e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 10 No 8 Tahun 2023 Hal. : 4051-4057

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

TANTANGAN TERHADAP MASA DEPAN PERTAHANAN NEGARA AKIBAT KECERDASAN BUATAN

Ardian Yudopratomo

Magister Terapan Strategi Operasi Laut Sekolah Staf dan Komando Angkatan Laut

Abstrak

Perkembangan kecerdasan buatan (Artificial Intelligence/AI) telah membawa perubahan signifikan dalam konteks pertahanan, menghadirkan tantangan dan peluang yang perlu ditangani dengan penyesuaian strategis yang tepat. Tulisan ini membahas penyesuaian strategis dalam menghadapi perubahan yang disebabkan oleh kecerdasan buatan dalam konteks pertahanan. Dalam menghadapi perubahan ini, empat aspek utama yang perlu diperhatikan adalah pengembangan dan penguasaan teknologi AI, perumusan kebijakan dan regulasi yang tepat, penguatan kemampuan manusia, serta kerja sama dan kemitraan yang kuat. Pengembangan teknologi dan infrastruktur yang memadai, bersama dengan regulasi yang jelas dan komprehensif, menjadi landasan untuk memastikan penggunaan AI dalam pertahanan dilakukan secara etis dan aman. Selain itu, penting juga untuk memberdayakan kemampuan manusia dan menjaga peran penting mereka sebagai pengambil keputusan akhir dalam konteks pertahanan. Kerja sama dan kolaborasi antara negara, lembaga pertahanan, industri, dan institusi akademik menjadi kunci untuk mengoptimalkan potensi kecerdasan buatan dalam pertahanan. Dengan penyesuaian strategis yang tepat, negara dapat menghadapi perubahan dengan cerdas dan efektif, menjaga keamanan dan pertahanan negara dalam menghadapi ancaman yang semakin kompleks.

Kata Kunci: Kecerdasan Buatan, Pertahanan, Penyesuaian strategis, Teknologi, Kerjasama.

PENDAHULUAN

Undang-Undang Republik Indonesia Nomor 34 Tahun 2004 mengatur tentang TNI sebagai alat pertahanan negara yang bertugas melaksanakan kebijakan pertahanan untuk menjaga kedaulatan, wilayah, dan keselamatan bangsa. TNI memiliki tugas pokok untuk melindungi bangsa dan negara dari ancaman militer dan non-militer. Sebagai komponen utama pertahanan negara, TNI harus mampu menghadapi ancaman dari dalam dan luar negeri yang dapat mengancam

*Correspondence Address : ardian.yudopratomo@gmail.com
DOI : 10.31604/jips.v10i8.2023.4051-4057

kedaulatan, wilayah, dan keselamatan bangsa.

Pasal 25 huruf a UUD 1945 menyebutkan bahwa Indonesia adalah negara kepulauan dengan batas dan wilayah yang ditetapkan oleh Undang-Undang. Wilayah Indonesia memiliki perbatasan darat dengan Malaysia, Papua Nugini, dan Timor Leste. Kepulauan yang luas meningkatkan risiko pertahanan negara terutama di wilayah perbatasan yang sulit untuk diawasi secara efektif. Oleh karena itu, ancaman ini perlu diantisipasi dan ditangani dengan cepat dan tepat.

Salah satu cara untuk mengatasi ancaman di wilayah perbatasan adalah dengan memanfaatkan teknologi dalam sistem pertahanan yang mendukung operasi pengamanan perbatasan TNI. Operasi ini melibatkan ancaman seperti kejahatan lintas negara, penyelundupan, pencurian sumber daya alam, dan penyeberangan batas secara ilegal. Oleh karena itu, penggunaan dan penguasaan teknologi oleh TNI dalam pemantauan lintas batas sangat penting untuk mendeteksi ancaman dengan cepat dan mengambil langkah pencegahan serta penindakan yang tepat.

