PERKEMBANGAN ARTIFICIAL INTELLIGENCE (AI) PENERAPAN CYBER LAW DI INDONESIA

Ni Putu Wulan Cintana Cita[1], Cokorde Istri Dian Laksmi Dewi[2], Kadek Ary Purnama Dewi [3]
E-mail: wulancintana26@gmail.com, cokdild@gmail.com, aryartana2213@gmail.com
Magister Hukum Universitas Ngurah Rai

Keywords:
Artificial Intelligence, Cybercrime, Information Technology

Abstract

The development of information and communication technology has significantly impacted various aspects of human life, including the emergence of new challenges in the form of cybercrime. The internet, as a global computer network, has become a medium that facilitates interaction and information access, but also creates opportunities for criminal acts in the virtual world. One of the responses to these threats is the utilization of Artificial Intelligence (AI) in cybersecurity and the enforcement of digital law (Cyber law). AI has the capability to detect, analyze, and respond to cyberattacks quickly and efficiently. This paper aims to explore the development and history of AI as well as its application in cyber law enforcement in Indonesia. In addition to providing insights into the dynamics of digital crime, this study is expected to enhance knowledge in the field of criminology, particularly regarding the role of technology in modern law enforcement. This discussion is crucial in strengthening national digital resilience and addressing the increasingly complex challenges of globalization.

Kata kunci:
Artificial Intelligence, Kejahatan Siber, Teknolog Informasi.

Abstrak

Perkembangan teknologi informasi dan komunikasi telah memberikan dampak signifikan terhadap berbagai aspek kehidupan manusia, termasuk munculnya tantangan baru dalam bentuk kejahatan siber (*cyber crime*). Internet sebagai jaringan global komputer telah menjadi medium yang memudahkan interaksi dan akses informasi, namun juga membuka peluang bagi tindak pidana dalam dunia maya. Salah satu respons terhadap ancaman tersebut adalah pemanfaatan *Artificial Intelligence* (AI) dalam bidang keamanan siber dan penegakan hukum digital (*cyber law*). AI memiliki kemampuan dalam mendeteksi, menganalisis, dan merespons serangan siber secara cepat dan efisien. Penulisan ini bertujuan untuk mengetahui perkembangan dan sejarah AI serta penerapannya dalam hukum siber di Indonesia. Selain memberikan wawasan tentang dinamika kejahatan digital, tulisan ini juga diharapkan dapat memperkaya pengetahuan di bidang kriminologi, khususnya mengenai peran teknologi dalam penegakan hukum modern. Adanya kajian ini menjadi penting dalam rangka pemanfaatan *Artificial Intelligence.*

PENDAHULUAN

Teknologi memegang peran penting di era globalisasi pada saat ini, dimana teknologi telah menjadi bagian yang tidak dapat dipisahkan dalam kehidupan sehari-hari. Perkembangan teknologi telah merubah struktur masyarakat dari yang bersifat lokal menuju ke arah masyarakat yang berstruktur global. Perubahan ini disebabkan oleh kehadiran teknologi informasi. Perkembangan teknologi informasi itu berpadu dengan media dan komputer yang kemudian melahirkan piranti baru yang disebut internet. Perubahan teknologi dan perkembangannya merupakan perubahan global yang berdampak cukup signifikan di dalam suatu negara. Begitu pula di Indonesia, perkembangan teknologi membawa dampak besar bagi kehidupan masyarakat. Perkembangan ini secara fundamental akan mengubah masyarakat, baik dari perilaku, pola hubungan bermasyarakat, maupun cara bekerja. Perkembangan teknologi telekomunikasi, teknologi penyiaran dan aplikasi teknologi informasi membuat hampir semua perangkat komputer dan perangkat elektronika canggih menggunakan *Artificial Intelligence* (AI) untuk membuat sistem lebih baik, efektif, dan efisien. Semua perangkat elektronika dan komputer menjadi jauh lebih cerdas dengan bantuan teknologi AI untuk mempermudah kehidupan manusia di berbagai bidang sektor kehidupan.

Ancaman *cyber* adalah isu yang semakin penting dalam era digital saat ini. Ancaman *cyber* berupa serangan atau tindakan ilegal 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.

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.

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.

