Jurnal Peperangan Asimteris
Volume 8, Nomor 2 2022 E-ISSN **2830-0475**

STRATEGI PERTAHANAN NEGARA INDONESIA DALAM MENGHADAPI ANCAMAN *ARTIFICIAL INTELLIGENCE*

(Indonesia State Defense Strategy In Facing Artificial Intelligence Threats)

Azizah Nur Rahmatika
Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan,Universitas Pertahanan Republik Indonesia
azizah.rahmatika@idu.ac.id

Abstrak

Artificial Intelligence (AI) adalah elemen penting dari era yang disebut sebagai Revolusi Industri Keempat. Teknologi dan aplikasi AI memiliki dampak yang luar biasa. AI telah mulai membuat dampak yang siginifikan dalam urusan militer dan strategis. Permasalahan penelitian adalah strategi pertahanan Indonesia dalam menghadapi ancaman AI. Tujuan dari penelitian ini adalah untuk mengetahui strategi pertahanan Indonesia dalam menghadapi ancaman AI. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif analitis, serta data diperoleh dari wawancara dan studi dokumentasi. Peneliti mewawancarai para informan yang telah ditunjuk dan mengumpulkan data sekunder, kemudian dianalisis menggunakan teknik analisa data Miles-Huberman, Saldana tahun 2014. Hasil penelitian ini adalah AI merupakan ancaman terhadap pertahanan Negara, penggunaan AI dalam pertahanan Negara mempengaruhi superioritas militer maupun informasi. Strategi dalam menghadapi ancaman penggunaan AI dalam pertahanan meliputi pembuatan berbagai kebijakan, UU dan peraturan yang memadai sebagai dasar, pemantapan kemampuan intelijen untuk memahami perkembangan ancaman AI, pembangunan industri pertahanan dalam negeri, perekrutan dan pelatihan sumber daya manusia yang berkelanjutan, pembangunan kekuatan yang terintegrasi diantara komponen utama, cadangan dan pendukung. Sarana yang digunakan dalam menghadapi ancaman penggunaan AI dalam pertahanan adalah alat-alat dengan teknologi AI baik yang dibeli dari luar negeri atau diproduksi sendiri dalam negeri.

Kata Kunci: Ancaman, Artificial Intelligence, Pertahanan Indonesia, Strategi, Teknologi

Abstract

Artificial Intelligence (AI) is an essential element of the era known as the Fourth Industrial Revolution. AI technology and applications are having a tremendous impact. AI has begun to

make a significant impact in military and strategic affairs. The research problem is Indonesia's defense strategy in the face of AI threats. The purpose of this study is to determine Indonesia's defense strategy in the face of AI threats. This research uses qualitative methods and analytical descriptive approach, and data obtained from interviews and documentation studies. The researcher interviews informants who had been appointed and collects secondary data, then analyzes using data analysis technique from Miles-Huberman-Saldana, 2014. The results of this study are that AI is a threat to national defense, the use of AI in national defense affects military superiority and information. Strategies in dealing with the threat of using AI in defense include making various policies, laws and adequate regulations as a basis, strengthening intelligence capabilities to understand the development of AI threats, developing the domestic defense industry, recruiting and training sustainable human resources, building an integrated force among main, spare and supporting components. The means that it being used in dealing with the threat of using AI in defense are tools with AI technology either purchased from abroad or produced domestically.

Keywords:, Artificial Intelligence, Indonesian Defense, Strategy, Technology, Threat

1. Pendahuluan

Perang dan teknologi selalu mempunyai hubungan yang kausal, artinya perang sangat berpengaruh terhadap kemajuan teknologi peralatan perang dan sebaliknya. Pertempuran di masa depan akan mengandalkan kekuatan satuan tempur dengan ukuran yang relatif lebih kecil dari sekarang, namun jauh lebih efektif dan mampu beroperasi melawan musuh dengan kemampuan yang tinggi. Sistem peralatan utama militer akan lebih bersifat tanpa awak, namun lebih tinggi tingkat otonominya. Teknologi militer yang akan berkembang antara lain: peralatan Cyber Warfare untuk ofensif, sistem penghitungan yang lebih maju, artificial intelligence, dll (Work & Brimley, 2014).