Dalam paparannya, Rektor Universitas Pertahanan RI menyoroti peran penting *big data* dan kecerdasan buatan (*Artificial Intelligence*/AI) dalam sistem keamanan negara. Pemanfaatan kecerdasan buatan (*Artificial Intelligence*/AI) dalam pertahanan negara bertujuan untuk meningkatkan akurasi sistem senjata, efisiensi penggunaan sumber daya, dan mengurangi jumlah korban prajurit dalam operasi militer (Juanda, 2020). Pemanfaatan big data dalam bidang pertahanan negara fokus pada validasi proses dan mekanisme berbagi informasi dari berbagai sumber data dengan berbagai jenis data. Tujuannya adalah untuk menyusun data secara prioritas dan memungkinkan pengambilan keputusan yang cepat dan tepat dalam konteks aksi militer dengan membangun kecerdasan buatan.

Kecerdasan buatan telah merevolusi dunia pertahanan dengan kemampuannya yang luar biasa. Namun, dengan kemajuan ini, timbul pula tantangan yang perlu diatasi agar penggunaan kecerdasan buatan dalam pertahanan dapat diimplementasikan secara efektif. Pendahuluan ini menguraikan pentingnya memahami tantangan ini dan mencari solusi yang tepat.

Dalam jurnal ini, peneliti akan mengeksplorasi tantangan-tantangan ini secara lebih mendalam dan membahas beberapa pendekatan yang dapat diambil untuk mengatasinya. Dengan demikian, diharapkan jurnal ini dapat memberikan wawasan yang berharga tentang bagaimana kecerdasan buatan akan mempengaruhi masa depan pertahanan negara dan bagaimana kita dapat menghadapi tantangan-tantangan yang ada dengan cerdas dan efektif.

METODE PENELITIAN

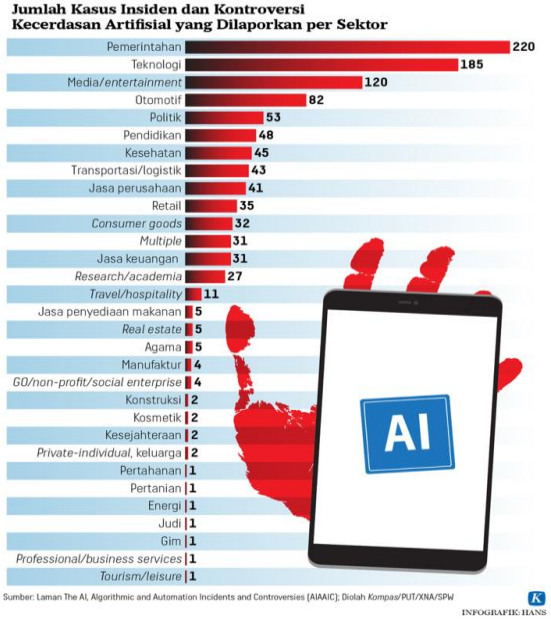
Dalam tulisan ini, digunakan metode kualitatif dengan teknik studi literatur untuk menjelaskan topik penelitian secara eksploratif. Pendekatan kualitatif memungkinkan eksplorasi yang mendalam dan analisis yang spesifik terkait dengan kecerdasan buatan dan tantangan ke depan dalam pertahanan. Data yang digunakan dalam penulisan ini adalah data sekunder yang dikumpulkan melalui studi literatur. Studi literatur yang dilakukan mengacu pada pengumpulan informasi dan identifikasi masalah penelitian dengan menggunakan berbagai buku dan majalah. Danial dan Warsiah (2009) mengutarakan pendekatan studi literatur memungkinkan peneliti untuk menggali informasi dari berbagai sumber yang sudah ada untuk mendukung analisis dan pemahaman topik yang diteliti.

Sumber-sumber yang digunakan meliputi buku, penelitian seperti skripsi, tesis, dan disertasi, artikel ilmiah yang dipublikasikan secara online, serta dokumen-dokumen dari lembaga-lembaga terkait di internet yang berkaitan dengan diskusi tentang pertahanan negara.

