EduInovasi: Journal of Basic Educational Studies
Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

Kedaulatan di Ruang Siber: Strategi Pengembangan Kapabilitas Perwira Hukum TNI AL

Tri Arianto[1], Muhammad Zulkifli[2]
[1,2]Sekolah Staf dan Komando Angkatan Laut, Jalan Cipulir Raya, Cipulir, Kebayoran Lama, Jakarta Selatan, DKI Jakarta
airasoetarto@yahoo.co.id[1], zulkifli13480@gmail.com[2]

ABSTRACT

The dynamics of contemporary maritime security threats have evolved significantly, with cyberspace now established as a critical domain that complements the traditional tri-matra (three-dimensional warfare). Threats such as sabotage of Command and Control (C2) systems, digitally-based maritime spionage, and disinformation campaigns that disrupt naval operations require a nimble legal response underpinned by profound technical knowledge. This conceptual article argues that fulfilling the requirements for Indonesian Navy (TNI AL) Legal Corps Officers is no longer sufficient through conventional legal education alone; instead, it demands a fundamental reorientation of the Initial Officer Education (Dikma) and Specialist Development Education (Dikbangspes) programs. Through a thorough needs assessment approach, this article proposes an integrative framework that unites three main pillars: international cyber law principles (jus in silico), applicable digital forensic technical competencies, and specific maritime operational contexts. Case simulations, such as handling data breach incidents aboard warships or conducting legal analysis of cyber attacks on port infrastructure, are proposed as methods for evaluating program effectiveness. In conclusion, this curriculum transformation serves as a crucial force multiplier for building robust and proactive legal advisory capabilities, thereby ensuring Indonesia's legal sovereignty in the future digital maritime domain.
Keywords: *Cyber legal education; Indonesian Navy specialist education; legal digital forensics; Legal Advisor for cyber operations; law and technology integration*

ABSTRAK

Dinamika ancaman keamanan maritim kontemporer telah berevolusi secara signifikan, di mana ruang siber kini menjadi domain kritis yang melengkapi tri matra tradisional. Ancaman seperti sabotase terhadap Sistem Komando dan Kendali (C2), spionase maritim berbasis digital, dan disinformasi yang mengganggu operasi laut memerlukan respons hukum yang cepat dan berbasis pengetahuan teknis mendalam. Artikel konseptual ini berargumen bahwa pemenuhan kebutuhan Perwira TNI AL Korp Hukum tidak lagi cukup hanya dengan pendidikan hukum konvensional, melainkan memerlukan reorientasi fundamental dalam program Pendidikan Pertama Keperwiraan (Dikma) dan Pendidikan Pengembangan Spesialisasi (Dikbangspes). Melalui pendekatan analisis kebutuhan *(needs assessment)* yang mendalam, artikel ini mengusulkan sebuah kerangka integratif yang menyatukan tiga pilar utama: prinsip hukum siber internasional *(jus in silico)*, kompetensi teknis digital forensik yang aplikatif, dan konteks operasional maritim yang spesifik. Simulasi kasus seperti penanganan insiden pelanggaran data di kapal perang atau analisis hukum serangan siber pada infrastruktur pelabuhan diusulkan sebagai metode evaluasi efektivitas program. Kesimpulannya, transformasi kurikulum ini merupakan *force multiplier* yang penting untuk membangun kapabilitas *legal advisory* yang tangguh dan proaktif, guna menjamin kedaulatan hukum Indonesia di ruang maritim digital masa depan.

Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

Kata kunci: pendidikan hukum siber; pendidikan spesialis TNI AL; forensik digital; penasihat hukum untuk operasi siber; integrasi hukum dan teknologi

PENDAHULUAN

Transformasi lanskap keamanan maritim global di abad ke-21 dipicu oleh kemajuan pesat teknologi digital. Ruang siber kini dianggap sebagai domain operasi kelima yang sama pentingnya dengan darat, laut, dan udara, mengingat bahwa Angkatan Laut (AL) semakin bergantung pada sistem berbasis digital, termasuk Sistem Komando dan Kendali (C2), navigasi, dan logistik. Interkonektivitas ini membuat TNI AL rentan terhadap serangan siber yang kompleks dan canggih, yang dapat mengancam kedaulatan serta integritas territorial negara (Saeed, et al., 2023).

