Journal of Industrial Engineering & Management Research
http://www.jiemar.org e-ISSN : 2722-8878
Vol. 7 No. 2 – April 2026

DETERMINING PRIORITIES FOR DEFENSE TECHNOLOGY DEVELOPMENT TO SUPPORT THE PROTECTION OF STRATEGIC VITAL AREAS OF THE INDONESIAN NAVY IN ORDER TO COUNTER MILITARY AND NON-MILITARY THREATS WITHIN THE TERRITORY OF THE REPUBLIC OF INDONESIA

Adhi Windarko[#1], Hendrik Kurniawan[#2], Sri Depranoto[#3]

[#] *Strategi Operasi Laut, Politeknik Angkatan Laut*
Jalan Ciledug Raya No.2, Seskoal, Jakarta selatan, DKI Jakarta, Indonesia 12230
adhiibhy@gmail.com

Abstract *— The development of modern defense technology has become a critical component of national security strategy in responding to increasingly complex and multidomain threats. This study examines the prioritization of defense technology development to support the protection of Strategic Vital Areas of the Indonesian Navy against both military and non-military threats. Using an integrated methodological approach, the study combines the Analytical Hierarchy Process (AHP) and SWOT analysis to generate objective and strategic recommendations. The AHP results indicate that cyber resilience is the highest priority, surpassing C-ISR and UAV technologies, highlighting its fundamental role in ensuring the effectiveness of modern network-centric defense systems. Without robust cyber capabilities, other defense technologies are vulnerable to disruption and degradation. Furthermore, the SWOT analysis positions the strategy within the W–O (turnaround) quadrant, emphasizing the need to leverage external opportunities to overcome internal limitations. The recommended strategies include developing an integrated cyber defense architecture, enhancing interoperability through international cooperation, strengthening domestic defense industry capabilities, and implementing layered cyber defense systems. Overall, this study underscores the importance of cyber resilience as the backbone of adaptive, integrated, and sustainable defense capabilities to safeguard national sovereignty in the era of asymmetric and hybrid threats.*

Keywords — *Cyber Resilience, Defense Technology, Strategies*

I. PENDAHULUAN

Permasalahan pengembangan teknologi pertahanan modern merupakan bagian tak terpisahkan dari strategi keamanan nasional yang efektif. Globalisasi, perkembangan teknologi, dan dinamika ancaman kontemporer telah mengubah wajah konflik dari sekadar konfrontasi militer konvensional menuju perang asimetris yang memanfaatkan kerentanan siber, ruang elektronik, dan informasi untuk mencapai tujuan politik tanpa deklarasi perang formal (Glenn, 2009). Dalam konteks ini, negara-negara berdaulat dituntut untuk merumuskan prioritas pengembangan teknologi pertahanan yang mampu menjawab ancaman kompleks dan lintas domain, terutama terhadap area objek vital strategis yang menjadi poros kedaulatan negara.

Fenomena tersebut bukan sekedar asumsi akademis, melainkan telah teruji dalam skala operasi intelijen dan militer besar. Salah satu contoh terkini adalah Operasi *Absolute Resolve,* dimana militer Amerika Serikat (AS) melaksanakan sebuah operasi besar-besaran untuk menangkap Presiden Venezuela, Nicolás Maduro pada 3 Januari 2026. Operasi ini melibatkan perencanaan matang selama berbulan-bulan oleh badan intelijen dan militer AS, termasuk koordinasi multi-alat (air, darat, laut, ruang siber, dan ISR) untuk melacak target, melumpuhkan pertahanan lokal, dan mengeksekusi penangkapan pada dini hari tanpa kehilangan personel AS. Konferensi pers resmi menyebutkan bahwa misi tersebut melibatkan lebih dari 150 pesawat tempur dan UAV, dukungan sinyal intelijen, serta operasi untuk mematikan listrik di sebagian wilayah Caracas guna mengurangi kapabilitas pertahanan musuh sebelum serangan dimulai.

Kasus ini memberikan pelajaran empiris penting bahwa superioritas teknologi, mulai dari intelijen, pengawasan, dan pengintaian terpadu (C-ISR), kemampuan UAV, serta ketahanan siber (*cyber resilience*), bukan lagi sekedar faktor penunjang, tetapi kunci dalam mendukung efektivitas dan presisi operasi. Di luar konteks geopolitik AS, pengalaman seperti itu menegaskan bahwa dalam era modern, kemampuan untuk mendeteksi, mengintegrasikan data intelijen, serta melumpuhkan infrastruktur lawan secara siber atau elektronik menjadi penentu dalam suksesnya sebuah operasi.

Bagi Indonesia, sebagai negara kepulauan terbesar di dunia dengan ribuan pulau dan garis pantai yang sangat panjang, tantangan pengamanan objek vital strategis menjadi semakin kompleks (Hermawan, 2022). Infrastruktur pesisir seperti pelabuhan, pangkalan militer, instalasi energi, dan jalur logistik nasional sangat rentan terhadap serangan yang memanfaatkan celah teknologi informasi dan asimetri strategi, termasuk infiltrasi di bidang siber dan elektronik. Kasus infiltrasi asing, gangguan jaringan komunikasi kritis, dan manipulasi data juga menunjukkan bahwa kedaulatan negara dapat dilumpuhkan tanpa melibatkan konflik militer konvensional.

Atas dasar dinamika lingkungan strategis tersebut, fokus tulisan ini adlaah pada urgensi penentuan prioritas pengembangan teknologi pertahanan di Area Objek Vital Strategis secara sistematis dan berbasis analisis. Pilihan antara penguatan C-ISR, peningkatan ketahanan siber (*cyber resilience*), atau optimalisasi penggunaan UAV tidak sekadar persoalan modernisasi Alutsista, melainkan menyangkut efektivitas daya tangkal nasional dalam menghadapi spektrum ancaman militer dan non-militer yang beroperasi secara asimetris dan lintas domain. Dalam konteks tersebut, juga diperlukan rumusan strategi yang mampu memperkuat postur teknologi pertahanan di Area Objek Vital Strategis TNI AL secara terintegrasi, sehingga tidak hanya meningkatkan kemampuan deteksi dini melalui superioritas informasi dan pengawasan, tetapi juga menjamin kapasitas respons yang cepat, presisi, dan berlapis dalam melumpuhkan potensi ancaman sebelum berkembang menjadi gangguan terhadap stabilitas dan kedaulatan NKRI.

Untuk menjawab permasalahan tersebut secara objektif dan terukur, tulisan ini menggunakan pendekatan metodologis yang terintegrasi antara *Analytical Hierarchy Process* (AHP) dan analisis *Strength, Weakness, Opportunity and Threat* (SWOT). Metode AHP diterapkan untuk menganalisis dan menentukan prioritas pengembangan teknologi pertahanan pada Area Objek Vital Strategis dengan membandingkan alternatif C-ISR, *cyber resilience*, dan UAV berdasarkan kriteria yang relevan, seperti efektivitas tempur, biaya investasi, dan ketahanan siber. Melalui proses pembobotan dan penilaian yang sistematis, AHP memungkinkan pengambilan keputusan yang rasional dan berbasis data dalam menentukan teknologi yang paling strategis untuk dikembangkan. Selanjutnya, analisis SWOT digunakan untuk merumuskan strategi penguatan postur teknologi pertahanan di Area Objek Vital Strategis TNI AL secara komprehensif dengan mengidentifikasi faktor kekuatan dan kelemahan internal, serta peluang dan ancaman eksternal yang mempengaruhi kesiapan pertahanan. Integrasi kedua metode tersebut diharapkan dapat menghasilkan rekomendasi strategis yang tidak hanya tepat dalam menentukan prioritas pengembangan teknologi, tetapi juga adaptif dan berkelanjutan dalam memperkuat kemampuan deteksi dini dan daya tangkal terhadap ancaman asimetris di wilayah NKRI.

