e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 10 No 2 Tahun 2023 Hal. : 779-788

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

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

PEMANFAATAN ARTIFICIAL INTELLIGENCE DALAM PERTAHANAN SIBER

Ishak Farid, Agus HS Reksoprodjo, Suhirwan

Prodi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan RI

Abstrak

Artificial Intelligence (AI) telah menjadi salah satu teknologi penting dalam pertahanan siber. AI memiliki kemampuan untuk memantau dan menganalisis aktivitas jaringan dan sistem informasi untuk mendeteksi serangan dan ancaman potensial. Penelitian ini bertujuan untuk mengeksplorasi pemanfaatan AI dalam pertahanan siber melalui metode penelitian deskriptif kualitatif. Metode penelitian deskriptif kualitatif difungsikan untuk mengumpulkan dan menganalisa data tentang pemanfaatan AI dalam pertahanan siber. Hasil dari penelitian ini menunjukkan bahwa AI memiliki potensi besar untuk meningkatkan efektivitas dan efisiensi pertahanan siber dengan memantau dan menganalisis aktivitas jaringan dan sistem informasi untuk mendeteksi serangan dan ancaman potensial. AI juga dapat membantu untuk memprediksi dan mencegah serangan dengan menganalisis pola perilaku dan aktivitas yang tidak normal dalam jaringan dan sistem informasi. Namun, penting untuk diingat bahwa AI juga memiliki kelemahan dan batasan, seperti masalah akurasi dan kesalahan dalam pengenalan pola, yang harus diperhitungkan dalam implementasi AI dalam pertahanan siber. Oleh karena itu, penting untuk memastikan bahwa AI digunakan sebagai bagian dari strategi pertahanan siber yang holistik dan dalam konteks regulasi yang sesuai untuk memastikan privasi dan keamanan data. Kesimpulan dari penelitian ini adalah bahwa AI memiliki potensi besar untuk meningkatkan pertahanan siber, tetapi perlu diimplementasikan dengan bijak dan dalam konteks regulasi yang sesuai untuk memastikan privasi dan keamanan data.

Kata Kunci: Artificial intelligence, Pertahanan Siber, Serangan siber.

*Correspondence Address : Faridz1987@gmail.com
DOI : 10.31604/jips.v10i2.2023.779-788
© 2023UM-Tapsel Press

PENDAHULUAN

Pertahanan Siber adalah upaya untuk melindungi sistem dan jaringan informasi dari ancaman *cyber* seperti serangan hacker, malware, dan lainnya. Dalam era digital saat ini, pertahanan siber menjadi sangat penting karena banyak aktivitas bisnis dan pemerintahan yang dilakukan secara online. Pertahanan siber sangat penting karena jaringan dan sistem digital saat ini menjadi bagian tak terpisahkan dari kehidupan sehari-hari dan bisnis. Serangan *cyber* bisa mengancam privasi, keamanan informasi, dan ekonomi. Oleh karena itu, pertahanan siber sangat penting untuk memastikan keamanan informasi dan jaringan.

Ancaman *cyber* adalah isu yang semakin penting dalam era digital saat ini. Ancaman *cyber* berupa serangan atau tindakan illegal yang dilakukan melalui jaringan atau sistem informasi, seperti internet. Ancaman *cyber* sangat beragam dan dapat mengancam keamanan informasi, privasi, dan ekonomi individu maupun organisasi. Serangan DDoS (*Distributed Denial of Service*) adalah salah satu contoh ancaman *cyber*. Serangan DDoS membuat jaringan atau situs web tidak bisa diakses dengan membanjiri jaringan dengan lalu lintas palsu. Serangan ini dapat mempengaruhi kinerja sistem dan membuat pelanggan tidak bisa mengakses layanan yang dibutuhkan.

Pencurian informasi rahasia seperti kartu kredit dan *password* nomor adalah ancaman *cyber* lainnya. Hacker dapat mencuri informasi ini dengan menyusup ke sistem jaringan dan mengambil informasi yang dikumpulkan oleh organisasi atau individu. Ini mengancam privasi dan keamanan finansial individu. Virus dan malware juga merupakan ancaman *cyber* yang serius. Virus dan malware dapat mempengaruhi kinerja sistem dan membahayakan informasi yang disimpan pada komputer. Virus dan malware juga dapat mengirimkan informasi sensitif kepada pihak yang tidak berwenang atau membuka jalan bagi serangan lebih lanjut. Ancaman *cyber* juga memiliki dampak ekonomi yang signifikan. Serangan DDoS dapat mempengaruhi kinerja bisnis dan membuat pelanggan tidak puas dengan layanan yang diterima. Pencurian informasi sensitif dapat menyebabkan kerugian finansial bagi individu dan organisasi. Virus dan malware juga dapat menyebabkan kerugian waktu dan uang untuk memperbaiki sistem yang terpengaruh.