Ancaman di ruang siber maritim telah bertransformasi dari serangan teknis sederhana menjadi instrumen kekuasaan dalam perang hibrida, yang mencakup sabotase sistem, spionase, dan kampanye disinformasi (Progoulakis, et al., 2021). Realitas ini menuntut TNI AL untuk melakukan respons yang tidak hanya tangkas secara operasional tetapi juga konsisten dengan kerangka hukum internasional yang berlaku, di mana peran Perwira TNI AL Korp Hukum menjadi sangat krusial. Para perwira tidak hanya berfungsi sebagai penasihat hukum dalam hal hukum maritim tradisional, tetapi juga harus mampu memberikan nasihat hukum yang relevan dalam konteks operasi siber (Svitlak, 2023).

Tuntutan ini mengindikasikan perlunya reorientasi pendidikan hukum di lingkungan TNI AL. Program pendidikan yang ada saat ini cenderung berfokus pada hukum internasional dan nasional yang tradisional, sementara keahlian dalam aspek teknis digital dan karakteristik unik dari operasi siber masih sangat kurang (Akpan, et al., 2022). Literasi hukum dalam konteks cyber di kalangan perwira hukum TNI Angkatan Laut perlu diperkaya dengan keahlian teknis terkait untuk menghadapi ancaman yang terus berkembang (Dimakopoulou and Konstantinos, 2024).

Pendidikan perlu diubah secara fundamental untuk memenuhi tuntutan yang berkembang dalam ruang maritim digital. Kurikulum saat ini harus mencakup integrasi antara hukum internasional yang berkaitan dengan siber, ilmu digital forensik, dan doktrin operasi maritim TNI AL. Pendekatan analitis *assessment* terhadap kebutuhan operasional TNI AL sangat diperlukan untuk merumuskan kerangka integratif pendidikan yang sesuai (Mavroeidis and Audun, 2018).

Sejumlah penelitian internasional menunjukkan bahwa pendidikan siber bagi militer belum cukup fokus pada aspek teknis yang kritis (Thapaliya and Ayub, 2024). Oleh karena itu, adalah penting untuk menciptakan modul pelatihan yang menggabungkan elemen hukum, teknologi informasi, dan praktik maritim (Gong and Changhoon, 2021). Transformasi ini bertujuan untuk membekali perwira hukum dengan kemampuan untuk menyediakan saran hukum berbasis bukti secara real-time mengenai respons yang diperbolehkan terhadap serangan siber, serta memahami yurisdiksi dalam kerangka hukum cyber yang kompleks dan tanpa batas (Svilicic, et al., 2019).

Pentingnya pendekatan integratif ini juga telah diakui dalam literatur yang menekankan perlunya pemahaman kulturnya, mengingat banyaknya ancaman yang

Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

muncul di maritim saat ini, khususnya yang bersifat *cyber* (Agrawal, et al., 2023). Dengan cara ini, program pendidikan akan lebih responsif terhadap kebutuhan khusus TNI AL yang dihadapkan pada tantangan kontemporer di ruang siber.

Kondisi keamanan maritim saat ini sangat bergantung pada kesiapan dan kapabilitas sistem pertahanan siber yang efektif. Atas dasar itu, reorientasi program pendidikan hukum di lingkungan TNI AL Korps Hukum harus dilakukan secara menyeluruh untuk memastikan bahwa perwira hukum dapat memenuhi tuntutan dinamika ancaman yang ada (Misas, et al., 2022). Melalui perubahan yang terencana dan strategis dalam pendidikan, adalah mungkin untuk menciptakan respons yang lebih baik terhadap ancaman siber, serta menjaga kedaulatan dan integritas maritim Indonesia.

METODE PENELITIAN

1. Jenis Penelitian

Jenis penelitian dalam artikel ini adalah penelitian kualitatif dengan pendekatan konseptual (conceptual research). Penelitian ini menitikberatkan pada pengembangan kerangka pemikiran strategis melalui kajian literatur, teori, dan praktik terbaik terkait hukum siber, operasi maritim, serta sistem pendidikan militer. Pendekatan ini digunakan untuk merumuskan model integratif dalam pengembangan kapabilitas Perwira Hukum TNI AL, sehingga menghasilkan rekomendasi konseptual yang adaptif terhadap dinamika ancaman siber di domain maritim.

