Triwikrama: Jurnal Ilmu Sosial
Volume 8 No. 4 Tahun 2025
E-ISSN: 2988-1986
Open Access:

ARTIFICIAL INTELLEGENCE DALAM PERTAHANAN GLOBAL : TRANSFORMASI STRATEGI DAN KEAMANAN MILITER DI INDONESIA

Andika Putra Setyawan[1], Atika Puspita Marzaman [2]
[1, 2]Departemen Ilmu Hubungan Internasional,
Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin, Makassar, Indonesia

ARTICLE INFO

Article history:
Received : May 2025
Revised: May 2025
Accepted: May 2025
Available online May 2025

Korespondensi: Email:
[1]andikasetyawanputra@gmail.com
[2]tika.marzaman@gmail.com

This is an open access article under the CC BY-SA license. Copyright © 2023 by Author. Published by Universitas Pendidikan Ganesha.

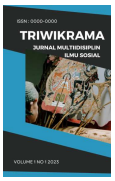
Abstrak

Artificial Intelligence adalah sebuah elemen penting di zaman revolusi saat ini. Teknologi ini sangat memberikan banyak manfaat bagi keberlangsungan kehidupan dunia saat ini. Artifical Intelligence menjadi salah satu asisten yang sangat dibutuhkan manusia dalam menyelesaikan masalah kehidupan manusia. Teknologi kecerdasan buatan ini memiliki dampak yang cukup signifikan dalam masalah pertahanan dan keamanan nasional bagi hampir seluruh negara di dunia. Penelitian ini bertujuan untuk mengkaji peran *Artificial Intelligence* dalam strategi pertahanan nasional Indonesia. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan analisis deskriptif berdasarkan data sekunder dari jurnal ilmiah, buku, laporan, dan dokumen terkait. Hasil penelitian menunjukkan bahwa penerapan *Artificial Intelligence* dalam pertahanan meningkatkan efisiensi operasional, mempercepat pengambilan keputusan, dan meningkatkan ketepatan dalam mendeteksi ancaman, termasuk ancaman siber. Teknologi seperti drone otonom, sistem pengawasan otomatis, serta integrasi *Artificial Intelligence* dengan blockchain memperkuat kemampuan pertahanan modern. Namun, tantangan seperti ketergantungan teknologi, serangan siber, isu etika, dan keterbatasan sumber daya manusia juga muncul. Penelitian ini menekankan pentingnya strategi nasional yang komprehensif untuk mengoptimalkan implementasi *Artificial Intelligence* di sektor pertahanan, termasuk penguatan regulasi, pengembangan sumber daya manusia, dan kolaborasi lintas sektor.

Kata Kunci: Artificial Intelligence; Strategi Pertahanan; Keamanan Nasional; Keamanan Siber; Modernisasi Militer.

Abstract

Artificial Intelligence (AI) has emerged as a pivotal component in the ongoing technological revolution, offering substantial benefits to global societal development. AI serves as a critical tool for addressing complex human challenges, particularly in enhancing national defense and security across nations. This study aims to explore the role of Artificial Intelligence in shaping Indonesia's national defense strategy. Employing a qualitative research method, this study utilizes descriptive analysis based on secondary data sourced from academic journals, books, official reports, and relevant documents. The findings indicate that the integration of AI in defense operations enhances operational efficiency, accelerates decision-making processes, and improves accuracy in threat detection, including cyber threats. Technologies such as autonomous drones, automated surveillance systems, and the convergence of AI with blockchain technology significantly strengthen modern defense capabilities. Nevertheless, several challenges persist, including technological dependency,



vulnerability to cyberattacks, ethical dilemmas, and limited human resource capacity. This research highlights the necessity of a comprehensive national strategy to optimize AI implementation in the defense sector. Such a strategy should encompass regulatory reinforcement, human resource development, and multi-sectoral collaboration.
***Keywords**: Artificial Intelligence; Defense Strategy; National Security; Cybersecurity; Military Modernization.*

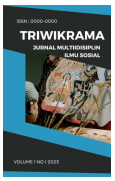
1. PENDAHULUAN

Sistem dan kebijakan yang mengatur dan menjaga pertahanan telah diatur dalam masing- masing kebijakan negara. Salah satunya Indonesia yang telah tercantum pada Undang- Undang Republik Indonesia Nomor 34 Tahun 2004. Pada Undang- undang tersebut mengatur perihal Tentara Nasional Indonesia (TNI) yang menjadi alat terkait pertahanan negara yang bertugas untuk menjaga wilayah, kedaulatan, dan kesalamatan bangsa. TNI memiliki tugas utama untuk melindungi bangsa dan negara dari segala ancaman baik itu ancaman berupa ancaman militer maupun non militer. Sebagai komponen terpenting dan utama dalam hal pertahanan dan keamanan negara, TNI harus mampu mengatasi ancaman dan serangan dari berbagai lini, baik dari dalam maupun luar negeri yang dapat mengancam keutuhan wilayah, kedaulatan dan keselamatan bangsa dan negara.

Salah satu cara yang perlu dilakukan untuk mengantisipasi dan mengatasi ancaman di wilayah perbatasan adalah dengan memanfaatkan teknologi seperti *Artificial Intelligence* yang dapat mendukung sistem dan kebijakan keamanan negara dalam operasi pengamanan perbatasan negara. Operasi yang dimaksud guna untuk mengantisipasi ancaman-ancaman yang kerap kali terjadi pada perbatasan negara seperti penyelundupan barang terlarang, pencurian sumber daya alam bahkan hingga penyeberangan batas yang dilakukan secara ilegal. Oleh karena itu, pengimplementasian dalam penggunaan dan penguasaan teknologi oleh aparat negara ini sangat diperlukan untuk mendeteksi bahkan mengantisipasi ancaman dengan sangat cepat dan mengambil langkah pencegahan dan penindakan secara tepat dalam mengatasi ancaman tersebut.

Contohnya seperti Amerika Serikat yang mengalami transformasi signifikan dalam strategi dan keamanan seiring perubahan konteks global dan perkembangan teknologi militer. Dalam era pasca terjadinya perang dingin, strategi keamanan Amerika Serikat tidak lagi hanya berfokus pada kekuatan militer konvensionalnya, tetapi juga mencakup pendekatan baru melalui liberalisasi industri pertahanan, kolaborasi multilateral, dan penggunaan konsep operasi ketimbang perang formal. Transformasi ini terlihat jelas dalam proyek besar seperti program F-35 Joint Strike Fighter, yang melibatkan banyak negara dalam pengembangan bersama, serta penggunaan dan pengadaan drone atau pesawat tanpa awak sebagai senjata strategis yang mencerminkan pergeseran ke arah peperangan non-konvensional yang memiliki dampak luas bagi sektor ekonomi dan politik.

