengan rekomendasi untuk menerapkan kode MASS wajib dan diarahkan pada tujuan (Choi & Qi, 2023). Rincian model empat pilar yang diusulkan digambarkan sebagai berikut:

a. Pilar 1: Sertifikasi dan Standarisasi Teknologi (*Security-by-Design*): Keamanan harus dimasukkan sejak awal desain MASS, daripada diturunkan ke lapisan tambahan. Memperbaiki kerentanan dalam sistem yang sudah beroperasi menimbulkan biaya yang jauh lebih tinggi dan terbukti kurang efektif daripada membangunnya dengan pertimbangan keamanan sejak awal. Pemerintah, melalui lembaga yang ditunjuk (misalnya, BSSN bekerja sama dengan Biro Klasifikasi Indonesia), harus mengamanatkan sertifikasi keamanan siber untuk semua MASS yang diantisipasi beroperasi di perairan Indonesia. Sertifikasi ini harus didasarkan pada standar internasional yang disesuaikan untuk konteks maritim, seperti IEC 62443 untuk keamanan sistem kontrol industri. Produsen kapal dan penyedia sistem harus membuktikan bahwa mereka telah mengadopsi prinsip siklus hidup pengembangan yang aman dan melakukan pengujian penetrasi yang ketat sebelum kapal diizinkan untuk berlayar. Pilar ini menjamin bahwa hanya teknologi yang terbukti tangguh yang diintegrasikan ke dalam ekosistem maritim nasional, sehingga secara substansif mengurangi permukaan serangan sejak awal.

b. Pilar 2: Regulasi Operasional dan Kompetensi SDM:

Bahkan teknologi yang paling aman akan tetap rentan jika dioperasikan dengan tidak aman oleh personel. Kesalahan manusia, baik disengaja atau tidak disengaja, terus mewakili salah satu vektor utama untuk serangan siber. Regulasi harus menetapkan standar keamanan fisik dan siber yang ketat untuk Remote Operation Center (ROC). Selain itu, harus ada protokol manajemen insiden siber yang jelas dan wajib, termasuk kewajiban untuk melaporkan setiap insiden atau percobaan serangan kepada otoritas nasional (misalnya, Pusat Keamanan Siber Maritim Nasional). Yang terpenting, operator ROC harus menjalani program pelatihan dan sertifikasi kompetensi keamanan siber yang terstandardisasi, memastikan mereka mampu mendeteksi anomali dan merespons serangan secara efektif. Strategi pertahanan harus fokus pada deteksi dan klasifikasi serangan, didukung oleh enkripsi dan sistem deteksi intrusi (Tabish & Chaur-Luh, n.d.). Pilar ini memastikan bahwa interaksi manusia dengan teknologi otonom diperkuat, bukan menjadi titik terlemah dalam rantai keamanan.

c. Pilar 3: Kolaborasi dan Berbagi Informasi Ancaman:

Tidak ada satu entitas pun, baik pemerintah maupun swasta, yang dapat menghadapi ancaman siber maritim sendirian. Ancaman bersifat dinamis dan sering kali menargetkan banyak organisasi secara bersamaan, sehingga pertahanan kolektif melalui berbagi informasi adalah satu-satunya strategi yang efektif. Pemerintah harus memfasilitasi pembentukan *Maritime Information Sharing and Analysis Center* (Maritime ISAC) Indonesia. Forum ini akan menjadi platform tepercaya bagi perusahaan pelayaran, operator pelabuhan, penyedia teknologi, TNI AL, Bakamla, dan BSSN untuk berbagi indikator ancaman (*Indicators of Compromise*), taktik serangan, dan praktik pertahanan terbaik secara anonim dan real-time. Keberhasilan ISAC di sektor lain, seperti sektor keuangan (FS-ISAC), membuktikan efektivitas model ini. Pilar ini mengubah pertahanan siber dari serangkaian benteng yang terisolasi menjadi sebuah jaringan intelijen yang terdistribusi dan responsif.

d. Pilar 4: Penegakan Hukum dan Atribusi yang Jelas:

Tanpa konsekuensi hukum yang jelas, tidak akan ada efek jera (*deterrence*) yang efektif terhadap pelaku serangan siber maritim. Ambiguitas dalam hukum nasional dan internasional saat ini memungkinkan pelaku kejahatan siber untuk beroperasi dengan impunitas relatif. Indonesia perlu merevisi Kitab Undang-Undang Hukum Pidana (KUHP) dan Undang-Undang Pelayaran untuk secara eksplisit mengkriminalisasi tindakan seperti "pembajakan siber" atau sabotase kapal dari jarak jauh, sejalan dengan usulan

untuk memperbarui Konvensi SUA (Choi & Qi, 2023). Selain itu, TNI Angkatan Laut dan Bakamla harus diberi wewenang hukum dan kapasitas teknis (forensik digital) untuk melakukan investigasi insiden siber di laut dan mendukung proses atribusi serangan, bekerja sama dengan Interpol dan lembaga penegak hukum negara lain. Peran IMO dalam menyelaraskan kerangka kerja global sangat penting untuk memastikan pendekatan yang kohesif (Corsi et al., 2023). Pilar ini memastikan bahwa ada "gigi" hukum di balik kerangka peraturan, mengubahnya dari sekadar pedoman teknis menjadi instrumen kedaulatan negara.