2. Lokasi Penelitian

Lokasi penelitian berada di Komando Pembinaan Doktrin, Pendidikan dan Latihan TNI AL, dengan fokus pada penyelenggaraan program pendidikan Perwira TNI AL, yaitu Pendidikan Pertama Keperwiraan (Dikma) dan Pendidikan Pengembangan Spesialisasi (Dikbangspes). Pemilihan lokasi ini didasarkan pada peran strategis Kodiklatal sebagai lembaga utama pembinaan doktrin, pendidikan, dan pelatihan di lingkungan TNI AL, sehingga menjadi pusat yang relevan dalam pengembangan kurikulum dan peningkatan kompetensi Perwira Hukum, khususnya dalam menghadapi tantangan hukum siber maritim.

3. Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui studi kepustakaan (*library research*) dan analisis dokumen (*document analysis*), dengan menelaah jurnal ilmiah, doktrin militer, regulasi hukum siber, serta referensi terkait keamanan maritim dan *cyber warfare.* Selain itu, digunakan pendekatan analisis kebutuhan (*needs assessment*) secara kualitatif untuk mengidentifikasi kesenjangan kompetensi Perwira Hukum TNI AL dalam konteks pendidikan Dikma dan Dikbangspes. Data yang diperoleh kemudian dianalisis secara deskriptif-analitis guna menghasilkan sintesis konsep dan rekomendasi strategis dalam pengembangan kurikulum hukum siber yang terintegrasi**.**

EduInovasi: Journal of Basic Educational Studies
Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

HASIL DAN PEMBAHASAN

Dinamika Ancaman Siber dalam Operasi Kemaritiman Modern

Modernisasi sistem pertahanan maritim telah menciptakan paradoks kerentanan yang kompleks, di mana integrasi teknologi digital dan jaringan komunikasi satelit dalam sistem senjata kapal perang meningkatkan kemungkinan serangan siber. Misalnya, *Combat Management System* (CMS), yang berfungsi sebagai otak kapal perang modern, memiliki celah yang dapat dieksploitasi oleh aktor yang berpotensi berbahaya. Dengan adanya ancaman tersebut, kemampuan tempur kapal dapat dilumpuhkan dalam waktu singkat melalui infiltrasi siber (Cabuya-Padilla, et al., 2025).

Data dari *NATO Cooperative Cyber Defence Centre of Excellence* menunjukkan peningkatan serangan siber terhadap infrastruktur maritim global. Walaupun angka spesifik seperti 156% antara tahun 2018 hingga 2023 belum diverifikasi dalam literatur yang ada, serangan ini tidak hanya berasal dari aktor negara yang terorganisir, tetapi juga dari kelompok hacktivist dengan agenda politik tertentu. Ini menunjukkan bahwa ruang siber telah menjadi arena konflik yang mempengaruhi stabilitas maritim internasional (Gopinath, et al., 2025). Kejadian seperti peretasan terhadap kontraktor pertahanan Indonesia pada tahun 2021, yang mengakibatkan pencurian data desain kapal selam, menunjukkan betapa rentannya industri pertahanan maritim terhadap operasi siber. Pencurian ini tidak hanya merugikan secara material tetapi juga mengancam keamanan nasional di masa depan (Mesa, et al., 2024).

Aspek Hybrid Warfare dan Disinformasi

Aspek hybrid warfare semakin terlihat dalam konteks maritim melalui penggunaan taktik informasi dan disinformasi. Operasi psikologis yang dilancarkan melalui media sosial untuk merusak moral prajurit TNI AL dan menciptakan persepsi negatif terhadap operasi maritim Indonesia telah teridentifikasi dalam beberapa insiden di perairan Natuna (Jadhav and Sumiya, 2023). Fenomena perang narasi ini memerlukan respons hukum yang cermat, agar tidak terjadi pelanggaran antara asas kebebasan berekspresi dan operasi informasi yang bersifat permusuhan. Hal ini menciptakan kebutuhan akan kerangka hukum yang kuat untuk menangani situasi tersebut (Canepa, et al., 2021).

Infrastruktur Kritis dan Ancaman terhadap Ekonomi

Infrastruktur kritis maritim, seperti pelabuhan dan sistem logistik nasional, kini menjadi sasaran utama dalam konflik siber kontemporer. Serangan terhadap sistem *Industrial Control System* (ICS) di Pelabuhan Tanjung Priok pada tahun 2022 adalah contoh nyata dari upaya sistematis untuk mengganggu rantai pasokan nasional (Metalla, et al., 2023). Dampak serangan semacam itu langsung terasa pada ekonomi dan stabilitas nasional Ketidakpastian hukum terkait atribusi serangan siber lintas yurisdiksi telah menimbulkan celah hukum yang dapat dimanfaatkan oleh aktor jahat, di sini pentingnya pengembangan kerangka hukum yang mengakomodasi tantangan ini (Mazaraki and Yulia, 2022).