Selain itu, Amerika Serikat juga merespon hilangnya batas antara perang dan damai, di mana kekuatan militer kini turut berperan sebagai alat penegakan hukum global atau aksi polisional, bukan hanya untuk perang terbuka. Dalam pandangan Mark Neocleous, perubahan ini mencerminkan bahwa Amerika Serikat tidak lagi membedakan secara tegas antara aksi militer dan operasi keamanan, melainkan menyatukannya dalam satu logika kekuasaan global yang lebih luas. Transformasi ini juga turut mendorong munculnya konsep militer pasca-modern, yang ditandai dengan profesionalisasi pasukan, outsourcing, dan dominasi penggunaan jaringan yaitu network-centric warfare seperti perang siber dan informasi.



Dengan demikian, transformasi terjadi dari yang sebelumnya didominasi oleh motivasi negara dalam merebut kekuatan guna mengimbangi ataupun mengancam negara lain (struggle for power), menjadi motivasi yang sifatnya pragmatis dan cenderung membentuk jejaring antar aktor baik negara maupun non-negara (Raden & Efriza, 2017). Salah satu contohnya pada strategi keamanan Amerika Serikat yang telah berevolusi dari orientasi militer tradisional ke arah pendekatan yang sudah terintegrasi, kolaboratif, dan berbasis teknologi, yang mencerminkan adaptasi terhadap tantangan keamanan baru di era globalisasi ini.

Artificial Intelligence telah mengubah jalannya kehidupan dunia dengan kemampuannya yang luar biasa. Namun, dibalik banyaknya manfaat dari kemajuan bidang teknologi ini, tentu banyak pula tantangan yang sangat perlu diatasi dan dilewati dalam penggunaan teknologi kecerdasan buatan dalam pertahanan ini guna untuk pengimplementasiaan yang efektif.

2. KAJIAN TEORITIS

Perkembangan teknologi kecerdasan buatan atau *Artificial Intelligence* (AI) telah membawa dampak besar terhadap dinamika pertahanan global maupun nasional, khususnya dalam konteks bagaimana strategi keamanan yang akan diterapkan oleh suatu negara. Secara teoritis, konsep terbentuknya artificial Intellegence berawal dari ilmu komputer yang bertujuan menciptakan mesin yang mampu meniru kecerdasan dan perilaku manusia, sebagaimana yang dijelaskan oleh John McCarthy dan diperluas oleh Russell & Norvig melalui bentuk dan konsep *Artificial Intelligence* ke dalam tiga tingkatan yaitu Kecerdasan Buatan Tingkat Rendah (Narrow AI), Kecerdasan Buatan Tingkat Menengah (General AI), dan Kecerdasan Buatan Tingkat Tinggi (Super AI). Dalam kerangka sistem pertahanan, pendekatan teoritis ini sejalan dengan teori pemanfaatan jaringan atau yang disebut *network-centric warfare* yang menekankan seberapa penting pemanfaatan informasi dan teknologi secara baik untuk menciptakan keunggulan dalam menghadapi serta mengantisipasi ancaman dalam keamanan negara. Transformasi strategi militer Amerika Serikat, seperti yang dianalisis oleh Mark Neocleous, menunjukkan terciptanya pergeseran dari kekuatan militer konvensional menuju kekuatan militer non konvensional yang berbasis teknologi dan profesionalisasi seperti dalam pengaplikasian drone sebagai salah satu senjata strategis di bidang militer. Sementara di Indonesia, penerapan *Artificial Intelligence* dalam strategi militer juga menekankan pentingnya penanganan berbagai bentuk ancaman, baik militer langsung maupun non-tradisional seperti ancaman siber, perbatasan, dan intelijen. Selain itu, teori kerjasama dan kolaborasi pada teknologi lintas sektor juga cukup relevan, karena *Artificial Intelligence* dalam pertahanan memerlukan konektivitas antara pemerintah, pasukan militer, dan akademisi. Dengan pendekatan ini, penggunaan Artificial Intelligence dalam sistem pertahanan dapat dipahami sebagai proses adaptasi strategis terhadap tantangan global yang bersifat kompleks dan lintas batas, sekaligus mempertegas posisi teknologi sebagai salah satu alat pada pertahanan negara yang bersifat strategis.

3. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif untuk menganalisa bagaimana *Artificial Intelligence* dalam pertahanan global dan bagaimana transformasi strategi dan keamanan militer di Indonesia. Sumber data utama dalam penelitian ini berasal dan bersumber dari jurnal-jurnal ilmiah, buku, laporan, dan dokumen terkait yang membahas Artificial Intelligence, konsep *Artificial Intelligence* dalam pertahanan dan keamanan negara, strategi

militer negara, implementasi *Artificial Intelligence* dalam bidang militer, dan transformasi strategis yang terjadi pada suatu negara. Proses pengumpulan data dilakukan dengan menelusuri literatur yang relevan melalui database akademik dan publikasi terpercaya. Data yang terkumpul kemudian dianalisis secara deskriptif dengan mengidentifikasi konsep-konsep utama, perdebatan teoritis, serta temuan empiris dari penelitian terdahulu. Analisis dilakukan untuk mendapatkan pemahaman yang komprehensif dan mendalam mengenai *Artificial Intelligence* dalam pertahanan global serta transformasi strategi dan keamanan militer Indonesia.

4. HASIL DAN PEMBAHASAN

4.1 Konsep dan Perkembangan *Artificial Intelligence* Dalam Pertahanan

Konsep *Artificial Intelligence* atau yang disebut kecerdasan buataan telah berkembang sangat pesat dalam beberapa tahun terakhir ini. Teknologi yang memiliki kemampuan untuk meniru dan mempelajari perilaku manusia disebut dengan kecerdasan buatan. Kemajuan teknologi informasi dan komunikasi menghadirkan berbagai macam sistem yang sangat canggih dan cerdas hingga saat ini. Adanya kemajuan teknologi ini membuat beberapa sistem yang canggih tersebut diterapkan di berbagai bidang kehidupan, salah satunya adalah bidang pertahanan dan keamanan baik negara maupun individu.

Artificial Intelligence (AI) atau yang disebut dengan kecerdasan buatan adalah salah satu bidang ilmu komputer yang sangat berdampak dan memiliki peran penting di kehidupan saat ini hingga di masa yang akan datang. John McCharty (1927-2011) merupakan sosok yang sangat berkaitan dengan istilah Artificial Intelligence. John McCharty merupakan seorang ilmuwan komputer yang mengajar di MIT dan Stanford University (Pabubung, 2023). Kecerdasan buatan adalah teknologi yang dapat meniru, mempelajari, hingga berinteraksi dengan manusia secara baik. Russell & Norvig (2016) menjelaskan bahwa kecerdasan buatan ini awalnya berkembang pada sekitar tahun 1943-1955 dengan adanya usaha untuk membuat mesin yang dapat meniru, menyamakan atau bahkan melampaui kemampuan manusia.