The United States Supreme Court mendefinisikan internet sebagai "an international network of interconnected computers," artinya jaringan internasional dari komputer-komputer yang saling berhubungan (Wahid dan Labib, 2010: 31). Internet memudahkan manusia untuk berinteraksi dan mencari informasi. Batas ruang dan waktu menjadi hilang dengan adanya jaringan internet. Dengan adanya perkembangan teknologi informasi ini tidak menutup kemungkinan akan melahirkan tindak pidana baru, yang membedakan adalah kejahatan ini dilakukan dengan media maya atau media virtual dan dalam melakukan tindak pidana tersebut menggunakan teknologi sebagai alat bantu. Tindak pidana dalam bentuk media maya atau dunia virtual disebut *cyber crime*. *Cyber crime* adalah tindak pidana dalam dunia maya atau dunia virtual yang merupakan tindak pidana yang timbul akibat revolusi teknologi informasi. *Cyber crime* merujuk pada suatu tindakan kejahatan yang berhubungan dengan dunia maya (*cyberspace*) dan tindakan kejahatan yang menggunakan komputer.

Cyber crime memiliki berbagai jenis tindak pidana, antara lain: *hacking dan cracking* (memasuki komputer atau sistem elektronik tanpa ijin), carding (mencuri nomor kartu kredit milik orang lain), *phishing* (penipuan website yang namanya hampir sama dengan aslinya), *defacing* (mengalihkan website asli ke website lain), *spamming* (pengiriman informasi atau berita secara berulang-ulang), *malware* (program atau software jahat yang menyusup ke dalam komputer atau sistem komputer) dan masih banyak lagi bentuk tindak pidana *cyber crime* tersebut. Rumusan masalah yang dibahas dalam tulisan ini adalah:

1) Bagaimana perkembangan dan sejarah *Artificial Intelligence* (AI)?
2) Bagaimanakah implikasi perkembangan *Artificial Intelligence* terhadap penegakan hukum siber di Indonesia?

METODE PENELITIAN

Penulisan ini menggunakan metode kualitatif melalui studi kepustakaan. Data *diperoleh* dari literatur relevan seperti buku, jurnal ilmiah, dan regulasi yang membahas *Artificial Intelligence* dan penerapannya dalam hukum siber di Indonesia. Analisis dilakukan secara deskriptif-kualitatif untuk mengkaji hubungan antara perkembangan AI dengan penegakan hukum terhadap kejahatan siber.

PEMBAHASAN

Perkembangan dan Sejarah *Artificial Intelligence (AI)*

Artificial Intelligence atau biasa disingkat AI adalah cabang ilmu komputer yang menggunakan kemampuan mesin untuk menyelesaikan tugas dan aktivitas yang biasa dilakukan oleh manusia. AI mengumpulkan dan mengolah berbagai data yang diterimanya menjadi informasi berguna agar dapat menyelesaikan tugas yang diberikan.

Sejak abad 20 istilah AI sudah mulai bermunculan baik dalam penelitian maupun dalam film genre fantasy. Kehadiran Atanasoff Berry Computer (ABC) pada

tahun 1940 membangkitkan semangat para ilmuwan untuk mengembangkan ide pembuatan *"electronic brain"* yang kemudian terus berkembang dan menjadi *Artificial Intelligence* yang kita kenal sekarang ini. Sejarah AI berawal di tahun 1950 oleh seorang ilmuwan matematika, Alan Turing dalam tulisannya berjudul *Computing Machinery and Intelligence* mengeluarkan pernyataan yang membangkitkan semangat pengembangan AI. Turing menyatakan bahwa jika manusia mampu menyelesaikan masalah dan membuat keputusan berdasarkan informasi dan tatanan yang tersedia.

Pada tahun 1956 nama *Artificial Intelligence* pertama tercetus dari John McCarthy dalam sebuah program AI *Darthmouth Summer Research Project on Artificial Intelligence* (DSRPAI). Namun sayangnya project ini tidak berjalan semulus rencana awal, karena kurangnya komitmen dari para peneliti yang terlibat. Pengembangan AI saat itu cenderung lambat, tetapi projek inilah yang memulai peluang AI hingga bisa berkembang seperti saat ini. Perkembangan pesat terjadi pada AI selama tahun 1960an, di mana komputer kini telah mampu menampung lebih banyak informasi dan lebih mudah untuk mendapat akses yang cepat dan murah. Beberapa algoritma machine learning juga mulai dipakai untuk menyelesaikan permasalahan spesifik.