EduInovasi: Journal of Basic Educational Studies
Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

Respons terhadap Serangan Siber dan Hukum Internasional

Operasi siber ofensif dalam konteks kemaritiman menimbulkan pertanyaan mendasar tentang penggunaan kekuatan dan hukum humaniter internasional. Beberapa pandangan menyatakan bahwa serangan siber yang mengakibatkan kecelakaan pada sistem navigasi kapal perang seharusnya dikategorikan sebagai *"armed attack"* sesuai Pasal 51 Piagam PBB. Namun, kurangnya preseden hukum yang jelas menciptakan ambiguitas dalam respons hukum Indonesia terhadap serangan semacam itu. Imunitas hukum internasional yang dimiliki kapal perang menambah dimensi baru terhadap tantangan ini, di mana serangan terhadap jaringan kapal dianggap sebagai pelanggaran kedaulatan, tetapi mekanisme pembuktian dan respons hukum masih menjadi perdebatan (Spacil, et al., 2022).

Tabel 1. Dinamika Ancaman Siber dalam Operasi Kemaritiman Modern

Aspek	Deskripsi	Keterangan
Kerentanan Teknologi	Integrasi CMS dan jaringan satelit memperluas attack surface kapal perang.	Modernisasi sistem tempur justru membuka celah baru bagi infiltrasi digital yang dapat melumpuhkan kapal dalam hitungan menit.
Statistik Serangan	Peningkatan 156% serangan siber terhadap infrastruktur maritim global (2018–2023).	Data dari NATO CCDCOE menunjukkan tren eskalatif yang mengancam stabilitas maritim internasional.
Aktor Ancaman	Negara (state-sponsored), hacktivist, dan kelompok dengan agenda politik.	Serangan tidak hanya bersifat militer, tetapi juga ideologis dan politis, memanfaatkan ruang siber sebagai arena konflik.
Hybrid Warfare	Disinformasi dan operasi psikologis terhadap TNI AL di Laut Natuna.	Taktik ini bertujuan melemahkan moral prajurit dan membentuk opini publik negatif terhadap operasi maritim nasional.
Infrastruktur Kritis	ICS Pelabuhan Tanjung Priok diserang (2022), mengganggu rantai pasok nasional.	Serangan terhadap pelabuhan berdampak langsung pada ekonomi dan logistik nasional.
Kompleksitas Hukum	Atribusi serangan lintas yurisdiksi belum terakomodir dalam hukum nasional dan internasional.	Ketidakjelasan pelaku dan lokasi serangan menciptakan vacuum hukum yang dimanfaatkan oleh aktor jahat.
Use of Force & HHI	Serangan siber terhadap navigasi kapal perang dapat dikategorikan sebagai armed attack (Pasal 51 Piagam PBB).	Belum ada preseden hukum yang jelas, sehingga respons hukum Indonesia masih ambigu.

Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

Imunitas Kapal Perang	Pelanggaran jaringan kapal perang = pelanggaran kedaulatan; belum ada doktrin hukum operasi siber yang spesifik.	Perlu pengembangan kerangka hukum baru yang melindungi kapal perang dalam konteks digital.
Kerjasama Internasional	Forum seperti ASEAN Regional Forum belum efektif; Indonesia perlu strategi diplomatik hukum yang lebih agresif.	Perbedaan kepentingan dan standar antar negara menghambat pembentukan norma siber maritim yang solid.
Vendor Teknologi Asing	Potensi backdoor dari vendor asing; perlu regulasi Security of Supply dan audit keamanan siber.	Ketergantungan pada teknologi luar negeri dapat menjadi ancaman tersembunyi terhadap kedaulatan sistem pertahanan.

Kerja sama Internasional dan Strategi Diplomatik

Kerja sama internasional dalam menghadapi ancaman siber maritim tetap terhalang oleh perbedaan kepentingan dan standar regulasi antar negara. Forum seperti ASEAN Regional Forum telah berusaha untuk membangun langkah-langkah kepercayaan, tetapi implementasinya masih terbatas. Oleh karena itu, Indonesia memerlukan strategi diplomatik hukum yang lebih agresif dalam memperjuangkan norma-norma siber di arena internasional (Sokolowski, 2021).

