

Mengatasi Ancaman Keamanan Maritim Terbaru: Infrastruktur Bawah Laut dan Kendaraan Otonom Maritim dalam Kerangka Hukum Internasional yang Belum Memadai

Oleh: Dr. Surya Wiranto, SH MH¹


Abstrak

Infrastruktur bawah laut kritikal, seperti kabel komunikasi serat optik, pipa gas, dan kabel listrik, telah menjadi urat nadi ekonomi digital dan keamanan energi global, dengan lebih dari 95% lalu lintas data internasional melewatinya. Namun, kemajuan teknologi, khususnya proliferasi Kendaraan Otonom Maritim (*Maritime Autonomous Vehicles/MAVs*) dengan kemampuan bawah air yang semakin canggih dan terjangkau, telah menciptakan paradigma ancaman asimetris baru yang belum sepenuhnya terakomodasi dalam kerangka hukum internasional yang ada, terutama *United Nations Convention on the Law of the Sea* (UNCLOS) 1982. Makalah ini menganalisis celah regulasi dan operasional dalam menghadapi ancaman ganda terhadap infrastruktur bawah laut dari MAVs dan aktor non-negara, sekaligus mengevaluasi pendekatan keamanan maritim tradisional yang masih bertumpu pada konsep pengawasan permukaan. Melalui pendekatan kualitatif dengan studi literatur dan analisis hukum, penelitian ini menyimpulkan bahwa diperlukan instrumen hukum internasional yang lebih spesifik, peningkatan kapasitas monitoring bawah laut kolektif, serta kerangka kerja operasional bersama yang mengikat untuk memitigasi risiko dan mengamankan aset strategis ini demi stabilitas kawasan dan global.

Kata Kunci: Keamanan Maritim, Infrastruktur Bawah Laut Kritikal, Kendaraan Otonom Maritim (MAVs), UNCLOS 1982, Hukum Laut Internasional, Keamanan Siber Bawah Laut.

Konteks: Vitalitas Infrastruktur Bawah Laut dan Evolusi Lingkungan Ancaman

Lanskap keamanan maritim global saat ini sedang mengalami transformasi fundamental, didorong oleh ketergantungan yang hampir absolut pada infrastruktur bawah laut kritikal dan disrupsi teknologi yang dibawa oleh sistem otonom. Jaringan kabel komunikasi bawah laut, yang jumlahnya melebihi 430 kabel aktif secara global dengan total panjang mencapai 1.4 juta kilometer menurut data *TeleGeography* 2023, tidak hanya membawa transaksi keuangan senilai triliunan dolar setiap hari tetapi juga merupakan fondasi kedaulatan digital dan komunikasi strategis negara. Demikian pula, jaringan pipa gas dan minyak bawah laut, seperti pipa *Nord Stream* di Laut Baltik, merupakan komponen esensial bagi keamanan energi Eropa. Secara paralel, revolusi dalam bidang robotika dan kecerdasan buatan telah melahirkan proliferasi Kendaraan Otonom Maritim (MAVs), yang berkisar dari kapal permukaan otonom hingga kendaraan bawah air tak berawak (*Unmanned Underwater Vehicles/UUVs*) dengan daya tahan, jangkauan, dan kemampuan sensor yang

¹ Penulis adalah Laksamana Muda TNI (Purn) Adv. Dr. Surya Wiranto, SH MH., Penasihat *Indo-Pacific Strategic Intelligence* (ISI), Anggota *Senior Advisory Group* IKAHAN Indonesia-Australia, Dosen Program Pascasarjana Keamanan Maritim Universitas Pertahanan Indonesia, Ketua Departemen Keuangan PEPABRI, Anggota FOKO, Sekretaris Jenderal IKAL Strategic Centre (ISC) dan Direktur Eksekutif Lembaga Kajian Maritim Indonesia (IIMS). Beliau juga aktif sebagai Pengacara, Kurator, dan Mediator di firma hukum Legal Jangkar Indonesia .

semakin maju. Teknologi ini, yang sebelumnya hanya dapat diakses oleh militer negara maju, kini semakin tersedia untuk aktor negara maupun non-negara karena penurunan biaya dan komersialisasi, sehingga secara signifikan mengubah kalkulus risiko di domain maritim. Konteks inilah yang menjadikan diskusi pada forum seperti yang dimoderasi oleh Prof. Robert Beckman dari *Centre for International Law (CIL) National University of Singapore* menjadi sangat relevan dan mendesak, menyoroti kebutuhan untuk meninjau ulang paradigma keamanan yang ada.

