JIHHP: Jurnal Ilmu Hukum, Humaniora dan Politik
E-ISSN: 2747-1993
P-ISSN: 2747-2000
https://dinastirev.org/JIHHP dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jihhp.v5i6

Tantangan Regulasi dan Implementasi *Artificial Intelligence (AI)* dalam Pengembangan Alutsista Indonesia: Perspektif Kebijakan Pertahanan

Tubagus Akbar Satria Primadana[1], Fokky Fuad[2], Sadino[3]
[1] Universitas Al Azhar Indonesia, Jakarta, Indonesia, *satriaprimadana@gmail.com*
[2] Universitas Al Azhar Indonesia, Jakarta, Indonesia, *fokkyf@gmail.com*
[3] Universitas Al Azhar Indonesia, Jakarta, Indonesia, *sadino@uai.ac.id*

Corresponding Author: *satriaprimadana@gmail.com*[1]

Abstract: *The utilization of AI in Alutsista must be balanced with defense policies that are responsive to the risk of dual-use technology (technology that can be used for civilian and military purposes) and cybersecurity vulnerabilities. Without clear regulations, AI implementation risks creating legal loopholes, both in terms of accountability for the use of autonomous systems and protection of strategic data. One of the main challenges in the integration of AI into Indonesia's defense sector is the fragmentation of regulations and the lag of the national legal framework in accommodating the development of disruptive technologies. This research will use a qualitative approach to gain an in-depth understanding of the regulatory and implementation challenges of AI in the defense equipment context. Based on the research findings, it provides recommendations for the development of a better legal framework in the utilization of AI for cybersecurity and national defense in Indonesia. The utilization of AI for threat detection, big data analysis, and automated response is a strategic solution. However, its effectiveness depends on a comprehensive and responsive legal framework. Currently, Indonesia has a number of regulations such as the Electronic Information and Transaction Law (ITE Law) and the Cyber Law (Law No. 11/2008 which was revised into Law No. 19/2016), but they do not specifically regulate the use of AI. In fact, AI requires regulation related to algorithmic accountability, protection of sensitive data, and mitigation of the risk of bias that can threaten security stability. Without a clear legal umbrella, AI integration has the potential to create a legal vacuum, especially in the context of national defense, which requires precision and adherence to jus in bello (law of war) principles.*

Keyword: *artificial intelligence, defense, defense equipment, technology crime,*

Abstrak: Pemanfaatan *AI* dalam Alutsista harus diimbangi dengan kebijakan pertahanan yang responsif terhadap risiko dual-use technology (teknologi yang dapat digunakan untuk tujuan sipil dan militer) serta kerentanan keamanan siber. Tanpa regulasi yang jelas, implementasi *AI* berisiko menciptakan celah hukum, baik dalam aspek akuntabilitas penggunaan sistem otonom maupun perlindungan data strategis. Salah satu tantangan utama dalam integrasi *AI* ke sektor pertahanan Indonesia adalah fragmentasi regulasi dan ketertinggalan kerangka hukum nasional

dalam mengakomodasi perkembangan teknologi disruptif. Penelitian ini akan menggunakan pendekatan yuridis normatif untuk mendapatkan pemahaman yang mendalam tentang tantangan regulasi dan implementasi *AI* dalam konteks alutsista. Berdasarkan temuan penelitian, memberikan rekomendasi untuk pengembangan kerangka hukum yang lebih baik dalam pemanfaatan *AI* untuk keamanan siber dan pertahanan nasional di Indonesia. Pemanfaatan *AI* untuk deteksi ancaman, analisis *big data*, dan respons otomatis menjadi solusi strategis. Namun, efektivitasnya bergantung pada kerangka hukum yang komprehensif dan responsif. Saat ini, Indonesia memiliki sejumlah regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Siber (UU No. 11/2008 yang direvisi menjadi UU No. 19/2016), tetapi belum secara spesifik mengatur pemanfaatan *AI*. Padahal, *AI* memerlukan pengaturan terkait akuntabilitas algoritmik, perlindungan data sensitif, dan mitigasi risiko *bias* yang dapat mengancam stabilitas keamanan. Tanpa payung hukum yang jelas, integrasi *AI* berpotensi menciptakan celah hukum (*legal vacuum*), terutama dalam konteks pertahanan nasional yang memerlukan presisi dan kepatuhan pada prinsip *jus in bello* (hukum perang).

Kata Kunci: kecerdasan buatan, pertahanan, alutsista, kejahatan teknologi,

PENDAHULUAN

Dalam konteks dinamika keamanan global yang semakin kompleks, integrasi *Artificial Intelligence (AI)* ke dalam sistem *Alat Utama Sistem Senjata* (Alutsista) menjadi imperatif strategis bagi Indonesia. Kemajuan teknologi *AI* menawarkan potensi transformatif untuk meningkatkan kapabilitas pertahanan, mulai dari sistem pengawasan berbasis *machine learning*, *autonomous weapons systems* (AWS), hingga analisis data intelijen secara real-time. Namun, adopsi AI dalam sektor pertahanan tidak hanya bersifat teknis, melainkan juga menuntut kerangka regulasi yang komprehensif untuk memastikan keselarasan dengan prinsip hukum internasional, etika pertahanan, dan kepentingan nasional.

Sebagai negara kepulauan dengan wilayah teritorial luas, Indonesia menghadapi tantangan asimetris seperti ancaman siber, pelanggaran kedaulatan maritim, dan proliferasi senjata canggih. Oleh karena itu, pemanfaatan *AI* dalam Alutsista harus diimbangi dengan kebijakan pertahanan yang responsif terhadap risiko *dual-use technology* (teknologi yang dapat digunakan untuk tujuan sipil dan militer) serta kerentanan keamanan siber. Tanpa regulasi yang jelas, implementasi *AI* berisiko menciptakan celah hukum, baik dalam aspek akuntabilitas penggunaan sistem otonom maupun perlindungan data strategis. Implementasi *AI* berisiko menciptakan celah hukum dalam akuntabilitas penggunaan sistem otonom dan perlindungan data strategis. Kesulitan menentukan tanggung jawab atas kesalahan dan ketidakjelasan regulasi dapat menghambat penegakan hukum. Selain itu, penggunaan *AI* dalam pengolahan data dapat melanggar privasi dan meningkatkan risiko kebocoran data. Untuk mengatasi celah hukum ini, diperlukan penguatan regulasi yang jelas, pendidikan bagi penegak hukum, dan kerjasama internasional untuk mengembangkan standar global dalam penggunaan *AI* yang aman dan bertanggung jawab(Wijayakusuma et al., 2024).

Dalam era globalisasi dan ancaman keamanan yang semakin kompleks, kerjasama internasional di bidang pertahanan menjadi sangat penting. Indonesia, dengan posisi geopolitik yang strategis, menghadapi tantangan keamanan yang bersifat domestik, regional, dan global. Untuk mengatasi hal ini, kebijakan kerjasama internasional dirumuskan guna memperkuat kapabilitas pertahanan nasional melalui sinergi dengan negara lain dan organisasi internasional. Kolaborasi ini diharapkan dapat meningkatkan efektivitas pertahanan Indonesia dalam menghadapi berbagai ancaman yang ada(Prakoso et al., 2024).