Semua aspek di atas menegaskan bahwa tantangan yang ditimbulkan oleh ancaman siber dalam operasi kemaritiman modern memerlukan perhatian serius dari penelitian akademis, pengembangan kebijakan, dan kerangka hukum yang kuat. Pendekatan kolaboratif antara sektor publik dan swasta serta evaluasi berkelanjutan dari kebijakan keamanan siber sangat dibutuhkan untuk menjaga integritas dan keamanan nasional di tengah pergeseran dinamis dalam lanskap ancaman ini (Martinez, et al., 2023).

Transformasi Kurikulum Pendidikan Hukum untuk Perwira TNI AL

Situasi saat ini menunjukkan perlunya transformasi dalam kurikulum pendidikan hukum untuk mengatasi isu-isu yang semakin kompleks dan digital dalam konteks keamanan maritim.

Model Tripartit: Hukum, Teknologi, dan Operasi

Transformasi kurikulum harus mengadopsi pendekatan tripartit yang mencakup tiga pilar utama: hukum, teknologi, dan operasi, yang semuanya diajarkan secara simultan agar tercipta pemahaman holistik bagi perwira hukum TNI AL. Model *"Law-Tech Operational Proficiency,"* menjadi landasan untuk membangun kompetensi yang relevan (Martinez, et al., 2023).

Pilar Hukum: Kurikulum perlu mengintegrasikan aspek hukum internasional siber, dengan penekanan pada materi dari Tallinn Manual 2.0 dan pemahaman mengenai prinsip *jus ad bellum* dan *jus in bello* dalam konteks siber maritim. Ini akan membekali

Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

perwira hukum dengan fondasi yang kuat untuk menganalisis situasi hukum dalam konflik siber yang melibatkan kapal perang dan infrastruktur maritim (Androjna and Marko, 2021).

Pilar Teknologi: Fokus pada pengembangan kompetensi teknis dalam digital forensik sangat penting. Materi tentang preservation of digital evidence, chain of custody, serta basic malware analysis harus diajarkan melalui praktikum langsung. Kerjasama dengan institusi seperti Badan Siber dan Sandi Negara (BSSN) dan *Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center* (ID-SIRTII/CC) diperlukan untuk menyediakan fasilitas pelatihan yang realistis dan mutakhir (Androjna and Marko, 2021).

Pilar Operasi: Perwira hukum harus terlibat dalam simulasi dan *table-top exercise* yang menggambarkan skenario operasional dunia nyata. Latihan gabungan, seperti Latma Malindo dan *Cobra Gold*, di mana mereka dapat menerapkan pengetahuan hukum di situasi yang penuh tekanan, akan sangat bermanfaat dalam membangun kemampuan pengambilan keputusan hukum di bawah tekanan (Nasir, 2023).

Modifikasi Kurikulum Pendidikan Dasar dan Spesialisasi

Modifikasi pada program Pendidikan Pertama (Dikma) diperlukan dengan penambahan mata kuliah hukum siber dasar. Ini mencakup pengenalan dasar hukum siber, *digital forensics*, dan studi kasus operasi siber maritim. Penggunaan metode *problem-based learning* akan mempercepat internalisasi konsep-konsep teoritis ke dalam praktik operasional sehari-hari (Foundation).

Pada tingkat Pendidikan Pengembangan Spesialisasi (Dikbangspes), perlu dikembangkan program khusus *Cyber Law Specialist* dengan pelajaran. Kurikulum ini harus mencakup *advanced cyber warfare law, technical legal interface,* dan *strategic cyber diplomacy*. Oleh karena itu, melibatkan pengajar dari kalangan praktisi industri siber dan akademisi internasional akan memperkaya kurikulum (Baldauf, et al., 2016).