HASIL DAN PEMBAHASAN

Tantangan Etika dalam Penggunaan Kecerdasan Buatan dalam Pertahanan

Penggunaan kecerdasan buatan dalam pertahanan menimbulkan berbagai dilema etika. Salah satu tantangan utama adalah kurangnya regulasi yang mengatur penggunaan kecerdasan buatan dalam pertahanan. Di Indonesia, misalnya, belum ada regulasi yang secara khusus mengatur penggunaan dan etika kecerdasan buatan (Rosalina, 2023a). Hal ini perlu untuk diantisipasi karena kecerdasan buatan dapat menjadi sebuah pedang yang bermata dua dan dapat memakan tuannya. Seperti terjadi adanya penggunaan Chat GPT sebuah kecerdasan buatan yang tenar pada era ini mampu untuk membuat segala tulisan yang enak dibaca namun tidak dapat divalidasi tentang keabsahannya (Rosalina, 2023b).



Sumber: https://www.kompas.id/baca/investigasi/2023/06/27/ai-pedang-bermata-dua-yang-makan-tuan

Regulasi yang jelas dan komprehensif diperlukan untuk memastikan bahwa penggunaan kecerdasan buatan dalam pertahanan dilakukan dengan memperhatikan aspek etika.

Penggunaan kecerdasan buatan dalam pertahanan membutuhkan transparansi dalam proses pengumpulan, penyatuan, dan pembagian data. Kurangnya transparansi dapat menimbulkan keraguan atau ketidakpercayaan dari pihak lain (Sekretariat Jenderal Komisi Yudisial Republik Indonesia, 2019). Oleh karena itu, penting untuk memastikan bahwa proses penggunaan kecerdasan buatan dalam pertahanan dilakukan secara transparan agar dapat membangun kepercayaan.

Microsoft sebagai salah satu perusahaan ternama menggunakan kemampuan kecerdasan buatan dengan melaksanakan enam prinsip yaitu:

1. Privasi dan keamanan. Sebuah tantangan tersendiri bagi perusahaan yang menggunakan teknologi *cloud* sistem AI harus patuh terhadap undang-undang privasi dan memastikan bahwa informasi yang bersifat sensitif dan pribadi dilindungi dari penyalahgunaan dan pencurian data
2. Transparansi. Penggunaan AI semakin memberikan pengaruh terhadap kehidupan setiap manusia sehingga Microsoft harus memberikan informasi yang bersifat kontekstual tentang bagaimana sistem AI bekerja sehingga pengguna dapat memberikan keputusan yang

tidak terlalu bias dan minim kesalahan.

3. Keadilan. Sistem AI diharapkan dapat memberikan keputusan rekomendasi yang sama di setiap permasalahan sehingga perlu untuk memahami bagaimana bias dapat memberikan pengaruh pada sistem kerja AI.
4. Keandalan. Penggunaan kecerdasan buatan dalam pertahanan, ada dua hal yang penting: pertama, sistem AI harus dirancang dengan parameter yang jelas dan menjalani pengujian yang ketat untuk memastikan respons yang aman dan sesuai dengan harapan; dan kedua, partisipasi masyarakat secara luas harus dipertimbangkan dalam pengambilan keputusan terkait kapan dan bagaimana sistem AI harus dikerahkan, dengan melibatkan dialog dan keterlibatan masyarakat untuk mencerminkan nilai-nilai dan aspirasi yang diinginkan oleh masyarakat.
5. Untuk memastikan inklusivitas dalam pengembangan solusi kecerdasan buatan, penting untuk menerapkan praktik desain yang inklusif. Praktik desain ini bertujuan untuk mengantisipasi dan mengatasi hambatan potensial dalam produk atau lingkungan yang dapat secara tidak sengaja mengucilkan seseorang, sehingga solusi AI dapat memenuhi berbagai kebutuhan dan pengalaman manusia secara menyeluruh.
6. Tanggung jawab utama bagi para desainer dan implementator sistem kecerdasan buatan adalah memastikan bahwa sistem yang mereka buat beroperasi dengan baik. Oleh karena itu, mereka perlu menjalankan tanggung jawab akuntabilitas dengan mengadopsi pengalaman dan praktik yang telah teruji di sektor lain, seperti praktik privasi kesehatan. Selain itu, kesadaran akan akuntabilitas harus dijaga dengan baik selama proses perancangan sistem dan terus dipatuhi ketika sistem tersebut beroperasi di kehidupan nyata.

