JIGE 6 (4) (2025) 3273-3288
JURNAL ILMIAH GLOBAL EDUCATION
ejournal.nusantaraglobal.ac.id/index.php/jige
DOI: https://doi.org/10.55681/jige.v6i4.4833

Pemetaan Elemen Artificial Intelligence Sesuai Tiga Struktur Pertahanan: Operational, Tactical, Dan Strategic

Katherine Erika[1], Asep Adang Supriyadi[1], Ghazalie[1], Alradix Djansena[1]
[1] Indonesia Defense University, Jl. Salemba Raya No. 14, Jakarta 10430, Indonesia
**Corresponding author email:* katherine.erika@doktoral.idu.ac.id

Article Info

Article history:

Received October 22, 2025
Approved November 25, 2025

Keywords:

Artificial Intelligence; Defense Policy; Machine Learning; Neural Networks; Natural Language Processing; Robotics; Cyber Defense

ABSTRACT

This research analyzes the AI components Machine Learning, Neural Networks, Natural Language Processing, and Robotics and their allocation within Indonesia's three-tiered defense structure: operational, tactical, and strategic. This paper explores the integration of Artificial Intelligence (AI) into Indonesia's national defense policy, examining opportunities, challenges, and strategic implications. AI's transformative potential spans operational efficiency, strategic decision-making, and robust cyber security. This research employs a qualitative approach, examining previously published scholarly articles across various journals to understand the multifaceted dimensions of Artificial Intelligence. Key challenges are identified: infrastructure requirements, dependence on foreign technology, ethical concerns including data bias, and transparency in AI-driven decisions. A comprehensive policy framework is proposed, emphasizing strategic partnerships, robust data governance, and ethical guidelines to mitigate risks and maximize AI's benefits. The discussion highlights the crucial need for AI-specific hardware investment, including microchips and supercomputing infrastructure, while advocating for fostering local expertise and reducing reliance on external providers. The paper argues that AI empowers Indonesia to enhance military capabilities, strengthen cyber defenses, and optimize strategic decision-making. However, a balanced approach that prioritizes ethical considerations, transparency, and a clearly defined command chain is crucial for responsible AI deployment. This research serves as a roadmap for Indonesian policymakers to navigate the complex landscape of AI in national defense, ensuring sovereignty, security, and ethical alignment in the digital age. The implementation of AI is not just an option but a strategic imperative.

.

ABSTRAK

Penelitian ini menganalisis komponen Kecerdasan Buatan (AI) – Pembelajaran Mesin (Machine Learning), Jaringan Syaraf Tiruan (Neural Networks), Pemrosesan Bahasa Alami (Natural Language Processing), dan Robotika – serta alokasinya dalam struktur pertahanan tiga tingkat Indonesia: operasional, taktis, dan strategis. Makalah ini mengeksplorasi integrasi AI ke dalam kebijakan pertahanan nasional Indonesia, dengan memeriksa peluang, tantangan, dan implikasi strategisnya. Potensi transformatif AI mencakup efisiensi operasional, pengambilan keputusan strategis, dan keamanan siber yang kuat. Penelitian ini menggunakan pendekatan kualitatif, dengan memeriksa artikel ilmiah yang diterbitkan sebelumnya di berbagai jurnal untuk memahami dimensi multifaset dari Kecerdasan Buatan. Tantangan utama yang diidentifikasi meliputi: persyaratan infrastruktur, ketergantungan pada teknologi asing, masalah etika termasuk bias data, dan transparansi dalam keputusan berbasis AI. Kerangka kebijakan komprehensif diusulkan, menekankan kemitraan strategis, tata kelola data yang kuat, dan pedoman etika untuk mengurangi risiko dan memaksimalkan manfaat AI. Diskusi menyoroti kebutuhan krusial akan investasi perangkat keras khusus AI, termasuk microchip dan infrastruktur superkomputer, sambil mengadvokasi peningkatan keahlian lokal dan mengurangi ketergantungan pada penyedia eksternal. Makalah ini berpendapat bahwa AI memberdayakan Indonesia untuk meningkatkan kemampuan militer, memperkuat pertahanan siber,

dan mengoptimalkan pengambilan keputusan strategis. Namun, pendekatan seimbang yang memprioritaskan pertimbangan etika, transparansi, dan rantai komando yang jelas sangat penting untuk penerapan AI yang bertanggung jawab. Penelitian ini berfungsi sebagai peta jalan bagi para pembuat kebijakan Indonesia untuk menavigasi lanskap kompleks AI dalam pertahanan nasional, memastikan kedaulatan, keamanan, dan keselarasan etika di era digital. Implementasi AI bukan sekadar pilihan, melainkan keharusan strategis.

How to cite: Erika, K., Supriyadi, A. A., Ghazalie, G. ,& Djansena, A. (2025). Pemetaan Elemen Artificial Intelligence Sesuai Tiga Struktur Pertahanan: Operational, Tactical, Dan Strategic. *Jurnal Ilmiah Global Education*, *6*(4), 3273–3288. https://doi.org/10.55681/jige.v6i4.4833

PENDAHULUAN

Perkembangan teknologi kecerdasan buatan (*Artificial Intelligence/* AI) telah mengubah lanskap keamanan global, termasuk pertahanan negara. AI tidak lagi merupakan alat pendukung industri teknologi, tetapi menjadi elemen kunci banyak bidang, termasuk strategi militer (Rashid et al., 2023). Integrasi AI dalam pertahanan tidak hanya mempercepat keputusan, tetapi juga meningkatkan efektivitas dan efisiensi berbagai aspek pertahanan nasional (Hadlington et al., 2023). Namun, keberhasilan implementasi AI dalam sistem pertahanan sangat bergantung pada pemahaman mengenai komponen utama AI dan bagaimana tiap komponen dioptimalkan di berbagai struktur pertahanan. Tujuan penelitian ini adalah: (1) memetakan elemen AI yang harus diutamakan pada tiap struktur pertahanan negara, (2) mengkaji penggunaan AI dalam keamanan siber nasional, dan (3) mengkaji keperluan infrastruktur AI untuk investasi negara.

Dalam pertahanan negara, terdapat tiga struktur utama yang menjadi kerangka penyusunan strategi dan pelaksanaan, yaitu *operation*, *tactical*, dan *strategy*. Masing-masing struktur memiliki peran berbeda namun saling terkait. Struktur *operation* fokus pada tingkat eksekusi lapangan, di mana tugas dijalankan sesuai perintah. Operasi mencakup patroli perbatasan, pengintaian, pertempuran langsung, dan logistik. Efektivitas bergantung pada kecepatan pengambilan keputusan dan sumber daya. Pada tingkat *tactical*, fokus utama adalah perencanaan jangka pendek, penempatan pasukan, strategi pertempuran, dan pemanfaatan teknologi situasi dinamis. Pengambilan keputusan *tactical* bergantung pada analisis intelijen dan komunikasi cepat. Sementara itu, *strategy* adalah level tertinggi struktur pertahanan dan fokus pada perencanaan jangka panjang serta kebijakan pertahanan nasional. Aspek ini mencakup perumusan doktrin, kerja sama internasional, modernisasi alutsista serta teknologi.

AI memiliki empat komponen utama yang berperan penting dalam dunia pertahanan: *Machine Learning* (ML), *Neural Networks* (NN), *Natural Language Processing* (NLP), dan *Robotics* (Baptista et al., 2013). Dalam hal ini, ML memainkan peran penting dalam analisis data besar (*big data*), memungkinkan sistem untuk mempelajari pola dan membuat prediksi akurat. Contoh pengaplikasian ML misalnya dalam pengenalan target otomatis, di mana sensor dan kamera pesawat tanpa awak (UAV) atau kendaraan tempur dapat mengidentifikasi musuh dengan akurat. NN berfungsi memproses data kompleks, mengenali pola, serta mengambil keputusan otonom. Dengan mengintegrasikan NN dengan teknologi *Convolutional Neural Networks* (CNN), militer dapat menganalisis gambar satelit atau drone untuk identifikasi musuh, perubahan mencurigakan, atau aktivitas militer tidak biasa. NN juga digunakan dalam perencanaan strategi dan simulasi skenario perang berdasarkan data historis dan parameter yang ditentukan. NLP memungkinkan sistem AI untuk menganalisis berbagai bahasa, yang berguna dalam intelijen dan diplomasi militer. Misalnya, NLP memungkinkan penyaringan ribuan laporan intelijen,

percakapan radio, dan media sosial untuk menemukan informasi ancaman. NLP juga digunakan dalam *chatbot* militer, untuk bertukar informasi taktis dengan cepat dalam sistem darurat. *Robotics* memiliki peran penting dalam pengembangan drone militer, kendaraan tempur otomatis, serta robot penyelamat darurat. Robot berguna dalam penjinakan bom (*Explosive Ordnance Disposal*) untuk mengamankan area yang dipasangi ranjau atau bom rakitan tanpa membahayakan personel. Selain itu, robot juga berguna dalam operasi pengintaian medan perang, membantu tentara mengumpulkan informasi *real-time* tanpa masuk zona bahaya.