Ada beberapa hal yang perlu dilakukan dalam pertahanan siber, seperti menggunakan teknologi keamanan yang efektif dan melakukan audit keamanan secara berkala. *Firewall* dan antivirus adalah teknologi keamanan yang penting untuk memblokir serangan *cyber* dan meminimalisir risiko serangan. Audit keamanan membantu menentukan area yang rentan dan memastikan bahwa sistem keamanan berfungsi dengan baik. Edukasi dan kesadaran tentang pertahanan siber juga penting. Individu dan organisasi harus sadar tentang ancaman *cyber* dan memahami bagaimana cara melindungi informasi dan jaringan mereka. Hal ini melibatkan memahami bagaimana serangan *cyber* bekerja dan mempraktikkan praktik keamanan yang baik seperti membuat *password* yang kuat dan memperbarui sistem keamanan secara berkala.

Pemerintah juga berperan penting dalam pertahanan siber. Pemerintah dapat membuat regulasi dan undang-undang untuk memastikan bahwa organisasi dan individu melakukan tindakan yang memadai untuk melindungi jaringan dan informasi mereka. Pemerintah juga dapat memberikan dukungan dan bantuan teknis untuk memastikan bahwa pertahanan siber efektif. Secara keseluruhan, pertahanan siber adalah hal yang penting bagi setiap individu dan

organisasi dalam era digital saat ini. Untuk memastikan bahwa informasi dan jaringan aman, perlu adanya tindakan dan usaha yang konsisten dari semua pihak. Teknologi keamanan, edukasi dan kesadaran, dan dukungan pemerintah semuanya penting untuk memastikan bahwa pertahanan siber berfungsi dengan baik dan melindungi informasi dan jaringan dari ancaman *cyber*.

Namun, meskipun teknik dan teknologi yang digunakan dalam pertahanan siber sudah canggih, masih ada beberapa tantangan yang harus dilewati. Salah satunya adalah masalah pembaruan, karena ancaman *cyber* berkembang dengan cepat dan sistem keamanan harus diperbarui secara berkala untuk tetap efektif. Tantangan lain adalah masalah budaya, karena banyak orang masih belum memahami pentingnya pertahanan siber dan tidak melakukan praktik keamanan yang baik. Secara keseluruhan, pertahanan siber adalah hal yang penting bagi keamanan sistem dan jaringan informasi.

Untuk mengatasi ancaman *cyber*, pemanfaatan *Artificial Intelligence* (AI) dalam pertahanan siber menjadi hal yang penting. AI memiliki kemampuan untuk memproses dan menganalisis data dalam jumlah sangat banyak dengan cepat dan akurat. Ini membuat AI sangat berguna dalam membantu mencegah dan mengatasi ancaman *cyber*. *Artificial Intelligence* (AI) adalah cabang dari ilmu komputer yang berkonsentrasi pada pembuatan mesin yang dapat melakukan peran yang biasanya dilakukan oleh manusia, seperti memecahkan masalah, membuat keputusan, dan mengadaptasi dengan situasi baru.

AI dapat berupa sistem software yang memiliki kemampuan untuk mengambil tindakan atau membuat keputusan dengan sendirinya, tanpa intervensi manusia. AI memiliki banyak manfaat untuk masyarakat, seperti mempermudah pekerjaan dan mempercepat proses bisnis. AI dapat membantu dalam memecahkan masalah yang rumit dan membuat keputusan yang akurat dengan cepat. Hal ini membuat AI sangat berguna dalam berbagai bidang, seperti perawatan kesehatan, transportasi, dan produksi. Kemajuan dalam AI juga memunculkan pertanyaan tentang masa depan pekerjaan dan bagaimana AI akan mempengaruhi lapangan pekerjaan. Beberapa orang khawatir bahwa AI akan menggantikan pekerjaan manusia, namun sebagian besar ahli berpendapat bahwa AI akan membuka peluang kerja baru dan membantu manusia dalam tugas-tugas yang berat dan membosankan.