Kecerdasan buatan atau Artificial Intelligence (AI) adalah elemen penting dari era Revolusi Industri Keempat. Teknologi dan aplikasi AI memiliki dampak yang luar biasa (Allen & Chan, 2017). AI telah mulai membuat dampak yang siginifikan dalam urusan militer dan strategis. Beberapa analis berpendapat bahwa AI memiliki potensi untuk menjadi teknologi keamanan nasional yang transformatif, setara dengan senjata nuklir, pesawat terbang, komputer, dan bioteknologi (Allen dan

Chan, 2017). Perkembangan AI secara eksponensial ke ranah militer akan memberikan dampak terhadap pembentukan kembali fungsi militer secara signifikan. Hal tersebut secara radikal akan mengubah konsep peperangan dan operasi militer di masa depan. Pada saat yang sama, peperangan sendiri sedang mengalami perubahan pada tingkat konseptual karena kemajuan teknologi yang pesat.

Pada awal September 2017, Presiden Rusia Vladimir Putin membawa AI dari laboratorium Silicon Valley, dan ruang bawah tanah Pentagon ke garis depan politik internasional. Putin berkata, "AI adalah masa depan, tidak hanya untuk Rusia, tapi untuk seluruh umat manusia. Datang dengan peluang kolosal, tapi juga ancaman yang sulit diprediksi. Siapapun yang menjadi pemimpin dalam bidang ini akan menjadi penguasa dunia" (Vincent, 2017). Pernyataan Putin mencerminkan keyakinan, yang berkembang di berbagai sektor dan wilayah di seluruh dunia, bahwa kemajuan dalam AI akan sangat penting untuk masa depan di berbagai bidang seperti pekerjaan, masyarakat, dan kekuatan militer.

AI telah berkembang sangat pesat dalam beberapa tahun terakhir dan telah menghasilkan berbagai aplikasi, baik sipil maupun militer. Di bidang militer, AI berpotensi berdampak pada "semua domain baik darat, laut, udara, ruang dan informasi dan semua tingkat peperangan baik tingkat politik, strategis, operasional dan taktis" (Svenmarck, Peter et al., 2018).

AI dapat mengubah sifat fundamental dari konflik konvensional antar negara. AI akan mendorong evolusi dalam peperangan asimetris, dimana dominasi informasi dan pemahaman dapat terbukti menentukan dengan meningkatkan kecepatan, ketepatan, dan keefektifan informasi yang digunakan dalam konflik. Integrasi data real-time yang digerakkan oleh AI memungkinkan pemahaman yang lebih dalam tentang pola perilaku, hubungan, pola kehidupan, dan keahlian perdagangan. Kemampuan ini memungkinkan komandan untuk lebih cepat dan

efektif menanggapi kemampuan peperangan tidak teratur musuh dengan mengidentifikasi, membentuk, dan mengganggu upaya subversif secara real time.

Fenomena pemanfaatan teknologi AI untuk mendukung pertahanan dan tugas-tugas militer telah lama dilakukan oleh banyak militer di dunia seperti di Amerika Serikat, Cina, Rusia, dan Israel.

Meskipun AI masih dalam tahap juvenile atau baru, tidak dapat dipungkiri bahwa AI memiliki kapasitas untuk mengubah lanskap sektor pertahanan dan keamanan dan akibatnya akan mengubah keseimbangan ekonomi dan militer saat ini dalam sistem internasional. Menyadari potensi AI, lebih dari 20 negara telah mengumumkan strategi AI nasional mereka, dan lebih banyak negara bagian dan organisasi non-negara mengambil langkah-langkah yang menentukan dalam penelitian dan pengembangan (R&D) AI.

Di Indonesia sendiri, pemanfaatan AI dalam bidang pertahanan belum banyak. Namun memang penelitian dan pengembangan AI sedang dilakukan. Pada tahun 2020 ini, Indonesia mengeluarkan Strategi Nasional Kecerdasan Artifisial (STRANAS-KA) yang di dalamnya mencakup rencana pemanfaatan AI di berbagai aspek nasional, yaitu kesehatan, pendidikan, pangan, pemerintahan, dan kota cerdas (smart city). Dalam STRANAS-KA ini belum membahas penggunaan AI dalam bidang pertahanan sebagai strategi pertahanan Negara.

Berdasarkan yang telah diuraikan, maka masalah dan tujuan yang akan dibahas adalah bagaimana strategi pertahanan negara Indonesia dalam menghadapi ancaman AI.