Indonesia memerlukan pendekatan kebijakan yang holistik untuk menyeimbangkan inovasi AI dengan prinsip kehati-hatian (precautionary principle). Pertama, Kementerian Pertahanan bersama DPR perlu merevisi Undang-Undang Pertahanan Negara dengan memasukkan klausul khusus tentang penggunaan AI, termasuk standar interoperabilitas, tata kelola data, dan mekanisme pengawasan parlemen. Kedua, pembentukan National AI Governance Board yang melibatkan pemangku kepentingan multisektor (militer, akademisi, industri, dan masyarakat sipil) untuk merumuskan pedoman etis penggunaan AI dalam Alutsista. Ketiga, memperkuat kemandirian teknologi melalui alokasi anggaran riset pertahanan yang memadai, serta skema public-private partnership untuk pengembangan AI open source yang dapat dimodifikasi sesuai kebutuhan operasional. Keempat, diplomasi pertahanan harus dioptimalkan untuk memperjuangkan kepentingan Indonesia dalam forum global seperti PBB terkait regulasi sistem senjata otonom, sekaligus menjalin kerja sama teknis dengan negara sahabat untuk transfer teknologi yang berkelanjutan. Terakhir, peningkatan kapasitas SDM melalui pendidikan spesialisasi AI di akademi militer dan program pelatihan bersama dengan negara-negara ASEAN.

Dengan langkah-langkah tersebut, Indonesia dapat memanfaatkan AI sebagai force multiplier tanpa mengorbankan prinsip kedaulatan, keamanan, dan keselarasan dengan hukum internasional. Dengan mempertimbangkan rumusan masalah mengenai kesiapan kerangka hukum Indonesia dalam pemanfaatan AI dalam sistem pertahanan nasional.

Artikel ini akan mengkaji tantangan regulasi dan implementasi AI dalam pengembangan alutsista Indonesia?. serta memberikan rekomendasi kebijakan yang dapat mendukung integrasi teknologi canggih ini secara efektif dan aman dalam konteks pertahanan negara?. Tantangan regulasi dan implementasi AI dalam pengembangan alutsista Indonesia mencakup aspek keamanan siber, perlindungan data, dan kebutuhan untuk kebijakan yang adaptif. Rekomendasi kebijakan meliputi penguatan infrastruktur teknologi, pelatihan sumber daya manusia, serta kolaborasi antara pemerintah dan sektor swasta untuk memastikan integrasi yang aman dan efektif.

METODE

Penelitian ini akan menggunakan pendekatan yuridis normatif untuk mendapatkan pemahaman yang mendalam tentang tantangan regulasi dan implementasi *AI* dalam konteks alutsista. Pendekatan ini memungkinkan peneliti untuk mengeksplorasi perspektif berbagai pemangku kepentingan. Mengumpulkan dan menganalisis dokumen-dokumen kebijakan, regulasi, dan undang-undang yang berkaitan dengan penggunaan *AI* dalam pertahanan dan keamanan siber di Indonesia. Menganalisis laporan-laporan penelitian, artikel ilmiah, dan publikasi terkait yang membahas tantangan dan peluang *AI* dalam alutsista.

Memilih beberapa studi kasus spesifik di mana *AI* telah diterapkan dalam alutsista di Indonesia atau negara lain yang relevan. Menganalisis bagaimana regulasi dan kebijakan di negara tersebut mendukung atau menghambat implementasi *AI* dalam konteks pertahanan.

Berdasarkan temuan penelitian, memberikan rekomendasi untuk pengembangan kerangka hukum yang lebih baik dalam pemanfaatan *AI* untuk keamanan siber dan pertahanan nasional di Indonesia. Dengan metode penelitian ini, diharapkan dapat memberikan wawasan yang komprehensif mengenai tantangan regulasi dan kesiapan kerangka hukum Indonesia dalam memanfaatkan AI untuk keamanan siber dan pertahanan nasional.

HASIL DAN PEMBAHASAN

Penggunaan & Resiko Kecerdasan Buatan (*AI*) dalam Sistem Pertahanan

Menurut pendapat Kurtis H. Simpson dan rekan-rekannya dalam sebuah artikel yang diterbitkan oleh *Centre for International Governance Innovation*, penggunaan kecerdasan buatan (*AI*) dalam bidang pertahanan dapat dikategorikan menjadi delapan jenis. Kategori-

kategori tersebut meliputi: Sistem Komando dan Kontrol; Intelijen, Pengintaian, dan Pengawasan; Simulasi dan Pelatihan; Pengenalan Target Secara Otomatis; Sistem dan Kendaraan Otonom; Operasi Informasi dan Perang Elektronik; Pemeliharaan Prediktif dan Logistik; serta Aplikasi Medis(Simpson et al., 2025).

Menurut Adib Bin Rashid dan rekan-rekannya, terdapat tujuh kategori pola dalam penggunaan *AI*, yaitu: sistem yang berfokus pada tujuan (*goal-driven systems*) seperti penggunaan drone otonom; sistem otonom (*autonomous systems*) seperti kendaraan tanpa awak; interaksi manusia (*conversational/human interactions*) seperti chatbot; analisis prediktif (*predictive analytics*) yang mencakup analisis perilaku konsumen; hiper-personalisasi (*hyperpersonalization*) yang menggunakan machine learning untuk memberikan rekomendasi yang disesuaikan; sistem pendukung keputusan (*decision support*); serta pengenalan pola dan anomali (*pattern & anomaly recognition*)(Rashid et al., 2023).

Merujuk pada kedua pendapat tersebut, maka berikut adalah beberapa cara *AI* diterapkan dalam konteks pertahanan:

A) Analisis Data dan Intelijen:

Regulasi menjadi fondasi krusial untuk memastikan implementasi *AI* dalam pengolahan data besar (seperti dari satelit, drone, atau sensor) dapat berjalan akuntabel, aman, dan sesuai kebutuhan strategis. Tanpa kerangka hukum yang matang, potensi *AI* dalam meningkatkan kecepatan dan akurasi keputusan intelijen seperti identifikasi pola ancaman atau dukungan keamanan siber akan terhambat oleh risiko seperti ambigu tanggung jawab atas kesalahan algoritma, kerentanan kebocoran data sensitif, atau ketidakselarasan standar etika dengan praktik global.

Pada tahun 2021 di Bandung, Mayor Jenderal TNI Dr. Anton Nugroho, MMDS., M.A., selaku Komandan Sekolah Staf dan Komando TNI AD, menekankan pentingnya kebijakan pemerintah dalam pengembangan R&D *Artificial Intelligence* (*AI*) untuk mendukung inovasi teknologi di bidang pertahanan. Kebijakan tersebut diharapkan mendorong akademisi dan pakar teknologi *AI* dalam penerapan *AI* sebagai alutsista TNI, termasuk drone radar, guna menjaga kedaulatan negara. Selain itu, diperlukan peningkatan alokasi anggaran untuk modernisasi alutsista dan kerjasama dengan BPPT serta Kemenristek/BRIN, serta persiapan sumber daya manusia prajurit TNI dalam Transfer of Technology dan Transfer of Knowledge(Nugroho, 2021).