Setiap komponen AI memiliki karakteristik unik yang dapat disesuaikan dengan struktur pertahanan Indonesia: *operation, tactical*, dan *strategy*. Sebagai contoh, ML dan NN dapat digunakan dalam analisis strategi jangka panjang, NLP dapat membantu dalam analisis komunikasi intelijen di tingkat taktis, sementara Robotics dapat diterapkan dalam sistem pertahanan operasional seperti penggunaan drone dan kendaraan otonom dalam operasi militer (Rasch et al., 2003). Oleh karena itu, pemerintah Indonesia harus menentukan bagaimana setiap komponen AI dapat dialokasikan secara optimal dalam setiap tingkatan struktur pertahanan guna meningkatkan efektivitas serta responsivitas sistem pertahanan nasional.

Selain mendukung strategi pertahanan, AI juga memiliki peran krusial dalam menjaga keamanan siber (cyber security). Keamanan siber dalam konteks pertahanan negara dapat ditinjau dari dua aspek utama: offense dan defense (Deng et al., 2022). Dalam sisi *offense*, AI dapat digunakan untuk mengidentifikasi kelemahan lawan dan mengeksploitasi celah mereka. Sementara dari sisi *defense*, AI dapat meningkatkan deteksi dan mitigasi serangan siber terhadap infrastruktur kritis negara. Implementasi AI dalam keamanan siber juga dapat dikategorikan berdasarkan aspek perangkat keras (hardware) dan perangkat lunak (software). Dari sisi perangkat keras, pengembangan AI membutuhkan komponen khusus seperti prosesor AI yang memungkinkan analisis data *real-time* dan efisien (Berggren et al., 2020). Sementara itu, dari sisi perangkat lunak, AI memerlukan algoritma canggih yang dapat mengolah data dalam jumlah besar secara cepat untuk mendeteksi serta merespons ancaman siber secara otomatis (Wei et al., 2020). Penerapan AI untuk keamanan siber berguna secara *offense* dan *defense*.

Namun demikian, meskipun AI menawarkan berbagai manfaat, implementasinya tetap menghadapi berbagai tantangan, terutama dalam aspek infrastruktur. Pembuatan AI sangat bersifat *infrastructure-intensive*, baik dari sisi perangkat lunak maupun perangkat keras (Deng et al., 2022). Selain itu, keamanan data menjadi tantangan utama, memerlukan sistem perlindungan canggih untuk menjaga kerahasiaan informasi pertahanan negara. Dari segi perangkat lunak, AI memerlukan data dalam jumlah besar. Sementara itu, dari sisi perangkat keras, AI membutuhkan investasi infrastruktur besar karena memerlukan komputasi tinggi, data berskala masif, serta perangkat keras khusus seperti AI chips dan server, *data center*, juga sistem pendinginan yang kompleks. Pengembangan AI bergantung pada rantai pasok global yang melibatkan berbagai negara (Park & Lee, 2020). Ketergantungan ini menjadi tantangan serius bagi Indonesia dalam membangun kemandirian teknologi pertahanan berbasis AI.

Selain tantangan infrastruktur, AI dalam pertahanan juga menghadapi berbagai isu etika dan transparansi. Salah satu permasalahan utama dalam penggunaan AI di sektor militer adalah bias data dan kurangnya transparansi dalam pengambilan keputusan (Schraagen, 2023). Keputusan berbasis AI dapat terpengaruh bias dalam data, sehingga menghasilkan kesimpulan yang tidak akurat atau bahkan diskriminatif. Selain itu, aspek akuntabilitas dalam sistem AI juga menjadi tantangan yang harus diperhatikan. Dalam konteks pertahanan, penting untuk mengetahui siapa yang bertanggung jawab atas keputusan yang dihasilkan oleh AI, terutama jika keputusan tersebut berdampak pada keselamatan manusia atau strategi militer nasional. Lebih lanjut, perdebatan mengenai etika penggunaan AI dalam konteks militer sering kali berfokus

pada pengembangan senjata otonom yang dapat mengambil keputusan sendiri dalam melakukan serangan (Meerveld et al., 2023). Meskipun AI memiliki potensi besar dalam meningkatkan efisiensi dan efektivitas operasi militer, penggunaannya harus tetap memperhatikan prinsip-prinsip etika dan hukum humaniter internasional.

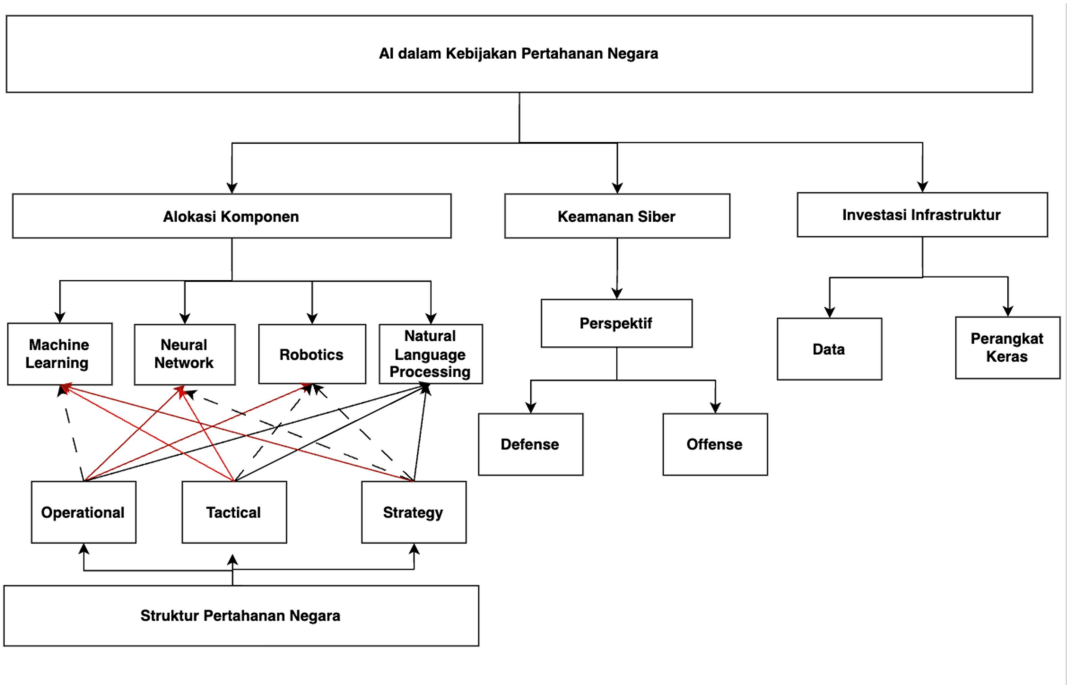
METODE

Metode penelitian yang digunakan dalam studi ini adalah studi literatur secara selektif, dengan hanya menggunakan artikel-artikel jurnal ilmiah yang terindeks Scopus dan berasal dari kuartil 1 (Q1) dan kuartil 2 (Q2). Pendekatan ini dipilih untuk memastikan bahwa sumber-sumber yang dianalisis memiliki kualitas akademik tinggi, relevan secara substansial, dan telah melalui proses review yang ketat. Dengan demikian, hasil analisis yang diperoleh diharapkan memiliki tingkat validitas dan kredibilitas yang tinggi dalam menjelaskan fenomena yang diteliti.