Revolusi Industri Keempat (yang sekarang) sangat bergantung pada kecerdasan buatan (AI). Pengaruh aplikasi dan teknologi AI sangat signifikan. AI mulai berdampak besar pada masalah militer dan geopolitik. Menurut beberapa pengamat, kecerdasan buatan (AI) memiliki potensi yang sama untuk merevolusi teknologi keamanan nasional seperti senjata nuklir, pesawat terbang, komputer, dan bioteknologi (Work & Brimley, 2014). Pertumbuhan eksponensial AI di sektor militer akan secara signifikan mempengaruhi pemulihan operasi militer. Operasi militer di masa depan dan konsep pertempuran akan diubah secara drastis oleh ini. Kemajuan teknis yang cepat juga mengubah landasan intelektual pertempuran itu sendiri.

Banyak sekali militer di seluruh negara, termasuk di Amerika Serikat, Cina, Rusia, dan Israel, telah lama menggunakan teknologi AI untuk menunjang kegiatan pertahanan dan tugas militer. Meskipun AI masih dalam proses awal atau tahap awal, tidak dapat disangkal AI memiliki potensi untuk mengubah dinamika industri keamanan dan pertahanan, yang selanjutnya dapat mengubah keseimbangan kekuatan saat ini antara militer dan ekonomi dalam sistem internasional. Pada tahun 2020,

peluncuran Strategi Nasional Kecerdasan Buatan Indonesia (STRANAS-KA), yang menguraikan tujuan penerapan AI ke sejumlah domain nasional, termasuk pemerintah, *smartcity*, pangan, kesehatan, dan pendidikan. Pemanfaatan AI di ranah pertahanan sebagai metode pertahanan negara belum tercakup dalam STRANAS-KA ini.

METODE PENELITIAN

Metode penelitian dapat dipahami sebagai cara ilmiah untuk memperoleh data penelitian untuk mencapai tujuan dan maksud tertentu. Pendekatan ilmiah untuk mengumpulkan data, tujuan dan sasaran tertentu. Ada tiga pendekatan penelitian berbeda yang dapat diterapkan, termasuk kualitatif, kuantitatif, dan kombinasi keduanya (metode campuran). Perbedaan paling mendasar antara metode penelitian kuantitatif dan kualitatif terletak pada bentuknya. Penelitian kuantitatif merupakan penelitian yang dilakukan memakai angka-angka dan berdasarkan pertanyaan-pertanyaan tertutup, sementara penelitian kualitatif dilakukan dengan menggunakan kata-kata yang membentuk kalimat dan berdasarkan pertanyaan yang terbuka (Creswell, 2014).

Untuk mendeskripsikan dan mengkaji penggunaan kecerdasan buatan dalam pertahanan siber, penelitian ini memanfaatkan rancangan penelitian kualitatif deskriptif analitis. Karena penelitian kualitatif dianggap memenuhi persyaratan yang diminta oleh peneliti, maka dipilihlah penelitian kualitatif semacam ini. Hal ini sejalan dengan pernyataan Sari Wahyuni (2019) bahwa teknik penelitian kualitatif adalah pendekatan yang berasal dari ilmu sosial yang dapat memungkinkan seorang peneliti untuk mengkaji suatu fenomena sosial dan budaya.

HASIL DAN PEMBAHASAN

1. Teknologi Kecerdasan Buatan atau *Artificial Intelligence*

Kata teknologi berasal dari kata Yunani technologia, yang menunjukkan pendekatan metodis terhadap seni dan kerajinan. Asal-usul kata ini berasal dari kata *techne* dan *logos* atau (kata dan bicara). Orang Yunani kuno menyadari arti kata asal *techne*, yaitu "seni," dan "kerajinan". Seni pada awalnya mengacu pada sesuatu yang diciptakan oleh manusia untuk dikontraskan dengan istilah alami, tetapi sejak itu mengacu pada keterampilan (keterampilan) yang digunakan untuk membuat item. Selain itu, istilah "teknologi" digunakan secara luas pada awal abad kedua puluh satu untuk menggambarkan berbagai cara, prosedur, dan konsep. Hingga pertengahan abad ke-20, definisi teknologi ini diperluas untuk mencakup "sarana atau kegiatan yang dengannya sarana berusaha merubah atau mengelola lingkungannya" (Soemitro, 1990).