Penggunaan kecerdasan buatan (AI) dalam pertahanan dapat membantu memperkuat sistem pertahanan negara dengan memberikan analisis informasi yang lebih akurat dan cepat (Universitas Medan Area, 2023). Namun, penggunaan teknologi AI dalam pertahanan juga membawa risiko-risiko yang perlu diperhatikan, terutama dalam hal keamanan. Risiko-risiko ini dapat terjadi jika penggunaan kecerdasan buatan dalam pertahanan tidak diatur dengan baik dan tidak memperhatikan aspek keamanan yang penting.

Tantangan keamanan merupakan isu yang penting dalam penggunaan kecerdasan buatan dalam pertahanan. Hal ini seperti risiko serangan siber, manipulasi data, dan penyalahgunaan teknologi oleh musuh negara serta solusi yang diperlukan untuk melindungi sistem pertahanan negara dari ancaman ini.

Salah satu fenomena yang mengganggu keamanan nasional dan internasional adalah perang siber atau *cyber warfare.* Fenomena ini dianggap sebagai ancaman baru yang muncul di era modern ini (Baby, 2015).

Walfajri (2021) menulis dalam *website* kontan.co.id menyatakan bahwa Kementerian Komunikasi dan Informasi telah menerima hampir 200.000 aduan terkait serangan siber dalam sektor perbankan, dimana serangan ini melibatkan penggunaan aplikasi WhatsApp dan Instagram. Untuk menghadapi situasi darurat terkait serangan siber dan perang siber, Indonesia membutuhkan kehadiran tenaga profesional yang memiliki pengetahuan dan keterampilan di bidang keamanan siber. Selain itu, regulasi yang kuat dan tegas diperlukan sebagai upaya untuk mengatasi serta mencegah serangan siber yang ditujukan kepada negara. Dalam konteks ini, penguasaan teknologi menjadi salah satu syarat utama yang harus dimiliki oleh Indonesia guna menjaga dan mengamankan negara dari serangan siber yang semakin kompleks. Dalam konteks ini, penting untuk menjaga kesiapan keterampilan dan infrastruktur teknologi agar Indonesia tetap sejalan dengan perkembangan teknologi yang pesat. Kelemahan dalam penguasaan teknologi dan regulasi yang kurang ketat dalam pertahanan siber dapat menghadirkan risiko serius bagi negara (Nainggolan, 2017).

Pengembangan teknologi dan infrastruktur yang memadai sangat penting dalam mendukung penggunaan kecerdasan buatan (AI) dalam pertahanan. Revolusi industri 4.0 membawa terobosan teknologi dalam sejumlah bidang, termasuk kecerdasan buatan (Helmi, 2019). Oleh karena itu, perlu adanya kesamaan pemahaman tentang pengembangan dan penerapan AI di Indonesia, sesuai yang dilansir oleh Yusuf (2020) pada akhir tahun 2019, Kementerian Kominfo berhasil menyelesaikan sejumlah proyek nasional, termasuk Palapa Ring, yang merupakan jaringan serat optik bawah laut yang menghubungkan 514 Kabupaten/Kota di Indonesia. Infrastruktur nasional pendukung AI harus terus dikembangkan untuk memastikan bahwa penggunaan kecerdasan buatan dalam pertahanan dapat dilakukan dengan efektif.