2. Metode Penelitian

Metode Penelitian yang digunakan adalah metode kualitatif dengan pendekatan deskriptif analitis. Pendekatan deskriptif merupakan metode untuk mendefinisikan atau menyajikan gambaran umum objek yang diteliti melalui data atau sampel yang diperoleh tanpa mengevaluasi atau menarik asumsi umum

(Sugiyono, 2015). Ini berarti bahwa deskriptif analitis mempertimbangkan masalah atau merefleksikan topik yang muncul dan diteliti, dan memproses serta menganalisis temuan untuk menarik kesimpulan.

Penelitian ini dimulai dengan memperhatikan dan menelaah fokus pada fenomena AI dan penggunaannya yang semakin masif secara global. Dalam hal ini, Peneliti bermaksud menganalisis penggunaan AI di bidang pertahanan, sejauh apa penggunaan tersebut di Indonesia dan bagaimana strategi pertahanan negara dalam menghadapi ancaman Artificial Intelligence.

Agar penelitian ini memperoleh data, maka peneliti menentukan tempat dilaksanakannya penelitian ini adalah Kementerian Pertahanan, Badan Pengkajian dan Penerapan Teknologi (BPPT) dan Indonesian Resources Development Institute (IRDI).

Subjek penelitian adalah sesuatu, baik orang, benda, atau lembaga (organisasi) yang keadaannya diteliti. Subjek penelitian yang kemudian menjadi informan memberikan berbagai informasi yang diperlukan selama proses penelitian. Berikut informan yang menjadi narasumber, antara lain Dirjakstra Strahan Kemhan, Dirtekindhan Pothan Kemhan, Kabid Jam Kam Pushansiber Kemhan, Staf PTIPK BPPT, Kepala IRDI. Obyek penelitian ini adalah pemanfaatan serta strategi Artificial Intelligence dalam bidang pertahanan.

Dalam pengumpulan data, peneliti menggunakan teknik wawancara, studi dokumentasi dan studi pustaka. Dalam wawancara, peneliti menggunakan teknik wawancara semi terstruktur artinya, selama wawancara peneliti menyiapkan pertanyaan tertulis sebagai pedoman wawancara, namun tidak menutup kemungkinan untuk mengembangkan pertanyaan wawancara sesuai dengan permasalahan yang ditemukan.

Pemeriksaan Keabsahan Data dilakukan dengan Teknik pemeriksaan derajat kepercayaan (credibility), Teknik keteralihan (transferability), Teknik kebergantungan (dependability), Teknik kepastian (confirmability) dari J. Moleong

(Moleong, 2016). Peneliti menggunakan model triangulasi sumber sebagai alat untuk menguji keabsahan data.

Teknik Analisis Data yang digunakan dari Miles, Huberman, dan Saldana yaitu pengumpulan data, kondensasi data, penyajian data, dan penarikan kesimpulan yang dilakukan secara interaktif dan berlangsung secara terus menerus sampai tuntas, sehingga datanya mencapai jenuh (Miles, Huberman, & Saldana, 2014).

3. Literatur Review

3.1 Artificial Intelligence (AI)

AI didefinisikan sebagai kemampuan mesin dan sistem untuk memperoleh dan menerapkan pengetahuan, dan untuk melakukan perilaku cerdas (Organisation for Economic Co-operation and Development (OECD), 2016). Ini mencakup berbagai tugas kognitif, contohnya penginderaan, memproses bahasa lisan, bernalar, belajar, membuat keputusan dan menunjukkan kemampuan untuk memindahkan dan memanipulasi objek secara tepat. Sistem cerdas ini menggunakan kombinasi analitik data besar, komputasi cloud, komunikasi mesin-mesin dan Internet of Things (IoT) untuk beroperasi dan belajar.

Pada dasarnya, AI adalah perangkat lunak dan umumnya berbasis algoritme walaupun fungsinya perlu dicerminkan oleh substansi fisik seperti robot, contohnya berbicara atau bermain game. Dalam pengertian ini, AI seperti otak manusia. Sampai saat ini, pengembangan AI secara umum difokuskan pada domain tertentu (lihat Tabel 1).