Jenis Kecerdasan Buatan:

- Kecerdasan Buatan Tingkat Rendah (Narrow AI)

  Kecerdasan buatan tingkat rendah ini merupakan jenis kecerdasan buatan yang paling rendah. Kecerdasan buatan pada jenis ini dapat melakukan hal-hal yang cukup terbatas, seperti pengenalan wajah, pengenalan suara, dan pengenalan teks. Contoh aplikasi kecerdasan buatan tingkat rendah adalah:

  a) Pengenalan Wajah, yaitu sistem atau kecerdasan buatan yang dapat mengidentifikasi wajah, mendeteksi wajah, hingga membedakan berbagai wajah, seperti melalui pengenalan orang, pengenalan ekspresi dan mimik wajah, serta pengenalan gerakan wajah.
  b) Pengenalan Suara, yaitu sistem atau kecerdasan buatan yang dapat membedakan serta mengidentifikasi berbagai suara, seperti nama, pelafalan kata, dan juga frasa.
  c) Pengenalan Teks, yaitu sistem yang dapat membedakan dan mengidentifikasi berbagai teks atau tulisan, seperti pengenalan paragraf, pengenalan kata dan frasa.

- Kecerdasan Buatan Tingkat Menengah (General AI)

  Kecerdasan buatan tingkat menengah ini merupakan jenis kecerdasan buatan yang dapat menyelesaikan pekerjaan atau tugas yang lebih luas, kompleks dan berinteraksi dengan manusia secara lebih efisien. Pada kecerdasan buatan tingkat

menengah ini, bisa dikatakan mereka lebih canggih dibanding kecerdasan buatan tingkat rendah. Kecerdasan buatan tingkat ini lebih dapat mempelajari, meniru, membuat keputusan, hingga dapat berpikir luas seperti layaknya manusia.

- Kecerdasan Buatan Tingkat Tinggi (Super AI)

  Kecerdasan buatan tingakt tinggi ini merupakan kecerdasan buatan yang dapat menyelasaikan tugas yang sangat kompleks dan dapat berinteraksi dengan manusia hingga dapat menggantikan tugas manusia seperti meniru perilaku manusia, membuat keputusan, berpikir seperti manusia, hingga bekerja layaknya manusia secara lebih efektif dan efisien dibandingkan 2 tipe kecerdasan lainnya.

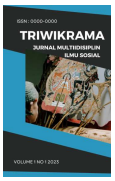
4.2 Perkembangan dan Implementasi *Artificial Intelligence* Dalam Pertahanan Global

Kecerdasan buatan telah membawa perubahan yang sangat besar di berbagai aspek kehidupan manusia, salah satunya adalah dalam pertahanan negara. Adanya perkembangan teknologi membuat banyak perubahan bagi sejumlah negara. Kecerdasan buatan telah berkembang dengan sangat pesat dalam beberapa tahun terakhir termasuk dalam sektor militer dan sipil (dualuse). Kecerdasan buatan atau *Artificial Intelligence* juga cukup dibutuhkan dalam era baru medan pertempuran multi-domain (sektor darat, laut, udara, ruang angkasa, ruang cyber, dan spektrum elektronika). Untuk menghadapi perubahan tersebut, negara perlu melakukan penyesuaian strategis yang tepat dan efisien agar negara dapat mengoptimalkan potensi dari perkembangan teknologi kecerdasan buatan ini dan menjawab tantangan yang muncul.

Pada abad ke-21, terjadi peningkatan signifikan dalam proses globalisasi industri pertahanan, yang sebenarnya telah berkembang sejak era 1970 hingga 1980-an. Perkembangan ini terlihat dari meningkatnya intensitas kerja sama antarnegara dalam membangun industri pertahanan masing-masing (Eshel & Kimhi, 2016). Negara-negara maju cenderung lebih memilih menjalin kolaborasi internasional dibandingkan mengembangkan industri pertahanannya secara mandiri, karena kerja sama tersebut dinilai mampu menekan biaya secara substansial (Danugroho, 2021). Pilihan ini dipengaruhi oleh berbagai faktor, seperti kebijakan penghematan anggaran, tingginya biaya untuk riset dan pengembangan, serta semakin ketatnya persaingan dalam pasar industri pertahanan. Globalisasi di sektor ini juga telah menggeser sistem pengadaan persenjataan dari yang sebelumnya bersifat mandiri (autarki) menjadi saling bergantung (interdependen), menandakan era baru kolaborasi dan kerja sama intensif dalam produksi senjata (Pranowo, 2010).

Menurut Sentientdigital. Inc (2024), pengimplementasian dan pengaplikasiaan kecerdasan buatan atau artificial intellegence dalam dunia militer meliputi *Warfare Systems, Strategic Decision Making, Data Processing & Research, Combat Simulation, Target Recognition, Threat Monitoring, Drone Swarms, Cybersecurity, Transportation and Causalty Care & Evacuation*.

- *Warfare Systems* adalah sistem persenjataan yang dapat berupa semi otonom, otonom terawasi, dan otonom penuh, navigasi, sensor, aviasi, dan pengawasan yang dilakukan secara lebih efektif dan efisien dan mengurangi keterlibatan manusia.
- *Data Processing & Research* adalah kemampuan pada pemilihan serta penyaringan data dan informasi secara cepat seperti pemrosesan bahasa alami atau biasa yang disebut dengan *Natural Language Processing (NLP)*. Pemrosesan bahasa secara alami secara otomatis dapat memproses, menganalisis, dan mengarsipkan dokumen berukuran besar, chatbot, menjawab pertanyaan 5W+1H, mengklasifikasikan, dan mengesktraksi teks, dan menggunakannya untuk menganalisis data teks dan ucapan.



Selain itu, penggunaan jaringan syaraf tiruan, juga dikenal sebagai Artificial Neural Network (AAN), juga memiliki fitur yang mirip dengan sistem saraf otak manusia, yang dapat digunakan dalam penelitian dan pengolahan data militer. Arsitektur jaringan syaraf tiruan yang memiliki lapisan tersembunyi dan lebih dalam, juga dianggap bermanfaat bagi militer.

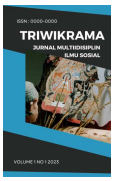
- *Combat Simulation* adalah perangkat lunak simulasi perang (wargame) yang dirancang untuk meningkatkan keterampilan tempur prajurit, salah satunya melalui teknologi Augmented Reality (AR) dan Virtual Reality (VR).
- *Target Recognition* berfungsi untuk meningkatkan ketepatan dalam mengenali sasaran. Threat Monitoring membantu personel militer dalam mengumpulkan serta menganalisis data melalui sistem tak berawak seperti drone, dengan tujuan meningkatkan keamanan dan keselamatan di medan perang.
- *Drone Swarms* mengacu pada sekelompok drone yang bekerja secara terkoordinasi dalam menjalankan misi tertentu, seperti menjelajahi area yang sulit dijangkau oleh manusia.
- Sementara itu, *Cybersecurity* atau keamanan siber berperan dalam melindungi program, data, jaringan, dan sistem komputer dari ancaman peretasan serta malware yang dapat mengganggu sistem pertahanan, mengacaukan operasi pertempuran, hingga membahayakan keselamatan personel militer.

Transportation memanfaatkan kecerdasan buatan untuk merancang rute perjalanan yang paling efisien, mengidentifikasi permasalahan pada armada militer, serta mendukung operasional kendaraan militer tanpa awak (Unmanned Military Vehicle). Sementara itu, *Casualty Care & Evacuation* menggunakan algoritma dan database medis untuk mengakses data kasus trauma prajurit, termasuk diagnosis, tanda vital, serta rekomendasi pengobatan terbaik bagi prajurit yang mengalami cedera.