HASIL DAN PEMBAHASAN

Pengembangan kecerdasan buatan (AI) adalah sebuah prestasi besar di abad ini, yang sangat membantu dalam analisis masalah kompleks apabila diterapkan dengan benar (Johnson, 2021). Salah satu sektor yang dapat sangat diuntungkan dengan penggunaan AI adalah sektor militer karena kompleksitasnya yang tinggi. Namun penggunaan AI untuk aplikasi militer adalah salah satu bidang yang paling menuntut dari segi sumber daya, baik dalam aspek perangkat keras maupun perangkat lunak, karena persyaratan pertahanan yang tidak sedikit. Proses ini membutuhkan investasi yang sangat besar karena kompleksitas teknologi yang terlibat, baik dalam pembuatan microchip canggih yang harus diimpor dari luar negeri maupun dalam pengumpulan dan pengolahan data dalam jumlah yang masif. AI dalam bidang pertahanan memerlukan komputer berkecepatan tinggi, prosesor khusus, dan sistem penyimpanan data yang mampu menangani jumlah informasi yang sangat besar dalam waktu nyata. Saat ini, pengembangan AI bagi kegunaan umum saja masih termasuk berada pada tahap dini, maka pengembangan AI untuk aplikasi militer yang memiliki data lebih terbatas dan dirahasiakan tentu lebih menantang. Negara maju seperti Amerika Serikat saja saat ini baru dapat mengaplikasikan AI secara "sempit" untuk kegunaan militer, yaitu untuk kesadaran situasional, pertahanan siber, logistik, command and control, juga sistem otomasi tak berawak (Mori, 2018). Namun, teknologi semacam ini tidak dapat diproduksi dengan mudah dan sering kali membutuhkan komponen yang harus diimpor dari luar negeri. Namun demikian, tidak dipungkiri bahwa teknologi AI menawarkan potensi yang sangat besar bagi pertahanan negara dan tidak mengintegrasikan teknologi AI dalam pertahanan negara dapat menjadi suatu kesalahan yang fatal bagi Indonesia.

Dalam dunia pertahanan modern, kecerdasan buatan (AI) memainkan peran penting dalam tiga tingkat struktur pertahanan: operasi (operation), taktik (tactical), dan strategi (strategy). AI terdiri dari empat komponen utama: Robotics, Neural Networks, Machine Learning, dan Natural Language Processing (NLP). Penggunaan AI dalam pertahanan bergantung pada tingkat struktur yang diterapkan dan teknologi AI yang paling sesuai untuk setiap tingkatannya.



Gambar 1. Pemetaan Elemen AI dalam Pertahanan Nasional

Pada bagian alokasi komponen, garis merah: dominan, garis hitam: penunjang, garis putus-putus: kurang relevan

Pada tingkat operasional, Robotics dan Neural Networks menjadi komponen utama dalam penerapan AI. Robotics digunakan dalam berbagai sistem senjata otonom, kendaraan tak berawak, serta sistem pengawasan yang dapat beroperasi di medan perang tanpa campur tangan manusia. Neural Networks memungkinkan analisis cepat terhadap data yang dikumpulkan dari sensor, drone, dan satelit untuk memberikan respons yang tepat dalam situasi pertempuran. Dalam konteks ini, pemrosesan informasi secara real-time menjadi faktor kunci dalam pengambilan keputusan cepat di medan perang, di mana Internet of Things (IoT) dan teknologi analitik real-time berperan penting dalam mendukung respons otomatis dan adaptif (Tien, 2017).

Pada tingkat taktis, Neural Networks dan Machine Learning menjadi teknologi utama yang digunakan untuk mendukung pengambilan keputusan berbasis data. Neural Networks memungkinkan analisis pola pergerakan musuh, mengidentifikasi titik lemah dalam pertahanan, serta mengoptimalkan strategi pertempuran. Machine Learning membantu dalam pengembangan sistem pendukung keputusan yang memungkinkan komandan untuk membuat keputusan yang lebih akurat berdasarkan informasi yang tersedia. AI telah terbukti mampu mengidentifikasi pola dalam taktik lawan dan menghasilkan strategi yang tidak dapat dibedakan dari strategi manusia, sebagaimana dibuktikan dalam penelitian tentang model TacticAI dalam sepak bola (Wang et al., 2024). Pendekatan ini mencakup Information Fusion dan Situation Awareness untuk meningkatkan persepsi medan perang serta Human-Machine Interface guna mengoptimalkan interaksi antara sistem AI dan personel militer (Galán, Carrasco, & LaTorre, 2022). Selain itu, AI dalam konteks taktis juga berkontribusi dalam pelatihan militer dengan menggunakan simulasi berbasis AI untuk meningkatkan kesiapan tempur pasukan (Johnson & Valente, 2009). Penelitian dalam taktik militer menunjukkan bahwa meskipun AI dapat memberikan wawasan berbasis data, masih ada keterbatasan dalam menghasilkan strategi presisi tinggi dalam lingkungan yang dinamis dan melibatkan banyak interaksi agen (Roccetti, Tenace, & Cappiello, 2024). Namun, AI tetap berguna dalam mengolah data dari berbagai sensor,

membangun kesadaran situasional, serta memberikan rekomendasi dalam sistem pendukung keputusan. Dalam operasi udara, misalnya, salah satu tantangan utama adalah bahwa banyak penelitian asumsi tentang pertempuran udara mengandalkan informasi sempurna, padahal dalam kondisi nyata, sensor memiliki keterbatasan yang menyebabkan informasi yang tidak lengkap atau tidak akurat (Reinisch, Strohal, & Stütz, 2023). Oleh karena itu, integrasi AI yang adaptif dalam lingkungan informasi yang terbatas menjadi krusial dalam pengambilan keputusan taktis.

Pada tingkat strategis, Machine Learning memiliki peran dominan dalam perencanaan jangka panjang dan simulasi skenario masa depan. Sistem berbasis AI dapat menganalisis data historis serta memprediksi tren geopolitik dan ancaman potensial di masa depan. Meskipun AI dapat memberikan wawasan strategis, penerapan teknologi pada tingkat ini masih terbatas dalam pengambilan keputusan yang memerlukan kapasitas empati manusia, sehingga keputusan strategis kemungkinan besar tetap berada di tangan manusia (Reis et al., 2021). Perbedaan utama antara pengambilan keputusan manusia dan AI terletak pada faktor-faktor seperti spesifikasi ruang pencarian keputusan, interpretabilitas hasil, dan kecepatan serta replikabilitas proses pengambilan keputusan (Shrestha, Ben-Menahem, & Von Krogh, 2019). Selain itu, AI masih menghadapi kesulitan dalam menerapkan logika prediktif yang mempertimbangkan ketidakpastian dan preferensi manusia dalam pengambilan keputusan (Pomerol, 1997). Oleh karena itu, kombinasi antara AI dan keputusan manusia menjadi pendekatan optimal dalam strategi pertahanan. Oleh karena itu, AI di tingkat strategi lebih berfungsi sebagai alat bantu dalam proses perencanaan dan analisis risiko.

Pada ketiga struktur pertahanan ini, NLP dapat menjadi komponen penunjang yang sangat berharga. NLP membantu dalam analisis komunikasi intelijen, pemrosesan dokumen strategis, serta memahami informasi dari berbagai sumber bahasa asing yang dapat digunakan dalam operasi militer. NLP juga dapat mendokumentasikan seluruh jejak komunikasi untuk dipelajari di model AI selanjutnya. Dengan demikian, penerapan AI dalam struktur pertahanan harus dilakukan secara menyeluruh dengan mempertimbangkan kebutuhan spesifik dari masing-masing tingkat operasi.