B) Sistem Pertahanan Sibernetik:

AI digunakan untuk mendeteksi dan merespons ancaman siber secara otomatis. Algoritma pembelajaran mesin dapat mengenali perilaku yang mencurigakan dan mengambil tindakan untuk melindungi jaringan militer dari serangan. Tantangan utama terletak pada ketidaksiapan regulasi Indonesia, seperti absennya payung hukum khusus yang mengatur akuntabilitas *AI* saat mengambil tindakan otomatis (misalnya, false positive yang mengganggu operasi militer), ambiguitas penggunaan data intelijen, serta ketidaksinkronan UU Siber dan Pertahanan dengan kebutuhan teknologi terkini. Tanpa kerangka hukum yang jelas, implementasi *AI* berisiko menimbulkan kerentanan seperti pelanggaran privasi, ketergantungan pada vendor asing, atau sanksi internasional akibat ketidaksesuaian dengan standar global. Untuk itu, diperlukan regulasi khusus yang menetapkan batasan otonomi *AI*, harmonisasi kebijakan dengan prinsip *human-in-the-loop* ala NATO/ASEAN, serta pembentukan badan pengawas multidisiplin guna memastikan *AI* menjadi solusi efektif, bukan ancaman baru, bagi pertahanan siber Indonesia.

C) Otonomi dalam Kendaraan Militer:

Kendaraan udara tak berawak (UAV) dan kendaraan darat otonom menggunakan *AI* untuk navigasi dan pengambilan keputusan. Ini memungkinkan mereka untuk melakukan misi pengintaian, pengawasan, dan bahkan serangan tanpa intervensi manusia

langsung. Penggunaan *AI* untuk navigasi dan pengambilan keputusan dalam misi pengintaian, pengawasan, atau serangan tanpa intervensi manusia langsung memunculkan tantangan regulasi krusial, seperti akuntabilitas hukum atas kesalahan fatal sistem *AI*, kerentanan siber terhadap serangan peretasan atau manipulasi data, serta kesenjangan antara regulasi Alutsista konvensional (misal UU No. 16/2012) dengan kompleksitas teknologi otonom.

Persoalan ini diperparah oleh belum adanya payung hukum spesifik yang mengatur prinsip *meaningful human control*, sertifikasi algoritma, atau protokol darurat untuk sistem otonom, sementara kebijakan pertahanan nasional dituntut mengantisipasi risiko strategis seperti pelanggaran hukum humaniter internasional atau *legal vacuum* dalam operasi militer. Untuk itu, diperlukan percepatan harmonisasi regulasi, seperti mengadopsi model *DoD Directive 3000.09* (AS) tentang senjata otonom, memperkuat peran BSSN dalam keamanan siber sistem militer, dan mengintegrasikan aspek pertahanan dalam RUU Kecerdasan *Artifisial*, agar pemanfaatan *AI* tidak justru menjadi ancaman akibat ketidaksiapan kerangka hukum yang holistik.

D) Perencanaan dan Logistik:

AI dapat membantu dalam perencanaan operasi militer dan manajemen logistik dengan menganalisis data untuk mengoptimalkan penggunaan sumber daya, mengurangi biaya, dan meningkatkan efisiensi. Pemanfaatan *AI* dalam analisis data logistik, *prediksi* kebutuhan sumber daya, dan efisiensi alutsista memerlukan kerangka hukum yang menjamin keamanan data, akuntabilitas algoritma, dan interoperabilitas sistem. Namun, ketidaksiapan regulasi Indonesia—seperti belum adanya payung hukum untuk integrasi data antarlembaga, standar etika *AI*, dan perlindungan sistem dari serangan siber—dapat menghambat kolaborasi teknis, meningkatkan risiko keamanan, dan menimbulkan ambiguas tanggung jawab jika terjadi kegagalan sistem. Tanpa regulasi yang adaptif, potensi efisiensi *AI* dalam pertahanan tidak tercapai maksimal, sementara kerentanan terhadap ancaman siber dan kesenjangan kebijakan berpotensi melemahkan ketahanan nasional. Oleh karena itu, artikel ini menekankan urgensi percepatan RUU terkait data dan *AI*, standarisasi sistem, serta kolaborasi multisektor untuk menciptakan kebijakan pertahanan yang seimbang antara inovasi teknologi dan mitigasi risiko.

E) Pengawasan dan Keamanan:

AI dapat digunakan dalam sistem pengawasan untuk mendeteksi aktivitas mencurigakan atau ancaman di area tertentu, baik melalui analisis video maupun sensor lainnya. Tantangan utama terletak pada ketidaksiapan regulasi Indonesia yang belum *sepenuhnya* mengatur aspek krusial seperti privasi data, transparansi algoritma, dan batasan otoritas pengawasan, sehingga berpotensi menimbulkan risiko penyalahgunaan teknologi, pelanggaran hak sipil, atau kerentanan keamanan sistem. Implementasi *AI* dalam sistem pertahanan, meski meningkatkan efisiensi deteksi ancaman, juga menghadapi dilema etis dan teknis, seperti risiko pengawasan massal tanpa dasar hukum atau kerentanan algoritma terhadap serangan siber. Celah regulasi ini memperlemah interoperabilitas sistem pertahanan Indonesia dengan standar global (seperti *NATO/ASEAN*) dan menghambat akuntabilitas penggunaan *AI*, terutama terkait UU Perlindungan Data Pribadi. Untuk itu, diperlukan percepatan penyusunan regulasi khusus yang mencakup standar teknis, audit algoritma, dan sinergi antarlembaga pertahanan, siber, dan teknologi, agar pemanfaatan *AI* tidak hanya efektif secara operasional tetapi juga beretika, aman, dan selaras dengan prinsip pertahanan nasional yang berkelanjutan.

F) Sistem Komando dan Kontrol:

Akurasi tinggi atas analisis data berdasarkan basis data dalam jumlah besar (*big data*) menjadi hal yang membuat *AI* dianggap menarik. Dalam hal ini keputusan-keputusan besar berbasis akurasi tinggi dapat dilakukan dengan memanfaatkan hasil predictive

analysis *AI*. Sehingga, bukan tidak mungkin *AI* dapat dimanfaatkan juga sebagai bagian dari alat pendukung pengambilan kebijakan pertahanan. Bahkan dalam konteks yang mungkin lebih harus diwaspadai, *AI* bukan hanya bertindak sebagai alat pendukung pengambilan kebijakan melainkan juga bertindak langsung sebagai penentu/pengambil kebijakan.