Berdasarkan latar belakang di atas, maka permasalahan dalam tulisan ini dapat dirumuskan sebagai berikut:

a. Bagaimana menetapkan prioritas pengembangan teknologi pertahanan pada Area Objek Vital Strategis (C-ISR, *cyber resilience*, atau UAV) secara objektif dan berbasis analisis kuantitatif guna meningkatkan efektivitas perlindungan terhadap ancaman infiltrasi asing di wilayah Indonesia?

b. Bagaimana merumuskan strategi penguatan postur teknologi pertahanan Area Objek Vital Strategis TNI AL yang terintegrasi, adaptif, dan berkelanjutan untuk mengatasi keterbatasan sistem yang ada serta meningkatkan kemampuan deteksi dini dan pelumpuhan ancaman militer maupun non-militer berbasis teknologi?

Untuk mendukung pembahasan dalam penelitian ini sehingga dapat mewujudkan konsep hasil penelitian yang komprehensif, maka peneliti menggunakan landasan pemikiran sebagai berikut:

a. Landasan Yuridis.

1) Undang-Undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Undang-Undang RI Nomor 3 Tahun 2002 tentang Pertahanan Negara merupakan landasan hukum utama dalam penyelenggaraan sistem pertahanan negara Indonesia yang bersifat semesta. Undang-undang ini menegaskan bahwa pertahanan negara diselenggarakan untuk menjaga dan melindungi kedaulatan negara, keutuhan wilayah NKRI, serta keselamatan segenap bangsa dari segala bentuk ancaman. Dalam Pasal 1 ditegaskan bahwa pertahanan negara adalah segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah, dan keselamatan bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara. Lebih lanjut, UU ini mengatur bahwa sistem pertahanan negara dilaksanakan melalui sistem pertahanan semesta yang melibatkan seluruh warga negara, wilayah, dan sumber daya nasional lainnya, serta dipersiapkan secara dini oleh pemerintah dan diselenggarakan secara total, terpadu, terarah, dan berlanjut. Dengan demikian, UU RI No. 3 Tahun 2002 tidak hanya mengatur aspek operasional militer, tetapi juga menekankan pentingnya pengelolaan sumber daya nasional, termasuk pengembangan ilmu pengetahuan dan teknologi, sebagai bagian integral dari pembangunan kekuatan pertahanan negara.

UU RI No. 3 Tahun 2002 menjadi landasan yuridis untuk membangun kekuatan pertahanan yang mampu menghadapi spektrum ancaman militer dan non-militer secara komprehensif. Pasal 4 menegaskan bahwa pertahanan negara bertujuan untuk menjaga dan melindungi kedaulatan negara serta keutuhan wilayah NKRI dari segala bentuk ancaman, baik yang bersifat tradisional maupun non-tradisional. Dalam konteks pertahanan Area Objek Vital Strategis TNI AL, ketentuan tersebut memberikan dasar hukum bagi pengembangan dan prioritisasi teknologi pertahanan sebagai bagian dari pembangunan kekuatan yang berbasis ancaman (threat-based defense planning). Selain itu, Pasal 10 menegaskan peran Tentara Nasional Indonesia sebagai komponen utama dalam menghadapi ancaman militer, yang dalam implementasinya memerlukan dukungan sistem teknologi seperti C-ISR, ketahanan siber, dan UAV guna meningkatkan kemampuan deteksi dini serta daya tangkal terhadap infiltrasi dan ancaman asimetris. Dengan demikian, pengembangan teknologi pertahanan untuk mendukung perlindungan Area Objek Vital Strategis TNI AL bukan sekadar kebijakan teknis, melainkan merupakan perwujudan langsung dari amanat konstitusional dan yuridis sebagaimana diatur dalam UU Nomor 3 Tahun 2002.

2) Undang-Undang RI Nomor 3 Tahun 2025 tentang Perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang TNI.

UU RI No. 3 Tahun 2025 tentang Perubahan atas UU No. 34 Tahun 2004 tentang Tentara Nasional Indonesia merupakan instrumen hukum strategis yang memperbarui pengaturan mengenai kedudukan, peran, tugas, dan fungsi TNI dalam menghadapi dinamika ancaman kontemporer. Perubahan ini pada prinsipnya diarahkan untuk menyesuaikan postur dan tata kelola TNI dengan perkembangan lingkungan strategis global, kemajuan teknologi militer, serta spektrum ancaman yang semakin kompleks dan multidimensional. Dalam perubahan tersebut ditegaskan kembali bahwa TNI berperan sebagai alat pertahanan negara yang bertugas menegakkan kedaulatan negara, mempertahankan keutuhan wilayah NKRI, dan melindungi segenap bangsa dari ancaman militer maupun ancaman bersenjata lainnya. Selain itu, pembaruan regulasi ini memperkuat aspek modernisasi alutsista, interoperabilitas antarmatra, serta peningkatan profesionalisme prajurit dalam kerangka transformasi pertahanan yang adaptif terhadap perkembangan teknologi informasi, siber, dan sistem persenjataan berbasis jaringan.

UU RI No. 3 Tahun 2025 menjadi landasan yuridis untuk memperkuat postur pertahanan nasional, termasuk dalam konteks perlindungan Area Objek Vital Strategis oleh TNI AL. Penegasan tugas TNI dalam menghadapi ancaman militer dan non-militer, termasuk ancaman hibrida dan asimetris, memberikan dasar yuridis bagi pengembangan serta prioritisasi teknologi pertahanan seperti C-ISR, ketahanan siber (*cyber resilience*), dan sistem UAV. Perubahan regulasi ini juga mendorong penguatan integrasi sistem pertahanan antarmatra dan peningkatan kesiapan menghadapi ancaman berbasis teknologi yang dapat menyasar infrastruktur strategis nasional. Dalam konteks tersebut, penentuan prioritas pengembangan teknologi pertahanan untuk mendukung pengamanan Area Objek Vital Strategis TNI AL bukan sekadar kebutuhan operasional, melainkan merupakan implementasi langsung dari kebijakan legislasi yang menekankan modernisasi, efektivitas daya tangkal, dan kesiapsiagaan nasional terhadap ancaman multidomain di wilayah NKRI.

b. Landasan Teoritis.

1) Teori *Revolution in Military Affairs.*

Teori *Revolution in Military Affairs* (RMA) berkembang pada akhir Perang Dingin sebagai kerangka konseptual yang menjelaskan transformasi mendasar dalam cara negara membangun dan menggunakan kekuatan militernya akibat kemajuan teknologi, doktrin, dan organisasi. Konsep ini banyak dikembangkan oleh para pemikir pertahanan seperti Andrew F. Krepinevich, yang mendefinisikan RMA sebagai perubahan signifikan dalam karakter perang yang dihasilkan oleh inovasi teknologi yang dipadukan dengan adaptasi doktrin dan struktur organisasi militer (Krepinevich, 1992). RMA menekankan bahwa keunggulan militer tidak lagi semata-mata ditentukan oleh jumlah personel atau platform persenjataan, melainkan oleh kemampuan mengintegrasikan sistem informasi, sensor, komando dan kendali (*Command and Control*/C2), serta presisi senjata dalam suatu jaringan terpadu (*network-centric warfare*) (Owens, 2000). Dalam perspektif ini, superioritas informasi, kesadaran situasional (situational awareness), dan kemampuan menyerang secara presisi menjadi faktor penentu dalam memenangkan konflik modern. Alvin dan Heidi Toffler bahkan menegaskan bahwa gelombang ketiga revolusi peradaban (ditandai oleh dominasi teknologi informasi) telah mengubah paradigma peperangan dari perang industri

menjadi perang berbasis pengetahuan dan informasi (Toffler, 1993). Dengan demikian, RMA bukan hanya transformasi teknologi, tetapi juga perubahan mendasar dalam paradigma strategis dan operasional militer.