Pengaplikasian AI yang benar akan memiliki peran yang krusial dalam meningkatkan keamanan siber bagi pertahanan militer. Sangat disayangkan bahwa semakin berkembangnya teknologi, maka ancaman siber pun semakin berkembang. Misalnya, sistem AI berbasis arsitektur cloud-edge-terminal memberikan kemampuan AI yang lebih ampuh dan cepat, namun hal ini juga meningkatkan kerentanan pertahanan siber program AI tersebut mengingat arsitekturnya yang berlapis (Zhang et al., 2025). Hal ini menggarisbawahi sangat dibutuhkannya pertahanan siber di kota-kota modern yang semakin rentan, karena sistem pertahanan siber saat ini belum mampu mendeteksi serangan siber berlapis karena keterbatasan kapasitas dan efisiensi (Jia et al., 2023). Saat ini, pertahanan siber untuk pelayanan online saja masih rapuh dan mahal mengingat perkembangan serangan siber yang begitu pesat dan bertubi-tubi (Zhou et al., 2020). AI digunakan untuk mendeteksi ancaman dengan cepat, mengidentifikasi pola serangan yang mencurigakan, serta memberikan respons otomatis dalam menghadapi serangan siber.

Dalam pengembangannya, AI memerlukan pelatihan dan pengujian data yang sangat besar agar mampu mengenali berbagai jenis ancaman yang terus berkembang. Data training yang digunakan harus mencakup berbagai skenario serangan siber, termasuk malware, phishing, serta serangan denial-of-service (DDoS), agar sistem AI dapat mengidentifikasi dan merespons ancaman dengan lebih akurat. Setelah melalui proses training, sistem AI kemudian diuji dengan data testing yang belum pernah dilihat sebelumnya untuk mengukur keefektifannya dalam mengenali dan menangani ancaman secara real-time. Adversarial attacks pada model AI dapat

terjadi pada tahap pelatihan maupun pengujian. Pada tahap pelatihan, serangan dapat dilakukan dengan memodifikasi dataset, manipulasi label, atau manipulasi fitur input, meskipun jarang terjadi di dunia nyata. Sebaliknya, pada tahap pengujian, terdapat dua jenis serangan utama: white-box dan black-box. Perbedaan utama antara serangan black-box dan white-box pada AI terletak pada akses informasi: white-box attack memungkinkan penyerang mengetahui algoritma, parameter, dan struktur model target untuk menghasilkan serangan yang lebih akurat, sedangkan black-box attack dilakukan tanpa informasi internal model, hanya mengandalkan perilaku keluaran untuk menyusun strategi serangan.Serangan white-box lebih efektif karena penyerang memiliki akses penuh terhadap parameter model, sementara serangan black-box lebih relevan dalam skenario dunia nyata karena tidak memerlukan akses langsung terhadap model (Gutierrez et al., 2019).

Seperti halnya menganalisis pembangunan AI dapat dilihat dari sudut pandang perangkat keras maupun perangkat lunak (program), penggunaan AI bagi pertahanan keamanan siber negara pun dapat ditinjau dari sudut pandang perangkat keras maupun perangkat lunak. Dari sudut pandang perangkat keras, menjalankan AI bagi sistem pertahanan siber memerlukan infrastruktur yang sangat kompleks. Seperti yang telah dijelaskan, diperlukan GPU dan TPU yang dioptimalkan untuk pembelajaran mesin agar AI dapat menganalisis pola serangan dengan cepat dan efisien. Namun, sebagian besar komponen ini harus diimpor dari luar negeri, seperti prosesor dari Amerika Serikat atau microchip dari Taiwan dan Korea Selatan. Ketergantungan pada teknologi impor ini menimbulkan risiko keamanan, di mana ada kemungkinan bahwa perangkat keras yang digunakan dapat disusupi dengan backdoor atau firmware yang telah dimodifikasi untuk tujuan spionase (Gjesvik & Willer, 2024). Hal ini dapat menyebabkan sistem pertahanan siber rentan terhadap serangan dari aktor negara atau kelompok peretas yang memiliki akses terhadap komponen yang digunakan dalam sistem AI militer. Mengantisipasi resiko ini sama sekali tidak termasuk berlebihan mengingat beberapa bulan lalu perangkat komunikasi pasukan Hizbullah telah dibajak dan ditanam peledak, yang diduga dilakukan oleh Israel.

Dari sudut pandang perangkat lunak, keamanan siber dalam konteks pertahanan militer dapat dikategorikan menjadi dua aspek utama, yaitu offense (penyerangan) dan defense (pertahanan). Kedua aspek utama pertahanan siber ini dapat diuntungkan dengan adanya AI, akan tetapi aspek defense (pertahanan) akan lebih diuntungkan dengan adanya AI. Hal ini karena saat ini aspek offense (penyerangan) lebih banyak dilakukan oleh mesin sementara aspek defense (pertahanan) lebih banyak dilakukan oleh manusia, mengingat aspek offense (penyerangan) dapat dilakukan tanpa pemahaman kontekstual, sementara aspek defense (pertahanan) masih memerlukan pemahaman kontekstual untuk membedakan ancaman dan bukan, sehingga masih memerlukan tenaga manusia. Oleh karena itu, dengan hadirnya AI yang dapat lebih memahami pemahaman kontekstual, aspek defense (pertahanan) akan jauh lebih terbantu (Schneider, 2018).

Dari aspek offense, AI dapat digunakan untuk melakukan operasi siber ofensif seperti penetrasi sistem lawan, penggalian data intelijen, serta penyebaran serangan otomatis yang dapat melumpuhkan infrastruktur siber musuh. AI dapat membantu dalam analisis kerentanan sistem lawan, merancang eksploitasi yang lebih efektif, serta mengotomatisasi penyebaran malware yang dapat merusak sistem pertahanan lawan. Kemampuan AI untuk mengolah data dalam jumlah besar memungkinkan identifikasi titik lemah yang dapat dimanfaatkan dalam operasi ofensif. Di sisi lain, defense berfokus pada perlindungan sistem dari serangan siber yang dilakukan oleh aktor jahat. AI dapat digunakan untuk memonitor lalu lintas jaringan, mendeteksi anomali yang mencurigakan, serta merespons serangan sebelum merusak sistem

secara signifikan. Sistem berbasis AI dapat menerapkan deteksi intrusi otomatis, melakukan analisis perilaku pengguna, serta memperkuat enkripsi data untuk memastikan bahwa informasi sensitif tidak mudah diakses oleh pihak yang tidak berwenang. Dengan pembelajaran mesin, AI juga mampu meningkatkan kemampuannya dari waktu ke waktu, menjadikannya lebih efektif dalam menghadapi ancaman baru yang terus berkembang.

Secara singkatnya, Truong, Diep dan Zalinka (2020) menjabarkan bahwa dalam pertahanan siber, AI dapat digunakan untuk mendeteksi dan mencegah berbagai ancaman digital seperti malware, yaitu program berbahaya yang bisa merusak perangkat atau mencuri data, baik pada komputer maupun Android. AI juga membantu mengenali upaya penyusupan ke dalam jaringan dengan mendeteksi aktivitas mencurigakan. Selain itu, AI sangat efektif dalam menangkal phishing, yaitu penipuan melalui email atau situs web palsu yang berusaha mencuri informasi pribadi, serta spam yang menyebarkan tautan berbahaya di media sosial dan email. Untuk serangan yang lebih canggih seperti Advanced Persistent Threats (APTs), AI mampu menganalisis pola aktivitas mencurigakan yang dilakukan secara diam-diam dalam jangka panjang. AI juga bisa mengenali situs web berbahaya yang dibuat secara otomatis oleh peretas menggunakan Domain Generation Algorithms (DGAs), sehingga membantu mencegah serangan sebelum terjadi. Dengan kecerdasannya dalam mengenali pola ancaman yang terus berkembang, AI membuat sistem keamanan siber lebih kuat dan responsif dalam melindungi data serta infrastruktur digital.

Salah satu jenis serangan siber yang dapat ditangani oleh AI adalah serangan DDoS (Distributed Denial-of-Service). Serangan ini bertujuan untuk membanjiri sistem target dengan lalu lintas yang sangat tinggi hingga membuat layanan menjadi tidak dapat diakses. AI dapat digunakan untuk mendeteksi pola serangan DDoS secara real-time, mengidentifikasi sumber lalu lintas berbahaya, serta mengaktifkan mekanisme mitigasi secara otomatis. Dengan menggunakan model pembelajaran mesin yang telah dilatih pada data lalu lintas jaringan yang luas, AI dapat membedakan antara lalu lintas normal dan lalu lintas serangan dengan tingkat akurasi yang tinggi, memungkinkan respons yang lebih cepat dan efektif dalam menanggulangi ancaman ini. Telah dibuktikan bahwa antisipasi serangan DDoS yang dini menciptakan sistem pertahanan siber yang lebih efektif, hal ini dapat dilakukan dengan antisipasi berbagai mekanisme komunikasi dan pengambilan keputusan dalam program DDoS, baik dalam aspek pertahanan maupun penyerangan siber (Khalaf et al., 2019).