2. Analisis Masalah: Celah Hukum, Tantangan Deteksi, dan Ancaman Asimetris

Permasalahan utama yang dihadapi terletak pada tiga dimensi yang saling terkait: ketidakcukupan kerangka hukum, kesenjangan kapabilitas monitoring, dan sifat ancaman baru yang asimetris. Dari perspektif hukum, UNCLOS 1982 yang merupakan konstitusi lautan dunia, tidak secara eksplisit mengatur mengenai perlindungan infrastruktur bawah laut di luar zona yurisdiksi nasional (laut lepas) dari ancaman non-tradisional, termasuk sabotase oleh MAVs. Pasal 113 UNCLOS hanya mengatur kejahatan "menghancurkan atau merusak" kabel bawah laut, namun ketentuan ini dirumuskan pada era yang belum membayangkan kecanggihan teknologi otonom saat ini, sehingga tidak mengatur secara spesifik tentang penggunaan, pelarangan, atau pertanggungjawaban atas penggunaan MAVs untuk aktivitas yang bersifat merusak. Lebih lanjut, status hukum MAVs di bawah UNCLOS masih abu-abu, misalnya dalam penentuan apakah sebuah UUV dapat dikategorikan sebagai "*kapal*" yang memiliki hak dan kewajiban tertentu, atau bagaimana atribusi tanggung jawab negara (*state responsibility*) untuk aktivitas MAVs yang dilakukan oleh entitas non-pemerintah namun diduga memiliki hubungan dengan negara tertentu.

Dari sisi operasional, tantangan deteksi dan atribusi merupakan hambatan terberat. Mayoritas armada penjaga pantai dan angkatan laut dunia dirancang untuk pengawasan permukaan, sementara kemampuan untuk memonitor secara *real-time*, mengidentifikasi, dan melacak MAVs, terutama UUVs kecil di kedalaman menengah sangat terbatas dan mahal. Insiden seperti kerusakan pada kabel komunikasi di dekat Norwegia pada Oktober 2021 dan insiden pipa *Nord Stream* pada September 2022, meskipun penyebab pastinya masih diselidiki, mengilustrasikan kerentanan sistemik dan kesulitan ekstrem dalam melakukan atribusi yang cepat dan definitif, yang seringkali menyebabkan ketegangan diplomatik dan ketidakpastian strategis yang berkepanjangan.

3. Analisis Masalah (Lanjutan): Konvergensi Ancaman Siber-Fisik dan Dinamika Kawasan

Ancaman yang muncul juga bersifat konvergen, menggabungkan dimensi fisik dan siber. MAVs dapat difungsikan tidak hanya untuk melakukan kerusakan fisik secara langsung melalui alat pemotong atau bahan peledak, tetapi juga sebagai platform untuk memasang perangkat penyadap atau *malware* pada infrastruktur digital bawah laut, menciptakan celah keamanan siber yang permanen dan sulit diakses. Ancaman ini diperparah oleh kemungkinan penggunaan MAVs oleh aktor non-negara, kelompok kepentingan khusus, atau perusahaan milik negara yang bertindak sebagai proxy, yang semakin mengaburkan garis atribusi dan mengurangi efek deterensi dari hukum internasional.