Teori RMA menjadi landasan teoritis dalam menentukan prioritas pengembangan teknologi pertahanan untuk mendukung perlindungan Area Objek Vital Strategis TNI AL. Dalam kerangka RMA, penguatan sistem C-ISR, ketahanan siber (*cyber resilience*), dan penggunaan UAV merupakan manifestasi konkret dari transformasi pertahanan berbasis jaringan dan informasi. Perlindungan Area Objek Vital Strategis di era ancaman militer dan non-militer yang bersifat asimetris menuntut integrasi sensor, sistem pengawasan maritim, sistem komando terpusat, serta kemampuan respons presisi yang terhubung secara *real-time.* Tanpa integrasi tersebut, keunggulan teknologi tidak akan menghasilkan efek strategis yang optimal. Oleh karena itu, penentuan prioritas teknologi pertahanan sebagaimana dikaji dalam tulisan ini selaras dengan prinsip RMA, yakni membangun postur pertahanan yang berorientasi pada superioritas informasi, interoperabilitas sistem, dan kemampuan respons cepat terhadap ancaman multidomain. Implementasi RMA dalam konteks TNI AL menjadi krusial untuk memastikan bahwa pengamanan Area Objek Vital Strategis tidak hanya bersifat reaktif, tetapi proaktif dan berbasis keunggulan teknologi yang mampu menciptakan daya tangkal yang kredibel di wilayah NKRI.

2) Teori *Network-Centric Warfare.*

Teori *Network-Centric Warfare* (NCW) berkembang pada akhir 1990-an sebagai bagian dari transformasi militer modern yang dipengaruhi oleh kemajuan teknologi informasi dan komunikasi. Konsep ini secara sistematis dikembangkan oleh Alberts, et al., yang mendefinisikan NCW sebagai pendekatan peperangan yang berorientasi pada penciptaan keunggulan informasi melalui jaringan yang menghubungkan sensor, pengambil keputusan, dan penembak (*sensor–decision maker–shooter link*) dalam suatu arsitektur terpadu (Alberts*, et al.,* 1999). Dalam kerangka ini, kekuatan tempur tidak lagi semata-mata ditentukan oleh platform persenjataan, melainkan oleh kemampuan berbagi informasi secara real-time, meningkatkan kesadaran situasional bersama (*shared situational awareness*), serta mempercepat siklus pengambilan keputusan (OODA loop). Alberts dan Garstka menegaskan bahwa "*information superiority*" yang dihasilkan melalui jaringan akan meningkatkan efektivitas tempur dengan memungkinkan kolaborasi yang lebih cepat, presisi serangan yang lebih tinggi, serta sinkronisasi operasi lintas matra. Dengan demikian, NCW menekankan bahwa integrasi sistem komunikasi, komando dan kendali (C2), intelijen, pengawasan, dan pengintaian (ISR) dalam satu jaringan yang interoperabel merupakan fondasi utama dalam membangun kekuatan militer modern.

Teori NCW menjadi landasan teoritis untuk meningkatkan pertahanan Area Objek Vital Strategis TNI AL melalui integrasi teknologi pertahanan yang berbasis jaringan. Dalam konteks ancaman militer dan non-militer yang bersifat asimetris, perlindungan Area Objek Vital Strategis tidak dapat mengandalkan sistem yang terfragmentasi, melainkan memerlukan konektivitas antara C-ISR, sistem UAV, serta ketahanan siber dalam satu arsitektur pertahanan terpadu. Prinsip NCW menekankan bahwa semakin kuat jaringan informasi yang menghubungkan sensor maritim, pusat komando, dan elemen respons, maka semakin tinggi pula kemampuan deteksi dini dan daya tangkal terhadap infiltrasi atau gangguan berbasis teknologi. Oleh karena itu, penentuan prioritas pengembangan teknologi pertahanan sebagaimana dibahas dalam tulisan ini selaras dengan paradigma NCW, yakni membangun postur pertahanan yang berbasis keunggulan informasi, interoperabilitas sistem, dan kecepatan pengambilan keputusan untuk menghadapi ancaman multidomain di wilayah NKRI. Implementasi NCW dalam lingkungan TNI AL menjadi krusial untuk memastikan bahwa pengamanan Area Objek Vital Strategis mampu bertransformasi dari pola reaktif menuju sistem pertahanan proaktif yang terintegrasi dan adaptif terhadap dinamika ancaman kontemporer.

3) Teori *Analytical Hierarchy Process.*

Teori *Analytical Hierarchy Process* (AHP) merupakan metode pengambilan keputusan multikriteria yang dikembangkan oleh Thomas L. Saaty pada awal 1970-an untuk membantu pengambil kebijakan dalam menghadapi persoalan kompleks yang melibatkan berbagai alternatif dan kriteria yang saling berinteraksi. AHP bekerja dengan memecah suatu masalah ke dalam struktur hierarkis yang terdiri atas tujuan, kriteria, subkriteria, dan alternatif, kemudian melakukan perbandingan berpasangan (pairwise comparison) untuk menghasilkan bobot prioritas secara kuantitatif (Saaty, 1980). Melalui skala fundamental 1 sampai 9 yang diperkenalkan oleh Saaty,

penilaian subjektif para pengambil keputusan dapat dikonversi menjadi nilai numerik yang terukur, sehingga menghasilkan peringkat alternatif berdasarkan tingkat kepentingannya. Salah satu keunggulan utama AHP adalah kemampuannya menguji konsistensi logis dari penilaian responden melalui *consistency ratio,* sehingga keputusan yang dihasilkan tidak hanya bersifat intuitif tetapi juga memiliki validitas matematis. Dengan demikian, AHP banyak digunakan dalam perencanaan strategis, kebijakan publik, manajemen pertahanan, dan evaluasi investasi teknologi karena mampu mengintegrasikan pertimbangan kuantitatif dan kualitatif dalam satu kerangka analitis yang sistematis.

Dalam tulisan ini, metode AHP digunakan untuk menentukan prioritas pengembangan teknologi pertahanan secara objektif dan rasional dalam mendukung perlindungan Area Objek Vital Strategis TNI AL. Pemilihan antara penguatan C-ISR, peningkatan *cyber resilience,* atau optimalisasi penggunaan UAV melibatkan berbagai kriteria seperti efektivitas tempur, biaya investasi, interoperabilitas sistem, serta ketahanan terhadap ancaman siber dan elektronik. Dalam konteks ini, AHP menyediakan instrumen metodologis untuk membandingkan alternatif tersebut secara terstruktur berdasarkan bobot kepentingan masing-masing kriteria, sehingga menghasilkan keputusan yang transparan dan dapat dipertanggungjawabkan secara akademis maupun strategis. Dengan penerapan AHP, proses penentuan prioritas teknologi tidak lagi didasarkan semata pada preferensi institusional atau pertimbangan sektoral, melainkan pada analisis multikriteria yang selaras dengan kebutuhan peningkatan deteksi dini dan daya tangkal terhadap ancaman militer dan non-militer di wilayah NKRI.

4) Teori SWOT.