Menurut pembahasan di atas tentang definisi dan perkembangan teknologi maka tidak memungkinkan untuk ke depannya manusia bisa hidup tanpa teknologi. Oleh sebab itu dari sudut pandang pertahanan saat ini sudah seharusnya mulai menggunakan atau memanfaatkan perkembangan teknologi yang ada di dalam pertahanan negara itu sendiri. Memanfaatkan kecerdasan buatan adalah salah satu kemajuan teknologi terbaru yang dapat digunakan di bidang keamanan nasional dalam upaya mengikuti perkembangan teknologi (AI). Kecerdasan buatan (AI) saat ini sedang banyak digunakan di semua bidang masyarakat, membuat pekerjaan dan kehidupan manusia lebih ringan dan meningkatkan output serta meningkatkan produktivitas dari hasil pekerjaan.

Secara luas, AI memiliki potensi untuk meningkatkan produktivitas dan

mempercepat inovasi. AI juga memberi kemudahan bagi masyarakat yaitu kemampuan untuk mengatasi masalah, seperti penyakit, kelaparan, perubahan iklim, dan bencana alam. Banyak bisnis di kawasan Asia Pasifik telah melihat keuntungan finansial yang nyata karena AI. Misalnya, operator transportasi peti kemas global teratas OOCL mengklaim bahwa menggunakan AI telah membantu mereka dapat menghemat hingga USD 10 juta (Rp 139 miliar) per tahun (Mamduh, 2018). Seperti yang terjadi di Amerika Serikat, di mana AI mampu mendeteksi penyakit Alzheimer lebih dini daripada menggunakan metode yang ada saat ini, penerapan AI dalam industri kesehatan juga mulai menunjukkan hasil yang menjanjikan. Sejumlah aplikasi AI yang sukses dalam berbagai bidang semakin mendorong pengembangan lebih banyak aplikasi AI yang memiliki manfaat bagi manusia. Maka dari itu, pemanfaatan AI dalam pertahana negara di Indonesia harus dimulai saat ini agar tidak semakin tertinggal dari kemajuan teknologi.

2. Pertahanan Siber

Pertahanan merupakan sebuah konsep yang memiliki beragam definisi, terutama dalam penyelenggaraan suatu negara. Konsep pertahanan seringkali dihubungkan dengan aspek kehidupan bernegara dengan ide bertahanan demi keberlangsungan hidup yang memiliki hubungan dengan rasa aman (keamanan) setiap sumber daya yang berada di dalam negara tersebut dari segala ancaman yang dapat bersumber dari dalam maupun luar negeri. Menurut Syarifudin Tippe (2016), objek dari ilmu pertahanan adalah perilaku negara untuk menjaga dan mengembangkan keberlangsungan kehidupan negara tersebut. Ilmu militer dan perang merupakan cikal bakal ilmu pertahanan yang memiliki saripati konsep dan ide terkait pengembangan organisasi, strategi, dan taktik militer dalam mencapai kepentingan negara (Tippe, 2016). Dalam perjalanannya, berbagai ancaman yang berdampak pada pertahanan negara terus berubah sebagai akibat dari perkembangan lingkungan yang dinamis dan konteks strategis. Ancaman militer, nonmiliter, dan hibrida adalah beberapa kategori ancaman berbeda yang membentuk kompleksitas ancaman. Ancaman ini dapat dibagi menjadi ancaman nyata dan hipotetis. (Buku Putih Pertahanan Negara, 2015).

Ancaman terhadap keamanan siber mungkin dalam berbagai ukuran atau bentuk. Kecerdasan buatan, atau AI, berpotensi menjadi sangat penting dalam tindakan pencegahan militer. AI mungkin akan menjadi peralatan penting untuk meningkatkan operasi dan keamanan siber. Komandan Komando Siber AS Laksamana Michael Rogers mengatakan pada tahun 2016 selama penampilannya di hadapan Komite Senat Angkatan Bersenjata bahwa hanya bergantung pada kecerdasan yang dimiliki manusia di dunia maya adalah "strategi yang kalah." Peretas cukup melakukan pengubahan kode yang digunakan umtuk untuk melewati pertahanan karena sistem keamanan siber tradisional mencari kesamaan historis dengan kode rahasia yang diketahui. Di sisi lain, teknologi berkemampuan AI bisa dilatih untuk mengenali penyimpangan atau ketidakbiasaan dalam pola jaringan yang lebih luas, memberikan pertahanan yang menyeluruh dan dinamis terhadap serangan (Macri, 2016).