4.3 *Cyber Security*: Kolaborasi Artificial Inttelligence Dalam Mendeteksi Ancaman Siber

Dasbor intelijen siber saat ini masih memiliki beberapa kelemahan. Keterbatasan tersebut mencakup tidak tersedianya data statistik historis serangan siber pada tingkat negara, ketidakmampuan dalam memprediksi ancaman siber spesifik suatu negara, serta belum adanya metode deteksi anomali spektrum siber berbasis CNN pada tingkat negara (Fahim Sufi, 2023). Maka dari itu, Penggunaan *Artificial Intelligence* dalam cyber defense menawarkan beberapa peluang untuk berkolaborasi dan berintegrasi dengan teknologi lain.

Pemanfaatan kecerdasan buatan (AI) dalam keamanan siber membuka peluang untuk kolaborasi dan integrasi dengan teknologi lain, salah satunya dengan blockchain yang memiliki potensi besar. Kombinasi AI dan blockchain dapat meningkatkan integritas serta transparansi data melalui sistem buku besar yang tidak dapat diubah, memastikan bahwa wawasan dan tindakan yang dihasilkan oleh AI tetap autentik dan dapat diverifikasi. Selain itu, teknologi blockchain menciptakan lingkungan keamanan suatu negara kolaboratif yang memungkinkan deteksi ancaman secara terdesentralisasi, mempercepat respons terhadap serangan, serta meningkatkan akurasi dalam mengidentifikasi ancaman yang dapat mengancam pertahanan dan keamanan negara. Hal ini semakin memperkuat sistem keamanan siber dalam menghadapi ancaman keamanan negara tingkat lanjut yang terus berkembang. Integrasi AI dan blockchain yang terdesentralisasi juga berpotensi mengatasi berbagai tantangan yang sedang dihadapi oleh beberapa negara dalam keamanan siber saat ini yang dapat meminimalisir adanya kegiatan siber yang dapat mengancam suatu negara (B. D. Deebak & Fadi Al Turjman, 2021).

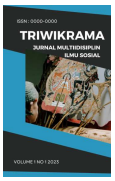


Setelah suatu peluang berbahaya ditemukan dan dengan tidak adanya regulasi yang memadai terkait penggunaan *Artificial Intelligence* ini, aturan deteksi antara AI dan Blockchain yang ada harus terus diperbarui dan ditingkatkan guna mencegah akses oleh pihak penyerang yang dapat mengancam pertahanan dan keamanan negara. Pembuatan aturan deteksi secara manual untuk serangan yang telah diketahui membutuhkan waktu yang lama dan berisiko terjadi kesalahan. Oleh karena itu, beberapa pihak menyarankan penggunaan metode otomatis dalam menghasilkan aturan deteksi untuk serangan yang telah teridentifikasi (Yan Jia, dkk., 2023).

4.4 Strategi Penerapan *Artificial Intelligence* Dalam Operasi Tentara Nasional Indonesia (TNI)

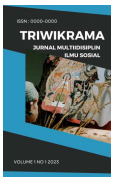
Dalam penerapan dan penggunaan *Artificial Intelligence* dalam operasi militer TNI diperlukan strategi yang matang dan tepat guna meminimalisir dampak yang dapat terjadi apabila strategi tersebut tidak direncanakan secara matang dan presisi. Oleh karena itu, penulis mencoba untuk menjabarkan bagaimana strategi yang perlu di persiapkan dengan melihat aspek seperti kekuatan, kelemahan, peluang dan ancaman dari strategi dalam penggunaan Artificial Intellegence dalam operasi militer tersebut. Berikut ini analisis SWOT yang telah dilakukan oleh Muhammad Alvin Maulidina Firdaus Putra, Deborah Kurniawati, Pulut Suryati, dan Sumiyatun:

- **Kekuatan (Strengths)**
  1. Analisis Data Dengan Cepat, Tepat dan Akurat: Dengan penggunaan teknologi *Artificial Intelligence* yang memiliki kemampuan untuk mengolah data dalam jumlah besar dengan kecepatan dan ketepatan tinggi, yang sangat membantu dalam identifikasi serta pencegahan aksi kejahatan dalam operasi militer seperti terorisme, perang, dan kejahatan siber.
  2. Peningkatan Kinerja Intelijen: *Artificial Intelligence* juga mendukung peningkatan kapabilitas intelijen dengan menganalisis secara mendalam pola-pola serta perilaku mencurigakan yang terdeteksi dari berbagai sumber.
  3. Pengawasan Otomatis: Dengan adanya otomatisasi seperti pengawasan video dan sistem pengenalan wajah, *Artificial Intelligence* dapat meningkatkan efektivitas pemantauan dan identifikasi individu yang terindikasi dapat menjadi ancaman pada saat operasi militer berlangsung.
  4. Kemampuan Prediksi Terhadap Ancaman: Algoritma Artificial Intillegence dapat mengidentifikasi dan mendeteksi potensi ancaman dengan memanfaatkan analisis data historis dan waktu nyata, memungkinkan tindakan pencegahan dilakukan secara lebih awal.
  5. Integrasi Data dari Berbagai Sumber: AI mampu menggabungkan dan mengkolaborasi informasi dari media sosial, aktivitas keuangan, serta komunikasi digital untuk memberikan pemahaman menyeluruh mengenai aktivitas-aktivitas kejahatan yang dapat mengganggu kedaulatan negara.
- **Kelemahan (Weaknesses)**
  1. Ketergantungan pada Teknologi: Pemanfaatan *Artificial Intelligence* yang intensif dapat menciptakan timbulnya ketergantungan tinggi terhadap sistem digital ini, sehingga apabila terjadi gangguan teknis atau serangan siber, operasi militer yang dilakukan menggunakan *Artificial Intelligence* bisa terganggu secara signifikan.



2. Keterbatasan Infrastruktur: Implementasi Artificial Intelligence membutuhkan infrastruktur teknologi tingkat lanjut yang biayanya cukup tinggi dan belum tentu tersedia secara merata di seluruh wilayah operasional TNI untuk mendukung TNI dalam operasi militernya.
3. Kualitas dan Ketersediaan Data: *Artificial Intelligence* hanya akan bekerja maksimal jika didukung oleh data yang berkualitas dan terstruktur, sementara pengumpulan data yang akurat dan konsisten sering menjadi kendala.
4. Isu Privasi dan Etika: Penggunaan *Artificial Intelligence* untuk pengawasan menimbulkan tantangan terkait etika dan perlindungan privasi individu dan negara, yang dapat menimbulkan kritik dan penolakan dari masyarakat.
5. Kekurangan Tenaga Ahli: Kurangnya Sumber Daya Manusia yang memiliki kemampuan dan keahlian khusus dalam bidang teknologi *Artificial Intelligence* dapat menjadi hambatan utama dalam mengaplikasikan teknologi ini secara maksimal di lingkungan militer bagi TNI.