Teori SWOT (*Strengths, Weaknesses, Opportunities, Threats*) merupakan salah satu kerangka analisis strategis yang digunakan untuk mengidentifikasi dan mengevaluasi faktor-faktor internal dan eksternal yang memengaruhi pencapaian tujuan suatu organisasi. Konsep ini pertama kali dipopulerkan dalam kajian manajemen strategis oleh Albert Humphrey pada dekade 1960-an dan kemudian dikembangkan secara sistematis dalam literatur strategi oleh para pakar seperti Kenneth R. Andrews. Analisis SWOT membagi lingkungan strategis ke dalam dua dimensi utama, yaitu faktor internal yang terdiri atas kekuatan (*strengths*) dan kelemahan (*weaknesses*), serta faktor eksternal yang meliputi peluang (*opportunities*) dan ancaman (*threats*) (Andrews, 1971). Melalui pemetaan tersebut, organisasi dapat merumuskan strategi yang memaksimalkan kekuatan untuk memanfaatkan peluang (strategi SO), meminimalkan kelemahan dengan memanfaatkan peluang (strategi WO), menggunakan kekuatan untuk mengatasi ancaman (strategi ST), serta mengurangi kelemahan guna menghindari ancaman (strategi WT). Dengan demikian, SWOT tidak hanya berfungsi sebagai alat identifikasi situasi, tetapi juga sebagai instrumen formulasi strategi yang komprehensif dan adaptif terhadap dinamika lingkungan strategis.

Relevansi teori SWOT dengan judul tulisan ini terletak pada kebutuhan merumuskan strategi penguatan postur teknologi pertahanan di Area Objek Vital Strategis TNI AL secara terintegrasi dan berkelanjutan. Dalam konteks ancaman militer dan non-militer yang semakin kompleks, analisis SWOT memungkinkan identifikasi kekuatan internal seperti kapasitas C-ISR yang telah dimiliki, kompetensi sumber daya manusia, serta dukungan kebijakan nasional; sekaligus mengungkap kelemahan seperti keterbatasan interoperabilitas sistem atau kerentanan siber. Di sisi eksternal, peluang berupa perkembangan teknologi pertahanan dan kerja sama strategis dapat dioptimalkan, sementara ancaman seperti infiltrasi siber, GPS *spoofing,* dan operasi hibrida dapat dipetakan secara sistematis. Dengan pendekatan SWOT, strategi pengembangan dan prioritisasi teknologi pertahanan tidak hanya berfokus pada aspek teknis, tetapi juga mempertimbangkan konteks lingkungan strategis yang lebih luas, sehingga mendukung terciptanya sistem pertahanan Area Objek Vital Strategis TNI AL yang adaptif, resilien, dan mampu meningkatkan daya tangkal nasional di wilayah NKRI.

II. METODE

Metode analisis yang digunakan dalam tulisan ini merupakan pendekatan terpadu yang mengombinasikan AHP dan analisis SWOT guna menghasilkan keputusan strategis yang objektif dan komprehensif dalam penentuan prioritas pengembangan teknologi pertahanan di Area Objek Vital Strategis TNI AL. AHP digunakan sebagai instrumen kuantitatif untuk melakukan pembobotan dan perbandingan berpasangan terhadap alternatif teknologi, yaitu C-ISR, *cyber resilience*, dan UAV, berdasarkan kriteria utama seperti efektivitas tempur, biaya investasi, dan ketahanan siber. Pendekatan ini memungkinkan proses pengambilan keputusan dilakukan secara

Journal of Industrial Engineering & Management Research
http://www.jiemar.org e-ISSN : 2722-8878
Vol. 7 No. 2 – April 2026

sistematis, terstruktur, dan terukur melalui uji konsistensi rasio, sehingga menghasilkan prioritas yang rasional dan dapat dipertanggungjawabkan secara akademis. Selanjutnya, hasil prioritas tersebut dianalisis lebih lanjut menggunakan kerangka SWOT untuk merumuskan strategi penguatan postur teknologi pertahanan yang mempertimbangkan faktor internal (kekuatan dan kelemahan organisasi) serta faktor eksternal (peluang dan ancaman lingkungan strategis). Integrasi kedua metode ini menghasilkan model analisis yang tidak hanya menentukan teknologi mana yang paling prioritas untuk dikembangkan, tetapi juga merumuskan strategi implementasi yang adaptif, berkelanjutan, dan selaras dengan kebutuhan peningkatan kemampuan deteksi dini serta daya tangkal terhadap ancaman militer dan non-militer di wilayah NKRI.

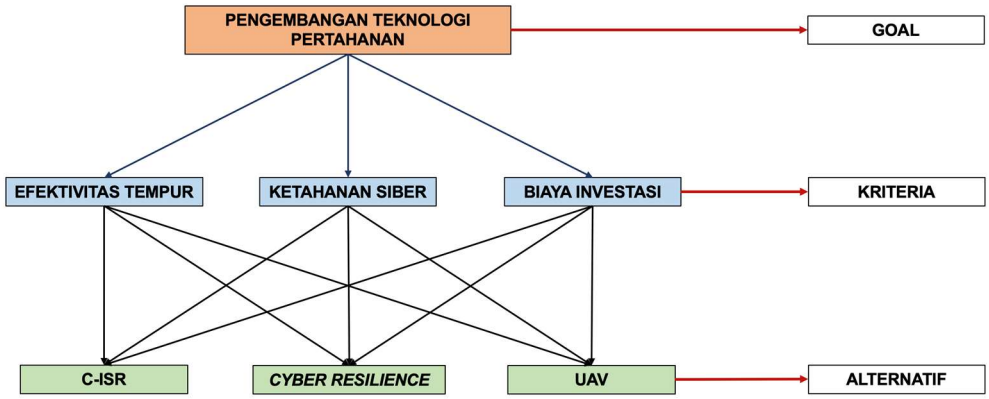
III. HASIL DAN PEMBAHASAN

Pembahasan dalam tulisan ini dapat diuraikan sebagai berikut:

a. Analisis Data.

1) Penentuan prioritas pengembangan teknologi pertahanan menggunakan metode AHP.

a) Menggambarkan struktur hierarki kriteria dan alternatif pengembangan teknologi pertahanan.



Gambar 1. Struktur Hierarki AHP

b) Melakukan perbandingan kriteria.

Tabel 1. Perbandingan Kriteria

Efektivitas Tempur	3	1/3	Ketahanan Siber
Efektivitas Tempur	3	1/3	Biaya Investasi
Ketahanan Siber	3	1/3	Biaya Investasi

c) Melakukan perhitungan perbandingan kriteria.

Tabel 2. Perhitungan Perbandingan Kriteria

	Efektivitas Tempur	Ketahanan Siber	Biaya Investasi	Nilai Eigen			Jml	Rata-rata
Efektivitas Tempur	1,00	3,00	3,00	0,60	0,69	0,43	1,72	0,57
Ketahanan Siber	0,33	1,00	3,00	0,20	0,23	0,43	0,86	0,29
Biaya Investasi	0,33	0,33	1,00	0,20	0,08	0,14	0,42	0,14
Jumlah	**1,67**	**4,33**	**7,00**					

d) Melakukan perbandingan alternatif pada masing-masing kriteria.

(1) Melakukan perbandingan alternatif pada Kriteria Efektivitas Tempur.