Mengutip pada Lampiran Peraturan Menteri Pertahanan Republik Indonesia Nomor 12 Tahun 2021 tentang Kebijakan Penyelenggaraan Pertahanan Negara Tahun 2020 – 2024 (Jakgara Hanneg 2020-2024), Revolusi Industri 4.0 sudah mengubah medan perang abad ke-21, dengan beberapa cara berbeda, yaitu ruang angkasa dan satelit. Ruang pertempuran saat ini tidak hanya di darat, laut, dan udara, tapi saat ini sudah mencakup pada satelit ruang angkasa dan siber. Selain itu perkembangan lainnya adalah teknologi kecerdasan buatan (*artificial intelligence*) yang membantu proses pengambilan keputusan secara mandiri, big data, machine learning, sistem otomatis, dan teknologi robot. Revolusi Industri 4.0 telah mendorong munculnya serangkaian sistem senjata baru yang inovatif, termasuk senjata elektromagnetik (railgun), senjata energi terarah, proyektil kecepatan tinggi, dan rudal hipersonik. Revolusi Industri 4.0 telah menambah dimensi pertempuran dari darat, laut, dan udara meluas ke ranah ruang angkasa dan ruang siber. Paradigma perang modern di masa yang akan datang antara lain perang asimetris dan perang tak terbatas yang mengandalkan kecanggihan teknologi informasi dan komunikasi, unsur militer, serta aspek nirmiliter. Karakteristik perang modern antara lain: terjadinya ancaman secara sistematis, bersamaan dan simultan; perang keunggulan teknologi persenjataan (*Network Centric Warfare*); perang berbasis kecerdasan buatan seperti teknologi robot telah melahirkan perang dengan menggunakan wahana tak berawak, dan perang siber.

Jika melihat penjelasan dalam bagian latar belakang Jakgara Hanneg 2020-2024 di atas, hal tersebut menunjukan bahwa Pemerintah Republik Indonesia sudah memahami bagaimana penggunaan *AI* dalam konteks pertahanan negara memiliki dampak positif sekaligus merupakan ancaman tersendiri bagi pertahanan negara. Dalam konteks manfaat, selain dapat dilihat pada pembahasan sebelumnya mengenai cara *AI* diterapkan pada sistem pertahanan, sebenarnya manfaat penggunaan *AI* dalam konteks pertahanan tentu secara umum sama dengan alasan awal *AI* ada, percepatan, akurasi, efisiensi adalah bagian umum dari manfaatnya.

Mengutip pada pendapat Jimena Sofia Viveros Alvarez, anggota dari *The United Nation Secretary General (UNSG) High Level Advisory Body* on *AI*, dikatakan bahwa kemampuan penargetan *AI* yang telah diperbarui masih belum diketahui dan meskipun ada beberapa kelebihan yang diduga, teknologi ini tidak memiliki standar pengujian dan peninjauan yang sesuai sebelum digunakan. Selain itu, sebagai hasil aktivitas manusia, sistem ini juga rentan terhadap kesalahan karena sifatnya yang tidak dapat diprediksi dan tidak dapat dijelaskan, data yang digunakan untuk melatihnya tidak akan pernah sempurna, dan risikonya yang melekat hanya akan semakin parah jika penggunaan *AI-DSS* yang terus meningkat dapat menyebabkan bias otomatisasi di medan perang. Inilah sebabnya mengapa penilaian manusia yang efektif harus menjadi persyaratan yang sangat penting sebelum dan selama keseluruhan operasi militer apa pun(Álvarez, 2024).

Selain berkenaan dengan resiko nyata penggunaan sistem AI yang berbasis pada tujuan (*goal-driven*) seperti *drone* yang dilengkapi dengan kemampuan pendeteksian dan juga senjata, resiko juga melekat pada perubahan ambang batas para pembuat kebijakan. Menurut Michael C. Horowitz and Paul Scharre, Integrasi *AI* ke dalam sistem militer, dikombinasikan dengan pergeseran ke arah struktur kekuatan yang lebih robotik, juga dapat mengubah ambang batas pengambilan risiko para pembuat kebijakan, baik karena mereka percaya bahwa lebih sedikit nyawa manusia yang terancam atau bahwa sistem *AI* memungkinkan presisi yang lebih tinggi, atau mungkin karena mereka melihat sistem *AI* sebagai sesuatu yang sangat berbahaya.

Ketersediaan sistem *AI* yang dirasakan dapat mengubah keyakinan para pembuat kebijakan tentang kemampuan mereka untuk meramalkan hasil konflik atau untuk menang(Horowitz & Scharre, 2021).

Mengutip catatan Komite *Internasional Palang Merah* (ICRC) yang dikutip oleh Robert Weismann dan Savannah Wooten, ICRC mencatat bahwa "proses di mana sistem senjata otonom berfungsi: menimbulkan risiko bahaya bagi mereka yang terkena dampak konflik bersenjata, baik warga sipil maupun kombatan, serta bahaya eskalasi konflik; menimbulkan tantangan untuk mematuhi hukum internasional, termasuk hukum *humaniter* internasional, khususnya, aturan tentang perilaku permusuhan untuk melindungi warga sipil; dan menimbulkan masalah etika mendasar bagi kemanusiaan, yang pada dasarnya menggantikan keputusan manusia tentang hidup dan mati dengan proses sensor, perangkat lunak, dan mesin(Robert Weissman & Wooten, 2024).

Permasalahan Etika dan Konsep Tata Kelola AI (AI Governance)

Dr. Alexander Blanchard, *Senior Researcher* pada *Stockholm International Peace Research Institute (SIPRI)*, sebagaimana disampaikan pada webinar dengan tema Penggunaan AI dalam Domain Militer yang diselenggarakan oleh *Vienna Center for Disarmament and Non-Proliferation (VCDNP)* pada tanggal 26 Maret 2024, menekankan mengenai potensi besar penggunaan *AI* dalam pertahanan nasional, dengan menyoroti bahwa, seiring penerapannya beralih dari fungsi pendukung ke penggunaan yang bersifat permusuhan, pertimbangan etika menjadi lebih kompleks. Pendekatan umum di bidang sipil yang terdiri dari pengembangan serangkaian prinsip tentang penggunaan *AI* yang bertanggung jawab telah mendapatkan popularitas di ranah militer, khususnya di negara-negara Barat. Pendekatan ini memiliki tantangan tersendiri, terutama karena pendekatan ini tidak menawarkan banyak hal untuk memastikan standarnya terpenuhi dalam praktik. Ke depannya, Dr. Blanchard menekankan perlunya standar bersama di seluruh kementerian pertahanan dan angkatan bersenjata tentang penggunaan *AI* dan menekankan perlunya keterlibatan berbagai pemangku kepentingan untuk mengatasi pertanyaan etika(Zarka, 2024).