- **Peluang (Opportunities)**
  1. Kerja Sama internasional: Pemanfaatan *Artificial Intelligence* dapat membuka peluang kolaborasi dengan negara-negara maju dalam bidang teknologi untuk memperkuat strategi dalam menghadapi ancaman militer seperti terorisme.
  2. Penguatan Inovasi Lokal: Kolaborasi antara TNI, akademisi, dan industri dalam negeri dapat mendorong pengembangan teknologi *Artificial Intelligence* buatan lokal yang sesuai dengan kebutuhan nasional.
  3. Peningkatan Keamanan Nasional: Penggunaan *Artificial Intelligence* dapat memperkuat efektivitas operasi dalam menghadapi ancaman militer seperti terorisme, sehingga mendukung stabilitas dan keselamatan masyarakat.
  4. Respon Terhadap Ancaman Modern: Teknologi *Artificial Intelligence* bersifat fleksibel dan dapat disesuaikan untuk menghadapi bentuk-bentuk ancaman baru yang dapat menggangu kedaulatan negara seperti serangan siber dan terorisme digital.
  5. Meningkatkan Citra dan Kepercayaan Publik: Keberhasilan TNI dalam menerapkan kolaborasi *Artificial Intelligence* secara professional pada operasi militer mereka dapat memperkuat citra institusi dan meningkatkan kepercayaan masyarakat terhadap kemampuan pertahanan negara Indonesia.
- **Ancaman (Threats)**
  1. Risiko Serangan Siber: Sistem *Artificial Intelligence* sendiri bisa menjadi target serangan siber yang dapat mengganggu operasional serta membocorkan informasi sensitive yang dimiliki negara sehingga dapat mengancam keberadaan negara.
  2. Ketidakpastian Regulasi: Perubahan kebijakan atau peraturan mengenai privasi dan teknologi dapat mempengaruhi keberlangsungan penerapan *Artificial Intelligence* dalam bidang militer yang dilakukan oleh TNI.
  3. Kemajuan Teknologi Lawan: Kelompok yang melakukan kejahatan seperti teroris dan hacker pun dapat memanfaatkan kemajuan teknologi canggih saat ini untuk menghindari deteksi, dan menciptakan tantangan baru bagi aparat keamanan.
  4. Perdebatan Publik: Penggunaan *Artificial Intelligence* dalam pengawasan negara berisiko menimbulkan kontroversi yang berkaitan dengan HAM dan privasi negara, yang bisa berdampak negatif terhadap dukungan publik.



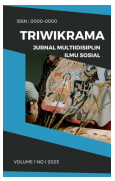
4.5 Studi Kasus dan Implementasi Dalam Pertahanan Indonesia

Indonesia merupakan negara yang dikenal dengan memiliki ribuan pulau. Dengan memiliki karakteristik wilayah seperti itu, Indonesia menjadi negara yang memiliki wilayah perairan yang luas dan memiliki perbatasan wilayah dengan banyak negara yang dapat menimbulkan resiko terhadap pertahanan negara yang seringkali tidak terawasi dengan baik. Hal tersebut perlu diihat sebagai salah satu ancaman dan harus di antisipasi dengan cepat, tepat dan tanggap. Salah satu cara yang dapat dilakukan oleh Indonesia untuk mengatasi ancaman yang berada di wilayah perbatasan Indonesia adalah dengan memanfaatkan penggunaan teknologi kecerdasan buatan atau *Artificial Intelligence* (AI) pada sistem pertahanan negara untuk mendukung terwujudnya operasi sasaran pengamanan wilayah perbatasan yang dilakukan oleh TNI. Operasi pengamanan wilayah perbatasan dapat meliputi pencurian sumber daya alam, pelayaran lintas batas ilegal, penyelundupan barang terlarang, dan kriminalitas lintas negara. Oleh karena itu, melihat semakin berkembangnya teknologi hingga sekarang, penguasan serta penggunaan teknologi oleh lembaga pertahanan negara yaitu TNI dalam mengawasi lintas batas negara merupakan hal yang sangat penting dalam pengoperasiaan pengamanan perbatasan tersebut, guna untuk mengetahui secara lebih cepat jika adanya suatu ancaman, sehingga dapat dicegah dan ditindaklanjuti dengan langkah pencegahan dan penindakan yang tepat.

Wilayah Indonesia saat ini berbatasan darat dengan 3 negara yaitu Malaysia, Papua New Guinea, dan Timor Leste. Jika nantinya akan terjadi perang modern antar wilayah atau negara, akan sangat bergantung pada teknologi maju yang berjalan berdampingan dengan Kecerdasan Artificial seperti Internet-of-Things (IoT), Cyber-Physical Systems (CPS), dan Big Data. Teknologi canggih tersebut akan memainkan peran utama dan menjadi peran yang sangat penting dalam kerangka kerja Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR).

Melihat dinamika perkembangan teknologi dunia semakin pesat, Tentara Nasional Indonesia (TNI) harus mampu beradaptasi, salah satunya melalui modernisasi alutsista yang berbasis kecerdasan buatan (AI). Penerapan AI dalam sistem pertahanan menjadi suatu keharusan yang harus dilakukan TNI dalam menjaga pertahanan Indonesia mengingat pola ancaman yang terus berkembang dan semakin kompleks. Penggunaan teknologi canggih sangat relevan untuk memastikan keamanan wilayah perbatasan dan menjaga keutuhan Negara Kesatuan Republik Indonesia (NKRI) sebagai prioritas utama. Dalam menjalankan tugas pengamanan perbatasan, pemanfaatan kecerdasan buatan atau *Artificial Intelligence* seperti drone, radar, dan sinyal akan meningkatkan efektivitas operasional.

Saat ini, sistem pertahanan Indonesia masih menghadapi berbagai kendala, khususnya terkait dengan kesiapan Alat Utama Sistem Persenjataan (Alutsista) yang belum optimal. Penyempurnaan alutsista menjadi agenda utama dalam pembinaan pertahanan negara, karena kelengkapan dan kualitas alutsista sangat menentukan kekuatan pertahanan Indonesia (Yahya, 2008:98). Dalam konteks pertahanan modern, alutsista menjadi elemen kunci dalam menjaga kedaulatan negara. Namun, tantangan utama yang dihadapi adalah keterbatasan jumlah dan kualitas alutsista yang dimiliki TNI dalam menjalankan tugas pengamanan perbatasan. Sistem pertahanan berbasis teknologi di wilayah perbatasan masih tergolong minim, sehingga diperlukan kajian lebih lanjut mengenai penerapan kecerdasan buatan dalam pengembangan alutsista TNI guna meningkatkan efektivitas dan keamanan nasional.



4.6 Dampak Artificial Intelligence Terhadap Keamanan Strategi Militer

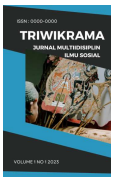
Dalam penerapan *Artificial Intelligence* dalam bidang militer ini, terdapat beberapa dampak positif dan negatif yang penulis coba jabarkan bagaimana dampak positif dan dampak negatif implementasi *Artificial Intelligence* dalam bidang militer yang menyangkut pertahanan dan keamanan negara.