Tabel 3. Perbandingan Alternatif pada Kriteria Efektivitas Tempur

Journal of Industrial Engineering & Management Research
http://www.jiemar.org e-ISSN : 2722-8878
Vol. 7 No. 2 – April 2026

C-ISR	1/2	2	Cyber Resilience
C-ISR	2	1/2	UAV
Cyber Resilience	2	1/2	UAV

Tabel 4. Perhitungan Perbandingan Alternatif pada Kriteria Efektivitas Tempur

EFEKTIVITAS TEMPUR	C-ISR	Cyber Resilience	UAV	Nilai Eigen			Jml	Rata-rata
C-ISR	1,00	0,50	2,00	0,29	0,25	0,40	0,94	0,31
Cyber Resilience	2,00	1,00	2,00	0,57	0,50	0,40	1,47	0,49
UAV	0,50	0,50	1,00	0,14	0,25	0,20	0,59	0,20
Jumlah	**3,50**	**2,00**	**5,00**					

(2) Melakukan perbandingan alternatif pada Kriteria Ketahanan Siber.

Tabel 5. Perbandingan Alternatif pada Kriteria Ketahanan Siber

C-ISR		3	Cyber Resilience
C-ISR	2		UAV
Cyber Resilience	3		UAV

Tabel 6. Perhitungan Perbandingan Alternatif pada Kriteria Ketahanan Siber

KETAHANAN SIBER	C-ISR	Cyber Resilience	UAV	Nilai Eigen			Jml	Rata-rata
C-ISR	1,00	0,33	2,00	0,22	0,20	0,33	0,76	0,25
Cyber Resilience	3,00	1,00	3,00	0,67	0,60	0,50	1,77	0,59
UAV	0,50	0,33	1,00	0,11	0,20	0,17	0,48	0,16
Jumlah	**4,50**	**1,67**	**6,00**					

(3) Melakukan perbandingan alternatif pada Kriteria Biaya Investasi.

Tabel 7. Perbandingan Alternatif pada Kriteria Biaya Investasi

C-ISR		2	Cyber Resilience
C-ISR	2		UAV
Cyber Resilience	2		UAV

Tabel 8. Perhitungan Perbandingan Alternatif pada Kriteria Biaya Investasi

BIAYA INVESTASI	C-ISR	Cyber Resilience	UAV	Nilai Eigen			Jml	Rata-rata
C-ISR	1,00	0,50	2,00	0,29	0,25	0,40	0,94	0,31
Cyber Resilience	2,00	1,00	2,00	0,57	0,50	0,40	1,47	0,49
UAV	0,50	0,50	1,00	0,14	0,25	0,20	0,59	0,20
Jumlah	**3,50**	**2,00**	**5,00**					

e) Menentukan Prioritas (Perankingan).

Tabel 11. Prioritas Teknologi Pertahanan

Journal of Industrial Engineering & Management Research
http://www.jiemar.org e-ISSN : 2722-8878
Vol. 7 No. 2 – April 2026

C-ISR	0,29
CYBER RESILIENCE	0,52
UAV	0,19

Berdasarkan perhitungan dengan metode AHP diketahui bahwa nilai C-ISR sebesar 0,29, nilai *Cyber Resilience* sebesar 0,52 dan nilai UAV sebesar 0,19, sehingga dapat disimpulkan bahwa jenis teknologi pertahanan terbaik yang perlu dikembangkan adalah *Cyber Resilience.*

2) Rumusan strategi untuk memperkuat postur teknologi pertahanan Area Objek Vital Strategis menggunakan SWOT.

Untuk merumuskan strategi penguatan postur teknologi pertahanan di Area Objek Vital Strategis TNI AL, penulis menggunakan metode SWOT untuk menganalisis faktor-faktor internal (strengths dan weakness) dengan faktor-faktor eksternal (opportunities dan threats) sehingga dapat menentukan suatu langkah yang tepat dan ditujukan terhadap objek dan subjek dalam penelitian, dengan tahapan sebagai berikut:

a) Menentukan faktor-faktor internal.

Tabel 12. Faktor-Faktor Internal (*Internal Factors Analysis Summary* / IFAS)

Faktor – Faktor Internal	
Strength	***Weakness***
Kompetensi prajurit TNI AL.	Keterbatasan interoperabilitas.
Sistem komando dan kendali (C2) yang jelas dan terpusat.	Ketergantungan pada komponen impor.
Pengalaman operasional dalam pengamanan Area Objek Vital Strategis.	Kerentanan terhadap ancaman siber.
Integrasi sistem pengawasan maritim.	Keterbatasan alokasi sumber daya.

b) Menentukan faktor-faktor eksternal.

Tabel 13. Faktor-Faktor Eksternal (*External Factors Analysis Summary* / EFAS)

Faktor – Faktor Eksternal	
Opportunity	***Threat***
Perkembangan teknologi pertahanan.	Meningkatnya ancaman siber.
Dukungan kebijakan nasional.	Operasi infiltrasi asing.
Kerja sama pertahanan (multilateral dan bilateral).	Meningkatnya aktivitas intelijen ilegal.
Peningkatan kesadaran nasional terhadap ancaman siber dan hibrida.	Eskalasi konflik kawasan.

c) Perhitungan bobot faktor-faktor internal dan eksternal.

Berdasarkan identifikasi *strength, weakness, opportunity* dan *threat* di atas, selanjutnya dilakukan penyebaran kuisioner kepada 12 orang *expert* (melalui *Small Group Discussion*/SGD) untuk mengetahui nilai bobot faktor-faktor internal dan eksternal, dengan nilai bobot berkisar antara 0.0 (tidak penting), 0.25 (kurang penting), 0.5 (cukup penting), 0.75 (penting) dan 1.0 (sangat penting).

Tabel 14. Matriks Perhitungan Bobot Faktor-faktor Internal

Journal of Industrial Engineering & Management Research
http://www.jiemar.org e-ISSN : 2722-8878
Vol. 7 No. 2 – April 2026

No.	Faktor Internal	Nilai					Jml	Total	Bobot
		TP 0	KP 0,25	CP 0,5	P 0,75	SP 1			
	Strength								
1.	Kompetensi prajurit TNI AL.			2	5	5	12	9,75	0,295
2.	Sistem komando dan kendali (C2) yang jelas dan terpusat.			5	5	2	12	8,25	0,250
3.	Pengalaman operasional dalam pengamanan Area Objek Vital Strategis.		2	3	5	2	12	7,75	0,235
4.	Integrasi sistem pengawasan maritim.		4	2	3	3	12	7,25	0,220
								33	**1**
	Weakness								
1.	Keterbatasan interoperabilitas.			4	4	4	12	9	0,273
2.	Ketergantungan pada komponen impor.		2	3	4	3	12	8	0,242
3.	Kerentanan terhadap ancaman siber.			5	4	3	12	8,5	0,258
4.	Keterbatasan alokasi sumber daya.		3	2	5	2	12	7,5	0,227
								33	**1**

Tabel 15. Matriks Perhitungan Bobot Faktor-faktor Eksternal

No.	Faktor Eksternal	Nilai					Jml	Total	Bobot
		TP 0	KP 0,25	CP 0,5	P 0,75	SP 1			
	Opportunity								
1.	Perkembangan teknologi pertahanan.			4	4	4	12	9	0,288
2.	Dukungan kebijakan nasional.		4	3	5		12	6,25	0,200
3.	Kerja sama pertahanan (multilateral dan bilateral).		2	2	4	4	12	8,5	0,272
4.	Peningkatan kesadaran nasional terhadap ancaman siber dan hibrida.		3	3	3	3	12	7,5	0,240
								31,25	**1**
	Threat								
1.	Meningkatnya ancaman siber.		3	4	3	2	12	7	0,230
2.	Operasi infiltrasi asing.		4	4	4		12	6	0,197
3.	Meningkatnya aktivitas intelijen ilegal.			3	4	5	12	9,5	0,311
4.	Eskalasi konflik kawasan.		3	2	3	4	12	8	0,262
								30,5	**1**

d) Perhitungan rating faktor-faktor internal dan eksternal.