3. Pemanfaatan *Artificial Intelligence* dalam Pertahanan Siber

Ancaman yang sangat lemah bagi pertahanan nasional adalah tumbuhnya cyberwarfare. Ini ditunjukkan oleh banyak contoh situs web pemerintah yang diretas; contoh terbaru adalah situs web Komisi Pemilihan Umum (KPU), yang

menampilkan data hasil aktual pilkada serentak 2018 dan memiliki alamat situs web infopemilu.kpu.go.id. yang menayangkan informasi hasil suara secara langsung dalam Pilkada sementara 2018. Situs KPU diretas oleh orang yang tidak bertanggungjawab. Kemudian hal yang sama dialami oleh situs yang dimiliki Ditjen Pajak, yang diserang peretas pada 10 Juni 2018.

Tiga serangan terhadap teknologi digital yang saat ini dapat berdampak pada kehidupan masyarakat adalah *ransomware*, rekayasa sosial, dan aktivitas orang dalam yang berbahaya, menurut pertemuan pejabat ekonomi, politik, dan sosial internasional di Swiss dalam kegiatan World Economic Forum. Bank Sentral Republik Indonesia, juga dikenal sebagai Bank Indonesia, menjadi target serangan siber pada minggu ketiga tahun 2022 yang berbentuk *ransomware Conti*, yang mengenkripsi sebagian data Bank Indonesia. Hal ini bukanlah kejadian baru; pada tahun 2017, Kementerian Keuangan mengalami situasi serupa yang menyebabkan sistem layanan pajak nasional dan sistem komunikasinya "runtuh" selama beberapa jam. Kejadian lain yang mulai terjadi sekitar awal tahun 2022 adalah kesadaran masyarakat Indonesia dari berbagai kalangan bahwa ada pasar seni virtual di mana karya dijual sebagai foto dan kemudian dijual dengan kurs pasar dengan menggunakan mata uang digital atau *cryptocurrency*. NFT, atau *Non Fungible Token*, telah menjadi subjek penelitian oleh berbagai entitas, termasuk pejabat pemerintah dan bahkan siswa sekolah menengah. Tentu saja, fenomena ini perlu diselidiki lebih lanjut oleh lembaga penegak hukum yaitu POLRI, Kejaksaan, dan KPK. Karena sangat mungkin kejahatan pencucian uang yang melibatkan teknologi ini pada akhirnya akan terjadi di masa depan. Oleh karena itu, pemerintah dan juga masyarakat Indonesia secara keseluruhan mesti faham teknologi dan berpikir menggunakan basis iptek yang saat ini berkembang dengan sangat pesat. Meskipun tidak terkait dengan militer, bahaya dan masalah kontemporer memiliki dampak signifikan pada kehidupan masyarakat dalam hal ekonomi, politik, dan keamanan mereka. Untuk mengatasi ancaman dan tantangan ini, diperlukan kebijakan dan tindak strategis yang berkelanjutan.

Kemajuan ilmu pengetahuan dan teknologi suatu bangsa juga semakin pesat di bidang keamanan dan pertahanan. Salah satu bahaya terbesar bagi ketahanan dan kedaulatan suatu negara adalah perang asimetris, yang dapat menyerang kapan saja dan dari lokasi mana pun. Dengan kemajuan teknologi sensor dan kapasitas komputer untuk berpikir secara mandiri dalam mengambil keputusan penembakan, perkembangan teknologi senjata kini telah berubah. Konsep pertahanan yang saat ini digunakan didasarkan pada teknologi digital, yang juga memiliki kapasitas untuk menyembunyikan atau menjaga kekuatan yang kita miliki dari lawan dan mengirimkan penilaian dari sensor langsung ke senjata. Dalam menjaga kerahasiaan strategi perang yang sedang direncanakan saat ini, informasi strategis seperti halnya adalah intelijen terkait pasukan musuh dan ukuran kekuatan perang kita harus dapat disimpan dengan baik. Akan lebih baik lagi jika kita dapat sepenuhnya mencegah tindakan intelijen atau pengamatan musuh dengan menggunakan teknologi penginderaan yaitu dengan drone dan satelit. Konsep pertahanan yang saat ini sedang ramai dibicarakan yaitu *Anti Access* atau *Area Denial System,* yang secara konseptual dan telah digunakan pada perang tradisional seperti perang salib. Ide A2 atau AD ini secara umum mengacu pada taktik pertahanan yang memiliki prioritas pada pencegahan atau konstruksi pertahanan yang mampu