4.6.1 Dampak Positif dan Keunggulan *Artificial Intelligence* Dalam Keamanan Negara

Pemanfaatan kecerdasan buatan (AI) dalam bidang keamanan suatu negara memberikan dampak yang sangat menguntungkan. Teknologi ini mampu menggantikan metode konvensional yang cenderung lambat dengan sistem yang bekerja secara otomatis dan responsif dalam mengidentifikasi serta menangani ancaman yang di dapat oleh suatu negara yang dapat menganggu kedaulatan suatu negara secara langsung. *Artificial Intelligence* ini memiliki kemampuan untuk mengenali pola serta mendeteksi ancaman secara cepat dan tepat, sehingga memungkinkan sistem untuk mengantisipasi serangan sebelum terjadi. Selain itu, *Artificial Intelligence* juga efektif dalam mengelola data dalam jumlah besar yang sulit dianalisis secara manual, serta membantu tim keamanan dan militer dalam memprioritaskan penanganan pada ancaman yang paling mendesak. Keunggulan lainnya adalah pada saat pengoperasian *Artificial Intelligence* ini memiliki akurasi yang tinggi dalam memberikan respons terhadap serangan melalui penerapan algoritma pembelajaran mesin dan pembelajaran mendalam. Penggunaan *Artificial Intelligence* juga terbukti meningkatkan kepuasan pengguna terhadap sistem keamanan digital karena kinerjanya yang cepat, efisien, dan tepat. Secara keseluruhan, *Artificial Intelligence* dipandang sebagai solusi strategis untuk memperkuat sistem pertahanan dan keamanan negara terutama terkait cyber security suatu negara dalam menghadapi tantangan ancaman digital yang terus berkembang.

Penerapan *Artificial Intelligence* ini tidak hanya memberikan keuntungan dalam aspek taktis, tetapi juga mendukung pemanfaatan sumber daya secara lebih optimal dalam menghadapi berbagai ancaman modern yang semakin kompleks pada sektor keamanan di era globalisasi saat ini. Dalam sistem pertahanan, *Artificial Intelligence* berkontribusi besar terhadap peningkatan responsivitas dan efisiensi. Dengan kemampuan *Artificial Intelligence* dalam memproses data dalam jumlah besar secara instan, *Artificial Intelligence* dapat menganalisis informasi intelijen secara lebih cepat dan tepat dibandingkan manusia. Hal ini memungkinkan pengambilan keputusan yang lebih efisien, terutama saat menghadapi situasi darurat di mana kecepatan menjadi hal yang sangat penting. Dalam hal ini, *Artificial Intelligence* menjadi alat yang sangat strategis untuk penanganan krisis dan konflik suatu negara.

Salah satu bentuk penerapan *Artificial Intelligence* yang paling signifikan dalam dunia pertahanan adalah pada sistem drone dan kendaraan militer otonom. Dengan teknologi Artificial Intelligence, perangkat ini dapat digunakan untuk melakukan pengintaian, pemantauan, bahkan pelaksanaan serangan secara presisi. Kemampuannya untuk beroperasi di area berisiko tinggi tanpa perlu melibatkan personel langsung membantu mengurangi potensi korban jiwa. Dalam konteks peperangan masa kini, efektivitas dan keselamatan dalam menjalankan misi merupakan hal krusial.



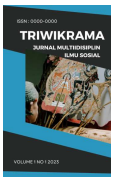
Selain itu, *Artificial Intelligence* juga memiliki peran vital dalam ranah keamanan siber. Mengingat meningkatnya ancaman digital yang kerap dimanfaatkan oleh negara maupun aktor non-negara untuk menyerang infrastruktur penting, *Artificial Intelligence* juga melalui teknologi pembelajaran mesin mampu mengidentifikasi pola-pola serangan dan mendeteksi ancaman jaringan secara dini. Kemampuan ini memberikan perlindungan tambahan yang dapat mencegah atau meminimalkan dampak dari serangan siber yang berpotensi mengganggu stabilitas nasional sebuah negara

4.6.2 Dampak Negatif, Ancaman, dan Resiko Artificial Intelligence

Artificial Intelligence dapat meningkatkan kemampuan militer suatu negara, tetapi juga perlu ditekankan bahwa perlunya kebiajksanaan dalam mengatasi masalah dalam etika serta keamanan dan memanfaatkan *Artificial Intelligence* ini dengan sebaik-baiknya. Pada industri pertahanan dan keamanan negara, meskipun dengan adanya *Artificial Intelligence* ini memberikan manfaat yang cukup banyak bagi pertahanan negara, tentu saja terdapat risiko besar yang perlu di antisipasi, salah satunya adalah masalah etika dan moral suatu negara dalam menggunakan *Artificial Intelligence* ini untuk kepentingan tujuan ofensif negara. *Artificial Intelligence* juga dapat dipengaruhi oleh pihak negara lain, misalnya dalam cyber security dan penggunaan senjata otonom yang tidak dapat dikendalikan.

Selain itu, berbagai tantangan dan permasalahan yang perlu ditangani dengan cermat. Salah satu tantangan utama adalah masalah kompatibilitas, di mana perbedaan teknologi keamanan dan algoritma pembelajaran dan perkembangan system pada kecerdasan buatan tersebut dapat menyebabkan perbedaan sumber data yang masuk dan data yang keluar sehingga dapat menimbulkan kesalahpahaman jika suatu negara sedang bekerjasama dengan negara lain yang dapat membahayakan keamanan suatu negara. Oleh karena itu, pemilihan sumber data harus dilakukan secara hati-hati untuk memastikan kesesuaian sistem. Masalah akurasi juga menjadi perhatian ketika mekanisme pembelajaran mesin digunakan untuk memprediksi fenomena global tertentu. Kesalahan dalam kumpulan data atau pengaturan model dapat menyebabkan ketidakakuratan dalam hasil prediksi. Selain itu, kerentanan dalam mekanisme keamanan menjadi risiko yang signifikan karena dapat mengakibatkan data sensitif terekspos, dimodifikasi, atau bahkan tidak dapat diakses sehingga dapat menganggu keamanan suatu negara. Oleh sebab itu, pengujian protokol keamanan harus dilakukan dengan ketat untuk memastikan perlindungan terhadap serangan, misalnya melalui pengujian logika AVISPA (Mohammad Wazid, dkk., 2022).

Di luar tantangan teknis, perlindungan data negara dan aspek etika juga menjadi faktor penting dalam penerapan kecerdasan buatan pada industri pertahanan dan keamanan negara. Dengan tidak adanya regulasi yang jelas dan memadai, penggunaan *Artificial Intelligence* ini perlu berhati-hati, karena jika salah digunakan maka suatu negara dapat menimbulkan ancaman baru yang dapat membahayakan keamanan nasional mereka sendiri maupun keamanan global.