Penyesuaian Strategis dalam Menghadapi Perubahan yang Disebabkan oleh Kecerdasan Buatan

Kecerdasan buatan telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan dan industri. Untuk menghadapi perubahan ini, diperlukan penyesuaian strategis yang tepat agar negara dapat mengoptimalkan potensi kecerdasan buatan dan menjawab tantangan yang muncul. Peneliti berfokus pada empat aspek penting dalam penyesuaian strategis untuk menghadapi perubahan yang disebabkan oleh kecerdasan buatan.

Pertama, penyesuaian strategis yang diperlukan adalah dalam hal pengembangan dan penguasaan teknologi AI. Penggunaan kecerdasan buatan dalam pertahanan membutuhkan pengetahuan mendalam dan penguasaan teknologi yang relevan. Negara dan lembaga pertahanan perlu memprioritaskan investasi dalam riset, pengembangan, dan pelatihan untuk menghasilkan tenaga ahli yang mampu mengoperasikan, mengelola, dan memanfaatkan teknologi AI secara efektif dalam pertahanan negara.

Kedua, penyesuaian strategis melibatkan aspek kebijakan dan regulasi dalam penggunaan kecerdasan buatan dalam pertahanan. Kebijakan dan regulasi yang relevan harus dirumuskan untuk memastikan bahwa penggunaan kecerdasan buatan dalam pertahanan tetap sesuai dengan nilai-nilai etika, hukum, dan prinsip-prinsip pertahanan negara. Hal ini meliputi perlindungan privasi dan keamanan data, pemastian akuntabilitas dalam pengambilan keputusan AI, dan pengaturan

penggunaan teknologi AI dalam operasi militer dan keamanan.

Selanjutnya **ketiga**, penyesuaian strategis juga melibatkan penguatan kemampuan manusia dalam konteks pertahanan yang didukung oleh kecerdasan buatan. Meskipun AI dapat memberikan keunggulan dan efisiensi dalam operasi pertahanan, penting untuk tetap mengakui peran penting manusia sebagai pengambil keputusan akhir. Penyediaan pelatihan yang sesuai, pengembangan keterampilan, dan pemahaman yang mendalam tentang kecerdasan buatan harus menjadi fokus dalam meningkatkan kemampuan dan kapasitas manusia dalam pertahanan. Kementerian Pertahanan akan dihadapkan pada tuntutan untuk terus meningkatkan kualitas sumber daya manusia, terutama dalam bidang keamanan siber, guna memastikan keamanan dan pertahanan negara mencapai tingkat maksimal dalam menghadapi berbagai ancaman, baik yang bersifat tradisional maupun non-tradisional di masa depan. (Hasan, 2022).

Dan terakhir **keempat**, penyesuaian strategis yang penting adalah dalam hal kerja sama dan kemitraan. Perubahan yang disebabkan oleh kecerdasan buatan membutuhkan kerja sama yang erat antara negara, lembaga pertahanan, industri, dan institusi akademik. Kolaborasi dan pertukaran pengetahuan, sumber daya, dan teknologi antara pihak-pihak yang terlibat dapat memperkuat kapabilitas pertahanan dan mendorong inovasi yang lebih baik dalam penerapan kecerdasan buatan dalam pertahanan.

SIMPULAN

Dalam menghadapi perubahan yang disebabkan oleh kecerdasan buatan (AI) dalam konteks pertahanan, diperlukan penyesuaian strategis yang tepat. Penyesuaian strategis melibatkan pengembangan dan penguasaan teknologi AI, perumusan kebijakan dan regulasi yang tepat, penguatan kemampuan manusia, serta kerja sama dan kemitraan yang kuat.