Tabel 1. Domain besar AI

Domain AI	Deskripsi
Machine Learning skala besar	Desain algoritma pembelajaran, serta penskalaan algoritma yang ada, untuk bekerja dengan kumpulan data yang besar.

Deep learning	Model terdiri dari input seperti gambar atau audio dan beberapa lapisan tersembunyi dari sub-model yang berfungsi sebagai input untuk lapisan berikutnya dan pada akhirnya merupakan output dari fungsi aktivasi.
Natural language processing (NLP)	Algoritma yang memproses input bahasa manusia dan mengubahnya menjadi representasi yang dapat dimengerti
System kolaborasi	Model dan algoritma untuk membantu mengembangkan sistem otonom yang dapat bekerja secara kolaboratif dengan sistem lain dan dengan manusia.
Computer vision (analisis gambar)	Proses menarik informasi yang relevan dari gambar atau set gambar untuk klasifikasi dan analisis lanjutan.
Algorithmic game theory and computational social choice	Sistem yang membahas dimensi komputasi ekonomi dan sosial AI, seperti bagaimana sistem dapat menangani insentif yang berpotensi tidak selaras, termasuk peserta manusia atau perusahaan yang tertarik, dan agen berbasis AI otomatis yang mewakili mereka.
Soft robotics (robotic process automation)	Otomatisasi tugas berulang dan proses umum seperti layanan pelanggan dan penjualan tanpa perlu mengubah peta sistem TI yang ada.

Sumber: Pricewaterhouse Coopers (2019)

AI dapat meningkatkan kapasitas manusia dengan memproses dan menganalisis kumpulan data besar jauh lebih cepat daripada manusia. Misalnya, dalam perawatan medis, AI dapat membantu menganalisis data dari sejumlah besar individu dan mengidentifikasi pola untuk diagnosis penyakit. Di sektor hukum, AI digunakan untuk menyaring dokumen pengadilan dan catatan hukum untuk informasi yang relevan dengan kasus. Dalam industri mobil, robot yang digerakkan oleh AI telah digunakan pada jalur perakitan. Potensi mereka untuk domain pertahanan sangat besar karena solusi AI diharapkan muncul di bidang kritis seperti pertahanan dunia maya, sistem pendukung keputusan, manajemen risiko,

pengenalan pola, kesadaran situasi dunia maya, proyeksi, deteksi malware, dan korelasi data.

3.2 Artificial Intelligence dalam Pertahanan

Saat ini, penggunaan AI di pertahanan sebagian besar eksis dalam enam bidang utama (Roth, 2019), yaitu :

a. Penargetan senjata dan senjata otonom, saat ini platform senjata otonom menggunakan visi komputer untuk mengidentifikasi dan melacak target. Senjata otonom terutama menjadi otonom ketika sistem dapat mengidentifikasi, dan melacak target di ruang yang telah dikerahkan untuk dijaga. Kecerdasan buatan di belakang penargetan perlu dilatih tentang apa sebenarnya target strategis yang layak untuk memfokuskan daya tembaknya dan memberitahu operator yang memantau platform. Ini mungkin pesawat musuh yang terbang ke wilayah udara yang diperebutkan dengan kecepatan ekstrem, roket yang ditembakkan ke kota, atau pengangkut personel lapis baja yang melaju di jalan kecil. Senjata otonom memungkinkan "mata" penglihatan komputer yang selalu waspada dengan dilatih untuk mencegah serangan roket mendadak dengan cara menargetkan dan menembak jatuh roket musuh di udara sebelum dapat meledak di daerah berpenduduk.

b. Pengawasan (intelligence, surveillance, reconnaissance). AI sangat berguna dalam intelijen karena kumpulan data besar yang tersedia untuk analisis. Misalnya, pada fase pertama Project Maven melibatkan otomatisasi pemrosesan intelijen untuk mendukung kampanye kontra-ISIL. Secara khusus, tim Project Maven menggabungkan visi komputer dan algoritma pembelajaran mesin ke dalam sel pengumpulan intelijen yang akan menyisir rekaman dari kendaraan udara tak berpenghuni dan secara otomatis mengidentifikasi

aktivitas bermusuhan untuk penargetan. Dalam kapasitas ini, AI dimaksudkan untuk mengotomatiskan pekerjaan analis manusia yang saat ini menghabiskan berjam-jam dalam memilah video untuk mendapatkan informasi yang dapat ditindaklanjuti, berpotensi membebaskan analis untuk membuat keputusan yang lebih efisien dan tepat waktu berdasarkan data (Corrigan, 2017).