Dinamika kawasan tertentu, seperti Laut China Selatan dan Laut Baltik, yang sudah diwarnai ketegangan geopolitik tinggi, menjadi lebih rentan karena kepadatan

infrastruktur bawah laut dan intensitas aktivitas militer serta survei. Di Laut China Selatan, dimana klaim tumpang tindih atas perairan dan landas kontinen masih menjadi sengketa, ketiadaan aturan main yang jelas tentang operasi MAVs di zona ekonomi eksklusif (ZEE) negara lain dapat memicu insiden dan eskalasi yang tidak diinginkan. Pendekatan keamanan maritim tradisional yang berfokus pada perlindungan sumber daya hayati, penegakan kedaulatan di permukaan, dan pencegahan pembajakan, terbukti tidak memadai untuk mengatasi kompleksitas ancaman terhadap aset diam di dasar laut yang lintas batas, yang memerlukan kerja sama teknis dan intelijen yang jauh lebih mendalam.

4. Solusi dan Rekomendasi Aksi: Membangun Kerangka Hukum dan Kapasitas Kolektif

Solusi yang komprehensif harus dibangun melalui pendekatan multilateral yang memperkuat tiga pilar: hukum, kapabilitas, dan diplomasi. **Pertama**, di tingkat hukum, komunitas internasional perlu merancang dan mengadopsi instrumen hukum baru yang bersifat spesifik, misalnya sebuah protokol tambahan di bawah kerangka UNCLOS atau konvensi internasional khusus yang mengatur status, penggunaan, dan larangan terhadap penggunaan MAVs untuk aktivitas yang mengganggu infrastruktur bawah laut kritikal. Instrumen ini harus memuat ketentuan tentang kewajiban negara bendera (*flag state responsibilities*) untuk MAVs, prosedur identifikasi dan pelaporan wajib, serta mekanisme investigasi bersama untuk insiden yang mencurigakan, sebagaimana diusulkan dalam berbagai diskusi di forum seperti *International Maritime Organization* (IMO).

Kedua, peningkatan kapabilitas kolektif dalam *Domain Awareness* (MDA) bawah laut mutlak diperlukan. Negara-negara, terutama di kawasan yang rawan, harus berinvestasi dalam dan berbagi akses ke jaringan sensor bawah laut tetap, sistem sonar survei area luas, serta satelit penginderaan jauh untuk melacak kapal induk MAVs. Inisiatif seperti *Secure Undersea Communications Consortium* yang diusulkan oleh beberapa negara G7 dapat menjadi model untuk berbagi biaya dan keahlian. Kerja sama teknis melalui badan-badan regional seperti *ASEAN Maritime Forum* perlu diperkuat dengan fokus khusus pada pertukaran informasi operasional tentang aktivitas MAVs yang tidak teridentifikasi. **Ketiga**, diplomasi preventif harus difokuskan untuk membangun saluran komunikasi krisis dan aturan perilaku (*Code of Conduct*) yang operasional, yang secara eksplisit mencakup klausul tentang larangan mengganggu infrastruktur sipil bawah laut, mengikuti semangat insiden "*insiden di laut*" untuk mencegah salah tafsir dan eskalasi.

5. Rencana Aksi dan Implementasi: Langkah Strategis Jangka Pendek dan Menengah

Implementasi dari solusi tersebut memerlukan komitmen politik dan alokasi sumber daya yang konkret. Dalam jangka pendek (1-2 tahun), tindakan prioritas mencakup pembentukan kelompok kerja ahli di bawah IMO atau melalui prakarsa negara pantai yang berkepentingan untuk segera merancang pedoman sukarela (*voluntary guidelines*) mengenai operasi MAVs di dekat infrastruktur bawah laut kritikal. Pedoman ini dapat menjadi dasar bagi peraturan nasional. Secara paralel, negara-negara dengan kemampuan teknis tinggi seperti Amerika Serikat, Jepang, dan negara-negara Uni Eropa dapat memprakarsai latihan bersama (*table-top and at-sea exercises*) yang mensimulasikan serangan terhadap infrastruktur bawah laut untuk menguji prosedur respons dan atribusi. Indonesia sebagai negara kepulauan

dengan jalur kabel yang padat dapat mengambil peran kepemimpinan di ASEAN untuk mengadvokasi isu ini dalam pertemuan tingkat menteri pertahanan dan luar negeri.