Selanjutnya melakukan perhitungan rating faktor-faktor internal dan eksternal berdasarkan hasil kuesioner yang telah diberikan kepada 12 orang *expert* (melalui *Small Group Discussion*/SGD), dengan rentang nilai 1 – 4, dengan rincian 1 (tidak signifikan), 2 (cukup signifikan), 3 (signifikan), dan 4 (sangat signifikan).

Tabel 16. Matriks Perhitungan Rating Faktor-faktor Internal

Journal of Industrial Engineering & Management Research
http://www.jiemar.org e-ISSN : 2722-8878
Vol. 7 No. 2 – April 2026

No.	Faktor Internal	Nilai				Jml	Total	Rating
		TS 1	CS 2	S 3	SS 4			
	Strength							
1.	Kompetensi prajurit TNI AL.		2	4	6	12	40	3,333
2.	Sistem komando dan kendali (C2) yang jelas dan terpusat.		4	3	5	12	37	3,083
3.	Pengalaman operasional dalam pengamanan Area Objek Vital Strategis.	1	2	5	4	12	36	3,000
4.	Integrasi sistem pengawasan maritim.	2	5	3	2	12	29	2,417
	Weakness							
1.	Keterbatasan interoperabilitas.		2	5	5	12	39	3,250
2.	Ketergantungan pada komponen impor.		3	4	5	12	38	3,167
3.	Kerentanan terhadap ancaman siber.		3	5	4	12	37	3,083
4.	Keterbatasan alokasi sumber daya.		4	6	2	12	34	2,833

Tabel 17. Matriks Perhitungan Rating Faktor-faktor Eksternal

No.	Faktor Eksternal	Nilai				Jml	Total	Rating
		TS 1	CS 2	S 3	SS 4			
	Opportunity							
1.	Perkembangan teknologi pertahanan.		3	3	6	12	39	3,250
2.	Dukungan kebijakan nasional.	2	5	3	2	12	29	2,417
3.	Kerja sama pertahanan (multilateral dan bilateral).		3	5	4	12	37	3,083
4.	Peningkatan kesadaran nasional terhadap ancaman siber dan hibrida.		4	5	3	12	35	2,917
	Threat							
1.	Meningkatnya ancaman siber.	4	3	3	2	12	27	2,250
2.	Operasi infiltrasi asing.		4	3	5	12	37	3,083
3.	Meningkatnya aktivitas intelijen ilegal.		3	3	6	12	39	3,250
4.	Eskalasi konflik kawasan.	2	2	4	4	12	34	2,833

e) Perhitungan skor dari faktor-faktor internal dan eksternal.

Melakukan perhitungan skor dari *Internal Factor Analysis Summary* (IFAS) dan *External Factor Analysis Summary* (EFAS), sebagai berikut:

Tabel 18. *Internal Factor Analysis Summary* (IFAS)

Journal of Industrial Engineering & Management Research
http://www.jiemar.org e-ISSN : 2722-8878
Vol. 7 No. 2 – April 2026

No	*Internal factor Analysis Summary* (IFAS)	Bobot	Rating	Skor
	Strength			
1.	Kompetensi prajurit TNI AL.	0,295	3,333	0,983
2.	Sistem komando dan kendali (C2) yang jelas dan terpusat.	0,250	3,083	0,771
3.	Pengalaman operasional dalam pengamanan Area Objek Vital Strategis.	0,235	3,000	0,705
4.	Integrasi sistem pengawasan maritim.	0,220	2,417	0,532
	Total *Strength*			**2,991**
	Weakness			
1.	Keterbatasan interoperabilitas.	0,273	3,250	0,887
2.	Ketergantungan pada komponen impor.	0,242	3,167	0,766
3.	Kerentanan terhadap ancaman siber.	0,258	3,083	0,795
4.	Keterbatasan alokasi sumber daya.	0,227	2,833	0,643
	Total *Weakness*			**3,092**

Tabel 19. *External Factor Analysis Summary* (EFAS)

No	*External factor Analysis Summary* (EFAS)	Bobot	Rating	Skor
	Opportunity			
1.	Perkembangan teknologi pertahanan.	0,288	3,250	0,936
2.	Dukungan kebijakan nasional.	0,200	2,417	0,483
3.	Kerja sama pertahanan (multilateral dan bilateral).	0,272	3,083	0,839
4.	Peningkatan kesadaran nasional terhadap ancaman siber dan hibrida.	0,240	2,917	0,700
	Total *Opportunity*			**2,958**
	Threat			
1.	Meningkatnya ancaman siber.	0,230	2,250	0,518
2.	Operasi infiltrasi asing.	0,197	3,083	0,607
3.	Meningkatnya aktivitas intelijen ilegal.	0,311	3,250	1,011
4.	Eskalasi konflik kawasan.	0,262	2,833	0,742
	Total *Threat*			**2,878**

f) Menentukan koordinat SWOT.

Setelah mendapatkan nilai dari masing-masing aspek, maka dilakukan penentuan koordinat SWOT dengan menggunakan matriks koordinat sebagai berikut:

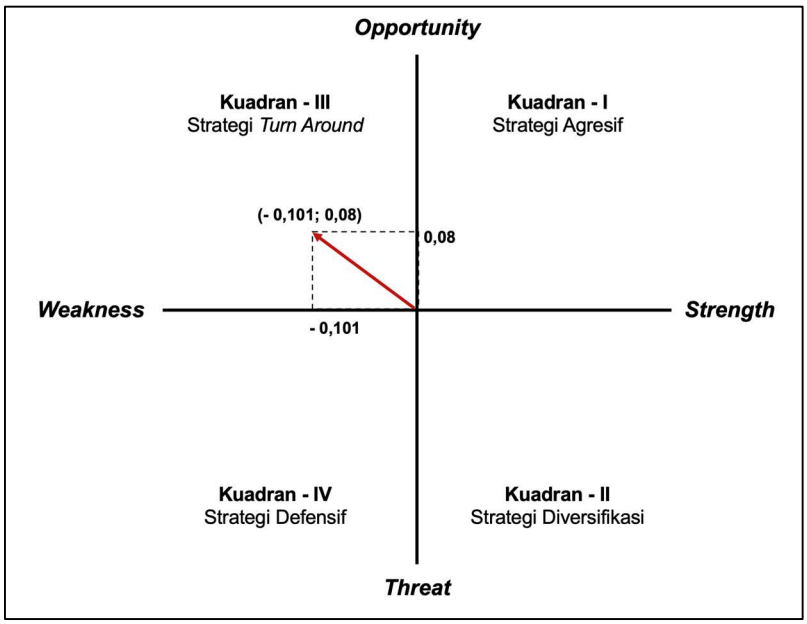
Tabel 20. Tabel Matriks Koordinat SWOT

INTERNAL (X)	NILAI	EKSTERNAL (Y)	NILAI
Strength	**2,991**	*Opportunity*	**2,958**
Weakness	**3,092**	*Threat*	**2,878**
Selisih	**- 0,101**	**Selisih**	**0,08**

g) Membuat grafik diagram SWOT.