Pernyataan mengenai pentingnya etika penggunaan *AI* dalam aspek militer juga ditegaskan oleh Sebastian Clapp dalam tulisannya yang berjudul *Defence and Artificial Intelligence yang diterbitkan European Parliamentary Research Service (EPRS)* pada April 2025. Ia mengatakan bahwa integrasi *AI* ke dalam peperangan menimbulkan beberapa masalah etika yang penting. Salah satu masalah yang signifikan adalah akuntabilitas dan tanggung jawab. Menentukan siapa yang bertanggung jawab ketika sistem *AI* membuat keputusan otonom adalah hal yang rumit. Jika sistem *AI* menyebabkan kerusakan yang tidak diinginkan, menetapkan tanggung jawab menjadi sulit, yang mengarah pada kekhawatiran tentang akuntabilitas dalam operasi militer(Clapp, 2025).

Berkenaan dengan permasalahan etika pada penggunaan *AI*, dalam konteks permasalahan Kesehatan, etika juga menjadi perhatian utama. Dalam hal ini *World Health Organization* (*WHO*) telah membuat *ethical guidelines* sebagai panduan etika dalam penggunaan *AI* di dunia kesehatan. Dalam hal ini secara spesifik *WHO* mengenalkan konsep "Kerangka Kerja untuk Tata Kelola Penggunaan *AI* Untuk Kesehatan". Dalam konteks ini WHO membahas dimensi etika dari beberapa area tata kelola, seperti 1) Tata kelola data (*governance of data*) yang meliputi perlindungan data, kontrol komunitas atas data, data sharing, dan lain-lain; 2) Kontrol dan pembagian keuntungan (*control & benefit sharing*) seperti kepemilikan produk AI; 3) Tata kelola sektor swasta (*governance of the private sector*) seperti peran *self-governance*, *Publics-private partnership for AI for healthcare*, dan lain-lain; 4) Tata kelola sektor public (*governance of the public sector*) seperti penilaian (*assessing*) mengenai kelayakan *AI*, akuntabilitas *AI*, perlindungan sosial, dan lain-lain; 5) Pertimbangan peraturan (*regulatory considerations*); 6) Observatorium kebijakan dan model legislasi (*Policy*

observatory and model legislation); dan 7) Tata kelola global mengenai *AI* (*global governance of AI*)(Worl Head Organization, 2021).

Semestinya, landasan etik yang diperlukan dalam penggunaan *AI* dalam konteks pertahanan maupun kesehatan tidak akan begitu berbeda secara prinsip, meskipun secara teknis tentu berbeda, sehingga framework penggunaan *AI* dalam perspektif kesehatan yang dikeluarkan WHO masih dapat relevan untuk juga diterapkan dalam perspektif pertahanan.

Kesiapan Kerangka Hukum Indonesia dalam Pemanfaatan Artificial Intelligence (AI) untuk Pertahanan Nasional

Dalam era transformasi digital, kecerdasan buatan (*AI*) telah menjadi instrumen kritis dalam memperkuat keamanan siber dan pertahanan nasional. Indonesia, sebagai negara dengan populasi digital terbesar keempat di dunia, menghadapi ancaman siber yang semakin kompleks, mulai dari serangan ransomware hingga infiltrasi sistem pertahanan berbasis teknologi. Pemanfaatan *AI* untuk deteksi ancaman, analisis *big data*, dan respons otomatis menjadi solusi strategis. Revolusi Industri 4.0 mendorong penggunaan kecerdasan buatan (*AI*) di berbagai sektor, termasuk industri pertahanan. Para pemimpin dunia menekankan pentingnya pengembangan *AI*, dengan anggapan bahwa penguasaan teknologi ini akan menentukan kekuatan global. *AI* kini krusial dalam medan pertempuran multi-domain, mencakup darat, laut, udara, dan siber(Dwipratama, 2024).

Namun, efektivitasnya bergantung pada kerangka hukum yang komprehensif dan responsif. Saat ini, Indonesia memiliki sejumlah regulasi seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Siber (UU No. 11/2008 yang direvisi menjadi UU No. 19/2016), tetapi belum secara spesifik mengatur pemanfaatan AI. Padahal, AI memerlukan pengaturan terkait akuntabilitas algoritmik, perlindungan data sensitif, dan mitigasi risiko bias yang dapat mengancam stabilitas keamanan. Tanpa payung hukum yang jelas, integrasi AI berpotensi menciptakan celah hukum (legal vacuum), terutama dalam konteks pertahanan nasional yang memerlukan presisi dan kepatuhan pada prinsip jus in bello (hukum perang).

Kesiapan kerangka hukum Indonesia untuk pemanfaatan kecerdasan buatan (AI) dalam keamanan siber dan pertahanan nasional sangat penting di era digital. Indonesia perlu mengembangkan regulasi yang jelas, termasuk penyesuaian Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), untuk mengatasi ancaman siber yang kompleks. Kolaborasi antara pemerintah, sektor swasta, dan masyarakat juga diperlukan untuk menciptakan ekosistem yang aman(Cahya et al., 2024).

Kerangka hukum Indonesia untuk keamanan siber dan pertahanan saat ini bersifat sektoral dan belum terintegrasi dengan visi pemanfaatan AI. UU No. 3/2002 tentang Pertahanan Negara mengamanatkan perlindungan kedaulatan melalui sistem pertahanan berlapis, tetapi tidak menyebutkan peran teknologi seperti *AI*. Sementara itu, Peraturan Presiden No. 47/2016 tentang Badan Siber dan Sandi Negara (BSSN) hanya mengatur penguatan kapasitas keamanan siber tanpa mengakomodasi inovasi *AI*. Di sisi lain, Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) yang sedang dibahas dapat menjadi landasan untuk mengatur etika *AI*, namun belum menyentuh aspek pertahanan.

Implementasi *AI* dalam pertahanan nasional menghadapi tantangan hukum multidimensi. Pertama, aspek *accountability*: siapa yang bertanggung jawab jika sistem *AI* gagal mendeteksi ancakan atau justru melakukan serangan otomatis yang melanggar kedaulatan negara lain? Regulasi Indonesia belum mengatur *liability* untuk keputusan berbasis *AI*, baik dalam konteks operasi militer maupun keamanan siber. Kedua, interoperabilitas sistem: *AI* memerlukan integrasi data lintas instansi (TNI, Polri, BSSN), tetapi UU No. 43/2008 tentang Kearsipan dan UU No. 14/2008 tentang Keterbukaan Informasi Publik membatasi berbagi data sensitif. Ketiga, dinamika ancaman siber yang berkembang cepat tidak diimbangi dengan fleksibilitas

regulasi. Misalnya, penggunaan *deepfake* untuk disinformasi strategis belum diantisipasi dalam UU ITE.

Diperlukan pembentukan *regulatory sandbox* untuk menguji coba *AI* dalam lingkungan terkendali, serta amendemen UU yang memasukkan mekanisme *sunset clause* agar regulasi dapat diperbarui sesuai perkembangan teknologi. Menegaskan pentingnya adaptasi TNI, khususnya Angkatan Udara, terhadap kemajuan zaman dan penerapan AI untuk tugas-tugas berisiko tinggi. TNI AU telah mengimplementasikan AI dalam sistem komunikasi dan pusat komando. Selain itu, KSAU menekankan perlunya persiapan personel yang kompeten dalam bidang AI, agar dapat menerapkan pengetahuan yang diperoleh setelah pendidikan. TNI berkomitmen untuk terus berkolaborasi dengan akademisi dan ahli dalam pengembangan AI(Yakub & Indrawan, 2023).