c. Keamanan siber. Ancaman keamanan siber datang dalam berbagai bentuk dan ukuran. Kecerdasan buatan atau AI memiliki kemampuan untuk memainkan peran besar dalam tindakan pencegahan bagi suatu militer. AI kemungkinan akan menjadi teknologi kunci dalam memajukan operasi dan keamanan siber. Dalam kesaksiannya tahun 2016 di hadapan Komite Senat Angkatan Bersenjata, Komandan Komando Siber AS Laksamana Michael Rogers menyatakan bahwa mengandalkan kecerdasan manusia saja di dunia maya adalah "strategi yang kalah". Alat keamanan siber konvensional mencari kecocokan historis dengan kode berbahaya yang diketahui, jadi peretas hanya perlu memodifikasi sebagian kecil dari kode itu untuk menghindari pertahanan. Alat berkemampuan AI, di sisi lain, dapat dilatih untuk mendeteksi anomali dalam pola aktivitas jaringan yang lebih luas, sehingga menghadirkan penghalang yang lebih komprehensif dan dinamis untuk menyerang (Macri, 2016).

d. Keamanan dalam negeri. Salah satu kemampuan inti dari kecerdasan buatan adalah mengidentifikasi tren dan pola dalam kumpulan data untuk kemudian memprediksi kemungkinan dan kapan tren itu akan terjadi lagi. Ini disebut analitik prediktif, dan saat ini diterapkan pada masalah keamanan dalam negeri. Model analisis prediktif dapat digunakan untuk menghubungkan tanda-tanda persiapan untuk aktivitas yang melanggar hukum, seperti membeli senjata atau bahan pembuatan bom darurat di toko, yang memungkinkan badan intelijen untuk mencegah tindakan tersebut sebelum plot terungkap. Perangkat lunak analitik prediktif juga dapat

memberikan prediksi kemungkinan tersangka kejahatan berdasarkan berbagai faktor lingkungan dan data catatan kriminal masa lalu.

e. Logistik. AI mungkin memiliki kegunaan masa depan di bidang logistik militer. Angkatan Udara AS, misalnya, mulai menggunakan AI untuk pemeliharaan pesawat prediktif. Alih-alih melakukan perbaikan saat pesawat rusak atau sesuai dengan jadwal pemeliharaan seluruh armada standar, Angkatan Udara AS sedang menguji pendekatan berkemampuan AI yang menyesuaikan jadwal pemeliharaan dengan kebutuhan masing-masing pesawat. Pendekatan ini, yang saat ini digunakan oleh Sistem Informasi Logistik Autonom F-35, mengekstrak data sensor real-time yang tertanam di mesin pesawat dan sistem onboard lainnya dan memasukkan data ke dalam algoritma prediktif untuk menentukan kapan teknisi perlu memeriksa pesawat atau mengganti suku cadang (Weisgerber, 2017).

f.Kendaraan otonom. Sebagian besar Negara sekarang berusaha untuk memasukkan AI ke dalam kendaraan semi-otonom dan otonom, termasuk pesawat tempur, drone, kendaraan darat, dan kapal angkatan laut. Aplikasi AI dalam bidang ini serupa dengan kendaraan komersial semi-otonom, yang menggunakan teknologi AI untuk melihat lingkungan, mengenali hambatan, fuse sensor data, merencanakan navigasi, dan bahkan berkomunikasi dengan kendaraan lain (Congressional Research Service, 2018).

4. Hasil dan Pembahasan

4.1 Ancaman Artificial Intelligence

Hasil yang didapatkan dari penelitian ini antara lain bahwa penggunaan AI merupakan ancaman terhadap pertahanan, terutama pada siber. Terlebih, dalam pertahanan Indonesia belum ada pemanfaatan teknologi AI dalam bidang siber serta belum ada hukum yang kuat untuk melindungi data-data dalam dunia maya. Apalagi mayoritas di Indonesia masih memakai server luar, makanya sebisa

mungkin yg penting seperti pertahanan atau LAPAN itu punya server sendiri agar jika ada data-data penting negara akan ada kepentingan untuk melindungi itu.