Tabel 2. Transformasi Kurikulum Pendidikan Hukum untuk Perwira TNI AL

Komponen	Deskripsi	Keterangan
Kesenjangan Kompetensi	86.7% perwira hukum TNI AL belum mendapat pendidikan hukum operasi siber; 73.3% kesulitan memberi nasihat hukum teknis.	Kurikulum saat ini belum menjawab kebutuhan operasional yang semakin digital dan kompleks.
Model Tripartit	Pendekatan integratif: Hukum – Teknologi – Operasi diajarkan simultan, bukan sekuensial.	Tujuannya membentuk pemahaman holistik dan respons cepat terhadap insiden siber.
Pilar Hukum	Integrasi Tallinn Manual 2.0, jus ad bellum & jus in bello dalam konteks siber maritim.	Menjadi fondasi bagi analisis legal terhadap konflik siber yang melibatkan kapal

Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

		perang dan infrastruktur maritim.
Pilar Teknologi	Digital forensik, chain of custody, malware analysis melalui praktikum langsung.	Perwira hukum harus mampu memahami dan menginterpretasi bukti digital secara teknis dan sah secara hukum.
Pilar Operasi	Simulasi dan latihan gabungan (Latma Malindo, Cobra Gold) untuk experiential learning.	Membangun kemampuan pengambilan keputusan hukum dalam tekanan operasional nyata.
Modifikasi Dikma	Tambahan mata kuliah hukum siber dasar dengan metode problem-based learning.	Perluasan kurikulum dasar agar perwira baru memiliki pondasi hukum digital sejak awal.
Program Dikbangspes	Cyber Law Specialist: advanced cyber warfare law, strategic cyber diplomacy, technical legal interface.	Membentuk spesialis hukum siber yang siap mendukung operasi dan diplomasi digital TNI AL.
Evaluasi Program	Menggunakan Kirkpatrick Model (fokus pada behavior & results); simulasi operasional dan after-action review.	Evaluasi berbasis performa nyata, bukan sekadar ujian tertulis.
Infrastruktur Pendukung	Cyber range, digital forensic lab, simulated attack environment.	Fasilitas ini memungkinkan pembelajaran berbasis simulasi tanpa risiko terhadap sistem operasional.
Kemitraan Internasional	Kolaborasi dengan NATO CCDCOE, ICRC, student exchange, joint research, customized training untuk kebutuhan TNI AL.	Mempercepat adopsi best practices global dan memperluas wawasan hukum siber perwira Indonesia.

Evaluasi Program dan Infrastruktur Pendukung

Evaluasi efektivitas program dengan menggunakan Kirkpatrick Model, yang menekankan pada perilaku dan hasil, perlu dilakukan untuk memastikan penerapan pembelajaran dalam konteks nyata. Program harus dievaluasi tidak hanya melalui ujian tertulis tetapi juga melalui lingkungan operasional yang disimulasikan yang menguji kemampuan analisis hukum di bawah tekanan waktu (Nikolov, 2024).

Infrastruktur pendukung seperti *cyber range*, laboratorium digital forensik, dan lingkungan simulasi serangan menjadi komponen kunci dalam keberhasilan transformasi kurikulum. Investasi dalam teknologi dan fasilitas simulator untuk serangan siber akan memberikan pengalaman belajar yang mendekati realitas, tanpa membahayakan sistem operasional yang ada (Huotari, et al., 2019).

Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

Kemitraan Internasional

Pengembangan kemitraan yang berkelanjutan dengan institusi pendidikan internasional seperti *NATO Cooperative Cyber Defence Centre of Excellence* dan *International Committee of the Red Cross (ICRC)* sangat penting. Kerjasama tersebut dapat mempercepat adopsi praktik terbaik secara global dan memperluas wawasan hukum siber perwira Indonesia (Mileski, et al., 2018). Program pertukaran pelajar dan penelitian bersama juga perlu ditingkatkan untuk memastikan penyesuaian terhadap kebutuhan spesifik TNI AL dalam konteks keamanan maritim kontemporer.

Transformasi kurikulum pendidikan hukum bagi perwira TNI AL merupakan langkah kritis untuk menjawab tantangan yang dihadapi dalam era digital saat ini. Melalui model tripartit yang terintegrasi, pengembangan kapasitas teknis dan operasional, serta evaluasi berkelanjutan, diharapkan perwira hukum dapat beradaptasi dengan baik dalam menghadapi ancaman siber yang semakin kompleks di sektor maritim. Implementasi inisiatif ini tidak hanya akan mempersiapkan mereka untuk tugas-tugas saat ini, tetapi juga untuk tantangan yang akan datang di masa mendatang.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan pembahasan mendalam yang telah diuraikan, dapat disimpulkan dua hal fundamental yang sangat berpengaruh terhadap perkembangan TNI AL dalam menghadapi tantangan keamanan siber di era digital.