Penggunaan teknologi deepfake dalam konteks disinformasi strategis di Indonesia belum diatur secara memadai dalam Undang-Undang No 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE). Meskipun terdapat ketentuan mengenai penyebaran berita bohong, regulasi tersebut tidak secara eksplisit mencakup penggunaan deepfake sebagai alat untuk menyebarkan informasi yang menyesatkan. Hal ini menciptakan kekosongan hukum yang berpotensi menimbulkan ketidakpastian hukum dan penyalahgunaan teknologi. Oleh karena itu, diperlukan revisi atau penambahan regulasi yang lebih komprehensif untuk mengakomodasi perkembangan teknologi ini dan memberikan sanksi yang tegas terhadap pelanggaran yang terjadi(Nabhila, 2024).

Pemanfaatan AI untuk keamanan siber dan pertahanan berpotensi berbenturan dengan hak privasi dan etika jika tidak diatur secara ketat. Pengawasan massal (mass surveillance) berbasis AI, meski efektif mendeteksi ancaman, dapat melanggar Pasal 28G UUD 1945 tentang hak atas rahasia pribadi. Selain itu, algoritma *AI* yang dilatih dengan data bias berisiko melakukan diskriminasi dalam analisis ancaman, seperti mengkategorikan kelompok tertentu sebagai "berisiko tinggi" tanpa dasar empiris. Indonesia perlu mengadopsi prinsip *privacy by design* dan *ethics by default* dalam regulasi, sebagaimana diatur dalam *General Data Protection Regulation* (GDPR) Uni Eropa. Namun, hal ini harus diselaraskan dengan kebutuhan pertahanan, misalnya melalui penerapan *security exception* yang diatur ketat. UU No. 9/2013 tentang Pencegahan dan Pemberantasan Tindak Pidana Pendanaan Terorisme dapat menjadi acuan untuk menyeimbangkan kepentingan keamanan dan hak asasi, dengan menetapkan mekanisme pengawasan independen terhadap penggunaan *AI* oleh instansi pertahanan. Meski demikian, pengembangan teknologi *AI* di dunia pertahanan akan terus dilakukan untuk memperkuat persenjataan TNI(Patoppoi, 2024).

Bentuk Ideal atas Kerangka Hukum Pemanfaatan AI dalam Konteks Pertahanan Nasional

Hal dilematis dalam permasalahan etika penggunaan *AI* adalah bahwa meskipun nantinya dalam hukum internasional terdapat kesepakatan mengenai landasan etik penggunaan AI, namun tidak ada yang dapat menjamin bahwa negara-negara sebagai subjek hukum internasional akan mematuhi landasan etik tersebut. Sehingga, secara nasional, masing-masing negara pada akhirnya akan menyesuaikan landasan etiknya dengan coraknya masing-masing.

Dalam konteks Indonesia, meskipun tidak secara spesifik berkenaan dengan sistem pertahanan, penggunaan AI secara umum setidaknya sudah memiliki landasan etik, sekalipun belum dalam bentuk regulasi yang komperhensif. Landasan etik mengenai penggunaan *AI* secara umum dibahas dalam Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial. Hal ini menunjukan bahwa aspek etik menjadi salah satu faktor mendesak untuk memastikan peran AI tidak justru kontra produktif dengan tujuan awal pemanfaatan *AI*.

Namun demikian, dalam menghadapi resiko *AI* khususnya dalam aspek pertahanan, regulasi harus dibuat secara komperhensif, landasan etik tidak bisa hanya berada pada level

prinsip, melainkan harus dapat diejawantahkan dalam bahasa yang jauh lebih teknis. Sebagai contoh, penggunaan *AI* dalam konteks pertahanan harus mengedepanan prinsip transparansi, salah satunya adalah dengan membentuk peraturan teknis berkenaan dengan tata kelola (governance) penggunaan *AI* seperti batasan-batasan kewenangan, teknis pengambilan persetujuan dan keputusan penggunaan *AI*, kewajiban teknis pemetaan area yang telah dan akan menggunakan *AI*, kewajiban audit *AI* secara berkala atas penggunaan *AI* yang sudah dilakukan, kewajiban untuk melakukan penilaian resiko atas rencana penggunaan *AI*, kewajiban pengujian pemahaman dan kemampuan pengguna *AI*, hingga permasalahan teknis penegakan hukum pemanfaatan *AI* yang tidak sesuai. Terkait permasalahan penegakan hukum, tentu dalam konteks pertahanan akan lebih kompleks mengingat wilayah penegakannya berada pada lingkup peradilan militer.

Untuk memastikan kesiapan kerangka hukum Indonesia, diperlukan langkah-langkah strategis. Pertama, menyusun RUU Kecerdasan Buatan yang mengatur pemanfaatan *AI* di bidang pertahanan dan keamanan siber, termasuk standar transparansi, akuntabilitas, dan tata kelola data. Kedua, merevisi UU Pertahanan dan UU Siber dengan memasukkan klausul tentang penggunaan teknologi otonom, batasan *lethal autonomous weapons* (LAWs), serta kolaborasi sipil-militer dalam riset *AI*. Ketiga, membentuk lembaga pengawas *AI* multidisiplin yang melibatkan pakar hukum, etika, dan teknologi untuk memastikan kepatuhan regulasi. Keempat, memperkuat kerja sama internasional melalui ratifikasi konvensi seperti *Budapest Convention on Cybercrime* dan inisiatif *Global Partnership on Artificial Intelligence* (GPAI) untuk harmonisasi standar. Kelima, meningkatkan kapasitas SDM melalui pendidikan hukum teknologi di perguruan tinggi dan pelatihan spesialis *AI* untuk aparat penegak hukum. Dengan langkah-langkah ini, Indonesia dapat membangun ketahanan siber yang adaptif tanpa mengorbankan prinsip demokrasi dan hak asasi manusia.

Salah satu tantangan utama dalam integrasi *AI* ke sektor pertahanan Indonesia adalah fragmentasi regulasi dan ketertinggalan kerangka hukum nasional dalam mengakomodasi perkembangan teknologi disruptif. Saat ini, payung hukum utama seperti Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) belum secara spesifik mengatur penggunaan AI dalam konteks militer. Padahal, *AI* memerlukan standar hukum yang jelas terkait *liability* (tanggung jawab hukum) saat terjadi kegagalan sistem, *data governance* (tata kelola data), dan *interoperabilitas* dengan sistem pertahanan sekutu. Misalnya, penggunaan *predictive maintenance* berbasis *AI* untuk pesawat tempur memerlukan protokol keamanan siber yang ketat guna mencegah kebocoran data teknis sensitif.