Selain DDoS, AI juga dapat menangani serangan malware dan phishing yang semakin canggih. Serangan berbasis malware dapat bersembunyi dalam sistem selama berbulan-bulan tanpa terdeteksi, mengumpulkan data rahasia, atau bahkan memanipulasi operasi militer (Sameen, Han & Hwang, 2020). AI dapat digunakan untuk menganalisis pola aktivitas file, mendeteksi perubahan mencurigakan dalam sistem, serta mengidentifikasi kode berbahaya sebelum dapat menyebabkan kerusakan. Dengan teknik deteksi berbasis perilaku, AI dapat mengenali ancaman yang tidak terdeteksi oleh sistem keamanan tradisional yang hanya mengandalkan basis data tanda tangan malware. Phishing juga merupakan ancaman besar dalam keamanan siber militer. Serangan ini sering kali menargetkan personel militer dengan mengelabui mereka agar memberikan informasi sensitif melalui email atau pesan yang tampak sah. AI dapat membantu dalam mendeteksi phishing dengan menganalisis isi pesan, pola komunikasi, serta sumber email untuk menentukan apakah suatu pesan berpotensi menjadi ancaman. Dengan menggunakan pemrosesan bahasa alami (NLP), AI dapat mengenali tanda-tanda phishing dalam pesan elektronik dan memberikan peringatan kepada pengguna sebelum mereka jatuh ke dalam perangkap peretas.

Penerapan AI dalam keamanan siber militer menghadirkan keuntungan yang signifikan dalam hal deteksi dan respons terhadap ancaman digital, namun juga menimbulkan tantangan besar terkait keamanan perangkat keras dan ketergantungan pada teknologi luar negeri. Meskipun AI mampu meningkatkan pertahanan siber dengan mendeteksi serangan lebih cepat dan lebih akurat, keamanan sistem tetap harus dijaga dengan memastikan bahwa perangkat keras yang digunakan tidak memiliki celah yang dapat dimanfaatkan oleh pihak luar. Selain itu, AI harus terus diperbarui dan dilatih dengan data terbaru agar mampu menghadapi ancaman siber yang semakin kompleks di masa depan. Oleh karena itu, pengembangan AI untuk keamanan siber militer harus dilakukan dengan strategi matang, baik secara teknologi, sumber daya, maupun infrastruktur pendukungnya. Salah satu tantangan utama dalam penerapan AI adalah transparansi dalam pengambilan keputusan, terutama dalam situasi kritis seperti pertahanan udara. Sebuah studi menunjukkan bahwa meskipun AI telah banyak diterapkan dalam pertempuran udara, masih terdapat kesenjangan dalam menjelaskan keputusan yang diambil oleh agen AI. Dengan mengembangkan sistem explainability berbasis reinforcement learning dan reward decomposition, AI dapat memberikan pemahaman lebih jelas tentang pola keputusan taktisnya, sehingga dapat dioptimalkan untuk meningkatkan efektivitas operasional dalam berbagai skenario tempur (Saldiran et al., 2024). Aspek transparansi dan edukasi juga merupakan satu komponen penting bagi pengembangan AI, karena kurangnya transparansi dan interpretabilitas AI dapat menyebabkan risiko seperti bias, ketidakadilan, dan penyalahgunaan pengambilan keputusan (Courtland, 2018; Zou & Schiebinger, 2018).

Setelah mengetahui komponen AI yang dapat diprioritaskan untuk diimplementasikan dalam struktur pertahanan Indonesia dan dampak AI bagi keamanan siber di Indonesia, penting bagi Indonesia untuk menghitung investasi yang harus dilakukan untuk membangun teknologi AI di Indonesia. Teknologi AI ini melibatkan beberapa komponen utama yang tidak dapat dilewatkan. Microchip merupakan komponen utama dalam perangkat AI militer. Prosesor seperti GPU (Graphics Processing Unit), TPU (Tensor Processing Unit), dan FPGA (Field-Programmable Gate Array) memainkan peran penting dalam mendukung algoritma pembelajaran mesin yang kompleks. Berbagai platform perangkat keras digunakan untuk mendukung aplikasi AI, dengan GPU menjadi pilihan utama karena kecepatan komputasinya yang tinggi dan kompatibilitasnya dengan berbagai algoritma. Di sisi lain, FPGA menawarkan efisiensi energi lebih baik dibandingkan GPU, meskipun dengan kecepatan yang lebih rendah. Sementara itu, ASIC dirancang untuk efisiensi daya, tetapi kurang fleksibel dalam konfigurasi ulang, sehingga lebih cocok untuk algoritma spesifik seperti jaringan saraf konvolusional dalam AI militer (Gupta, 2021).

Salah satu tantangan utama dalam pengembangan AI adalah tingginya kebutuhan daya komputasi. Untuk mengatasi ini, akselerator perangkat keras seperti FPGA, GPU, dan ASIC dikembangkan guna mempercepat tugas komputasi yang intensif, memungkinkan AI dan pembelajaran mesin untuk beroperasi dengan efisiensi yang lebih tinggi tanpa mengorbankan akurasi (Talib et al., 2021). Chip yang mampu menjalankan model AI berkecepatan tinggi ini sebagian besar diproduksi oleh perusahaan teknologi besar di negara-negara seperti Amerika Serikat, Taiwan, dan Korea Selatan. Produksi microchip canggih seperti TSMC 3nm atau NVIDIA A100 membutuhkan infrastruktur manufaktur yang sangat mahal dan teknologi litografi canggih yang hanya dimiliki oleh segelintir perusahaan global. Selain karena produksinya yang susah, perkembangan AI pun begitu pesat sehingga desain microchip untuk AI juga terus berganti hanya dalam beberapa dekade terakhir dengan kelebihan dan kekurangan spesifik yang disesuaikan untuk peruntukannya (Lee et al., 2020).

Selain itu, memori menjadi komponen yang paling dominan dalam penelitian dan pengembangan perangkat keras AI, mengingat konsumsi energinya yang besar dan perannya dalam pergerakan data antara unit pemrosesan dan penyimpanan, yang sering kali menjadi faktor pembatas dalam arsitektur von Neumann (Boybat et al., 2022). Contohnya, perkembangan terbaru dalam AI melahirkan berbagai inovasi silikon yang terinspirasi dari otak manusia, yang disebut 'silicon photonic neural network', yang melakukan komputasi menggunakan cahaya dan bukan daya listrik, dengan spesifikasi yang bermacam-macam pula (Bai et al., 2020). Ketergantungan pada produsen luar negeri menciptakan risiko strategis bagi negara yang ingin mengembangkan AI militer secara mandiri. Pembatasan ekspor atau sanksi perdagangan dapat menjadi hambatan besar dalam mendapatkan microchip dengan spesifikasi militer.

Dibandingkan dengan arsitektur von Neumann, sistem neuromorphic menawarkan pendekatan baru dalam AI dengan meniru cara kerja otak manusia melalui jaringan neuron tiruan. Implementasi sistem ini semakin berkembang dengan adanya algoritma Hopfield yang telah menunjukkan kemampuannya dalam berbagai proyek perangkat keras skala besar (Yu et al., 2020). Namun, pemilihan arsitektur perangkat keras yang tepat untuk menjalankan algoritma AI tetap menjadi tantangan utama. Efisiensi daya perangkat keras menjadi isu penting dalam AI militer. Salah satu strategi yang banyak dikembangkan adalah mengurangi presisi data masukan dan bobot perangkat keras untuk menekan konsumsi daya. Namun, terdapat kompromi antara presisi dan akurasi, sehingga optimalisasi harus dilakukan agar efisiensi daya tidak mengorbankan keakuratan inferensi AI (Park & Kim, 2021; Dias, Antunes dan Mota, 2004). Pada akhirnya penerapan sistem AI yang lebih efisien juga harus disertai dengan peningkatan perangkat keras yang sesuai agar mencapai penghematan energi yang optimal (Lee & Lee, 2023).