Penggunaan AI dalam pertahanan di bidang siber bisa untuk mencari trend, AI untuk prediksi konten merupakan termasuk open source intelligence (OSINT). Penggunaan AI dalam siber atau dunia maya dapat memperkuat pertahanan dengan kemampuannya untuk mendeteksi kelemahan dan anomali-anomali yang terjadi apabila diserang sekaligus dapat meningkatkan daya serang dengan otomatisasi tanpa henti untuk dapat mencari celah dan menyerang kelemahan lawan.

Kemajuan dalam teknologi AI akan mempengaruhi kemampuan pengumpulan dan analisis data intelijen, serta pembuatan data dan media. Aplikasi AI dapat digunakan tidak hanya untuk menganalisis data, tetapi juga untuk memproduksinya, termasuk foto, video, dan teks yang dibuat secara otomatis. AI berguna baik untuk menggunakan data untuk sampai pada kesimpulan dan untuk menghasilkan data yang menyebabkan kesimpulan yang salah. Dengan kata lain, AI dapat membantu badan intelijen dalam menentukan kebenaran, tetapi juga memudahkan musuh untuk berbohong secara meyakinkan

Seperti dampak dunia maya, peningkatan pemanfaatan robotika dan sistem otonom akan menambah kekuatan aktor non-negara dan negara bangsa. Dalam jangka pendek, kemajuan AI kemungkinan akan memungkinkan dukungan robotik yang lebih otonom bagi para warfighter, dan mempercepat peralihan dari misi tempur berawak ke misi tempur tak berawak. Awalnya, kemajuan teknologi akan memberikan keuntungan terbesar bagi militer yang besar, didanai dengan baik, dan berteknologi canggih. Meskipun kemajuan dalam robotika dan otonomi akan meningkatkan kekuatan absolut semua jenis aktor, keseimbangan kekuatan relatif mungkin tidak bergeser dari negara bangsa terkemuka. Dalam jangka panjang, kemampuan ini akan mengubah kekuatan militer dan peperangan. Sistem robotik yang memungkinkan akan cukup mampu untuk mengubah kekuatan militer.

Penggunaan AI dalam pertahanan dalam bentuk kendaraan otonom, contohnya drone. Penggunaan AI dalam pertahanan yang sudah ada di Indonesia, baik yang membeli atau memproduksi sendiri, antara lain chip yang dipasang di perbatasan, pesawat tanpa awak seperti drone, dan robotic kapal-kapal drone laut. Contoh hasil inovasi dalam negeri adalah drone Elang Hitam.

Gambar 1. Pesawat Udara Nir Awak (PUNA) MALE Elang Hitam

Sumber: Badan Pengkajian dan Penerapan Teknologi (2019)

Pesawat ini diperkirakan dapat terbang non-stop selama 24 jam dan mengoperasikan banyak UAV secara bersamaan. Drone ini bertujuan untuk mengawal kedaulatan Negara Kesatuan Republik Indonesia, melalui pengawasan udara baik di wilayah darat maupun laut. Sementara dalam pertahanan siber, belum ada pemanfaatan AI, masih dikembangkan dan diharapkan sensor kita memiliki kemampuan AI, untuk membantu mempermudah dan mempersingkat analisa.

Peneliti mengaitkan dengan konsep ancaman yg dikemukakan John M Collins bahwa jika sudah memenuhi unsur-unsur kemampuan, intentions (niat/keinginan), dan kerentanan maka dapat dikatakan suatu hal dapat menjadi ancaman.

Kemampuan (capabilities) AI dalam pertahanan berpengaruh pada banyak lini, terutama pada siber dan bidang pengawasan serta pengambilan informasi. AI dapat meningkatkan kemampuan serta memperkuat daya serang.

Kemudian intentions atau niat, negara-negara besar seperti Amerika Serikat, Rusia, serta China sedang berlomba untuk meningkatkan penggunaan AI dalam pertahanan agar mereka tetap superior baik dalam militer atau informasi, hal ini juga digunakan untuk deterrence.

Sedangkan mengenai kerentanan (vulnerabilites), dapat dikatakan bahwa semakin tinggi kemampuan AI semakin tinggi pula tingkat kerentanannya. Baik itu kerentanan pengguna atau lawan. Dengan dunia yang semakin terhubung dan tanpa batas, penggunaan AI dapat mengancam keamanan siber.