Pengembangan teknologi dan infrastruktur yang memadai sangat penting dalam mendukung penggunaan AI dalam pertahanan. Regulasi yang jelas dan komprehensif diperlukan untuk memastikan penggunaan AI dilakukan dengan memperhatikan aspek etika dan keamanan. Penguatan kemampuan manusia juga perlu menjadi fokus untuk menjaga peran penting manusia sebagai pengambil keputusan akhir. Kerja sama dan kolaborasi antara negara, lembaga pertahanan, industri, dan institusi akademik juga menjadi kunci dalam mengoptimalkan potensi kecerdasan buatan dalam pertahanan.

Dengan penyesuaian strategis yang tepat, negara dapat menghadapi perubahan dengan cerdas dan efektif serta memanfaatkan potensi kecerdasan buatan untuk menjaga keamanan dan pertahanan negara.

DAFTAR PUSTAKA

Baby, S. A. M. (2015). Ancaman Perang Siber Di Era Digital Dan Solusi Keamanan Nasional Indonesia. . Jurnal Oratio Directa, 3(1), 425–442.

Danial, & Wasriah. (2009). Metode Penulisan Karya Ilmiah. Laboratorium Pendidikan Kewarganegaraan UPI.

Hasan, K. E. S. (2022). Perlunya Tentara Nasional Indonesia Memiliki Angkatan Siber Guna Menghadapi Era Cyber warfare. Journal of Education, Humaniora and Social Sciences (JEHSS), 5(1), 264–274. https://doi.org/10.34007/jehss.v5i1.1192

Helmi, N. (2019, April 30). Pusat barang milik negara kemhan RI. Kementerian Pertahanan RI. https://www.kemhan.go.id/pusbmn/2019/04/30/revolusi-industri-4-0-dan-pengaruhnya-bagi-industri-di-indonesia.html

Juanda, M. (2020, November 27). Pemanfaatan Big data dan AI dalam Pertahanan

Negara. Komite. https://www.komite.id/2020/11/27/pemanfaatan-big-data-dan-ai-dalam-pertahanan-negara/

Nainggolan, D. R. M. (2017). Sains Data, Big Data, Dan Analisis Prediktif: Sebuah Landasan Untuk Kecerdasan Keamanan Siber. Jurnal Pertahanan & Bela Negara, 7(2). https://doi.org/10.33172/jpbh.v7i2.187

Rosalina, M. P. (2023a, June 28). AI Bak Pedang Bermata Dua yang Bisa Memakan Tuannya. Harian Kompas. https://www.kompas.id/baca/investigasi/2023/06/27/ai-pedang-bermata-dua-yang-makan-tuan

Rosalina, M. P. (2023b, July 3). Indonesia Belum Punya Regulasi soal AI. Harian Kompas. https://www.kompas.id/baca/investigasi/2023/06/27/vakum-regulasi-kecerdasan-artifisial-di-indonesia

Sekretariat Jenderal Komisi Yudisial Republik Indonesia. (2019). Memperkuat peradaban hukum dan ketatanegaraan Indonesia: Bunga rampai. SEKRETARIAT JENDERAL KOMISI YUDISIAL REPUBLIK INDONESIA.

Universitas Medan Area. (2023, March 25). AI dan Pertahanan : Meningkatkan Keamanan Negara. Biro Administrasi Tata Laksana Rumah Tangga Dan Informasi Universitas Medan Area. https://batri.uma.ac.id/ai-dan-pertahanan-meningkatkan-keamanan-negara-dengan-teknologi-ai/

Walfajri, M. (2021, November 10). Indonesia sudah dalam situasi darurat kejahatan siber. Kontan. https://newssetup.kontan.co.id/news/indonesia-sudah-dalam-situasi-darurat-kejahatan-siber

Yusuf. (2020, February 21). Perlu Pemahaman Bersama terkait Pengembangan AI di Indonesia. Ditjen Aptika. https://aptika.kominfo.go.id/2020/02/perlu-pemahaman-bersama-tentang-pengembangan-ai-di-indonesia.