Kepala Staf TNI Angkatan Udara, Marsekal TNI Mohammad Tonny Harjono, pada Agustus 2024 di Jakarta, menegaskan pentingnya peningkatan kualitas prajurit dalam mengoperasikan alat utama sistem senjata (alutsista) berteknologi tinggi, termasuk kecerdasan buatan (AI). Dalam seminar di Lanud Halim Perdanakusuma, ia menyatakan bahwa pemahaman dan kemampuan personel sangat krusial untuk memanfaatkan teknologi ini secara efektif dan aman. Tonny juga menekankan upaya peningkatan kualitas SDM melalui pendidikan, pelatihan, dan pertukaran pelajar, agar TNI AU semakin kuat dalam menjaga kedaulatan udara Indonesia(Marison & Yakub, n.d.).

Selain itu, ketiadaan regulasi tentang *lethal autonomous weapons systems* (LAWS) berpotensi menimbulkan dilema etis jika sistem senjata otonom digunakan tanpa kontrol manusia yang memadai. Di tingkat internasional, Indonesia juga perlu meratifikasi instrumen seperti *Convention on Certain Conventional Weapons* (CCW) untuk memastikan keselarasan dengan norma global. Tanpa harmonisasi regulasi, implementasi *AI* dalam Alutsista berisiko melanggar prinsip *law of armed conflict* (LOAC) dan menurunkan kredibilitas diplomasi pertahanan Indonesia. Marsekal Pertama TNI Ardi Syahri, mengumumkan rencana pengembangan teknologi pertahanan berbasis kecerdasan buatan (AI) pada tahun 2025. Saat

ini, peralatan untuk siber dan AI masih belum lengkap dan akan diperbaiki berdasarkan evaluasi tahun 2024. Meskipun pengembangan AI untuk keamanan udara telah dimulai, masih diperlukan tambahan dana dan fasilitas, termasuk laboratorium di Skuadron Pendidikan 506 Bogor. TNI AU berkomitmen untuk serius dalam mengembangkan teknologi AI demi mendukung pertahanan Indonesia(Marison & Kusbiantoro, 2025).

Persoalan etis dan legal menjadi sentral dalam debat implementasi *AI* untuk pengembangan Alutsista, terutama terkait penggunaan sistem senjata otonom (*autonomous weapons systems*). Meskipun *AI* mampu meningkatkan presisi dan kecepatan respons militer, sistem ini berpotensi melanggar prinsip pembedaan (*distinction*) dan proporsionalitas (*proportionality*) dalam hukum humaniter internasional jika tidak dirancang dengan algoritma yang transparan. Misalnya, algoritma *AI* yang digunakan dalam sistem pertahanan udara mungkin kesulitan membedakan antara pesawat musuh dan sipil dalam situasi konflik ambigu. Pada tanggal 9 September 2024, diadakan Konferensi Tingkat Tinggi *REAIM* (The Responsible AI in the Military Domain) di Seoul, Korea Selatan, yang dihadiri oleh Menteri Pertahanan dari sekitar 90 negara. Pertemuan ini bertujuan untuk mengeksplorasi dan mendorong penggunaan *kecerdasan buatan* (*AI*) dalam konteks perdamaian dan keamanan internasional. Dalam sambutannya, Menteri Pertahanan Kim Yong-hyun menekankan pentingnya kolaborasi internasional untuk memahami penggunaan *AI* yang bertanggung jawab di bidang militer. Rapat utama membahas tema-tema krusial, dan pada penutupan, para pejabat tinggi menandatangani *Blueprint for Action*, yang berisi pedoman dasar penggunaan *AI* dalam konteks militer(Berita et al., 2024).

Di Indonesia, ketiadaan *ethical guidelines* khusus untuk pengembangan *AI* militer dapat memperparah risiko tersebut. Selain itu, aspek legal seperti *accountability gap* (kesenjangan akuntabilitas) muncul ketika kegagalan sistem menyebabkan korban sipil, tetapi tidak ada kejelasan apakah tanggung jawab berada di tangan operator, developer, atau institusi militer. Ketidakadaan panduan etis *AI* militer mengancam martabat manusia (prinsip Kant) dan otonomi moral. Senjata otonom menghilangkan akuntabilitas, berisiko eskalasi konflik tak terkendali. Tanpa batasan deontologis, teknologi menginstrumentalisasi manusia sebagai sarana perang. Diperlukan kebijakan global yang melarang *AI* otonom mematikan dan memastikan keputusan akhir oleh manusia untuk mencegah dehumanisasi dan pelanggaran HAM(Huda et al., 2024).

Tantangan lain adalah perlindungan data intelijen yang diolah *AI*, mengingat Undang-Undang Perlindungan Data Pribadi (PDP) belum sepenuhnya mengatur penggunaan data militer. Untuk itu, Kementerian Pertahanan perlu merumuskan *code of conduct* yang mengikat kerja sama dengan pihak ketiga (sektor swasta atau mitra asing) dalam pengembangan *AI*, termasuk mekanisme audit independen untuk memastikan kepatuhan terhadap prinsip *privacy by design* dan *security by default*. Dalam situasi seperti ini, penting bagi setiap individu untuk memiliki kesadaran moral dan etis yang tinggi dalam pengembangan dan penggunaan *AI* secara bertanggung jawab. Oleh karena itu, perlu ada penyusunan pedoman etika yang dilakukan secara kolaboratif dengan melibatkan berbagai pihak yang berkepentingan(Sudiro et al., 2024).

Implementasi *AI* dalam Alutsista Indonesia juga terkendala oleh kapasitas teknologi dalam negeri yang masih terbatas dan ketergantungan tinggi pada mitra asing. Meskipun Indonesia telah meluncurkan proyek strategis seperti *Defense Industry Holding* (Defend ID) untuk memperkuat kemandirian industri pertahanan, penguasaan teknologi *AI* masih bergantung pada transfer pengetahuan dari negara-negara seperti Turki, Prancis, atau Tiongkok. Hal ini menimbulkan kerentanan strategis, terutama terkait *backdoor access* (akses tersembunyi) yang dapat dimanfaatkan pihak asing untuk memata-matai sistem pertahanan nasional.

Selain itu, minimnya investasi dalam riset dan pengembangan (R&D) *AI* di lingkungan akademis-militer memperlambat pembentukan *talent pool* ahli *AI* bidang pertahanan. Padahal,

penguasaan teknologi kritis seperti *quantum computing* dan *neuromorphic engineering* menjadi kunci untuk mengembangkan sistem AI yang adaptif di medan perang modern. Untuk mengurangi ketergantungan, pemerintah perlu memperkuat kolaborasi triple helix antara TNI, industri lokal, dan universitas melalui program seperti *national AI strategy* yang berfokus pada kebutuhan pertahanan. Langkah ini harus didukung oleh insentif fiskal untuk riset *AI* serta pembentukan *cyber defense ecosystem* yang terintegrasi dengan sistem Alutsista.