4.2 Strategi Pertahanan Artificial Intelligence

Penggunaan AI dalam pertahanan telah berdampak bagi strategi pertahanan Indonesia. Untuk melihat lebih dalam hal tersebut, peneliti melakukan analisis menggunakan teori strategi dikaitkan dengan strategi pertahanan negara yang tercantum dalam Buku Putih Pertahanan tahun 2015. Menurut Arthur F. Lykke, strategi merupakan keterkaitan tiga unsur elemen, yakni cara (ways), sarana (means) dan tujuan (ends atau goals). Makna tujuan menjelaskan pembentukan masalah dan hasil dari penyelesaian langkah, diikuti oleh alat yang digunakan untuk mencapai tujuan, dan terakhir cara untuk mencapai tujuan. Berdasarkan teori tersebut, terdapat tiga indikator strategi yang harus dilaksanakan dalam menghadapi ancaman penggunaan AI, yaitu tujuan (ends), fasilitas/sarana prasarana (means), serta cara yang ditempuh (ways).

Tujuan (ends) dari strategi pertahanan ini adalah terciptanya kondisi atau keadaan yang aman dari ancaman AI. Revolusi Industri 4.0 dicirikan oleh AI, machine learning, big data, integrasi sistem, dan teknologi robotik telah berkontribusi pada revolusi ancaman dalam teknologi militer, namun dapat menjadi

ancaman non militer karena digunakan antara lain untuk menguasai pasar yang merugikan kepentingan dalam negeri.

Sarana prasarana (means) yang digunakan dalam menghadapi ancaman AI dalam pertahanan adalah alat-alat dengan teknologi AI baik yang membeli atau memproduksi sendiri, antara lain chip yang dipasang di perbatasan, pesawat tanpa awak seperti drone, dan robotic kapal-kapal drone laut. Sementara dalam pertahanan siber, belum ada pemanfaatan AI, masih dikembangkan dan diharapkan akan memiliki sensor dengan kemampuan AI, untuk membantu mempermudah dan mempersingkat analisa.

Untuk mencapai tujuan yang diinginkan dalam menghadapi ancaman AI dalam pertahanan dan memberikan dukungan bagi keamanan dan pertahanan Negara, maka diperlukan cara-cara/langkah-langkah (ways) sebagai berikut:

Pembuatan berbagai kebijakan, UU dan peraturan yang memadai sebagai dasar. Dalam Peraturan Presiden Nomor 8 Tahun 2021 tentang Kebijakan Umum Pertahanan tahun 2020-2045, dibahas bahwa pembangunan teknologi pertahanan diarahkan untuk memanfaatkan AI. Kemudian BPPT meluncurkan Strategi Nasional Kecerdasan Artifisial Indonesia (Stranas KA) 2020-2045, yang didalamnya merupakan arah kebijakan nasional dalam mengembangkan teknologi AI yang dijadikan pedoman di bidang operasi penelitian AI di Indonesia bagi Kementerian, organisasi, pemerintah daerah dan pemangku kepentingan lainnya. Ada pula pembuatan strategic planning jangka pendek, menengah, panjang yang di dalamnya termasuk terjaminnya kebutuhan anggaran yang cukup untuk menghadapi ancaman AI

Pemantapan kemampuan intelijen untuk memahami perkembangan ancaman AI dan mampu mengatasinya. Penentuan obyek vital nasional yang perlu diamankan dari serangan unmanned system / AI. Perkuatan sistem pertahanan wilayah dan sektor-sektor non militer

Pembangunan industri pertahanan dalam negeri. Sedang diupayakan pembangunan sistem pertahanan AI yang terintegrasi dan berkelanjutan dengan pembelian atau pengadaan peralatan anti serangan unmanned system barik dari dalam negeri maupun luar negeri.

Perekrutan dan pelatihan sumber daya manusia yang berkelanjutan. Minimnya dan masih tertinggalnya teknologi Indonesia, tidak apa kalau belum mampu dan belum bisa memproduksi sendiri, kita bisa membeli dengan catatan harus ada klausul-klausul alih teknologi, transfer teknologi, pelatihan-pelatihan agar kita bisa mampu membuat sendiri. Pembinaan sumber daya manusia harus mengadopsi standar keilmuan sehingga keterampilan yang diperoleh dari pelatihan dan studi dapat digunakan oleh institusi dan bangsa sebagai modal intelektual. Saat merancang sumber daya manusia untuk penguasaan teknologi pertahanan, fasilitas pembelajaran yang sesuai serta kurikulum dan lingkungan diperlukan untuk menumbuhkan hasil imajinatif dan inovatif

Pembangunan kekuatan yang terintegrasi diantara komponen utama, cadangan dan pendukung. Pembagian kewenangan, tugas, tanggung jawab dan fungsi yang jelas diantara lembaga/instansi Negara dalam menghadapi ancaman AI.