Strategi Implementasi dan Peran TNI Angkatan Laut

Implementasi kerangka kerja empat pilar ini memerlukan pendekatan bertahap dan kepemimpinan yang kuat, di mana TNI Angkatan Laut memainkan peran sentral tidak hanya sebagai penegak hukum, tetapi juga sebagai akselerator kapabilitas nasional. [Reason] Sebagai garda terdepan pertahanan maritim dan salah satu pengguna utama teknologi canggih, TNI AL memiliki kepentingan strategis dan kapasitas organisasi untuk memimpin upaya ini. Peta jalan implementasi dapat dikategorikan menjadi tiga fase yang berbeda:

a. Tahap 1 (1-2 Tahun): Pembentukan Satuan Tugas Nasional Keamanan Siber Massa di bawah kepemimpinan Kemenko Marves, yang terdiri dari anggota dari TNI AL, Kemenhub, BSSN, Bakamla, Kementerian Perindustrian, dan pemangku kepentingan industri. Tujuan utamanya adalah untuk merumuskan rancangan Peraturan Pemerintah (PP) yang menganut kerangka empat pilar dan untuk memulai dialog internasional dalam kerangka IMO dan ASEAN.

b. Tahap 2 (3-5 Tahun): Pengembangan Kapasitas dan Proyek Percontohan. TNI AL, dalam kemitraan dengan lembaga akademik dan sektor pertahanan, mendirikan pusat keunggulan yang didedikasikan untuk keamanan siber maritim. Proyek percontohan untuk MASS diluncurkan pada rute domestik bersertifikat untuk mengevaluasi dan menyempurnakan peraturan operasional bersama protokol respons insiden. Versi awal platform ISAC Maritim juga dikembangkan.

c. Tahap 3 (5+ Tahun): Implementasi dan Penegakan Aturan Penuh. Persyaratan sertifikasi penuh akan dikenakan pada semua MASS yang baru beroperasi di Indonesia. TNI AL dan Bakamla akan melakukan patroli dan audit keamanan siber rutin. Indonesia akan secara aktif mengadvokasi standarnya untuk menjadi tolok ukur di kawasan dan berpotensi dalam skala global.

Dalam kerangka strategis ini, peran TNI AL melampaui tanggung jawab konvensionalnya. Tahapan-tahapan ini telah berkembang menjadi inkubator bakat, pusat penelitian dan pengembangan, dan koordinator sistem pertahanan fisik cyber nasional, yang pada akhirnya meningkatkan postur pertahanan negara dalam konteks perang hibrida kontemporer.

D. PENUTUP

Kemajuan dalam teknologi Maritime Autonomous Surface Ships (MASS) bukan hanya pilihan tetapi kesimpulan yang sudah pasti yang secara fundamental akan mengubah sektor maritim global. Namun demikian, terlepas dari potensi peningkatan efisiensi dan modernisasi, ada kerentanan keamanan yang signifikan. Ketergantungan MASS pada sistem digital yang rumit membuatnya sangat rentan terhadap skenario ancaman hibrida, di mana serangan cyber dapat digunakan untuk menimbulkan kerusakan fisik, menyebabkan kekacauan ekonomi, dan merusak kedaulatan negara.

Analisis ini telah menunjukkan bahwa kerangka peraturan maritim yang ada saat ini belum memadai untuk menghadapi tantangan yang telah dibahas. Akibatnya, model kerangka kerja peraturan keamanan siber yang komprehensif untuk Indonesia dapat didasarkan pada empat pilar: (1) standardisasi teknologi yang aman dari tahap desain; (2) peraturan operasional dan peningkatan kompetensi sumber daya manusia; (3) berbagi informasi ancaman kolaboratif di antara para pemangku kepentingan; dan (4) langkah-langkah penegakan hukum yang menciptakan efek jera. Pelaksanaan kerangka kerja ini bukan semata-mata kebutuhan teknis tetapi juga pada tataran strategis, yang bertujuan untuk memastikan bahwa Indonesia dapat memanfaatkan teknologi otonom tanpa membahayakan keamanan dan kedaulatannya sebagai Poros Maritim Dunia.