Natural Language Processing (NLP) pertama, bernama STUDENT adalah model AI yang dibuat di Lisp untuk menyelesaikan permasalahan aljabar. STUDENT dianggap sebagai milestone awal dalam dunia AI NLP pada tahun 60an juga muncul ELIZA. Masih menggunakan NLP, ELIZA adalah chatbot pertama sebelum dikenal Siri, Alexa, dan berbagai robot NLP yang ada sekarang. Pemerintah saat itu menaruh harapan besar akan kehadiran ELIZA karena potensinya untuk menerjemahkan bahasa dengan sangat baik melalui data *processing*. Harapan ini meyakinkan pemerintah untuk memberi dukungan modal besar pada pengembangan AI di tahun 60-an. Pemerintah dan korporat yang selama ini mendanai penelitian AI merasa bahwa dalam 10 tahun terakhir para peneliti gagal memenuhi janjinya dan menciptakan kemajuan yang signifikan pada AI. Mereka akhirnya memutuskan untuk mengakhiri pembiayaan yang selama ini diberikan. Pada momen inilah dimana sejarah AI winter yang selama kurang lebih dua dekade sejak 1973 hingga tahun 1990 terjadi.

Para peneliti menemukan kesulitan untuk menciptakan mesin pintar karena keterbatasan utama yang dihadapi adalah komputer yang belum memadai. Pada Masa itu komputer yang digunakan belum cukup canggih untuk memproses data dalam jumlah masif disertai dengan kinerja komputer yang lambat. Komunikasi pun terhambat dan mempersulit pengembangan, di mana seseorang harus tau arti dari berbagai kata untuk dapat menciptakan satu kombinasi yang diharapkan. Memasuki tahap akhir abad milenium, rupanya nasib AI cukup baik untuk memasuki abad baru ini. Banyak milestone yang dicapai AI selama tahun 90an yang menjadi magnet pemikat untuk banyak perusahaan Amerika berinvestasi. Peran pemerintah Jepang yang yakin terhadap pengembangan komputer pintar juga berpengaruh pada pesatnya perkembangan AI di tahun 90an.

Pada tahun 1997 mesin Deep Blue yang dikeluarkan IBM untuk pertama kalinya dapat mengalahkan pemain catur kelas dunia, Garry Kasparov yang menjadi berita besar pada perkembangan AI di masa itu. Pada tahun yang sama pula Windows mengimplementasi penggunaan s*peech recognition software* pada Dragon Systems yang diciptakan. Tahun 1998 AI berkontribusi pada mainan anak-anak. Furby adalah binatang robot mainan pertama yang diciptakan dan memperoleh

banyak perhatian di kalangan orang tua. Dave Hampton dan Caleb Chung berhasil mengimplementasi AI tidak hanya dalam pekerjaan serius, tetapi juga untuk hiburan sehari hari.

Dilanjutkan dengan keluarnya *Artificial Intelligence RoBOt* (AIBO) oleh SONY pada tahun 1999. Robot berupa anjing ini mampu berinteraksi dengan dunia luar baik itu pemiliknya, lingkungan sekitar, bahkan AIBO dengan lainnya jika bertemu. Perkembangan AI sangat pesat pada saat menutup abad 20 tersebut. Di abad ini AI semakin siap untuk tampil di hadapan umum. Selama awal tahun 2000 penggunaan AI terus meningkat, dan informasi seputar AI semakin banyak disebarkan. Film adalah salah satu media penyebaran informasi AI, di mana saat itu banyak Film yang menceritakan tentang AI dan penggunaannya sehingga orang semakin paham gambaran AI seperti apa yang akan terjadi kedepannya.

Korporat juga semakin marak menggunakan AI dan terus mengembangkan *machine learning* dengan dukungan perangkat komputer yang sudah memadai. Pada tahun 2009 Google secara diam-diam telah memulai perancangan mobil tanpa pengemudi yang akhirnya diumumkan ke publik di tahun 2014 setelah lolos dari *Nevada's self-driving test*. Untuk sekarang kita sudah bisa mengatakan bahwa AI bukan lagi teknologi masa depan, melainkan teknologi saat ini. Kini penggunaan AI adalah hal yang umum dalam segala aspek kehidupan. Dalam kehidupan sehari-hari pun kita akan bertemu dengan banyak pemanfaatan AI yang membantu kita lebih mudah menyelesaikan berbagai tugas. Perkembangan AI yang sudah ada sejak 50 tahun lalu kini sudah mengalami banyak kemajuan. AI semakin pintar dan mampu membantu kehidupan manusia, bahkan memberikan jawaban yang lebih akurat atas suatu permasalahan. Kedepannya AI akan terus berkembang dengan berbagai kemungkinan yang dapat terjadi, bahkan yang tidak ada dalam bayangan kita sekalipun.

Implikasi Perkembangan *Artificial Intelligence* terhadap Penegakan Hukum Siber di Indonesia

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.