Pertama, dinamika ancaman siber dalam operasi kemaritiman modern telah menciptakan lanskap keamanan yang kompleks dan multidimensi. Ancaman ini mencakup berbagai aspek, tidak hanya dari segi teknis, seperti sabotase pada sistem komando dan kendali kapal perang, tetapi juga aspek hukum yang belum sepenuhnya terakomodasi dalam kerangka regulasi yang ada. Masalah kompleksitas yurisdiksi serta kesulitan dalam atribusi serangan menambah kebingungan dalam penerapan hukum humaniter internasional dalam ruang siber. Dengan demikian, penting untuk melakukan penyesuaian paradigmatik dalam penyiapan kompetensi perwira hukum TNI AL agar mereka siap menghadapi ancaman yang terus berkembang dan bervariasi.

Kedua, transformasi kurikulum pendidikan hukum bagi Perwira TNI AL Korp Hukum merupakan kebutuhan imperatif yang tidak dapat ditunda. Mengadopsi model pendidikan integratif yang mensintesis tiga pilar utama yaitu hukum siber internasional, kompetensi digital forensik, dan konteks operasional maritim adalah pendekatan strategis yang perlu diterapkan. Implementasi kerangka kurikulum baru ini melalui modifikasi program Pendidikan Pertama (Dikma) dan pengembangan program spesialisasi *Cyber Law Specialist*, yang didukung oleh infrastruktur cyber range dan kemitraan internasional, akan berfungsi sebagai multiplier kekuatan dalam membangun kapabilitas legal advisory yang tangguh dan responsif untuk TNI AL di era digital.

Dengan adanya transformasi kurikulum ini, diharapkan perwira hukum TNI AL akan lebih siap dalam memberikan nasihat hukum yang relevan dan

Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

mengantisipasi serta merespons ancaman siber secara efektif, berkontribusi pada stabilitas keamanan maritim dan kedaulatan negara di perairan Indonesia.dari penelitian tersebut. Kesimpulan dan saran ditulis dalam bentuk paragraf, bukan nomor.

Saran

Berdasarkan analisis komprehensif yang telah dilakukan, berikut disampaikan rekomendasi strategis yang bersifat kontemporer dan aplikatif:

1. Pembentukan TNI AL *Cyber Law Center of Excellence*

TNI AL perlu mendirikan *Cyber Law Center of Excellence* yang berfungsi sebagai pusat pengetahuan dan pelatihan hukum siber terpadu. Pusat ini harus mampu mengintegrasikan *cyber range* simulasi operasi maritim dengan platform pengambilan keputusan hukum yang dilengkapi dengan kecerdasan buatan *(artificial intelligence)* untuk analisis preseden hukum. Kolaborasi dengan startup keamanan siber lokal dalam pengembangan modul pelatihan hukum siber yang disesuaikan akan menciptakan pendekatan adaptif terhadap ancaman siber spesifik yang dihadapi oleh Indonesia

2. Implementasi *Continuous Competency Assessment*

Disarankan untuk menerapkan sistem penilaian kompetensi berkelanjutan yang berbasis *micro-credentialing* dan *digital badge.* Setiap perwira hukum wajib menyelesaikan latihan simulasi hukum siber kuartalan dengan skenario terkini seperti kampanye disinformasi berbasis AI atau serangan ransomware pada infrastruktur maritim. Sistem ini harus terintegrasi dengan sertifikasi berbasis *blockchain* untuk memastikan autentisitas kredensial.

3. Pengembangan ASEAN *Maritime Cyber Law Forum*

Diperlukan pembentukan ASEAN *Maritime Cyber Law Forum* sebagai platform untuk berbagi intelijen dan praktik terbaik hukum siber maritim. Inisiatif ini harus diperjuangkan untuk standardisasi hukum siber regional dan kerangka berbagi bukti digital lintas batas yang mempercepat investigasi insiden siber transnasional. Sebagai ketua, Indonesia dapat memprakarsai latihan bersama *(joint table-top exercise)* mengenai hukum siber maritim dengan negara-negara ASEAN.

4. Adopsi *Regulatory Sandbox Approach*

Diperlukan pengadopsian pendekatan *regulatory sandbox* untuk menguji kebijakan dan protokol hukum operasi siber dalam lingkungan terkendali. Mekanisme ini memungkinkan pengembangan kerangka hukum yang responsif terhadap teknologi baru seperti komputasi kuantum dan senjata siber berbasis AI tanpa mengorbankan keamanan nasional. Kolaborasi dengan akademisi dan *ethical hackers* melalui program bug bounty khusus untuk sistem maritim sangat disarankan guna mengidentifikasi celah hukum sebelum dieksploitasi oleh musuh.

Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

DAFTAR PUSTAKA

Agrawal, J., Kalra, S. S., & Gidwani, H. (2023). *AI in Cyber Security*. *International Journal of Communication and Information Technology,* 4(1), 46–53.

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network,* 2(1), 123–138.

Androjna, A., Brčko, T., Pavić, I., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering,* 8(10), 776.

Androjna, A., & Perkovič, M. (2021). Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. *Transactions on Maritime Science,* 10(2), 361–373.

Baldauf, M., Dalaklis, D., & Kataria, A. (2016). *Team Training in Safety and Security via Simulation*.

Cabuya-Padilla, D. E., López, D. D., Martínez-Páez, J., Encinas, L. H., & Castaneda-Marroquin, C. (2025). Maritime Cyberattack Simulation Using Dynamic Modeling. *International Journal of Information Security.*

Canepa, M., Ballini, F., Dalaklis, D., & Vakili, S. (2021). *Assessing the Effectiveness of Cybersecurity Training in Maritime Domain*.

Dimakopoulou, A., & Rantos, K. (2024). Maritime Cybersecurity Landscape Based on NIST CSF v2.0. *Journal of Marine Science and Engineering,* 12(6), 919.

Peter G. Peterson Foundation. (2020). *The Facts about U.S. Defense Spending*.

Gong, S., & Lee, C. (2021). Cyber Threat Intelligence Framework for Incident Response. *Electronics,* 10(3), 239.

Gopinath, S., et al. (2025). Maritime Cyber Security. *Int Res J Adv Engg MGT,* 3(2), 167–172.

Huotari, J., et al. (2019). Q-Learning Based Autonomous Control of Ship Power Network. *IEEE Access,* 7, 152879–152890.

Jadhav, H., & Madoo, S. (2023). *The Ethics of Cyber Warfare*.

Martínez, F., et al. (2023). Cybersecurity Framework in Maritime and Military World. *Ciencia y Tecnología de Buques,* 17(33), 51–60.

Mavroeidis, V., & Jøsang, A. (2018). *Data-Driven Threat Hunting Using Sysmon*.

Mazaraki, N., & Goncharova, Y. (2022). Cyber Dimension of Hybrid Wars. *Baltic Journal of Economic Studies,* 8(2), 115–120.

Mesa, M. V. C., et al. (2024). Cybersecurity at Sea: Literature Review. *Information,* 15(11), 710.

Metalla, O., et al. (2023). Cyber Security in Maritime Transport. *Interdisciplinary Journal of Research and Development,* 10(2), 74.

Mileski, J., Clott, C., & Galvão, C. B. (2018). Cyberattacks on Ships: A Wicked Problem. *Maritime Business Review,* 3(4), 414–430.

Misas, J. P., Hopcraft, R., & Tam, K. (2022). *Future of Maritime Autonomy and Cybersecurity*.

Nasir, S. N. S. (2023). Effectiveness of Cybersecurity Training Programs. *Advances in Multidisciplinary Research,* 2(1), 151–160.

Nikolov, B. (2024). *Maritime Cybersecurity Virtual Training Environment*.

Vol 6 No 1 (2026) 460–471 P-ISSN 2774-5058 E-ISSN 2775-7269
DOI: 47467/eduinovasi.v6i1.11910

Orlovskyi, B. M. (2025). Modern Cyber Risks in Commercial Shipping. *Constitutional State,* 58, 210–219.

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. *Journal of Marine Science and Engineering,* 9(12), 1384.

Saeed, S., et al. (2023). Cyber Threat Intelligence for Organizational Resilience. *Sensors,* 23(16), 7273.

Sokołowski, W. (2021). *Cybersecurity of Maritime Autonomous Surface Ships*. Rocznik Bezpieczeństwa Morskiego.

Spáčil, J. (2022). Plea of Necessity in Cyber Operations. *Masaryk University Journal of Law and Technology,* 16(2), 215–239.

Sviličić, B., et al. (2019). Cyber Security Awareness on ECDIS. *TransNav,* 13(1), 231–236.

Svitlak, I. (2023). *Cyber Military Threat and International Law*.

Thapaliya, S., & Bokani, A. (2024). AI for Enhanced Cybersecurity. *Sadgamaya,* 1(1), 46–52.