menahan serangan dari musuh yang lebih kuat. Tentunya agar dapat bertahan atau bahkan melakukan tindakan penanggulangan dalam rangka melindungi kedaulatan negara, rencana pertahanan dan serangan ini harus mampu melakukan integrasi terpadu secara keseluruhan dari masing-masing sumber daya pertahanan negara. Sebagai contohnya adalah, adanya konflik bersenjata di Nagorno-Karabakh, pertempuran antara dua mantan anggota Uni Soviet Armenia dan Azerbaijan, yang memakan korban yang signifikan, adalah ilustrasi yang sangat jelas tentang perkembangan teknologi dalam perang yang terjadi untuk sementara waktu (Syafi'i, Supriyadi, Prihantoro, & Gultom, 2023).

Ketika menghadapi ancaman non-militer, K/L dipaksa untuk bertindak sebagai elemen utama yang didukung oleh elemen kekuatan nasional lainnya, termasuk pemerintah daerah, di luar ranah pertahanan. Sementara itu, strategi pertahanan negara digunakan untuk mengatasi ancaman hibrida berdasarkan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara. Strategi ini menempatkan TNI sebagai komponen utama sekaligus mendapat dukungan dari lembaga dan institusi negara terkait sesuai dengan peran, tugas dan tanggung jawabnya masing-masing. Dengan menggunakan kekuatan militer dan non-militer sejalan dengan hukum negara dan keputusan politik, sistem pertahanan militer dan sistem pertahanan non-militer dapat digunakan untuk mengimplementasikan pertahanan tersebut secara terintegrasi.

Dalam hal melindungi aset pengguna dan lingkungan online secara keseluruhan, keamanan siber mengacu pada berbagai alat, aturan, ide keamanan, perlindungan, pedoman, teknik manajemen risiko, tindakan, pelatihan, dan teknologi. Organisasi dan sumber daya pengguna keamanan siber mencakup individu, infrastruktur, aplikasi, layanan, sistem telekomunikasi, perangkat komputer yang terhubung, dan semua informasi yang dikirim dan/atau disimpan dalam lingkungan virtual. Tujuan keamanan siber adalah untuk melindungi aset pengguna, aset organisasi, dan aset organisasi dari risiko keamanan yang berlaku di lingkungan siber. Tujuan keamanan siber adalah untuk melindungi aset pengguna, aset organisasi, dan aset organisasi dari risiko keamanan yang berlaku di lingkungan siber. Ketersediaan, Integritas, yang mencakup keaslian dan langkah-langkah potensial untuk mengurangi insiden penolakan, dan Kerahasiaan adalah tujuan keamanan umum. Kepastian Hukum, Tindakan Teknis dan Prosedural, Struktur Organisasi, Peningkatan Kapasitas dan Pendidikan Pengguna, dan Kerja Sama Internasional adalah lima bidang kegiatan yang membentuk keamanan siber global (termasuk gotong royong dalam upaya mengatasi ancaman siber) (Makarim, 2018).

Pertahanan siber adalah upaya untuk melindungi sistem dan jaringan komputer dari ancaman cyber, seperti serangan hacker, malware, dan pencurian data. Dalam era teknologi yang semakin maju, ancaman cyber menjadi semakin serius dan mengakibatkan kerugian besar bagi individu, perusahaan, dan negara. Untuk mengatasi ancaman cyber, pemanfaatan *Artificial Intelligence* (AI) dalam pertahanan siber menjadi hal yang penting. AI memiliki kemampuan untuk memproses dan menganalisis data dalam jumlah besar dengan cepat dan akurat. Ini membuat AI sangat berguna dalam membantu mencegah dan mengatasi ancaman cyber.