Melakukan kerjasama secara bilateral, multilateral di tingkat regional dan internasional. Melakukan kerjasama dan terintegrasi secara triple helix (pemerintah, industry, akademisi), sampai dengan multiple helix dalam pembangunan kekuatan AI nasional

5. Kesimpulan dan Rekomendasi

Penggunaan AI dalam pertahanan telah berdampak bagi strategi pertahanan Indonesia.

Tujuan (ends) ;terciptanya kondisi atau keadaan yang aman dari ancaman AI.

Sarana dan Prasarana (means); alat-alat dengan teknologi AI baik yang dibeli dari luar negeri atau diproduksi sendiri dalam negeri.

Cara/Langkah (ways); pembuatan berbagai kebijakan, UU dan peraturan yang memadai sebagai dasar.

Pemantapan kemampuan intelijen untuk memahami perkembangan ancaman AI dan mampu mengatasinya; Pembangunan industri pertahanan dalam negeri; Perekrutan dan pelatihan sumber daya manusia yang berkelanjutan; Pembangunan kekuatan yang terintegrasi diantara komponen utama, cadangan dan pendukung; Melakukan kerjasama di tingkat regional dan internasional.

Adapun berdasarkan kesimpulan penelitian tersebut, peneliti memberikan rekomendasi kepada pihak-pihak terkait dalam menghadapi ancaman penggunaan AI di Indonesia guna tercapainya kepentingan nasional terutama dalam melindungi keselamatan bangsa dan mendukung keamanan dan pertahanan Negara.

Peneliti merekomendasikan seluruh instansi/lembaga terkait untuk dapat menggunakan AI untuk mendukung strategi pertahanan secara lebih optimal dengan hal-hal berikut: Memprioritaskan riset dan inovasi produk AI; Membangun dan menggunakan produk industri pertahanan dalam negeri; Melakukan kerjasama secara bilateral, multilateral di tingkat regional dan internasional; Melakukan kerjasama dan terintegrasi secara triple helix (pemerintah, industry, akademisi), sampai dengan multiple helix dalam pembangunan kekuatan AI nasional

Daftar Pustaka

Congressional Research Service. (2018). U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress. CRS.

Corrigan, J. (2017, November 3). Three-Star General Wants AI in Every New Weapon System. Retrieved from Defense One: https://www.defenseone.com/technology/2017/11/three-star-general-wants-artificial-intelligence-every-new-weapon-system/142239/

Macri, G. (2016, September 13). NSA Chief Says Without Artificial Intelligence, Cyber 'Is a Losing Strategy'. Retrieved from Inside Sources: https://www.insidesources.com/nsa-chief-without-ai-cyber-is-a-losing-strategy/#:~:text=Technology-,NSA%20Chief%20Says%20Without%20Artificial,Cyber%20'Is%20a%20Losing%20Strategy'&text=Michael%20Rogers%2C%20who%20told%20Congress,%E2%80%9Cis%20a%20losing%20s

Organisation for Economic Co-operation and Development (OECD). (2016). OECD Science, Technology and Innovation Outlook 2016.

Roth, M. (2019, Februari 22). Artificial Intelligence in the Military – An Overview of Capabilities. Retrieved from Emerj: https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/

Svenmarck, Peter et al. (2018). Possibilities and Challenges for Artificial Intelligence in Military Applications. NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting. NATO Science and Technology Organisation.

Weisgerber, M. (2017, September 19). Defense Firms to Air Force: Want Your Planes' Data? Pay Up. Retrieved from Defense One: http://www.defenseone.com/technology/2017/09/military-planes-predictive-maintenance-technology/141133/

Work, R. O., & Brimley, S. (2014). 20YY: Preparing for War in the Robotic Age. Washington D.C.: Center for a New American Security.