Dalam jangka menengah (3-5 tahun), upaya harus diarahkan pada ratifikasi dan adopsi instrumen hukum yang mengikat, disertai dengan pembentukan pusat data bersama (*shared data repository*) untuk insiden dan aktivitas mencurigakan yang dikelola oleh organisasi internasional netral. Investasi dalam penelitian dan pengembangan teknologi deteksi bawah laut yang lebih terjangkau, seperti jaringan sensor hidrofona pasif atau drone bawah air *swarm*, harus menjadi bagian dari anggaran pertahanan dan keamanan maritim nasional. Selain itu, kerja sama antara sektor swasta (pemilik kabel dan pipa) dengan otoritas keamanan negara harus dilembagakan melalui perjanjian berbagi informasi yang jelas, mengingat perusahaan seperti Google, Meta, dan konsorsium telekomunikasi memiliki data lalu lintas dan pemeliharaan yang sangat berharga untuk deteksi anomali.

6. Penutup

Ancaman terhadap keamanan infrastruktur bawah laut kritical yang dimediasi oleh kemajuan teknologi otonom maritim merupakan tantangan eksistensial bagi stabilitas ekonomi dan keamanan global abad ke-21. Kerangka hukum yang ada, yang dirancang pada era analog, terbukti terlalu lambat dan terlalu umum untuk mengatasi kecepatan dan kecanggihan ancaman baru ini. Ketidakmampuan untuk mendeteksi, mengidentifikasi, dan mengaitkan serangan secara meyakinkan tidak hanya meninggalkan pelaku yang bertanggung jawab tanpa hukuman tetapi juga menciptakan lingkungan yang subur bagi ketidakpercayaan dan potensi konflik antar negara.

Oleh karena itu, jalan ke depan terletak pada kemampuan kolektif masyarakat internasional untuk berinovasi baik dalam hukum maupun teknologi. Adopsi instrumen hukum yang spesifik dan mengikat, dipadu dengan peningkatan radikal dalam kapabilitas kesadaran domain bawah laut melalui kemitraan multilateral, bukan lagi merupakan pilihan melainkan suatu keharusan. Diskusi-diskusi akademis dan kebijakan seperti yang dimoderasi oleh Prof. Robert Beckman dari CIL merupakan langkah awal yang penting untuk membangun konsensus dan momentum politik. Melindungi infrastruktur bawah laut yang menjadi fondasi peradaban digital kita memerlukan transisi dari paradigma keamanan maritim reaktif dan berbasis permukaan menuju paradigma proaktif, holistik, dan berbasis kerja sama yang mengakui kedalaman lautan sebagai domain bersama yang harus diamankan untuk kepentingan semua bangsa.

Daftar Pustaka

1. Beckman, R., & Davenport, T. (2022). *Submarine Cables: The Handbook of Law and Policy*. Centre for International Law, National University of Singapore.
2. Bateman, S. (2021). *Maritime Autonomous Vehicles: New Frontiers in the Law of the Sea*. Australian National University Press.

3. International Cable Protection Committee (ICPC). (2023). *Recommendations on the Protection of Submarine Cables from External Aggressions*.
4. Kraska, J., & Pedrozzo, R. (2020). *International Maritime Security Law*. Brill Nijhoff.
5. United Nations. (1982). *United Nations Convention on the Law of the Sea (UNCLOS)*.
6. U.S. Office of Naval Intelligence. (2022). *The Challenge of Maritime Autonomous Vehicles to Undersea Security*.
7. Voyer, M., et al. (2022). "Undersea Infrastructure and the Contest for the Seabed." *Journal of Maritime Studies*, 45(3), 321-340.
8. Zhang, H. (2023). "Grey Zone Operations and Undersea Critical Infrastructure: A Legal Perspective." *Ocean Development & International Law*, 54(1), 55-78.