Kecerdasan buatan yang selanjutnya disebut AI merupakan sebuah studi tentang bagaimana membuat komputer melakukan hal-hal yang pada saat ini dapat dilakukan lebih baik oleh manusia. Banyaknya permasalahan kompleks yang dihadapi manusia saat ini membuat manusia bahkan komputer sulit untuk menyelesaikannya. *Malware* atau *Malicous Software* merupakan perangkat lunak yang secara eksplisit didesain untuk melakukan aktivitas berbahaya atau perusak perangkat lunak lainnya. Keduanya merupakan buah dari perkembangan teknologi, AI yang merupakan hadiah dari inovasi teknologi pada akhirnya dapat menjadikan

Malware yang merupakan bencana perkembangan teknologi menjadi senjata yang mematikan dan mengancam keamanan. Contoh dari tindak pidana Malware-AI sudah banyak terjadi seperti *deepfake video* atau *voice, Jackpotting, phising spear* dan masih banyak lagi.

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. 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 pertahanan negara di Indonesia harus dimulai saat ini agar tidak semakin tertinggal dari kemajuan teknologi.

Ancaman yang sangat lemah bagi pertahanan nasional adalah tumbuhnya cyberwarfare. 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*. 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 paham 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.

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). 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. *Artificial Intelligence* dapat meningkatkan kapasitas manusia dengan cara memproses dan menganalisa 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.

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 dieksploitasi 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 *analysislog* yang memanfaatkan analisis log untuk mendeteksi aktivitas yang tidak sah dan membantu dalam investigasi serangan.

PENUTUP

Pada tahun 1997 mesin *Deep Blue* yang dikeluarkan IBM untuk pertama kalinya dapat mengalahkan pemain catur kelas dunia, Garry Kasparov yang menjadi berita besar pada perkembangan AI di masa itu. Pada tahun yang sama pula

Windows mengimplementasi penggunaan *speech recognition software* pada Dragon Systems yang diciptakan. Tahun 1998 AI berkontribusi pada mainan anak-anak. Furby adalah binatang robot mainan pertama yang diciptakan dan memperoleh banyak perhatian di kalangan orang tua. Dave Hampton dan Caleb Chung berhasil mengimplementasi AI tidak hanya dalam pekerjaan serius, tetapi juga untuk hiburan sehari hari, kemudian dilanjutkan dengan keluarnya *Artificial Intelligence RoBOt* (AIBO) oleh SONY pada tahun 1999. Robot berupa anjing ini mampu berinteraksi dengan dunia luar baik itu pemiliknya, lingkungan sekitar, bahkan AIBO dengan lainnya jika bertemu. Pada tahun 2009 Google secara diam-diam telah memulai perancangan mobil tanpa pengemudi yang akhirnya diumumkan ke publik di tahun 2014 setelah lolos dari *Nevada's self-driving test.*

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.

DAFTAR PUSTAKA

BUKU

Abdul Wahid dan Mohammad Labib. 2005, *Kejahatan Mayantara (Cyber crime),* Jakarta: PT. Refika Aditama.

Didik M Arief Mansur dan Elisatris Gultom. 2005. *Cyber law Aspek Hukum Teknologi Informasi.* Bandung: Refika Aditama.

Danrivanto Budhijanto, 2010, *Hukum Telekomunikasi, Penyiaran dan Teknologi Informasi: Regulasi & Konvergensi*, Bandung, Refika Aditama.

Elaine Rich. dan Kevin Knight. 1991. *Artificial Intelligence*. New York: McGraw-Hill.

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

Jurnal

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. Kramer, S. & Bradfield, J. C. 2010. "*A general definition of malware*". Journal in Computer Virology, 6 (2), 105–114.

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.

Internet

Corrigan, J. (2017, November 3). *Three Star General Wants AI in Every New Weapon System*. Retrieved from http://https//www.defenseone.com, diakses pada tanggal 14 Mei 2024.

Claureina Diana, 2021, *Mengenal Sejarah AI atau Artificial Intelligence*, https://algorit.ma, diakses pada tanggal 14 Mei 2024.

Makarim, E. (2018). *Indonesian Legal Framework for Cybersecurity*. Retrieved from http://www.nisc.go.jp, diakses pada tanggal 14 Mei 2024.

Mamduh, M. (2018, Mei 3). K*ecerdasan Buatan Dinilai Harus Punya Hukum*. Retrieved from medcom.id: https://www.medcom.id, diakses pada tanggal 14 Mei 2024.

Widya, *Sejarah Perkembangan Kecerdasan Buatan (AI)*, https://widya.ai, diakses pada tanggal 14 Mei 2024.