KESIMPULAN

Pemanfaatan *Artificial Intelligence* (*AI*) dalam sistem pertahanan Indonesia, khususnya Alat Utama Sistem Senjata (Alutsista), memiliki potensi besar untuk meningkatkan efektivitas, efisiensi, dan respons militer nasional. Namun, hal ini juga memiliki resiko yaitu menimbulkan tantangan signifikan dalam aspek regulasi, etika, dan teknologi. Indonesia saat ini belum memiliki kerangka hukum yang komprehensif dan adaptif terhadap dinamika teknologi *AI*, baik dalam konteks pertahanan. Padahal perkembangan teknologi *AI* bergerak secara cepat dan sangat rentan terhadap isu disrupsi teknologi.

Dalam menjawab tantangan tersebut, rekomendasi sejumlah langkah strategis menjadi sangat diperlukan, yaitu dilakukannya reformulasi regulasi nasional baik itu berupa pembentukan peraturan perundang-undangan baru yang mengatur secara khusus mengenai pemanfaatan *AI* secara umum maupun membentuk peraturan turunan yang sifatnya lebih sektoral yaitu dalam konteks pertahanan nasional. Pada prinsipnya merujuk pada pembahasan-pembahasan di atas, maka aspek terpenting dari pembentukan peraturan yang ideal berkenaan dengan pemanfaatan *AI* dalam pertahanan nasional adalah peraturan tersebut 1) Harus dapat adaptif mengikuti perkembangan teknologi *AI* untuk menghindari disrupsi teknologi; 2) Karena sifatnya lintas negara maka harus juga merujuk pada prinsip-prinsip hukum internasional; 3) Mengacu pada nilai-nilai etika pertahanan yang mana harus dapat diejawantahkan melalui teknis tata kelola *AI* (*AI governance*) yang komperhensif.

Dengan pendekatan holistik ini, Indonesia diharapkan mampu memanfaatkan *AI* secara optimal dalam pertahanan tanpa mengorbankan prinsip-prinsip kedaulatan, HAM, dan kepatuhan hukum internasional.

REFERENSI

Álvarez, J. S. V. (2024). *The risks and inefficacies of AI systems in military targeting support How does AI DSS affect targeting ? AI-supported targeting : enhancing precision or increasing civilian casualties ?*

Berita, F., Korea, T., & Kami, T. (2024). *Menteri-menteri Pertahanan Bertemu di Seoul untuk Diskusikan Penggunaan AI*. 3–8.

Cahya, A. N., Maksum, M. A., & Primadana, T. A. S. (2024). Transformasi Budaya Hukum dalam Era Digital (Implikasi Penggunaan AI dalam Perkembangan Hukum Di Indonesia). *IKRA-ITH HUMANIORA: Jurnal Sosial Dan Humaniora*, *8*(2), 361–373.

Clapp, S. (2025). *Defence and artificial intelligence*. *April*.

Dwipratama, G. P. (2024). *Implikasi Kecerdasan Buatan Dalam Industri Pertahanan : Tantangan Dan Peluang Bagi Indonesia*. Kemhan.Go.Id. https://www.kemhan.go.id/pothan/2024/03/20/implikasi-kecerdasan-buatan-dalam-industri-pertahanan-tantangan-dan-peluang-bagi-indonesia.htm

Horowitz, M., & Scharre, P. (2021). *AI and International Stability: Risks and Confidence-Building Measures*. 1–21.

Huda, A. N., Winarno, A., & Yahya, K. (2024). *Transhumanism Ethics : A Critical Analysis Of Ai Technology Development And Its Implications*. *3*(2), 273–292.

Marison, W., & Kusbiantoro, D. (2025). *TNI AU kembangkan teknologi pertahanan berbasis*

AI.

Marison, W., & Yakub, E. M. (n.d.). *KSAU tingkatkan kualitas prajurit agar gunakan alutsista teknologi AI*. Antaranews. Retrieved March 19, 2025, from https://www.antaranews.com/berita/4232223/ksau-tingkatkan-kualitas-prajurit-agar-gunakan-alutsista-teknologi-ai

Nabhila, C. (2024). *Pancasila LawReview Analisis Tentang Respon Hukum Terkait Penggunaan*. *1*(2), 69–87.

Nugroho, A. (2021). Analisis Penggunaan Kecerdasan Buatan (Artificialintelligence/Ai)Oleh Tni Ad Dalam Mendukung Sistem Pertahanan Negara. *Markas Besar Tni Angkatan Darat Sekolah Staf Dan Komando*, *AI dalam sistem pertahanan negara*, 1–69.

Patoppoi, B. (2024). *Kemenhan Pastikan Hati-Hati Adopsi Teknologi AI untuk Alutsista*. https://www.suarasurabaya.net/kelanakota/2024/kemenhan-pastikan-hati-hati-adopsi-teknologi-ai-untuk-alutsista/

Prakoso, L. Y., Soemantri, A. I., & Prasetyo, H. (2024). *Kebijakan Pertahanan Negara : Indonesia Emas 20245* (F. Z. Alman (ed.)). Widina Media Utama.

Rashid, A. Bin, 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*. https://doi.org/10.1155/2023/8676366

Robert Weissman, & Wooten, S. (2024). *A.I. Joe: The Dangers of Artificial Intelligence and the Military By*. 1–17.

Simpson, K. H., Paquette, S., Racicot, R., & Villanove, S. (2025). *Militarizing AI : How to Catch the Digital Dragon ? AI holds the potential to fundamentally rede fi ne modern warfare* . 1–8.

Sudiro, A., R., M., Syailendra, Ariesta, D., Sitabuana, T. H., Marhaen, D., Sanjaya, D., Amri, I. F., Lathif, N., Rasji, Kurnia, I., Yehezkiel, R., Chendarwan, P., Wardhana, A. P. K., Mamusung, L. Z., Kolopaking, A. D. A., Martinelli, I., Tjempaka, Anggraeni, R., … DP, S. H. (2024). Pembaharuan Hukum. In *Book Chapter* (pp. 1–23).

Wijayakusuma, U., Buatan, K., Kriminal, K., & Kejahatan, P. (2024). *Reformulasi Kebijakan Kriminal Dalam Penanggulangan*. *5*(2), 60–75.

Worl Head Organization. (2021). *Ethics and Governance Of Artificial Intelligence For Health*. https://doi.org/10.1142/9789811238819_0001

Xinhua, & Marboen, A. P. (2024). *Ratusan pasis Seskoau kunjungi China pelajari AI di bidang pertahanan*. https://www.antaranews.com/berita/4260415/ratusan-pasis-seskoau-kunjungi-china-pelajari-ai-di-bidang-pertahanan

Yakub, E. M., & Indrawan, H. S. (2023). *KSAU: TNI sudah amati perkembangan AI untuk pertahanan negara*. Antaranews. https://www.antaranews.com/berita/3854529/ksau-tni-sudah-amati-perkembangan-ai-untuk-pertahanan-negara

Zarka, M. (2024). *Artificial Intelligence in the Military Domain_ Technical, Legal, and Ethical Perspectives*.