4.7 Tantangan dan Etika Dalam Penggunaan Artifical Intelligence Untuk Pertahanan dan Keamanan

Penggunaan kecerdasan buatan dalam sektor pertahanan menghadirkan berbagai dilemma etika, terutama karena kurangnya regulasi yang mengatur penggunaan kecerdasan buatan dalam pertahanan negara. Di Indonesia, hingga saat ini belum ada kebijakan atau regulasi khusus yang mengatur etika serta pemanfaatan kecerdasan buatan dalam sistem pertahanan (Rosalina, 2023a). Hal ini perlu menjadi perhatian karena kecerdasan buatan bisa menjadi pedang bermata dua yang berpotensi memberikan dampak negatif jika tidak diatur dengan baik. Contohnya adalah penggunaan ChatGPT, yang dapat menghasilkan teks dengan struktur yang baik tetapi belum tentu memiliki keabsahan yang dapat divalidasi (Rosalina, 2023b). Diperlukan regulasi yang jelas dan menyeluruh untuk memastikan bahwa penerapan kecerdasan buatan dalam pertahanan memperhatikan aspek etika.

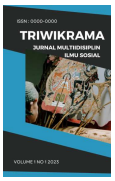
Penggunaan kecerdasan buatan dalam sektor pertahanan ini harus dilakukan dengan transparansi, terutama dalam proses pengumpulan, integrasi, dan distribusi data. Kurangnya transparansi dapat menimbulkan ketidakpercayaan dari berbagai pihak (Sekretariat Jenderal Komisi Yudisial Republik Indonesia, 2019). Oleh karena itu, keterbukaan dan transparansi dalam penerapan kecerdasan buatan sangat penting untuk membangun kepercayaan publik terhadap penggunaannya dalam pertahanan.

Microsoft, sebagai salah satu perusahaan terkemuka dalam bidang kecerdasan buatan, menerapkan enam prinsip utama dalam pengembangannya, yaitu:

1. Privasi dan Keamanan. Sistem *Artificial Intelligence* harus mematuhi peraturan privasi serta melindungi informasi sensitif dari penyalahgunaan dan pencurian data.
2. Transparansi. Microsoft berusaha memberikan informasi yang kontekstual mengenai cara kerja Artificial Intelligence sehingga pengguna dapat membuat keputusan yang lebih tepat.
3. Keadilan. *Artificial Intelligence* harus menghasilkan rekomendasi yang adil tanpa bias, sehingga keputusan yang dibuat bersifat objektif dan dapat dipertanggungjawabkan.
4. Keandalan. Sistem *Artificial Intelligence* harus dirancang dengan parameter yang jelas, menjalani pengujian ketat, serta melibatkan partisipasi publik dalam pengambilan keputusan terkait penggunaannya.
5. Inklusivitas. *Artificial Intelligence* harus dikembangkan dengan praktik desain yang inklusif untuk menghindari diskriminasi atau pengucilan pada pihak tertentu.
6. Tanggung Jawab. Para pengembang teknologi *Artificial Intelligence* harus bertanggung jawab atas sistem yang mereka buat, memastikan bahwa teknologi tersebut tetap berfungsi sesuai standar etika dan hukum yang berlaku.

Meskipun kecerdasan buatan dapat meningkatkan efektivitas sistem pertahanan dengan memberikan analisis yang lebih cepat dan akurat (Universitas Medan Area, 2023), tetapi penggunaan kecerdasan buatan dalam pertahanan ada risiko yang perlu diantisipasi terutama dalam hal keamanan. Risiko ini dapat terjadi apabila penggunaan kecerdasan buatan dalam pertahanan tidak diatur dengan baik dan tidak memperhatikan aspek keamanan yang penting, serta penggunaannya tidak seusai dengan aturan dan regulasi yang berlaku.

Tantangan keamanan merupakan hal yang penting dalam penggunaan teknologi kecerdasan buatan dalam pertahanan. Risiko- risiko utama yang dapat terjadi mencakup serangan siber, manipulasi data, dan penyalahgunaan teknologi oleh pihak musuh negara



yang tidak bertanggung jawab serta Solusi yang diperlukan untuk melindungi system pertahanan negara dari ancaman dan tantangan ini.

Cyber warfare atau perang siber menjadi ancaman baru dalam dunia modern yang harus diatasi dengan kesiapan yang baik di bidang keamanan siber serta regulasi yang kuat untuk melindungi negara dari serangan digital (Baby, 2015).

Di Indonesia, serangan siber telah menjadi masalah serius, seperti yang dilaporkan oleh Kementerian Komunikasi dan Informatika yang menerima hampir 200.000 aduan terkait serangan siber di sektor perbankan, yang sering kali dilakukan melalui aplikasi WhatsApp dan Instagram (Walfajri, 2021). Untuk menghadapi ancaman ini, Indonesia membutuhkan tenaga ahli di bidang keamanan siber serta regulasi ketat guna mencegah dan menanggulangi serangan digital. Kelemahan dalam penguasaan teknologi dan regulasi yang kurang ketat dalam pertahanan siber dapat menghadirkan risiko serius bagi negara (Nainggolan, 2017).

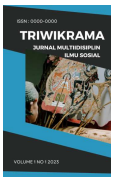
Dalam era Revolusi Industri 4.0, pengembangan infrastruktur teknologi menjadi faktor kunci dalam mendukung penggunaan kecerdasan buatan dalam pertahanan (Helmi, 2019). Untuk itu, diperlukan pemahaman lebih lanjut mengenai pengembangan *Artificial Intelligence* di Indonesia, seperti yang dilakukan oleh Kementerian Komunikasi dan Informatika melalui proyek Palapa Ring, yang menghubungkan seluruh wilayah Indonesia dengan jaringan serat optik bawah laut (Yusuf, 2020). Infrastruktur yang memadai harus terus dikembangkan agar implementasi dan penggunaan Artificial Intellegence dalam pertahanan dapat berjalan dan dilakukan secara efektif dan aman.

5. SIMPULAN DAN SARAN

Artificial Intelligence kini telah menjadi elemen penting dalam transformasi strategi pertahanan dan keamanan negara, termasuk di Indonesia. Penerapan *Artificial Intelligence* membawa perubahan mendasar dengan memperkuat kemampuan militer dalam hal efisiensi, kecepatan respons, akurasi pengambilan keputusan, serta efektivitas pengelolaan ancaman, baik dari sektor konvensional maupun non-tradisional seperti ancaman siber pada saat pengimplementasiannya. Dengan kemampuannya dalam menganalisis data besar secara akurat, *Artificial Intelligence* memungkinkan pengelolaan informasi intelijen yang jauh lebih cepat dan akurat dibandingkan metode konvensional. Hal ini berkontribusi terhadap kesiapan dan ketahanan negara dalam menghadapi ancaman yang kompleks dan bisa terjadi kapan saja di era globalisasi ini.

Dalam sektor pertahanan dan militer, implementasi *Artificial Intelligence* terlihat nyata dalam penggunaan drone, kendaraan militer otonom, sistem pengawasan otomatis berbasis pengenalan wajah, serta prediksi ancaman melalui analisis data historis dan real time. *Artificial Intelligence* juga mendukung operasi keamanan perbatasan dengan meningkatkan efektivitas deteksi ancaman lintas batas seperti penyelundupan, kejahatan lintas negara, hingga serangan siber yang dapat mengganggu kedaulatan nasional negara. Di sisi lain, *Artificial Intelligence* memperkuat aspek keamanan siber dengan kemampuan deteksi dini serangan serta integrasi teknologi blockchain untuk meningkatkan transparansi dan ketahanan sistem pertahanan digital.