Dalam eksplorasi arsitektur perangkat keras AI, simulasi berbasis perilaku seperti NAXT telah dikembangkan untuk menilai efisiensi desain neuromorfik. Pendekatan ini mencakup struktur hibrida yang mengombinasikan inti komputasi paralel untuk lapisan awal dan unit komputasi time-multiplexed untuk lapisan yang lebih dalam, memungkinkan efisiensi pemrosesan yang lebih baik (Abderrahmane et al., 2020). Menentukan apakah suatu sistem AI harus menggunakan perangkat keras di tempat (on-premise) atau berbasis cloud membutuhkan analisis yang kompleks karena sulit memprediksi perilaku algoritma pada berbagai arsitektur perangkat keras. Ini menjadi lebih sulit jika aplikasi AI harus memenuhi batasan kualitas layanan atau anggaran. Dalam hal ini, alat pendukung keputusan otomatis yang dapat mencocokkan algoritma AI, batasan pengguna, dan sumber daya perangkat keras akan sangat menguntungkan bagi perusahaan dan praktisi AI (De Filippo et al., 2022).

Selain chip, AI dalam pertahanan juga memerlukan superkomputer dengan kapasitas pemrosesan yang sangat tinggi. Misalnya, pengembangan AI untuk analisis citra satelit atau pengambilan keputusan taktis di medan perang membutuhkan sistem komputer yang dapat menangani perhitungan dalam skala besar secara real-time. Superkomputer ini tidak hanya memerlukan CPU dan GPU yang sangat canggih, tetapi juga membutuhkan sistem pendingin yang mahal, sumber daya listrik yang besar, serta jaringan komunikasi berkecepatan tinggi. Negara-negara yang ingin mengembangkan AI militer harus berinvestasi miliaran dolar hanya untuk membangun pusat data yang mampu menangani kebutuhan ini. Namun, keterbatasan bandwidth chip menjadi tantangan dalam pemrosesan AI skala besar. Oleh karena itu, diperlukan peningkatan dalam pemanfaatan kembali data di dalam chip serta optimalisasi transfer data antara chip dan memori eksternal untuk meningkatkan efisiensi sistem (Kim & Deka, 2021).

AI dalam militer tidak hanya terbatas pada komputer pusat, tetapi juga melibatkan berbagai sensor dan perangkat IoT (Internet of Things) yang digunakan di lapangan. Misalnya, drone militer yang menggunakan AI untuk navigasi dan deteksi target membutuhkan kamera termal, radar canggih, serta sensor LiDAR yang semuanya bergantung pada komponen mikroelektronika yang kompleks. Penelitian terbaru menunjukkan bahwa integrasi perangkat keras dan perangkat lunak dalam pengendalian berbasis pembelajaran mesin mampu meningkatkan keandalan dan keamanan sistem charging yang dikendalikan oleh AI, yang menunjukkan potensi besar dalam aplikasi AI militer untuk meningkatkan efisiensi energi dan ketahanan sistem (Park, Moura, & Lee, 2023). Akan tetapi, produksi dan integrasi perangkat keras ini juga memerlukan investasi yang besar dalam penelitian dan pengembangan. Tidak semua negara memiliki kemampuan untuk memproduksi sendiri teknologi ini, sehingga sering kali mereka harus membeli atau bermitra dengan perusahaan teknologi asing yang telah menguasai pasar ini.

Selain perangkat keras, AI untuk keperluan militer juga sangat bergantung pada ketersediaan data dalam jumlah besar, sesuai dengan pengaplikasiannya. Pengaplikasian AI bagi keperluan militer sangat luas, baik itu dalam deteksi dini ancaman, analisis keamanan perbatasan, hingga DNA profiling, sesuatu yang saat ini sedang dikembangkan oleh ahli AI (Murmu, 2024; Bahado-Singh et al., 2022). Data ini digunakan untuk melatih model AI agar dapat mengenali pola, membuat prediksi, dan mengambil keputusan dengan akurasi tinggi dalam situasi medan perang yang dinamis. Namun, pengumpulan dan pemrosesan data ini adalah proses yang memakan waktu bertahun-tahun dan membutuhkan infrastruktur yang kompleks. AI yang efektif membutuhkan dataset yang luas dan berkualitas tinggi, terutama dalam bidang-bidang seperti penginderaan satelit, analisis medan perang, pengenalan wajah, serta komunikasi taktis. Data militer sering kali bersifat rahasia dan tidak dapat dengan mudah dibagikan atau diperoleh dari sumber publik. Oleh karena itu, pengumpulan data untuk AI militer harus dilakukan secara tertutup, yang dapat memperlambat prosesnya. Penginderaan satelit menghasilkan petabyte data per hari yang harus diproses secara efisien agar dapat digunakan oleh sistem AI. Model AI tidak hanya membutuhkan data mentah, tetapi juga data yang telah dilabeli dan dianotasi dengan benar. Proses ini bisa sangat mahal dan memakan waktu bertahun-tahun untuk diselesaikan secara manual atau semi-otomatis.

Setelah data diperoleh, tantangan berikutnya adalah mengembangkan algoritma AI yang dapat belajar dari data tersebut dengan tingkat akurasi tinggi. Dalam konteks militer, AI harus mampu mengenali ancaman di medan perang dengan akurasi tinggi, mengolah informasi dalam waktu nyata untuk pengambilan keputusan taktis, dan menyesuaikan diri dengan kondisi lingkungan yang berubah-ubah, seperti cuaca buruk atau gangguan sinyal komunikasi (Conroy et al., 2022). Proses pelatihan model AI ini bisa memakan waktu bertahun-tahun, terutama karena kompleksitas dalam menyesuaikan model dengan skenario dunia nyata yang sangat dinamis. AI militer tidak bisa langsung diterapkan di medan perang tanpa melalui proses pengujian yang ketat. Simulasi dalam skala besar diperlukan untuk memastikan bahwa sistem AI bekerja sesuai dengan harapan dan tidak menimbulkan risiko yang tidak terduga. Misalnya, drone tempur berbasis AI perlu diuji dalam berbagai skenario, seperti operasi di lingkungan urban, kondisi medan berbukit, atau gangguan elektronik dari musuh. Simulasi ini membutuhkan infrastruktur yang mahal, termasuk simulator medan perang virtual yang realistis. Salah satu tantangan utama dalam pengujian AI adalah sifatnya yang sering dianggap sebagai ‘kotak hitam’ karena memberikan jawaban optimal tanpa kejelasan mengenai proses pengambilan keputusannya. Untuk mengatasi masalah ini, muncul konsep explainable artificial intelligence (XAI) yang memungkinkan interpretasi terhadap keputusan AI, sehingga

meningkatkan kepercayaan dalam sistem AI. Sebuah kerangka kerja perangkat keras XAI berbasis memristor yang hemat energi telah dikembangkan untuk meningkatkan transparansi sistem AI, yang dapat menjadi aspek penting dalam AI militer agar pengambilan keputusan dapat diaudit dan dipahami dengan lebih baik (Song et al., 2024).

Selain itu, pengujian AI dalam dunia nyata juga memerlukan kolaborasi dengan militer aktif, yang berarti adanya tambahan biaya untuk latihan militer, pengujian peralatan, dan peningkatan perangkat lunak secara berkala. Pembuatan AI dalam kegunaan militer adalah proyek yang sangat capital intensive, baik dari segi persyaratan perangkat keras maupun persyaratan program. AI militer memerlukan perangkat keras yang sangat kompleks, termasuk microchip canggih, superkomputer, dan sensor berkualitas tinggi yang sebagian besar masih harus diimpor dari luar negeri. Di sisi lain, AI juga membutuhkan data dalam jumlah yang sangat besar serta bertahun-tahun proses pelatihan dan pengujian sebelum dapat digunakan secara efektif dalam medan perang. Oleh karena itu, hanya negara dengan sumber daya ekonomi dan infrastruktur teknologi yang kuat yang mampu mengembangkan AI militer secara mandiri. Untuk negara yang masih dalam tahap pengembangan, pendekatan terbaik adalah bermitra dengan perusahaan teknologi global atau berinvestasi dalam riset jangka panjang guna mengurangi ketergantungan pada impor dan membangun ekosistem AI yang lebih mandiri, namun hal ini pun tidak luput dari resiko ancaman pembajakan.