Memasuki revolusi industri keempat, tidak dapat dipungkiri bahwa jika kemajuan teknologi disalahgunakan, mereka akan digunakan untuk membuat senjata otonom yang akan membunuh target. Serangan siber berbasis malware

seharusnya tidak menjadi satu-satunya hal yang harus diwaspadai; peningkatan teknologi kecerdasan buatan (AI) juga harus diwaspadai. Untuk menemukan dan menargetkan target, teknologi AI dapat diubah menjadi terhubung oleh big data, yang telah mengumpulkan data identitas yang telah beredar di media sosial (Hidayati & Gultom, 2019).

Artificial Intelligence dapat meningkatkan kapasitas manusia dengan cara memproses dan menganalisis kumpulan data besar jauh lebih cepat daripada manusia. Misalnya, dalam bidang kesehatan, *Artificial Intelligence* dapat membantu menganalisis data dari individu dan mengidentifikasi pola untuk melakukan diagnosis penyakit. Di bidang hukum, *Artificial Intelligence* digunakan sebagai penyaring dokumen pengadilan serta catatan hukum untuk memperoleh informasi yang relevan dengan kasus tersebut. Potensi mereka untuk bagian pertahanan sangat besar karena solusi *Artificial Intelligence* 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.

Karena ada begitu banyak kumpulan data yang tersedia untuk analisis, AI sangat membantu di bidang kecerdasan. Misalnya, fase awal Project Maven melibatkan otomatisasi pemrosesan intelijen untuk mendukung kegiatan anti-ISIL. Tim Project Maven, khususnya, telah menggunakan visi komputer dan algoritma pembelajaran mesin untuk membuat sel pengumpul intelijen yang akan memeriksa video dari kendaraan udara tak berawak dan secara otomatis mengidentifikasi perilaku bermusuhan untuk penargetan. Dalam peran ini, AI dimaksudkan untuk mengotomatisasi tenaga kerja analis manusia yang saat ini menghabiskan berjam-jam memilah-milah film untuk mengekstrak informasi yang berguna, berpotensi memungkinkan analis untuk membuat penilaian yang lebih efektif dan cepat berdasarkan data (Corrigan, 2017).

Pemanfaatan *Artificial Intelligence* pada pertahanan siber Pertama, AI dapat digunakan untuk deteksi serangan. AI dapat memonitor aktivitas jaringan dan mengenali pola yang tidak normal. Jika pola terdeteksi, AI dapat memperingatkan administrator jaringan dan memblokir serangan sebelum mereka menyebar dan merusak sistem. AI dapat digunakan untuk membantu dalam mendeteksi serangan pada pertahanan siber. AI dapat memanfaatkan algoritma pembelajaran mesin untuk mempelajari pola serangan yang berulang dan membedakan antara aktivitas normal dan aktivitas yang tidak biasa yang mungkin merupakan tanda serangan. AI juga dapat memonitor aktivitas jaringan secara real-time dan mempercepat deteksi serangan dengan memproses data dengan kecepatan yang lebih tinggi daripada manusia.

Kedua, AI dapat digunakan untuk analisis *comportamental*. AI dapat mempelajari dan menganalisis pola perilaku normal dari pengguna dan aplikasi, dan memperingatkan administrator jaringan jika ada perubahan dalam pola tersebut. Ini membantu mencegah serangan yang dikenali sebagai serangan manusia, seperti phishing. Dalam pertahanan siber, AI dapat digunakan untuk memantau dan menganalisis aktivitas jaringan dan sistem informasi untuk mendeteksi serangan dan ancaman potensial. AI juga dapat membantu untuk memprediksi dan mencegah serangan dengan menganalisis pola perilaku dan aktivitas yang tidak normal dalam jaringan dan sistem informasi. Dengan menggunakan algoritma pembelajaran mesin, AI dapat mempelajari dan mengidentifikasi pola perilaku yang dapat menunjukkan serangan atau tindakan tidak sah, seperti pencarian data rahasia atau aktivitas peretasan. AI

juga dapat membantu untuk memprioritaskan respon dan tindakan pertahanan siber dengan mengevaluasi tingkat ancaman dan potensi kerugian. Namun, penting untuk diingat bahwa AI juga memiliki kelemahan dan batasan, seperti masalah akurasi dan kesalahan dalam pengenalan pola, yang harus diperhitungkan dalam implementasi AI dalam pertahanan siber. Oleh karena itu, penting untuk memastikan bahwa AI digunakan sebagai bagian dari strategi pertahanan siber yang holistik dan dalam kontek regulasi yang sesuai untuk memastikan privasi dan keamanan data.