Namun, di balik manfaat tersebut, penerapan *Artificial Intelligence* dalam pertahanan juga membawa tantangan yang cukup serius. Ketergantungan terhadap teknologi menciptakan risiko baru seperti kerentanan terhadap serangan siber, kegagalan sistem, hingga manipulasi dan pemalsuan data. Selain itu, isu etika dan regulasi penggunaan *Artificial Intelligence* dalam operasi militer menjadi hal krusial yang belum sepenuhnya diantisipasi, khususnya di



Indonesia. Tanpa regulasi hukum yang jelas, penggunaan *Artificial Intelligence* berpotensi melanggar hak asasi manusia, privasi, dan membuka celah penyalahgunaan kekuasaan. Terlebih lagi, keterbatasan sumber daya manusia yang terampil dalam bidang *Artificial Intelligence* dan infrastruktur teknologi yang belum merata menjadi tantangan nyata dalam optimalisasi implementasi Artificial Intellegence di sektor pertahanan nasional.

Oleh karena itu, untuk mengoptimalkan potensi *Artificial Intelligence* dalam memperkuat sistem pertahanan nasional, dibutuhkan pendekatan yang komprehensif. Hal ini mencakup penguatan regulasi dan etika dalam penggunaan Artificial Intelligence, pembangunan infrastruktur teknologi yang mendukung, pengembangan kapasitas sumber daya manusia, serta kolaborasi intensif antara pemerintah, militer, industri teknologi, dan lembaga akademik. Indonesia juga perlu memperkuat kerja sama internasional dalam bidang *Artificial Intelligence* untuk mempercepat transfer teknologi, memperkuat keamanan siber, dan memastikan kesiapan dalam menghadapi ancaman berbasis teknologi. Dengan strategi yang terencana, dan adaptif *Artificial Intelligence* berpotensi menjadi pondasi penting dalam menjaga kedaulatan, integritas, dan stabilitas nasional di tengah dinamika geopolitik global yang terus berkembang.

6. DAFTAR PUSTAKA

Aditya, S. D., D. R., & Wadjdi, A. F. (2024). STRATEGI PENERAPAN ARTIFICAL INTELIGENCE DALAM OPERASI KONTRA-TERORISME TENTARA NASIONAL INDONESIA (TNI). *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* , 3079-3080.

Daniel Adolf Ohyver, SE, M.Pd, CHE, CDM, Dr. Ir. H. Sa'dianoor, S.T., M.Si., IPM, Satrio Junaidi, S.Pd., M.Kom, & Rabiah Adawiyah, S.Kom., M.Cs. (2024). *Buku Ajar Kecerdasan Buatan*. Jambi: PT. Sonpedia Publishing Indonesia.

Dewanto, A. C. (2023). RISIKO DAN MITIGASI PENGGUNAAN KECERDASAN BUATAN DALAM BIDANG PENDIDIKAN. *Prosiding Konferensi Ilmiah Pendidikan*, (hal. 2).

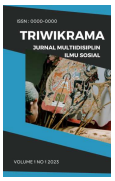
Dr. Anton Nugroho, M. M. (2021, Juni). *ANALISIS PENGGUNAAN KECERDASAN BUATAN (ARTIFICIAL INTELLIGENCE/AI) OLEH TNI AD DALAM MENDUKUNG SISTEM PERTAHANAN NEGARA*. Diambil kembali dari seskoad.mil.id: https://seskoad.mil.id/admin/file/kajian/69%20ARTIFICIAL.pdf

Gede Priana Dwipratama, S.E., M.M. (2024, Maret 20). *IMPLIKASI KECERDASAN BUATAN DALAM INDUSTRI PERTAHANAN : TANTANGAN DAN PELUANG BAGI INDONESIA*. Diambil kembali dari www.kemhan.go.id: https://www.kemhan.go.id/pothan/2024/03/20/implikasi-kecerdasan-buatan-dalam-industri-pertahanan-tantangan-dan-peluang-bagi-indonesia.html#:~:text=Kecerdasan%20buatan%20telah%20berkembang%20dengan%20pesat%20dalam%20beberapa,udara%2C%20ruang%20angkasa%2C%2

Humas. (2024, Oktober 03). *Peran AI dalam Pertahanan Negara: Meningkatkan Efektivitas dan Keamanan di Era Digital*. Diambil kembali dari ikalppsa24.id: https://ikalppsa24.id/index.php/2024/10/03/peran-ai-dalam-pertahanan-negara-meningkatkan-efektivitas-dan-keamanan-di-era-digital/

Mahdidah, D. D., Setiawans, A. D., Destira, T. A., & Danugroho, A. (2023). TRANSFORMASI KONSEPSI INDUSTRI PERTAHANAN BANGSA INDONESIA DI ERA GLOBALISASI. *Jurnal Paradigma: Jurnal Multidisipliner Mahasiswa Pascasarjana Indonesia*, 41-55.

Marissa Safira Dinanti, & Atika Puspita Marzaman. (2024). KEBIJAKAN KONSERVASI LAUT DI WAKATOBI DAN IMPLIKASINYA TERHADAP STATUS CAGAR BIOSFER UNESCO. *ejournal.warunayama*, 06.



Muhammad Alvin Maulidina Firdaus Putra, Deborah Kurniawati, Pulut Suryati, & Sumiyatun. (2024). INTEGRASI KECERDASAN BUATAN DALAM BERBAGAI SEKTOR: DAMPAK, PELUANG, DAN TANTANGAN. *Jurnal Cakrawala Ilmiah*, 3835.

Pongoh, A. G., Fahreza, R. A., Kindi, B. A., Pribadi, F. S., & Aprilianto, R. A. (2024). Systematic Literature Review (SLR): Dampak Pemanfaatan *Artificial Intelligence* Untuk Meningkatkan Cyber Security. *CyberSecurity dan Forensik Digital* , 37-38.

Rahmatika, A. N. (2022). STRATEGI PERTAHANAN NEGARA INDONESIA DALAM MENGHADAPI ANCAMAN . *Jurnal Peperangan Asimetris* .

Rasya Rafika Widalala, Amanda Novalina Khairunnisa, Juhar Ananda Dika, & Allysa Az Zahra Wijanarko. (2024). DAMPAK PENGGUNAAN *ARTIFICIAL INTELLIGENCE* PADA KEAMANAN SIBER: SEBUAH KAJIAN TERHADAP POTENSI KEUNTUNGAN DAN ANCAMAN. *Berajah Journal, Jurnal Pembelajaran dan Pengembangan Diri*, 1541-1552.

Yudopratomo, A. (2023). TANTANGAN TERHADAP MASA DEPAN PERTAHANAN NEGARA AKBIAT KECERDASAN BUATAN. *Jurnal Ilmu Pengetahuan Sosial*, 4051-4055.