Meski demikian, hal ini tidak untuk dijadikan alasan untuk tidak berinvestasi pada AI, karena AI akan banyak memberikan efek multiplier dalam pengembangannya, di mana AI tidak hanya digunakan untuk pertahanan, tetapi juga dapat membantu dalam mengembangkan AI itu sendiri. Konsep sistem siber-fisik berbasis AI semakin berkembang, di mana AI, data, dan perangkat keras bekerja secara terintegrasi dalam suatu ekosistem tertutup untuk meningkatkan efisiensi dan otomatisasi dalam berbagai aspek teknologi pertahanan (Tai et al., 2020). Lebih jauh, AI memungkinkan pengembangan arsitektur sistem yang dapat beradaptasi secara otomatis, mensinkronisasi pengetahuan yang tersebar, serta meningkatkan interaksi manusia-mesin dalam lingkungan operasi militer (Johnson & Treadway, 2019). Dengan memanfaatkan teknologi AI secara optimal, sistem pertahanan dapat menjadi lebih tangguh, responsif, dan adaptif terhadap berbagai tantangan keamanan di masa depan.

KESIMPULAN

Penerapan kecerdasan buatan (AI) dalam sistem pertahanan negara merupakan langkah yang tidak dapat dihindari dalam menghadapi dinamika keamanan global yang semakin kompleks. AI memiliki potensi besar dalam meningkatkan efisiensi operasional, mendukung pengambilan keputusan strategis, serta memperkuat pertahanan siber dalam menghadapi ancaman yang semakin canggih. Dengan memahami berbagai komponen AI—Machine Learning, Neural Networks, Natural Language Processing, dan Robotics—serta mengalokasikannya secara optimal dalam tiga struktur pertahanan utama (operation, tactical, dan strategy), Indonesia dapat mengembangkan sistem pertahanan yang lebih tangguh dan adaptif terhadap perubahan zaman. Pada tingkat operasional, Robotics dan Neural Networks dapat menjadi elemen penggerak utama. Pada tingkat strategis, Machine Learning menjadi elemen dominan. Pada tingkat strategis, Machine Learning tetap memiliki peran dominan. Pada ketiga tingkat, Natural Language Processing dapat menjadi elemen penunjang yang berharga.

Selain itu, AI akan memiliki peran krusial dalam keamanan siber, baik dalam aspek offense maupun defense. Dalam aspek offense, AI dapat digunakan untuk menganalisis sistem pertahanan siber musuh, menemukan celah, serta menyusun strategi serangan yang efektif. Sementara itu, dalam aspek defense, AI membantu meningkatkan perlindungan dengan mendeteksi pola serangan siber lebih cepat, membangun firewall berbasis machine learning, serta

mengembangkan sistem otomatis yang dapat menyesuaikan strategi pertahanan berdasarkan ancaman terbaru. Kontribusi AI pada keamanan siber akan lebih besar pada aspek defense daripada aspek offense. Hal ini dikarenakan saat ini aspek defense lebih human-intensive daripada aspek offense.

Meskipun memberikan manfaat besar, penerapan AI menghadapi tantangan terkait infrastruktur, ketergantungan pada teknologi asing, serta perlunya regulasi ketat guna memastikan penggunaan AI yang transparan, akuntabel, dan etis. Infrastruktur yang diperlukan untuk mendukung AI bersifat resource-intensive, baik dari segi perangkat keras maupun perangkat lunak. Pengolahan data dalam skala besar membutuhkan sistem yang aman dan terenkripsi untuk mencegah kebocoran informasi strategis. Selain itu, ketergantungan pada rantai pasokan global dalam pengadaan komponen perangkat keras seperti GPU, chips, dan server menimbulkan risiko keberlanjutan dan kemandirian teknologi. Oleh karena itu, dibutuhkan investasi yang besar dalam riset dan pengembangan lokal agar Indonesia dapat mengurangi ketergantungan terhadap teknologi asing dan membangun sistem pertahanan AI yang mandiri.

Di samping tantangan teknis, aspek etika dan transparansi juga menjadi isu krusial dalam penggunaan AI di sektor pertahanan. Potensi bias dalam algoritma AI dapat mengarah pada pengambilan keputusan yang tidak akurat atau diskriminatif, yang pada akhirnya dapat berdampak negatif pada operasi militer. Oleh karena itu, perlu adanya regulasi yang ketat serta standar transparansi yang tinggi untuk memastikan bahwa AI diterapkan secara bertanggung jawab, akuntabel, dan etis dalam kebijakan pertahanan nasional.

Ke depan, pemerintah Indonesia harus mengadopsi pendekatan komprehensif dalam pengembangan AI untuk pertahanan negara. Hal ini mencakup peningkatan investasi dalam infrastruktur AI, penguatan riset dan inovasi, serta kerja sama dengan akademisi dan industri dalam pengembangan teknologi AI sesuai kebutuhan militer Indonesia. Selain itu, membangun kemitraan strategis dengan negara-negara maju juga dapat mempercepat proses transfer teknologi dan peningkatan kapasitas sumber daya manusia di bidang AI pertahanan. Dengan strategi yang tepat dan investasi berkelanjutan, AI dapat menjadi pilar utama dalam memperkuat sistem pertahanan Indonesia. Reformulasi kebijakan pertahanan berbasis AI harus dilakukan secara adaptif, progresif, dan berkelanjutan agar Indonesia dapat mengantisipasi ancaman masa depan dengan lebih baik serta memastikan posisinya sebagai negara yang siap menghadapi tantangan geopolitik global. Mengintegrasikan AI dalam pertahanan bukan hanya pilihan, tetapi merupakan kebutuhan mendesak agar Indonesia tidak tertinggal dalam persaingan militer dan teknologi di era digital ini.

DAFTAR PUSTAKA

Abderrahmane, N., Lemaire, E., & Miramond, B. (2020). Design space exploration of hardware spiking neurons for embedded artificial intelligence. Neural Networks, 121, 366-386.

Bahado-Singh, R. O., Radhakrishna, U., Gordevičius, J., Aydas, B., Yilmaz, A., Jafar, F., ... & Vishweswaraiah, S. (2022). Artificial intelligence and circulating cell-free DNA methylation profiling: Mechanism and detection of Alzheimer's disease. Cells, 11(11), 1744.

Bai, B., Shu, H., Wang, X., & Zou, W. (2020). Towards silicon photonic neural networks for artificial intelligence. Science China Information Sciences, 63, 1-14.

Baptista, D., Abreu, S., Freitas, F., Vasconcelos, R., & Morgado-Dias, F. (2013). A survey of software and hardware use in artificial neural networks. Neural Computing and Applications, 23, 591-599.

Berggren, K., Xia, Q., Likharev, K. K., Strukov, D. B., Jiang, H., Mikolajick, T., ... & Raychowdhury, A. (2020). Roadmap on emerging hardware and technology for machine learning. Nanotechnology, 32(1), 012002.

Boybat, I., Payvand, M., Rhodes, O., & Serb, A. (2022). Hardware for artificial intelligence. Frontiers in Neuroscience, 16, 979495.

Conroy, B., Silva, I., Mehraei, G., Damiano, R., Gross, B., Salvati, E., ... & McFarlane, D. C. (2022). Real-time infection prediction with wearable physiological monitoring and AI to aid military workforce readiness during COVID-19. Scientific reports, 12(1), 3797.

Courtland, R. (2018). The bias detectives. Nature, 558(7710), 357-360.

De Filippo, A., Borghesi, A., Boscarino, A., & Milano, M. (2022). HADA: An automated tool for hardware dimensioning of AI applications. Knowledge-Based Systems, 251, 109199.

Deng, C., Fang, X., Wang, X., & Law, K. (2022). Software orchestrated and hardware accelerated artificial intelligence: Toward low latency edge computing. IEEE Wireless Communications, 29(4), 110-117.

Dias, F. M., Antunes, A., & Mota, A. M. (2004). Artificial neural networks: a review of commercial hardware. Engineering Applications of Artificial Intelligence, 17(8), 945-952.