Ketiga, AI dapat digunakan untuk meningkatkan keamanan aplikasi. AI dapat membantu menemukan kelemahan dalam aplikasi dan memperbaiki masalah keamanan sebelum mereka diexploitasi oleh penyerang. AI dapat membantu untuk memantau dan menganalisis aktivitas aplikasi untuk mendeteksi serangan dan ancaman potensial. AI juga dapat membantu untuk memprediksi dan mencegah serangan dengan menganalisis pola perilaku dan aktivitas yang tidak normal dalam aplikasi. Dengan menggunakan algoritma pembelajaran mesin, AI dapat mempelajari dan mengidentifikasi pola perilaku yang dapat menunjukkan serangan atau tindakan tidak sah, seperti pencarian data rahasia atau aktivitas peretasan. AI juga dapat membantu untuk memprioritaskan respon dan tindakan pertahanan siber dengan mengevaluasi tingkat ancaman dan potensi kerugian. AI dapat digunakan untuk meningkatkan keamanan aplikasi dengan cara seperti; Autentikasi dengan memverifikasi identitas pengguna dan mencegah akses yang tidak sah dengan menganalisis pola perilaku dan biometric, mendeteksi serangan dengan memantau aktivitas aplikasi dan mendeteksi serangan seperti injeksi SQL, DDoS, dan serangan lainnya, dan analisis log yang memanfaatkan analisis log untuk mendeteksi aktivitas yang tidak sah dan membantu dalam investigasi serangan.

SIMPULAN

Dapat disimpulkan bahwa, AI dapat digunakan untuk mengatasi masalah keamanan yang ada. AI dapat membantu mempercepat proses penyelesaian masalah dan memastikan bahwa solusi yang diterapkan efektif dan sesuai. Secara keseluruhan, pemanfaatan AI dalam pertahanan siber memiliki potensi untuk membuat sistem dan jaringan komputer lebih aman dan terlindung dari ancaman cyber. Namun, perlu adanya tindakan yang bertanggung jawab dan memastikan bahwa AI digunakan secara etis dan aman. Kemajuan dalam AI akan terus membuka peluang-peluang baru dan membantu memecahkan masalah-masalah besar dalam pertahanan siber.

DAFTAR PUSTAKA

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

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th Edition).* California: SAGE Publications.

Hidayati, S., & Gultom, R. A. (2019). Analisis Kebutuhan Senjata Siber dalam Meningkatkan Pertahanan Indonesia di Era Peperangan Siber. *Jurnal Teknologi Persenjataan Volume 1 Nomor 1* .

Macri, G. (2016, September 13). *NSA Chief Says Without Artificial Intelligence, Cyber 'Is a Losing Strategy'*. Retrieved from https://insidesources.com/nsa-chief-without-ai-cyber-is-a-losingstrategy/#:~:text=Technology-,NSA%20Chief%20Says%20Without%20Artificial,Cyber%20'Is%20a%20Losing%20Strategy'&text=Michael%20Rog

Makarim, E. (2018). *Indonesian Legal Framework for Cybersecurity.* Retrieved from http://www.nisc.go.jp/security-site/campaign/%20ajsympo/pdf/lecture2.pdf

Mamduh, M. (2018, Mei 3). *Kecerdasan Buatan Dinilai Harus Punya Hukum*. Retrieved from medcom.id: https://www.medcom.id/teknologi/news-teknologi/nN95V6RN-kecerdasan-buatan-dinilai-harus-punya-hukum

Soemitro, R. H. (1990, Desember 6). Hukum dan Perkembangan Ilmu Pengetahuan dan Teknologi di Dalam Masyarakat. Semarang, Jawa Tengah, Indonesia.

Syafi'i, M. H., Supriyadi, A. A., Prihantoro, Y., & Gultom, R. A. (2023). Kajian Ilmu Pertahanan dalam Strategi Pertahanan Negara guna Menghadapi Ancaman Teknologi Digital di Indonesia. *Journal on Education, Volume 05, No. 02*, 4063-4076.

Tippe, S. (2016). *Ilmu Pertahanan: Sejarah, Konsep dan Implementasi.* Jakarta: Salemba Humanika.

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