Setelah mendapatkan analisa dari faktor-faktor yang mempengaruhi dari internal maupun eksternal, maka dapat diketahui kuadaran strategi terpilih dan matriks strategi untuk digunakan sebagai pemecahan masalah, seperti terlihat pada gambar berikut:

Journal of Industrial Engineering & Management Research
http://www.jiemar.org e-ISSN : 2722-8878
Vol. 7 No. 2 – April 2026



Gambar 2. Diagram SWOT

Dari hasil analisis SWOT diketahui bahwa hasil perhitungan berada pada Kuadran III (W - O), sehingga strategi yang digunakan adalah model Strategi *Turn Around.* Strategi ini menitikberatkan pada upaya untuk mengatasi kelemahan yang ada dan mengubah kondisi yang kurang menguntungkan menjadi lebih baik, melalui langkah-langkah perbaikan yang signifikan.

h) Menyusun matriks strategi SWOT

Strategi *turn around* pada tulisan ini dapat dilihat pada tabel matriks kombinasi strategi berikut:

Tabel 21. Matriks Strategi SWOT

Journal of Industrial Engineering & Management Research
http://www.jiemar.org e-ISSN : 2722-8878
Vol. 7 No. 2 – April 2026

IFAS / EFAS	Kekuatan (S)	Kelemahan (W)
	1. Kompetensi prajurit TNI AL (S1). 2. Sistem komando dan kendali (C2) yang jelas dan terpusat (S2). 3. Pengalaman operasional dalam pengamanan Area Objek Vital Strategis (S3). 4. Integrasi sistem pengawasan maritim (S4)	1. Keterbatasan interoperabilitas (W1). 2. Ketergantungan pada komponen impor (W2). 3. Kerentanan terhadap ancaman siber (W3). 4. Keterbatasan alokasi sumber daya (W4).
Peluang (O) 1. Perkembangan teknologi pertahanan (O1). 2. Dukungan kebijakan nasional (O2). 3. Kerja sama pertahanan (multilateral dan bilateral) (O3) 4. Peningkatan kesadaran nasional terhadap ancaman siber dan hibrida (O4)	STRATEGI S-O	**W1O1, W1O2, W1O3, W1O4** **W2O1, W2O2, W2O3, W2O4** **W3O1, W3O2, W3O3, W3O4** **W4O1, W4O2, W4O3, W4O4**
Ancaman (T) 1. Meningkatnya ancaman siber (T1). 2. Operasi infiltrasi asing (T2). 3. Meningkatnya aktivitas intelijen ilegal (T3). 4. Eskalasi konflik kawasan (T4).	STRATEGI S-T	STRATEGI W-T

Berdasarkan tabel 21 di atas, maka dapat dirumuskan 16 kombinasi strategi (W – O), sebagai berikut:

Tabel 22. Tabel Pembobotan Strategi

NO	RUMUSAN STRATEGI	SKOR AKHIR		
		W	O	HASIL
1.	W_1O_1	0,887	0,936	0,830
2.	$W_1 O_2$	0,887	0,483	0,428
3.	$W_1 O_3$	0,887	0,839	0,744
4.	$W_1 O_4$	0,887	0,700	0,621
5.	$W_2 O_1$	0,766	0,936	0,717
6.	$W_2 O_2$	0,766	0,483	0,370
7.	$W_2 O_3$	0,766	0,839	0,643
8.	$W_2 O_4$	0,766	0,700	0,536
9.	$W_3 O_1$	0,795	0,936	0,744
10.	$W_3 O_2$	0,795	0,483	0,384
11.	$W_3 O_3$	0,795	0,839	0,667
12.	$W_3 O_4$	0,795	0,700	0,557
13.	$W_4 O_1$	0,643	0,936	0,602
14.	$W_4 O_2$	0,643	0,483	0,311
15.	$W_4 O_3$	0,643	0,839	0,539
16.	$W_4 O_4$	0,643	0,700	0,450

Berdasarkan diagram dan matriks strategi SWOT di atas, maka strategi terpilih untuk memperkuat postur teknologi pertahanan di Area Objek Vital Strategis TNI AL, adalah W_1O_1, W_1O_3, W_2O_1 dan W_3O_1.

b. Pembahasan.

1) Penentuan prioritas pengembangan teknologi pertahanan menggunakan metode AHP.

Berdasarkan tahapan metode AHP yang telah dilakukan, struktur hierarki keputusan disusun dengan tujuan utama menentukan prioritas pengembangan teknologi pertahanan untuk mendukung perlindungan Area Objek Vital Strategis TNI AL. Pada tingkat Kriteria, ditetapkan tiga variabel utama yang merepresentasikan pertimbangan strategis dalam pembangunan kekuatan pertahanan, yaitu efektivitas tempur, ketahanan siber, dan biaya investasi. Hasil perbandingan berpasangan antar kriteria menunjukkan bahwa efektivitas tempur memiliki bobot tertinggi (0,57), diikuti oleh ketahanan siber (0,29), dan biaya investasi (0,14). Hal ini mengindikasikan bahwa dalam konteks perlindungan Area Objek Vital Strategis, kemampuan operasional dalam mendukung deteksi dan respons ancaman masih menjadi pertimbangan dominan, meskipun aspek ketahanan sistem terhadap serangan siber dan efisiensi anggaran tetap menjadi variabel penting dalam pengambilan keputusan strategis.

Pada tahap berikutnya dilakukan perbandingan Alternatif, yaitu C-ISR, *Cyber Resilience*, dan UAV terhadap masing-masing kriteria. Pada Kriteria Efektivitas Tempur, *Cyber Resilience* memperoleh bobot tertinggi (0,49), disusul C-ISR (0,31) dan UAV (0,20), yang menunjukkan bahwa dalam konteks operasi modern, perlindungan sistem dan jaringan dari gangguan siber dinilai lebih menentukan keberhasilan operasi dibandingkan platform fisik semata. Hasil serupa terlihat pada Kriteria Ketahanan Siber, di mana *Cyber Resilience* memperoleh nilai dominan (0,59), mencerminkan urgensi penguatan sistem pertahanan siber dalam menghadapi ancaman infiltrasi dan perang hibrida. Sementara itu, pada Kriteria Biaya Investasi, Cyber *Resilience* kembali menempati posisi tertinggi (0,49), yang mengindikasikan bahwa dari perspektif rasio manfaat terhadap biaya, pengembangan sistem ketahanan siber dinilai lebih efisien dibandingkan investasi besar pada sistem C-ISR atau UAV secara mandiri.

Sintesis keseluruhan bobot global menunjukkan bahwa *Cyber Resilience* memperoleh nilai prioritas tertinggi sebesar 0,52, diikuti oleh C-ISR sebesar 0,29 dan UAV sebesar 0,19. Hasil ini secara akademis menegaskan bahwa dalam konteks ancaman militer dan non-militer yang semakin berbasis teknologi dan informasi, penguatan ketahanan siber menjadi fondasi utama dalam membangun postur pertahanan Area Objek Vital Strategis TNI AL yang adaptif dan berkelanjutan. Tanpa sistem siber yang tangguh, efektivitas C-ISR dan UAV berpotensi terdegradasi akibat gangguan jaringan, jamming, atau serangan siber. Dengan demikian, prioritas pada Cyber Resilience bukan berarti mengesampingkan teknologi lainnya, melainkan menempatkannya sebagai lapisan fundamental dalam arsitektur pertahanan berbasis jaringan (*network-centric defense system*) guna meningkatkan kemampuan deteksi dini, respons presisi, dan daya tangkal terhadap ancaman asimetris di wilayah NKRI.

2) Rumusan strategi untuk memperkuat postur teknologi pertahanan Area Objek Vital Strategis menggunakan SWOT.