Galán, J. J., Carrasco, R. A., & LaTorre, A. (2022). Military applications of machine learning: A bibliometric perspective. Mathematics, 10(9), 1397.

Gjesvik, L., & Willers, J. O. (2024). Beyond control? The political economy of private interception, intrusion, and surveillance markets. Review of International Political Economy, 31(6), 1840-1864.

Gupta, N. (2021). Introduction to hardware accelerator systems for artificial intelligence and machine learning. In Advances in Computers (Vol. 122, pp. 1-21). Elsevier.

Gutierrez, M. I., Ramos, A., Gutierrez, J., Vera, A., & Leija, L. (2019). Nonuniform Bessel-Based Radiation Distributions on A Spherically Curved Boundary for Modeling the Acoustic Field of Focused Ultrasound Transducers. Applied Sciences, 9(5), 911. https://doi.org/10.3390/app9050911

Hadlington, L., Binder, J., Gardner, S., Karanika-Murray, M., & Knight, S. (2023). The use of artificial intelligence in a military context: development of the attitudes toward AI in defense (AAID) scale. Frontiers in Psychology, 14, 1164810.

Jia, Y., Gu, Z., Du, L., Long, Y., Wang, Y., Li, J., & Zhang, Y. (2023). Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the MDATA model. Knowledge-Based Systems, 276, 110781.

Johnson, B. (2021). Artificial intelligence systems: unique challenges for defense applications. Acquisition Research Program.

Johnson, B., & Treadway, W. A. (2019). Artificial intelligence—an enabler of naval tactical decision superiority. Ai Magazine, 40(1), 63-78.

Johnson, W. L., & Valente, A. (2009). Tactical language and culture training systems: Using AI to teach foreign languages and cultures. AI magazine, 30(2), 72-72.

Khalaf, B. A., Mostafa, S. A., Mustapha, A., Mohammed, M. A., & Abduallah, W. M. (2019). Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access, 7, 51691-51713. https://doi.org/10.1109/ACCESS.2019.2908998

Kim, S., & Deka, G. C. (2021). Hardware accelerator systems for artificial intelligence and machine learning (Vol. 122). Academic Press.

Lee, D., & Lee, S. T. (2023). Artificial intelligence enabled energy-efficient heating, ventilation and air conditioning system: Design, analysis and necessary hardware upgrades. Applied Thermal Engineering, 235, 121253.

Lee, K. J., Lee, J., Choi, S., & Yoo, H. J. (2020). The development of silicon for AI: Different design approaches. IEEE Transactions on Circuits and Systems I: Regular Papers, 67(12), 4719-4732.

Meerveld, H. W., Lindelauf, R. H. A., Postma, E. O., & Postma, M. (2023). The irresponsibility of not using AI in the military. Ethics and Information Technology, 25(1), 14.

Mori, S. (2018). US Defense Innovation and Artificial Intelligence. Asia-Pacific Review, 25(2), 16–44. https://doi.org/10.1080/13439006.2018.1545488

Murmu, S., Sinha, D., Chaurasia, H., Sharma, S., Das, R., Jha, G. K., & Archak, S. (2024). A review of artificial intelligence-assisted omics techniques in plant defense: current trends and future directions. Frontiers in Plant Science, 15, 1292054.

Park, H., & Kim, S. (2021). Hardware accelerator systems for artificial intelligence and machine learning. In Advances in Computers (Vol. 122, pp. 51-95). Elsevier.

Tai, X. Y., Zhang, H., Niu, Z., Christie, S. D., & Xuan, J. (2020). The future of sustainable chemistry and process: Convergence of artificial intelligence, data and hardware. Energy and AI, 2, 100036.

Park, J. M., & Lee, B. G. (2020). Analysis of Research and Development Efficiency of Artificial Intelligence Hardware of Global Companies using Patent Data and Financial data. Journal of Korea Multimedia Society, 23(2), 317-327.

Park, S., Moura, S., & Lee, K. (2023). Integration of hardware and software for battery hardware-in-the-loop toward battery artificial intelligence. IEEE Transactions on Transportation Electrification, 10(1), 888-900.

Pomerol, J. C. (1997). Artificial intelligence and human decision making. European Journal of Operational Research, 99(1), 3-25.

Rasch, R., Kott, A., & Forbus, K. D. (2003). Incorporating AI into military decision making: an experiment. IEEE Intelligent Systems, 18(4), 18-26.

Rashid, A. B., Kausik, A. K., Al Hassan Sunny, A., & Bappy, M. H. (2023). Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. International journal of intelligent systems, 2023(1), 8676366.

Reinisch, F., Strohal, M., & Stütz, P. (2023, October). A Tactical Planning Process in Computer-Generated Forces Team Behavior Within Air Combat Simulations: Concept and First Implementations. In International Conference on Modelling and Simulation for Autonomous Systems (pp. 247-262). Cham: Springer Nature Switzerland.

Reis, J., Cohen, Y., Melão, N., Costa, J., & Jorge, D. (2021). High-tech defense industries: developing autonomous intelligent systems. Applied Sciences, 11(11), 4920.

Roccetti, M., Tenace, M., & Cappiello, G. (2024, September). Prescient Perspectives on Football Tactics: A Case with Liverpool FC, Corners and AI. In International Conference on Advances in Social Networks Analysis and Mining (pp. 231-239). Cham: Springer Nature Switzerland.

Saldiran, E., Hasanzade, M., Inalhan, G., & Tsourdos, A. (2024). Towards global explainability of artificial intelligence agent tactics in close air combat. Aerospace, 11(6), 415.

Sameen, M., Han, K., & Hwang, S. O. (2020). PhishHaven—An efficient real-time AI phishing URLs detection system. Ieee Access, 8, 83425-83443.

Schneier, B. (2018). Artificial intelligence and the attack/defense balance. IEEE security & privacy, 16(02), 96-96.

Schraagen, J. M. (2023). Responsible use of AI in military systems: Prospects and challenges. Ergonomics, 66(11), 1719-1729.

Shrestha, Y. R., Ben-Menahem, S. M., & Von Krogh, G. (2019). Organizational decision-making structures in the age of artificial intelligence. California management review, 61(4), 66-83.

Song, H., Park, W., Kim, G., Choi, M. G., In, J. H., Rhee, H., & Kim, K. M. (2024). Memristive explainable artificial intelligence hardware. Advanced Materials, 36(25), 2400977.

Talib, M. A., Majzoub, S., Nasir, Q., & Jamal, D. (2021). A systematic literature review on hardware implementation of artificial intelligence algorithms. The Journal of Supercomputing, 77(2), 1897-1938.

Tien, J. M. (2017). Internet of things, real-time decision making, and artificial intelligence. Annals of Data Science, 4, 149-178.

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial Intelligence in the Cyber Domain: Offense and Defense. Symmetry, 12(3), 410. https://doi.org/10.3390/sym12030410

Wang, Z., Veličković, P., Hennes, D., Tomašev, N., Prince, L., Kaisers, M., ... & Tuyls, K. (2024). TacticAI: an AI assistant for football tactics. Nature communications, 15(1), 1906.

Wei, Y., Zhou, J., Wang, Y., Liu, Y., Liu, Q., Luo, J., ... & Huang, L. (2020). A review of algorithm & hardware design for AI-based biomedical applications. IEEE transactions on biomedical circuits and systems, 14(2), 145-163.

Yu, Z., Abdulghani, A. M., Zahid, A., Heidari, H., Imran, M. A., & Abbasi, Q. H. (2020). An overview of neuromorphic computing for artificial intelligence enabled hardware-based hopfield neural network. Ieee Access, 8, 67085-67099.

Zhang, T., Kong, F., Deng, D., Tang, X., Wu, X., Xu, C., ... & Deng, R. H. (2025). Moving Target Defense Meets Artificial Intelligence-Driven Network: A Comprehensive Survey. IEEE Internet of Things Journal.

Zhou, Z., Kuang, X., Sun, L., Zhong, L., & Xu, C. (2020). Endogenous security defense against deductive attack: When artificial intelligence meets active defense for online service. IEEE Communications Magazine, 58(6), 58-64.

Zou, J., & Schiebinger, L. (2018). AI can be sexist and racist—it's time to make it fair.