Lanskap ancaman cyber yang terus berkembang memerlukan peningkatan regulasi pertahanan dan kerangka kerja teknologi secara terus-menerus (Rajesh & Ramesh, 2023). Namun demikian, melalui strategi proaktif yang digambarkan dalam wacana ini, Indonesia memiliki potensi untuk memantapkan dirinya tidak hanya sebagai peserta reaktif, tetapi sebagai pelopor dalam kemajuan operasi maritim otonom yang aman dan tangguh. Mengingat kesimpulan yang disebutkan di atas, beberapa rekomendasi yang dapat ditindaklanjuti sebagai berikut:

a. Untuk Pemerintah (Kemenko Marves, Kemenhub, BSSN): Segera membentuk Satuan Tugas Nasional yang bertugas mengembangkan kebijakan dan peraturan keamanan siber MASS, yang bertujuan untuk menghasilkan Peraturan Pemerintah dalam dua tahun mendatang. Mengalokasikan sumber daya untuk

pengembangan kapasitas dan pembentukan ISAC Maritim.

b. Untuk Angkatan Laut: Secara formal memasukkan doktrin perang cyber-maritim ke dalam kurikulum pendidikan (misalnya, di Seskoal) dan selama latihan militer gabungan. Memimpin inisiatif untuk menciptakan pusat keunggulan keamanan siber maritim yang berfungsi sebagai fasilitas penelitian dan pengembangan, pengujian, dan pelatihan untuk personel militer dan sipil.

c. Untuk Sektor Maritim dan Lembaga Akademik: Melakukan investasi proaktif dalam penelitian dan pengembangan teknologi Kapal Permukaan Otonom Maritim (MASS) yang aman. Terlibat secara aktif dalam Satuan Tugas Nasional dan selanjutnya Pusat Berbagi Informasi dan Analisis Maritim (ISAC) untuk menjamin bahwa peraturan yang dirumuskan terkait dengan persyaratan industri dan dapat dilaksanakan secara efektif.

E. DAFTAR PUSTAKA

AFCEA International. (2025). Fueling Cartels' Cybercrime. SIGNAL Magazine.

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A security evaluation of the automatic identification system (AIS). Proceedings of the 29th Annual ACM Symposium on Applied Computing, 1-8.

Choi, Y., & Qi, J. (2023). A study on the establishment of a cyber risk management system for autonomous ships. Journal of Marine Science and Engineering, 11(3), 541.

Coker, C., Fruhlinger, J., & Maloof, M. (2017, August 28). GPS spoofing in the Black Sea: What really happened? GPS World.

Corsi, A., De, M., & Galiano, F. (2023). Cybersecurity for maritime autonomous surface ships (MASS): A comprehensive review. Journal of Marine Science and Engineering, 11(5), 999.

Darktrace. (2024). Uncovering CyberCartel Threats in Latin America. Darktrace Blog.

Erbas, B., Ceran, G., & Aydogdu, Y. (2024). A systematic threat analysis and risk assessment framework for maritime autonomous surface ships. Ocean Engineering, 291, 116532.

Europol. (n.d.). Hackers deployed to facilitate drugs smuggling. Cyberbits. Diakses dari [Situs Resmi Europol].

Fox, L. (2016). Communication Security Failures of the Sinaloa Cartel and the Silk Road: An Analysis of the Encryption Threat Facing the US Drug Enforcement Administration (Tesis Master, American Public University System). ResearchGate.

Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. Wired.

Hoffman, F. G. (2007). Conflict in the 21st century: The rise of hybrid wars. Potomac Institute for Policy Studies.

International Maritime Organization. (2002). International Ship and Port Facility Security (ISPS) Code. IMO Publishing.

International Maritime Organization. (2021a). Maritime Autonomous Surface Ships (MASS). IMO.org.

International Maritime Organization. (2021b). Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.2). IMO.org.

International Maritime Organization. (2023, May 26). Autonomous shipping (MASS) - IMO's work to ensure a safe, secure and green future. IMO.org.

Kim, T., Jeong, H., & Park, J. (2022). A study on cybersecurity threats and countermeasures for the software supply chain of autonomous ships. Applied Sciences, 12(19), 9987.

NATO. (2021). NATO's response to hybrid threats. NATO.int.

Pemerintah Indonesia. (2017). Peraturan Presiden No. 16 Tahun 2017 tentang Kebijakan Kelautan Indonesia.

Rajesh, R., & Ramesh, V. (2023). An integrated cyber-physical security framework for maritime autonomous surface ships. Cyber-Physical Systems, 9(4), 315-340.

Singh, D. (2007). Cyber Crime. S. K. Kataria & Sons. (Dikutip dalam Revista Internacional Consinter de Direito, 2016).

Svilicic, B., Kamilaris, A., & Vucic, M. (2020). A survey of cybersecurity in the maritime sector: Threats, vulnerabilities, and recommendations. Journal of Network and Computer Applications, 165, 102694.

Tabish, R., & Chaur-Luh, L. (n.d.). Cyber security challenges and countermeasures for maritime autonomous surface ships (MASS). [Preprint/Unpublished Manuscript].

United Nations Office on Drugs and Crime (UNODC). (2024). Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia.

Valencia, D. (2015). The Evolving Dynamics of Terrorism: The Terrorist-Criminal Nexus of Hezbollah and The Los Zetas Drug Cartel. UTEP.

Yuzui, T., & Kaneko, S. (2023). A hybrid risk analysis methodology for maritime autonomous surface ships (MASS). Safety Science, 168, 106295.