Berdasarkan diagram dan matriks strategi SWOT di atas, maka strategi terpilih untuk memperkuat postur teknologi pertahanan di Area Objek Vital Strategis TNI AL, adalah sebagai berikut:

a) Strategi Pertama (W_1O_1), mengatasi keterbatasan interoperabilitas sistem melalui pembangunan arsitektur ketahanan siber terpadu berbasis *network-centric defense system* dengan memanfaatkan perkembangan teknologi pertahanan digital.

b) Strategi Kedua (W_1O_3), meningkatkan interoperabilitas sistem pertahanan siber melalui kerja sama bilateral dan multilateral dalam bentuk standarisasi protokol keamanan jaringan, pertukaran informasi ancaman siber (*cyber threat intelligence sharing*), serta pelatihan bersama dalam operasi pertahanan siber.

c) Strategi Ketiga (W_2O_1), mengurangi ketergantungan pada komponen impor dengan mengembangkan kapabilitas industri pertahanan dalam negeri di bidang teknologi keamanan siber, termasuk pengembangan perangkat lunak enkripsi nasional, *firewall* militer, dan sistem monitoring jaringan mandiri.

d) Strategi Keempat (W_3O_1), memperkuat ketahanan siber AOVS melalui implementasi sistem pertahanan siber berlapis (*layered cyber defense*) yang memanfaatkan teknologi terkini.

Dalam rangka mewujudkan strategi di atas, maka dilaksanakan upaya-upaya untuk mengatasi semua pokok-pokok persoalan yang ditemukan, dengan mempertimbangkan landasan pemikiran dan faktor-faktor yang mempengaruhi (eksternal dan internal). Berdasarkan pendekatan-pendekatan dalam teori *Revolution in Military Affairs* (RMA) dan teori *Network-Centric Warfare*, maka dapat dirumuskan upaya-upaya yang akan dilaksanakan, sebagai berikut:

1) Upaya Strategi – 1. Untuk mewujudkan strategi – 1, yaitu mengatasi keterbatasan interoperabilitas sistem melalui pembangunan arsitektur ketahanan siber terpadu berbasis *network-centric defense system* dengan memanfaatkan perkembangan teknologi pertahanan digital, maka dilakukan upaya-upaya sebagai berikut:

a) Menyusun blueprint arsitektur ketahanan siber terpadu di Area Objek Vital Strategis berbasis *network-centric defense system.*

b) Mengembangkan dan menerapkan standar interoperabilitas serta protokol keamanan jaringan militer.

c) Membangun *Cyber Security Operation Center* terintegrasi di lingkungan TNI AL.

d) Mengimplementasikan sistem pertahanan siber berlapis (*layered cyber defense*).

e) Meningkatkan kapasitas sumber daya manusia dalam operasi berbasis jaringan dan keamanan siber.

2) Upaya Strategi – 2. Untuk mewujudkan strategi – 2, yaitu meningkatkan interoperabilitas sistem pertahanan siber melalui kerja sama bilateral dan multilateral dalam bentuk standarisasi protokol keamanan jaringan, pertukaran informasi ancaman siber (*cyber threat intelligence sharing*), serta pelatihan bersama dalam operasi pertahanan siber, maka dilakukan upaya-upaya sebagai berikut:

a) Menyusun standar protokol keamanan siber.

b) Membangun mekanisme pertukaran intelijen ancaman siber.

c) Melaksanakan latihan bersama (*joint cyber defense exercise*) secara berkala.

d) Mendorong kerja sama alih teknologi dan pengembangan kapasitas keamanan siber.

e) Membentuk forum koordinasi keamanan siber maritim regional.

3) Upaya Strategi – 3. Untuk mewujudkan strategi – 3, yaitu mengurangi ketergantungan pada komponen impor dengan mengembangkan kapabilitas industri pertahanan dalam negeri di bidang teknologi keamanan siber, termasuk pengembangan perangkat lunak enkripsi nasional, *firewall* militer, dan sistem monitoring jaringan mandiri, maka dilakukan upaya-upaya sebagai berikut:

a) Membangun ekosistem penelitian dan pengembangan (Litbang) keamanan siber pertahanan berbasis kolaborasi triple helix (pemerintah–industri–akademisi).

b) Mendorong program alih teknologi dan *co-development* dengan mitra strategis.

c) Menyusun standar nasional keamanan siber militer dan sertifikasi produk pertahanan dalam negeri.

d) Mengembangkan pusat uji dan validasi keamanan siber pertahanan (*cyber security testbed laboratory*).

e) Meningkatkan kapasitas sumber daya manusia industri pertahanan siber.

4) Upaya Strategi – 4. Untuk mewujudkan strategi – 4, yaitu memperkuat ketahanan siber di Area Objek Vital Strategis TNI AL melalui implementasi sistem pertahanan siber berlapis (*layered cyber defense*) yang memanfaatkan teknologi terkini, maka dilakukan upaya-upaya sebagai berikut:

a) Menerapkan arsitektur pertahanan siber berlapis (*defense in depth*).

b) Mengintegrasikan sistem deteksi dan respons insiden berbasis Artificial Intelligence dan Machine Learning.

c) Membangun dan mengoperasikan *Cyber Security Operation Center*, khususnya di Area Objek Vital Strategis TNI AL.

d) Melaksanakan uji ketahanan siber secara berkala melalui *penetration testing* dan *red teaming exercise*.

e) Menyusun protokol manajemen krisis siber dan sistem redundansi jaringan (*redundancy and failover system*)

IV. KESIMPULAN

Berdasarkan uraian pemecahan masalah yang ditemukan, dapat disimpulkan beberapa hal sebagai berikut:

a. Hasil analisis AHP menunjukkan bahwa *Cyber Resilience* menjadi prioritas utama pengembangan teknologi pertahanan di Area Objek Vital Strategis TNI AL, karena memiliki bobot tertinggi dibandingkan C-ISR dan UAV. Hal ini menunjukkan bahwa dalam menghadapi ancaman militer dan non-militer berbasis teknologi, ketahanan siber merupakan fondasi utama yang menentukan efektivitas sistem pertahanan lainnya. Tanpa sistem siber yang kuat, kemampuan deteksi, pengawasan, dan respons tidak dapat berfungsi secara optimal.

b. Hasil analisis SWOT menempatkan strategi pada kuadran W–O (*turn around*), yang menekankan pemanfaatan peluang eksternal untuk mengatasi kelemahan internal. Strategi yang dirumuskan berfokus pada pembangunan arsitektur pertahanan siber terpadu, peningkatan interoperabilitas melalui kerja sama internasional, penguatan kemandirian industri pertahanan siber nasional, serta penerapan sistem pertahanan siber berlapis. Pendekatan ini diharapkan mampu memperkuat postur teknologi pertahanan di Area Objek Vital Strategis TNI AL secara terintegrasi, adaptif, dan berkelanjutan dalam menjaga kedaulatan NKRI.

REFERENSI

Alberts, D. S., Garstka, J. J., & Stein, F. P. (1999). *Network centric warfare: Developing and leveraging information superiority*. CCRP Publication Series.

Andrews, K. R. (1971). *The concept of corporate strategy*. Richard D. Irwin.

Glenn, R. W. (2009). Thoughts on hybrid conflict. *Small Wars Journal, 2*(1).

Hermawan, T., & Sutanto, R. (2022). Strategi pertahanan laut Indonesia dalam analisa ancaman dan kekuatan laut. *Jurnal Education and Development, 10*(2).

Krepinevich, A. F. (1992). *The military-technical revolution: A preliminary assessment*. Center for Strategic and Budgetary Assessments.

Owens, W. A. (2000). *Lifting the fog of war*. Farrar, Straus and Giroux.

Saaty, T. L. (1980). *The analytic hierarchy process: Planning, priority setting, resource allocation*. McGraw-Hill.

Toffler, A., & Toffler, H. (1993). *War and anti-war: Survival at the dawn of the 21st century*. Little, Brown and Company.

Undang-Undang Republik Indonesia Nomor 3 Tahun 2002 tentang Pertahanan Negara.

Undang-Undang Republik Indonesia Nomor 3 Tahun 2025 tentang Perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia.