شاپا چاپی: ۱۸۴۱-۲۷۸۳
شاپای الکترونیکی: ۱۹۲۲-۲۷۸۳

فصلنامه تمدن حقوقی

تمدن حقوقی

دوره ۶ - شماره ۱۸- زمستان ۱۴۰۲
ویژه‌نامه هوش مصنوعی

جایگاه هوش مصنوعی در صحت سنجی ادله داوری
همایون مافی، فاطمه قناد، محمدامین اسماعیل پور

هوش مصنوعی به عنوان دلیل در محاکمه کیفری
سالار صادقی

چالش ها و موانع مسئولیت کیفری در ربات های با قابلیت هوش مصنوعی
امین امیریان فارسانی، سیدمحمد حسینی

هوش مصنوعی و تاثیر آن بر سیستم قضایی
امیررضا محمودی، مریم بحرکاظمی

تاریخچه مختصری از هوش مصنوعی: گذشته، حال و آینده هوش مصنوعی
امین حاجی وند، علی خوش منظر، صابر سیاری زهان

هوش مصنوعی در نظام عدالت کیفری: روندها و احتمالات پیشرو
سالار صادقی

هوش مصنوعی و مسئولیت قانونی
سارا صلح چی، کیان بیگلربیگی

تعامل هوش مصنوعی و دیپلماسی برای پایداری محیط زیست
سبحان طیبی، نادر طیبی

جرایم هوش مصنوعی یک تحلیل بین رشته ای؛ تهدیدات و راه حل های قابل پیش بینی
زهرا وهبی

هوش مصنوعی و مردم‌سالاری؛ تأثیر اطلاعات غلط، ربات اجتماعی و هدف گذاری سیاسی
سارا صلح چی

کاربرد هوش مصنوعی در جرم یابی و تحقیقات جنایی؛ نمونه پژوهی: قتل های سریالی
حمیدرضا حیدرپور، محمد شهانقی، ژیلا مهرآرا

مجازانگاری استفاده اخلاقی از هوش مصنوعی با استفاده از نظریه فارابی درباره حقوق طبیعی و سعادت
محمدمهدی داور

هوش مصنوعی در نیروهای مسلح: مروری بر قابلیت ها، کاربردها و چالش ها
یاسر شاکری

Legal Civilization
Vol. 6, No. 18, Winter 2024
Pages: 201-250
Article Type: Translation
https://www.pzhfars.ir/article_193041.html
doi: 10. 22034/LC. 2024. 449459. 1457

تمدن حقوقی
دوره ۶، شماره ۱۸، ویژه‌نامه هوش مصنوعی، زمستان ۱۴۰۲
صفحات ۲۵۰-۲۰۱
نوع مقاله: ترجمه‌ای

Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges

Adib Bin Rashid
Industrial and Production Engineering Department, Military Institute of Science and Technology (MIST) , Dhaka, Bangladesh

Ashfakul Karim Kausik
Industrial and Production Engineering Department, Military Institute of Science and Technology (MIST) , Dhaka, Bangladesh

Ahamed Al Hassan Sunny
Industrial and Production Engineering Department, Military Institute of Science and Technology (MIST) , Dhaka, Bangladesh

Mehedy Hassan Bappy
Industrial and Production Engineering Department, Military Institute of Science and Technology (MIST) , Dhaka, Bangladesh

Yasser Shakeri
PhD in Criminal law and Criminology

Abstract
Artificial intelligence (AI) has become a reality in today's world with the rise of the 4th industrial revolution, especially in the armed forces. Military AI systems can process more data more effectively than traditional systems. Due to its intrinsic computing and decision-making capabilities, AI also increases combat systems' self-control, self-regulation, and self-actuation. Artificial intelligence is used in almost every military application, and increased research and development support from military research agencies to develop new and advanced AI technologies is expected to drive the widespread demand for AI-driven systems in the military. This research paper will discuss several AI applications in the military, as well as their capabilities, opportunities, and potential harm and devastation when there is instability. This present article looks at current and future potential for developing artificial intelligence algorithms, particularly in military applications. Most of the discussion focused on the seven patterns of AI, the usage and implementation of AI algorithms in the military, object detection, military logistics, and robots, the global instability induced by AI use, and nuclear risk. The article also looks at the current and future potential for developing artificial intelligence algorithms, particularly in military applications.

Keywords: Armed Forces, Artificial Intelligence, Opportunity, Damage.

Received: 2023/09/08 - Review: 2023/10/27 - Accepted: 2023/12/05

هوش مصنوعی در نیروهای مسلح: مروری بر قابلیت‌ها، کاربردها و چالش ها

ادیب بن راشد
گروه مهندسی صنایع و تولید، مؤسسه نظامی علوم و فناوری، داکا، بنگلادش
adib@me.mist.ac.bd
http://orcid.org/0000-0002-0681-7383

اشفاکول کریم کاسیک
گروه مهندسی صنایع و تولید، مؤسسه نظامی علوم و فناوری، داکا، بنگلادش
http://orcid.org/0000-0003-0899-7872

احمدالحسن ثانی
گروه مهندسی صنایع و تولید، مؤسسه نظامی علوم و فناوری، داکا، بنگلادش
http://orcid.org/0000-0002-1422-7586

مهدی حسن باپی
گروه مهندسی صنایع و تولید، مؤسسه نظامی علوم و فناوری، داکا، بنگلادش
http://orcid.org/0000-0002-5970-6396

یاسر شاکری
دکتری حقوق کیفری و جرم‌شناسی
ssssf200@gmail. com
http://orcid.org/0000-0001-7732-8125

چکیده
هوش مصنوعی با ظهور انقلاب صنعتی چهارم، به ویژه در نیروهای مسلح، در دنیای امروز به واقعیت تبدیل شده است. سیستم‌های هوش مصنوعی نظامی می‌توانند داده‌های بیشتری را به‌طور مؤثرتری نسبت به سیستم‌های سنتی پردازش کنند. با توجه به قابلیت‌های محاسباتی و تصمیم‌گیری ذاتی، هوش مصنوعی همچنین خودکنترلی، خودتنظیمی و خودگردانی سیستم‌های رزمی را افزایش می‌دهد. هوش مصنوعی تقریباً در هر برنامه نظامی استفاده می‌شود و انتظار می‌رود افزایش پشتیبانی تحقیق و توسعه از سوی آژانس‌های تحقیقاتی نظامی برای توسعه فناوری‌های جدید و پیشرفته هوش مصنوعی، تقاضای گسترده برای سیستم‌های مبتنی بر هوش مصنوعی در ارتش را افزایش دهد. در این پژوهش چندین کاربرد هوش مصنوعی در ارتش و همچنین قابلیت‌ها، فرصت‌ها و آسیب‌ها و ویرانی‌های احتمالی آن‌ها در هنگام بی‌ثباتی مورد بحث قرار می‌گیرد. پژوهش حاضر به پتانسیل فعلی و آینده برای توسعه الگوریتم‌های هوش مصنوعی، به ویژه در کاربردهای نظامی می‌پردازد. بیشتر بحث بر روی هفت الگوی هوش مصنوعی، استفاده و اجرای الگوریتم‌های هوش مصنوعی در ارتش، تشخیص اشیاء، تدارکات نظامی و ربات‌ها، بی‌ثباتی جهانی ناشی از استفاده از هوش مصنوعی و خطرات هسته‌ای متمرکز بود. این پژوهش همچنین به پتانسیل فعلی و آینده برای توسعه الگوریتم‌های هوش مصنوعی، به ویژه در کاربردهای نظامی می‌پردازد.

واژگان کلیدی: نیروهای مسلح، هوش مصنوعی، فرصت، آسیب.

دریافت مقاله: ۱۴۰۲/۰۶/۱۷ – بازنگری مقاله: ۱۴۰۲/۰۸/۰۸ – پذیرش مقاله: ۱۴۰۲/۰۹/۱۴

مقاله حاضر در نشریه International Journal of Intelligent Systems در سال ۲۰۲۳ میلادی منتشر شده است.

ارجاع:
بن راشد، ادیب؛ کاسیک، اشفاکول کریم؛ ثانی، احمدالحسن؛ باپی، مهدی حسن؛ (۱۴۰۲)، هوش مصنوعی در نیروهای مسلح: مروری بر قابلیت‌ها، کاربردها و چالش‌ها، ترجمه یاسر شاکری؛ تمدن حقوقی، شماره ۱۸، ویژه‌نامه هوش مصنوعی.

Copyrights:
Copyright for this article is retained by the author (s) , with publication rights granted to Legal Civilization. This is an open-access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4. 0) , which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

CC BY-NC-SA

پیشگفتار مترجم

با پیشرفت روزافزون فناوری‌های نوین در چند دهه گشته، امنیت کشورها نیز دارای ابعاد پیچیده‌تری شده است و این حوزه از تغییر و تحولات جهانی بی‌نصیب نمانده است. این فناوری‌ها به‌عنوان زیرساخت‌هایی که کار مدیریت، برنامه‌ریزی و خدمت‌دهی در زندگی روزانه مردم را بر عهده دارند، بسترهای طمع و وسوسه طرف‌های منازعه را برای تخریب اراده طرف مقابل و تحلیل اراده خود و ایجاد تفوق و سیطره فراهم آورده است. در عصر اطلاعات تقریبا تمامی امور زندگی انسان‌ها به نوعی با سیستم‌های دیجیتالی و رایانه‌ای گره خورده است. از این رو هرگونه ایجاد اختلال در این سیستم‌ها می‌تواند به نوعی در به هم زدن نظم اجتماعی و امنیت کشورها مؤثر باشد (ناظمی اردکانی و همکاران، ۱۳۹۵، ۱۴۵). هوش مصنوعی[1] کاربردهای مختلفی در حوزه‌های امنیتی و نظامی از جمع آوری داده و اطلاعات گرفته تا تجزیه و تحلیل داده‌ها، عملیات، فرماندهی و کنترل انواع وسایل نقلیه خودمختار و خودکار را شامل می‌گردد (نجات پور و همکاران، ۱۴۰۱، ۱۲).

هوش مصنوعی کاربردهای نظامی فراوانی دارد. از جمع آوری هوش مصنوعی، غربالگر و تجزیه و تحلیل اطلاعات نظامی تا ربات‌هایی که دارای قدرت پردازشی برای اجرای مأموریت‌ها با کلیک بر روی یک دکمه هستند. همان‌طور که ماشین‌های نیمه خودکار و کاملاً خودکار با هوش مصنوعی بیشتر مورد

1- Artificial Intelligence

اعتماد قرار می‌گیرند، به پهباد این استقلال را می‌دهد که تصمیم بگیرد چه موقع با هدفی درگیری پیدا کند و چه زمانی نادیده بگیرد و این حوزه هوش مصنوعی و کاربردهای نظامی آن هر روز واقعیت بیشتری پیدا می‌کند. ازجمله امکان استفاده از تراشه‌های رایانه‌ای که بر روی تسلیحات متصل شده و با استفاده از سیستم موقعیت یاب جهانی می‌تواند مختصات هدف را با درصد خطای بسیار کمی شناسایی و عملیات را انجام دهد (نجات پور و همکاران، ۱۴۰۱، ۲۱).

مقدمه

هوش مصنوعی با کمک داده‌ها، قدرت پردازش کامپیوتری و پیشرفت‌های یادگیری ماشینی به‌ویژه در دو دهه اخیر به‌تدریج در حال بهبود و تبدیل شدن به روشی کارآمدتر در سراسر جهان است. درنتیجه، هوش مصنوعی به طور فزاینده و مکرر در زندگی روزمره بخش‌های مختلف استفاده می‌شود. تعدادی از کاربردهای مختلف این فناوری عبارتند از: تشخیص گفتار، احراز هویت بیومتریک[۲]، نقشه‌برداری موبایل، سیستم‌های ناوبری، حمل و نقل و کنترل ترافیک، مدیریت، تولید، مدیریت زنجیره تأمین، جمع آوری داده‌ها و کنترل بازاریابی آنلاین هدفمند. بنابراین، جای تعجب نیست که هوش مصنوعی کاربردهای زیادی در بخش نظامی نیز در گستره وسیعی دارد (۱).

توانایی نظامی شاخص اندازه‌گیری فعلی هنگام تعیین قدرت[۳] یک کشور یا ملت است. وزارت دفاع

۲- زیست‌سنجی یا بیومتریک به نوع خاصی از روش‌های امنیتی گفته می‌شود که در آن برای کنترل دسترسی و برقراری امنیت از ویژگی‌های قابل اندازه‌گیری بدن انسان یا هر موجود زنده دیگر استفاده می‌شود. همانگونه که از واژه بیومتریک بر می‌آید در این روش با استفاده از الگوریتم‌های ریاضی از اندام‌ها برداشت‌های ثابت و یکتایی می‌شود که می‌توان از آن به‌عنوان یک گذرواژه یکسان و تقلیدناپذیر و گاه تغییرناپذیر استفاده کرد. به هر خصوصیت زیستی یا فیزیکی که با رایانه قابل اندازه‌گیری و بازشناسی خودکار باشد زیست‌سنجه گفته می‌شود.

۳- قدرت یا زور در اصطلاح علوم اجتماعی به معنی توانایی افراد یا گروه‌ها برای دست‌یابی به هدف‌ها یا پیش‌برد منافع خود از راه واداشتن دیگر افراد جامعه به انجام‌دادن کاری خلاف خواسته آن افراد است. قدرت یک مزیت اجتماعی است که در قشربندی مورد توجه قرار می‌گیرد. بسیاری از ستیزه‌ها در جامعه، مبارزه برای قدرت است؛ زیرا میزان توانایی یک فرد در دست‌یابی به قدرت بر این امر که تا چه اندازه می‌توانند خواست‌های خود را به زیان خواست‌های دیگران به مرحله اجرا درآورند، تأثیر می‌گذارد. قدرت می‌تواند از طریق عضویت در یک طبقه اجتماعی یا پذیرفتن یک نقش سیاسی به دست آید. فعالیت‌ها و ویژگی‌های فرد، ثروت فرد و عامل زور نیز می‌تواند در افزایش قدرت نقش داشته باشد.

ایالات متحده آمریکا[۴] صلاحیت یا توانایی نظامی را به‌عنوان توانایی دستیابی به یک هدف رزمی خاص تعریف می‌کند. به طور مستقیم یا غیرمستقیم تحت تأثیر نوسازی، ساختار، آمادگی و پایداری است. تجهیزات، زرادخانه[۵] و سطح پیچیدگی فنی تا حد زیادی درجه نوسازی را تعیین می‌کند (۲). اینترنت در حال جایگزینی روش مرسوم شروع جنگ است که از آغاز جنگ جهانی دوم[۶] برانگیخته شد. مطالعات نشان می‌دهد که حمله‌های هکری به شرکت‌های انتفاعی و مؤسسات دولتی در اطراف بخش هوش مصنوعی در حال حاضر رایج‌تر است. به گفته محققان، انتظار می‌رود سیستم‌های خودمختار مدرن و هوش مصنوعی در رویارویی‌های نظامی آینده بسیار مهم باشند (۳). تحقیق‌های علمی اخیر نشان می‌دهد که امروزه فناوری شبکه‌های عصبی تا چه اندازه در مبارزه سایبری رواج دارد. توسعه سیستم‌های حمل‌ونقل هوشمند[۷] یکی از نمونه‌های اصلی، همراه با پیش‌بینی و ارزیابی پدیده‌های زیست‌محیطی، جدا کردن توییت‌های اطلاعاتی از توئیت‌های غیراطلاعاتی و پیش‌بینی بازارهای متعارف[۸] پویا است. این نوع تقویت‌کننده به طرق مختلف به بخش نظامی کمک می‌کند و به‌عنوان بزرگ‌ترین سلاح در توسعه قابلیت‌های نظامی شناخته می‌شود (۴).

داده‌های مربوط به طیف گسترده‌ای از منابع و قابلیت‌ها که می‌توانند وظایف پیچیده‌ای از انواع مختلف را انجام دهند، مانند جمع‌آوری اطلاعات، حرکات، آتش سوزی‌های مستقیم و غیرمستقیم، زیرساخت‌ها و حمل و نقل باید در تصمیم گیری‌های نظامی در نظر گرفته شوند (۵). برای مثال، مؤلفه تصمیم‌گیری نیازمند یک چهارچوب یکپارچه است که می‌تواند فرایندهای لازم را انجام دهد، از گرفتن یک دوره عملیات سطح بالا[۹] تا اجرای یک تجزیه و تحلیل کامل فعالیت‌ها. یک امکان ایجاد رویکرد بر روی چندین روش هوش مصنوعی است، مانند زمان‌بندی خصمانه درهم و بسیاری دیگر به همین ترتیب جهان نظامی را در مسیرهای مختلف تقویت می‌کنند (۶).

۴- پنتاگون مرکز و مقر فرماندهی وزارت دفاع ایالات متحده آمریکا است.

۵- زرادخانه، به محل ساخت، تعمیر، ذخیره و نگهداری اسلحه و مهمات نظامی گفته می‌شود.

۶- جنگ جهانی دوم دومین جنگ جهانی بین سال‌های ۱۹۳۹ تا ۱۹۴۵ (نهم شهریور ۱۳۱۸ تا دهم شهریور ۱۳۲۴ خورشیدی) بود.

7- ITS
8- FX
9- CoA

این پژوهش همچنین چندین چالش و خطرات بالقوه مرتبط با استفاده از هوش مصنوعی در ارتش را شناسایی می‌کند، مانند احتمال نقص، هک و سایر اشکال حملات سایبری. پیامدهای اخلاقی و قانونی استفاده از هوش مصنوعی در ارتش به طور مفصل مورد بحث قرار می‌گیرد، به ویژه در رابطه با موضوعاتی مانند سلاح‌های خودمختار و احتمال آسیب ناخواسته. این مطالعه پتانسیل لازم برای اطلاع‌رسانی سیاست و تصمیم‌گیری در این زمینه را دارد، به ویژه در رابطه با موضوعاتی مانند نوسازی و آمادگی نظامی. یافته‌های پژوهش به طور بالقوه می‌تواند به توسعه دستورالعمل‌ها و مقررات برای استفاده مسئولانه از هوش مصنوعی در تنظیمات نظامی کمک کند.

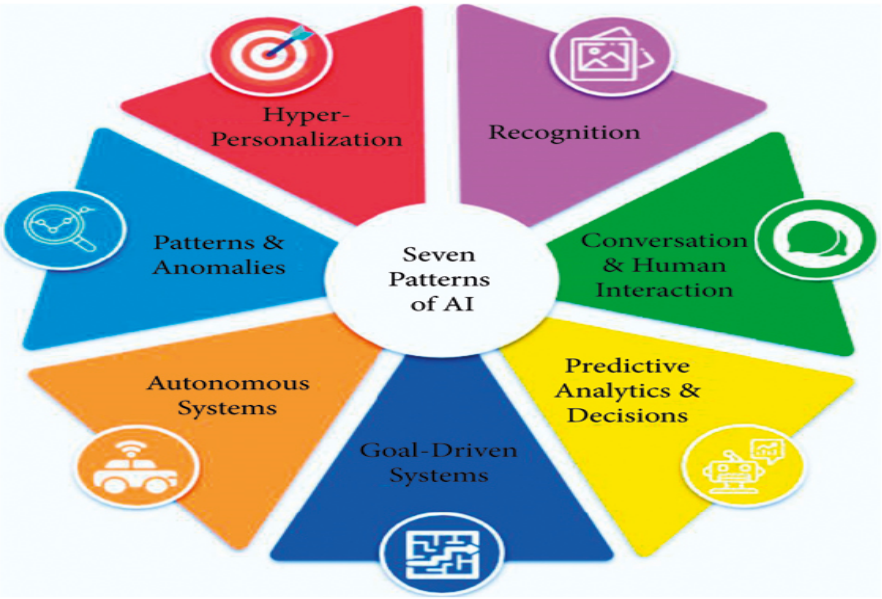
۱- هفت الگوی هوش مصنوعی[۱۰]

کاربردهای زیادی برای هوش مصنوعی وجود دارد، ازجمله ربات‌های چت، پهپادهای خودکار، تشخیص چهره[۱۱]، دستیاران مجازی، اتوماسیون شناختی، تشخیص تقلب، وسایل نقلیه خودران و برنامه‌های کاربردی برای تجزیه و تحلیل پیش‌بینی‌کننده. با این حال، صرفنظر از نحوه استفاده از هوش مصنوعی، هر یک از این برنامه‌ها دارای ویژگی‌های مشترک هستند. به رغم تنوع برنامه‌ها، افرادی که صدها یا حتی هزاران پروژه هوش مصنوعی ایجاد کرده‌اند می‌دانند که هر مورد استفاده از هوش مصنوعی در یک یا چند دسته از هفت دسته قرار می‌گیرد.

هفت الگوی هوش مصنوعی عبارتند از: سیستم‌های هدف‌محور، سیستم‌های خودمختار، تعاملات مکالمه انسانی، تجزیه و تحلیل پیش‌بینی‌کننده، فراشخصی‌سازی و پشتیبانی تصمیم‌گیری. این هفت الگوی هوش مصنوعی در سال‌های اخیر انقلابی در عملیات نظامی ایجاد کرده‌اند و قابلیت‌ها و برنامه‌های جدیدی را برای کارهایی مانند تشخیص اشیاء، پشتیبانی تصمیم‌گیری و تعاملات مکالمه ارائه می‌کنند. هر رویکرد شخصی به هوش مصنوعی نیاز به برنامه نویسی و طراحی دارد، زیرا صرفنظر از این که این روندها و نوآوری‌های فوق چگونه ترکیب شده‌اند، همه آن‌ها از اصول مشابهی پیروی می‌کنند. سپس، این هفت الگو به تنهایی یا در ترکیب‌های مختلف، بسته به موضوع خاصی که در آن هوش مصنوعی اعمال می‌شود، استفاده می‌شوند (۲۲).

10- Seven Patterns of AI

۱۱- سیستم تشخیص چهره یک تکنولوژی توانا در شناسایی و تأیید یک فرد از یک عکس دیجیتالی یا ویدئو می‌باشد. سیستم تشخیص چهره، سیستمی است که بر اساس تکنولوژی هوش مصنوعی و الگوریتم‌های یادگیری عمیق قادر به شناسایی چهره افراد با دقت بالا می‌باشد.



۱-۱- شخصی‌سازی بیش از حد[۱۲]

الگوی فراشخصی‌سازی راهی برای استفاده از یادگیری ماشینی برای ایجاد یک نمایه فردی و سپس یادگیری آن نمایه و تطبیق آن با گذشت زمان برای اهداف مختلف در پردازش، مانند نمایش محتوای مرتبط، توصیه محصولات مناسب و ارائه توصیه‌های شخصی است. هدف اصلی فراشخصی سازی، رفتار با هر فرد به صورت جداگانه است. چهار جزء یک طرح فراشخصی‌سازی عبارتند از: تصمیم گیری، بنیاد داده، طراحی و انتشار. بنیاد داده مهم‌ترین مؤلفه است زیرا رویکرد بیش سفارشی‌سازی به بازخورد مشتری برای ارائه تجربیات بستگی دارد، حتی اگر این مؤلفه‌ها مهم باشند. رویکرد فراشخصی‌سازی به ایجاد پایگاه داده مشتری کمک می‌کند. این امکان ارائه تجربیات فوق شخصی را در آینده فراهم می‌کند (۲۳).

پیاده‌سازی استراتژی‌های فراشخصی‌سازی می‌تواند توانایی تماس با مشتری و مشارکت مشتری را در صورت نیاز افزایش دهد. برای افزایش تعداد مشتریانی که می‌توانند تجارب بسیار سفارشی شده را دریافت کنند، درک تأثیر، اوج و محدودیت این تکنیک‌ها و بهترین لحظه برای اجرای یک تکنیک جدید ضروری است (۲۴). علاوه بر این، به جای ترکیب این دو، بیشتر تحقیقات بر روی ویترین فروشگاه‌های سنتی یا

12- Hyperpersonalization

تجارت الکترونیک متمرکز است. این ارزیابی تجربه مشتری با کمک فراشخصی‌سازی تقریباً شبیه به تجربه نظامی است. تیم‌های نظامی می‌توانند بهترین استراتژی را درک کنند و از طریق فراشخصی‌سازی مؤثرتر خواهند بود. این امر آن‌ها را در مورد آنچه که کارایی و کارگروهی آن‌ها را بیشتر از بسیاری از گزینه‌های موجود از طریق تجزیه و تحلیل ماشین افزایش می‌دهد، روشن می‌کند. گفته می‌شود که داده‌های بزرگ و فراشخصی‌سازی در ساخت استراتژی هنر نظامی جنگ است. در حال حاضر تقویت هوش مصنوعی با فراشخصی‌سازی آماده است تا اروپا و ایالات متحده آمریکا را در اختیار بگیرد. بخش تدارکات بخش نظامی در سراسر جهان بیشترین سود را از فراشخصی‌سازی می‌برد (۲۵).

مؤلفه تصمیم‌گیری الگوی فراشخصی‌سازی به تنهایی نقش بزرگی در قابلیت‌های نظامی ایفاء می‌کند. این جزء به ویژه در وسایل نقلیه هوایی بدون سرنشین (پهپادها[۱۳]) که معمولاً به‌عنوان هواپیماهای بدون سرنشین شناخته می‌شوند، ارزشمند است. پهپادها به طیف وسیعی از حسگرها، دوربین‌ها و سایر ابزارهای جمع آوری داده مجهز هستند که به آن‌ها اجازه می‌دهد تا حجم زیادی از داده‌ها را در مورد محیط و اهداف بالقوه جمع آوری کنند. مؤلفه تصمیم‌گیری فراشخصی‌سازی می‌تواند برای تجزیه و تحلیل این داده‌ها در زمان واقعی مورد استفاده قرار گیرد، بینش‌های عملی را در مورد فرماندهان نظامی ارائه می‌دهد و به آن‌ها اجازه می‌دهد تا تصمیمات آگاهانه‌تری بگیرند (۲۶).

به‌عنوان مثال، یک پهپاد مجهز به الگوریتم‌های فراشخصی‌سازی می‌تواند داده‌های یک میدان نبرد، مانند موقعیت رزمندگان دشمن، زمین و شرایط آب‌وهوایی را تجزیه و تحلیل کند تا بهترین اقدام را برای یک مأموریت خاص تعیین کند. این پهپاد می‌تواند بر اساس ویژگی‌های منحصر به فرد ماموریت و محیط، توصیه‌هایی را در زمان واقعی به فرماندهان ارائه دهد، مانند مکان استقرار نیروها یا اولویت‌بندی اهداف (۲۷). علاوه بر این، استفاده‌های دیگری از همین جزء در کاربردهای نظامی مانند تانک، خودرو، خودروهای نظامی و هواپیما نیز وجود دارد. به‌عنوان مثال، یک تانک مجهز به الگوریتم‌های

۱۳- پرنده هدایت‌پذیر از دور یا به اختصار پهپاد که به آن هواپیمای بدون سرنشین نیز می‌گویند، گونه‌ای هواگرد هدایت‌پذیر از راه دور بدون سرنشین با هدایت کنترلی است. پرواز پهپادها ممکن است تحت کنترل از راه‌دور توسط یک خلبان، یا با درجات مختلفی از خودمختاری، مانند کمک توسط خلبان خودکار، تا هواپیماهای کاملاً خودمختار که هیچ شرطی برای مداخله انسانی ندارند و بدون نیاز به هدایت انجام شود. پهپادها را می‌توان به روشی دیگر هدایت کرد. به این شکل که از قبل نقاطی برای آن‌ها انتخاب کرد و پهپاد روی این نقاط حرکت می‌کند و عملیات انجام می‌دهد.

فراشخصی‌سازی می‌تواند داده‌های حسگرها و دوربین‌های خود را تجزیه و تحلیل کند تا بهترین تصمیم را برای انتخاب آسان‌ترین مسیر برای رسیدن به یک مقصد خاص یا بهترین تاکتیک برای استفاده در یک موقعیت خاص اتخاذ کند.

یکی از نمونه‌های نوآوری اخیر در فراشخصی‌سازی برای تصمیم‌گیری نظامی، استفاده از شبکه‌های عصبی برای تجزیه و تحلیل داده‌های پهپاد است. در یک مطالعه اخیر، محققان از یک شبکه عصبی برای تجزیه و تحلیل داده‌های یک پهپاد در حال پرواز بر فراز یک زمین آموزشی نظامی، شناسایی اهداف بالقوه و ارائه توصیه‌های بلادرنگ به فرماندهان نظامی استفاده کردند. شبکه عصبی توانست اهداف را با دقت بالایی تعیین کند و کارایی کلی ماموریت را بهبود بخشد (۲۸).

به‌عنوان مثال، شبکه‌های متخاصم مولد[۱۴]، مدل‌های شبکه عصبی برای رسانه‌های معمولی تقویت شده با هوش مصنوعی هستند که از زمان معرفی فراشخصی سازی، توانایی ترکیب فراواقعی محتوای دیجیتالی محیط کار مدرن را به دست آورده‌اند. در این مدل یادگیری ماشینی، دو شبکه عصبی برای پیش‌بینی دقیق‌تر با هم رقابت می‌کنند. به‌عنوان مثال می‌توان به ایجاد عکس‌های واقع گرایانه، شبیه‌سازی صدا، انیمیشن چهره و ترجمه تصویر از یک فرمت به فرمت دیگر اشاره کرد. بنابراین، به کارگیری این تکنیک در جنگ نظامی به آن‌ها امکان می‌دهد از طریق ارزیابی داده‌ها بهترین پیش‌بینی را بدانند و استراتژی بهتری را تعیین کنند.

یک تکنیک جدید تصویربرداری مغز با کمک هوش مصنوعی (طیف‌سنجی عملکردی نزدیک به مادون قرمز) [۱۵]، می‌تواند تغییرات غلظت هموگلوبین قشر مغز در طول زمان را بدون ایجاد مزاحم اندازه‌گیری کند. در اینجا، نور نزدیک به مادون قرمز در پردازش به سطح جمجمه بدن هدایت می‌شود و در درجه اول توسط دو نوع هموگلوبین همراه با انتشار آن در داخل قشر مغز[۱۶] جذب می‌شود که هموگلوبین اکسیژن[۱۷] و هموگلوبین بدون اکسیژن[۱۸] هستند. با مشاهده مداوم تضعیف نور، طیف‌سنجی عملکردی نزدیک به مادون قرمز ممکن است نوسانات غلظت قشر هموگلوبین اکسیژن و هموگلوبین بدون اکسیژن را بازسازی و ایجاد کند. فعالیت عصبی محلی را می‌توان از آنجا استنباط کرد. اساس

14- GAN
15- fNIRS
16- HbR
17- HbO
18- HbO

فیزیولوژیکی تقریباً مشابه سایر روش‌های تصویربرداری است، مانند تصویربرداری رزونانس مغناطیسی عملکردی[۱۹]. با این حال، به دلیل هزینه بالا، انعطاف‌پذیری و مزایای قابل حمل بودن، بهتر است در کنار تخت یا در محیط‌های بالینی چالش برانگیز استفاده شود. اگر بتوان هزینه را به حداقل رساند، استفاده از این سیستم در ارتش از منظر تصویربرداری بهتر از تیم دشمن، دقیق‌تر خواهد بود و بر عامل تعیین‌کننده درگیر شدن یا عدم درگیری بسیار مؤثر خواهد بود (۲۵-۲۶-۲۷).

برای آموزش یک مدل مولد با شبکه‌های متخاصم مولد، کار به‌عنوان یک مسئله یادگیری نظارت شده با دو مدل فرعی در نظر گرفته می‌شود: مدل مولد، که همه برای ایجاد نمونه‌های جدید آموزش می‌دهند و مدل تفکیک‌کننده که سعی می‌کند نمونه‌ها را به‌عنوان واقعی از دامنه طبقه‌بندی کند.

۱-۲- الگوشناسی[۲۰]

تشخیص الگو[۲۱] یک روش محاسباتی قدرتمند برای ارزیابی عینی داده‌های بصری است. به طور خلاصه، یادگیری ماشینی نظارت شده یک استراتژی متمایز یادگیری ماشینی است که در آن الگوریتم به دنبال الگوهای مهمی است که پس از آموزش بر روی نمونه‌ها به چند گروه تقسیم می‌شوند. از سوی دیگر، فرایند یادگیری بدون نظارت، تکنیکی است که در یادگیری ماشین و تقویت هوش مصنوعی استفاده می‌شود که در آن رایانه انواع جدیدی از الگوها را بدون تکیه بر نمونه‌هایی از آموزش یا عملیات قبلی می‌آموزد. به طور معمول، با اعمال مجموعه‌ای از قوانین از پیش تعریف شده و از پیش تعیین شده انجام می‌شود. خوشه‌بندی تکنیک‌های یادگیری تشخیص الگوی بدون نظارت، یک مجموعه داده را براساس معیارهای عملیات از پیش تعیین‌شده به گروه‌های مختلف تقسیم می‌کند و در نهایت یک خوشه یا چند خوشه ایجاد می‌کند (۲۹).

روابط عمومی نسبت به سایر فرایندها مزایای زیادی دارد. در مقایسه با راه‌اندازی پردازش دستی تصویر، استفاده از تصاویر کامل فرایند تشخیص الگو برای شناسایی کاشی‌های تصویر در یک شبکه بدون هیچ مرحله شناسایی منطقه قبلی بسیار سودمندتر است. می‌توان آن را با الگوریتم‌های تقسیم‌بندی برای بهینه‌سازی مزایای هر دو استراتژی استفاده کرد. به معنای محدود، مانند ارزیابی ماتریس‌های سردرگمی در آزمایش‌های طبقه‌بندی است. داده‌های کمی تولید شده توسط این تکنیک‌های روابط عمومی با داده‌های تولید شده

19- fMRI
20- Pattern Recognition
21- PR

توسط الگوریتم‌های تقسیم‌بندی که بهتر، سودمندتر و کارآمدتر هستند، متفاوت است. برخلاف الگوریتم تقسیم‌بندی، روابط عمومی می‌تواند منجر به یافته‌های تجربی کیفی بهتری شود، مانند شناسایی «بازدیدها» روی صفحه (۳۰). ازآنجایی که از فرضیاتی مبنی بر ماهیت یا وجود تغییرات مورفولوژیکی در آزمایش تصویربرداری خالی است، یک آزمایش تصویربرداری اکتشافی مناسب است. استفاده از روابط عمومی براساس این مزایا در حال حاضر در تجارت و سایر صنایع رواج یافته است.

به همین ترتیب، در امتیازات صنعتی، ارتش نیز با فرایند تشخیص الگو تقویت می‌شود. فرماندهی نبرد مؤثر به فرماندهان نیاز دارد که نشانه‌های بصری مانند نقشه‌ها و پوشش‌ها را به‌سرعت بخوانند، بنابراین تشخیص الگو برای بهترین و کارآمدترین فرمان روی زمین بسیار مهم است. به افسران ارتش دستورالعمل‌ها و رویه‌ها برای فرماندهی کارآمد داده می‌شود، اما دستورالعمل‌های خاصی در مورد رمزگشایی و به کارگیری الگوهای میدان جنگ ارائه نمی‌شود. دانشی که فرماندهان در قالب الگوها جمع آوری کرده‌اند ممکن است علت تخصص آن‌ها باشد. براساس تحقیقات بیست سال گذشته، تشخیص الگوی ماهرانه نشانه‌ای از تخصص است. به‌عنوان مثال، برنامه نویسان خبره می‌توانند الگوهای مهم کد برنامه را به طور مؤثرتری نسبت به کدهایی که به قراردادهای برنامه نویسی تأیید شده پایبند نیستند، تکرار کنند [۳۱]. شطرنج بازان استاد می‌توانند مهره‌های شطرنج را بهتر به یاد بیاورند که روی صفحه شطرنج با الگوهای معنی دار چیده شوند تا مهره‌های شطرنج که به طور تصادفی چیده شده‌اند (۳۲-۳۳). نشان داده شده است که افراد ماهر در خواندن نقشه‌های معماری، خواندن نمودارهای مدار و رمزگشایی تصاویر اشعه ایکس[۲۲] بهترین توانایی را برای تشخیص الگوهای مهم در آن زمینه‌ها دارند (۳۴-۳۵).

۱-۳- الگوی مکالمه[۲۳]

در طول سال‌ها، راه حل‌های پیشرفته مختلفی براساس یکی از کلی‌ترین الگوهای هوش مصنوعی مکالمه ایجاد شده است. محل کار مدرن قرن بیست و یکم مملو از ربات‌های اجتماعی[۲۴] و کمک‌های زنده با

۲۲- پرتو ایکس یا اشعه ایکس نوعی از تابش الکترومغناطیسی با طول موج حدود یکصدم تا ده نانومتر معادل با سی پتاهرتز تا سی اگزاهرتز و انرژی بین یکصد الکترون‌ولت تا یکصد کیلوالکترون‌ولت است.

23- Conversational Pattern

۲۴- یک ربات اجتماعی، یک ربات خودمختار است که با پیروی کردن از رفتارها و قوانینی که مربوط به نقشش است با انسان‌ها یا سایر واحدهای فیزیکی خودمختار تعامل و ارتباط برقرار می‌کند. بر اساس این تعریف ربات اجتماعی باید تجسم فیزیکی داشته باشد.

هوش مصنوعی است. در بسیاری از صنایع، ازجمله ارتش، اهمیت تعامل بین انسان و ربات‌ها به طور فزاینده‌ای آشکار می‌شود. با کمک فناوری هوش مصنوعی، این تعامل به‌عنوان الگوی مکالمه نامیده می‌شود. این به‌عنوان اشکال مکالمه‌ای از تعامل و اطلاعات پخش شده در رسانه‌های مختلف، ازجمله فرمت‌های صدا، متن و تصویر بین ماشین‌ها و انسان‌ها مشخص می‌شود. این تعامل بین انسان و ماشین و ارتباطات رفت و برگشتی آن‌ها را پوشش می‌دهد. هدف این الگو این است که این امکان را برای ماشین‌ها فراهم کند که با مردم به همان شیوه‌ای که مردم انجام می‌دهند، تعامل داشته باشند. در طول سال‌ها، یکی از پیشرفت‌های قابل توجه، توسعه عوامل مکالمه مبتنی بر الگوهای مکالمه، تشخیص گفتار، اشیاء و درک زبان طبیعی بوده است (۳۶).

زیرمجموعه‌ای از حوزه‌های بزرگ‌تر هوش مصنوعی و پردازش زبان طبیعی[۲۵] تفسیر زبان طبیعی[۲۶] است که اختراعی عمیق در بخش الگوهای محاوره‌ای هوش مصنوعی است. اکثر کاربران اینترنت احتمالاً ناآگاهانه با فناوری پردازش زبان طبیعی از طریق ابزارهای ترجمه ماشینی و موتورهای جست‌وجو و همچنین هوش مصنوعی با استفاده ناخواسته از منابع مالی و برنامه‌های بازی‌های ویدیویی مواجه شده‌اند (۳۶). برای ایجاد و توسعه نرم‌افزارهای مرتبط با زبان، پردازش زبان طبیعی، زیرشاخه‌ای از علوم رایانه، ساختار و عملکرد را بررسی می‌کند و استفاده از زبان را در مدل‌های محاسباتی براساس الگوهای مکالمه مرتب می‌کند. یکی از اولین ربات‌های گفت‌وگو الگوی مکالمه سنتی الیزا[۲۷] بود که در سال ۱۹۶۶ میلادی ایجاد شد. الیزا یک محیط گفتمانی ایجاد کرد که اساساً نیازی به تخصص دنیای واقعی از نرم افزار نداشت. ربات‌های آلیس[۲۸] یکی از مؤثرترین پیاده‌سازی‌های چت ربات از الگوهای مکالمه و موجودیت رایانه‌ای زبانی مصنوعی در اینترنت بود. در حال حاضر، موفقیت بزرگی در هوش مصنوعی به دست آورده است (۳۸).

عصر مدرن چند ربات چت را به ارمغان آورد که در بحث الگوهای مکالمه هوش مصنوعی مثال زدنی هستند. ویچت[۲۹] یکی از آن انقلاب‌های مدرن در ایجاد الگوی مکالمه است. ویچت یک سیستم

25- NLP
26- NLI
27- ELIZA
28- ALICE

۲۹- ویچت نام یک سرویس پیام‌رسانی چندمنظوره برای تلفن‌های همراه است که به دست تنسنت در چین ساخته شده است. اولین انتشار آن در ژانویه ۲۰۱۱ میلادی بوده است. این برنامه در اندروید، آی‌فون، بلک‌بری، ویندوز فون و سیستم عامل‌های موبایل در دسترس است.

پیام فوری اصلی در چند کشور تأثیرگذار و دیجیتال است. همراه با عملکردهای اساسی مانند چت، خدمات خاصی را نیز برای مصرف کنندگان خود ایجاد کرد (۴۰). سیستم و کاربر می‌توانند با استفاده از زبان طبیعی گفت‌وگو کنند. عوامل مکالمه یا ربات‌ها ظهور کرده‌اند و احتمالاً با رشد هوش مصنوعی تأثیر بیشتری خواهند گذاشت. هیچ مجموعه داده‌ای در ارتباطات نظامی به اندازه مجموعه داده‌های یافت شده با کمک الگوهای مکالمه دقیق نیست. به‌عنوان مثال، اشخاص نظامی برای انجام وظایف خود در یک مکان نامعلوم به اطلاعاتی در مورد محیط اطراف خود و دستورالعمل‌ها نیاز دارند. مطالعه روی الگوهای مکالمه برای ارتش بیشتر به ایجاد سیستم‌های مکالمه برای موقعیت‌های مشابه مربوط می‌شود. بسیاری از کشورها براساس این داده‌ها در سناریوهای نظامی با استفاده از الگوهای مکالمه پیشرفت‌هایی در این زمینه داشته‌اند. علاوه بر این، با استقرار یک عامل نظامی مکالمه، اشخاص نظامی در حین کار بر روی کارهای تکراری با تلاش و هزینه کمتر، پاسخ‌های سریع و مناسبی دریافت خواهند کرد (۴۱).

۱-۴- تجزیه و تحلیل پیش‌بینی‌کننده[۳۰]

تخمین زده شده که تا سال ۲۰۲۵ میلادی، قیمت نرم افزار برای اطلاعات تجاری و تجزیه و تحلیل داده‌ها تنها در ایالات متحده آمریکا ممکن است حداکثر به یکصدونودویک میلیارد دلار برسد (۴۲). شرکت‌های آمریکایی بیشتر روی این پول خرج می‌کنند زیرا یکی از هفت الگوی هوش مصنوعی، تحلیل پیش‌بینی‌کننده، طلوع جدیدی تضمین می‌کند. به دلیل توسعه گسترده در داده‌های دیجیتالی تولید شده توسط مصرف کنندگان و بخش خدمات ناشی از آن، اکنون بالاترین بخش از بازار نرم افزارهای تحلیل پیشگویانه را به دلیل ضرورت استخراج اطلاعات استراتژیک و حیاتی در اختیار دارد، سرمایه‌گذاران بیش از پیش بر روی این چشم انداز هوش مصنوعی تمرکز می‌کنند. . برای کسب و کارها، تجزیه و تحلیل رفتار مصرف‌کننده و توسعه استراتژی‌های بازاریابی خاص هوش مصنوعی تحلیلی پیش‌بینی شده ضروری‌تر از همیشه است. همچنین، اگر از فناوریاینترنت اشیاء[۳۱]، که یکی دیگر از نرم‌افزارهای تحلیلی پیش‌بینی‌کننده است، برای به دست آوردن بینش تعامل استفاده شود، افراد می‌توانند دوستی‌های پربار و پایدار ایجاد کنند.

هنگامی که صحبت از جمع آوری داده‌های میدان نبرد می‌شود، تیم‌های نظامی می‌توانند با استفاده از پهپادهای بدون سرنشین، دوربین‌ها و حسگرها به کمک اینترنت اشیاء، میدان نبرد را اسکن کرده و زیرنظر

30- Predictive Analytics
31- IoT

داشته باشند. این پهپادهای مسلح می‌توانند داده‌های بی‌درنگ را در اختیار مرکز فرماندهی قرار دهند، عکس‌های زنده بگیرند و موقعیت و زمین دشمن را ردیابی کنند. همین فناوری‌ها به آن‌ها در تعیین و شناسایی دشمنان کمک می‌کند. دشمنان می‌توانند با نشان‌های سرقت شده وارد تأسیسات نظامی شوند یا خود را غیرنظامی نشان دهند (۴۳).

حسگرهای اینترنت اشیاء ممکن است اثر انگشت[۳۲]، اسکن عنبیه[۳۳] و سایر داده‌های بیومتریک را برای شناسایی افراد و کسانی که ممکن است یک تهدید باشند جمع‌آوری کنند. پایگاه‌های نظامی می‌توانند از حسگرها و دستگاه‌های اینترنت اشیاء برای بهبود عملکرد، راحتی تجهیزات و خدمات خود استفاده کنند. کمک اینترنت اشیاء در تعیین و نظارت بر سلامت سربازان در حال حاضر در نیروهای نظامی هر کشور بسیار رایج است. حسگرهایی در داخل یونیفورم آن‌ها قرار داده شده است تا وضعیت جسمی و روانی سربازان را ردیابی یا به طور مرکزی نظارت کنند. ضربان قلب، دمای بدن، توزیع حرارتی و برخی از ویژگی‌های رفتاری مانند الگوهای گفتار همگی می‌توانند توسط حسگرها کنترل شوند. یک عملیات نظامی موفق به تحویل مؤثر پرسنل و مهمات و نگهداری معمول خودروهای نظامی بستگی دارد (۴۴).

حسگرها و تجزیه و تحلیل‌های متصل فناوری اینترنت اشیاء امکان ردیابی کالاها را از نقطه مبدا تا مکان‌هایی در میدان نبرد که به آن‌ها نیاز است، می‌دهد. جدای از آن، آن‌ها کاربردهای دیگری در بخش نظامی دارند. ارتش همیشه در خط مقدم فناوری پیشرفته بوده است. اینترنت یکی از مهم‌ترین برنامه‌های کاربردی

۳۲- اثر انگشت در انسان، اثری از سایش شیارهای پایانه انگشت است. با توجه به این که هیچ دو انسانی اثر انگشت مشابه ندارند، می‌توان از این اثر برای شناسایی افراد بهره‌برد. اثر انگشت برجستگی‌های بسیار ریز (قابل رؤیت با چشم غیرمسلح) است که در لایه اپیدرم پوست کف دست‌ها و پاها وجود دارد. به علت ترشحات چربی زیر پوست این آثار انگشت بر اجسام صاف قرار می‌گیرد که همچنین برای وضوح آن می‌توان از پودری استفاده کرد که جذب این چربی‌ها شده و آن‌ها را به صورت واضح نمایان سازد. اثر انگشت افراد منحصربه‌فرد است و در طول عمر فرد تغییر نمی‌کند، بنابراین می‌توان از آن به‌عنوان یک امضاء یا ابزار تشخیص هویت استفاده کرد. همچنین، اثر انگشت افرادی که قهوه می‌نوشند، افراد سیگاری و مصرف‌کنندگان مواد مخدر در علوم قانونی و با کمک روش نانو ذرات طلا قابل تشخیص و تمایز است.

۳۳- اسکنر عنبیه یک فناوری شناسایی بیومتریک است که برای تشخیص هویت افراد با استفاده از شناسایی الگوی عنبیه چشم استفاده می‌شود. این فناوری با کمک یک دوربین خاص، الگوی عنبیه را تصویربرداری و با استفاده از الگوریتم‌های پیچیده، هویت فرد را شناسایی می‌کند.

روزانه است که توسط یا با استفاده نظامی در ذهن ایجاد می‌شود. با این حال، ارتش تجزیه و تحلیل‌های پیش‌بینی را با سرعت کمتری نسبت به بقیه مشاغل و صنعت اجرا می‌کند. با این حال، ممکن است کاربردهای دیگری برای این فناوری وجود داشته باشد که آن‌ها ترجیح می‌دهند از آن استفاده نکنند. عملکرد اصلی تجزیه و تحلیل پیش‌بینی‌کننده، پیش‌بینی براساس گذشته است (۴۵). استفاده از یادگیری ماشین یا هوش مصنوعی همیشه ضروری نیست. در ابتدایی‌ترین شکل آن، تنها چیزی که لازم است کمی عقل سلیم است.

چه در میدان جنگ باشد و چه نباشد، ارتش از وسایل نقلیه مختلفی برای عملیات خود استفاده می‌کند که به شدت به تقویت هوش مصنوعی و مجموعه داده‌ها متکی هستند. این ممکن است آنقدرها هم که به نظر می‌رسد ساده نباشد زیرا تعمیر و نگهداری معمول به تنهایی ممکن است برای حفظ وضعیت آن‌ها در طول عملیات فعال کافی نباشد. به دلیل استفاده مکرر از وسایل نقلیه نظامی، قطعات ممکن است بدون هشدار شکسته شوند و اگر نرم افزار هوش مصنوعی با تعمیر و نگهداری منظم در نظر گرفته نشود، ممکن است دچار اختلال شود. ارتش می‌تواند با تجزیه و تحلیل پیش‌بینی‌کننده، نقص و خرابی خودرو را در طول عملیات کاهش دهد. منظور از تعمیر و نگهداری پیش‌بینی در اینجا است. وسایل نقلیه ممکن است با استفاده از روش‌های مختلف، داده‌ها را جمع‌آوری کنند (۴۶).

۱-۵- الگوی سیستم‌های هدف محور[۳۴]

یکی از الگوهای اصلی هوش مصنوعی «الگوی سیستم‌های هدف محور» از بین هفت الگوی هوش مصنوعی است. مانند سایرین، این نوع هوش مصنوعی برای رسیدگی به مجموعه‌ای از مسائل مشترک استفاده می‌شود که در غیر این صورت به توانایی شناختی انسان نیاز دارند. یافتن بهترین پاسخ برای یک موضوع چالشی است که ماشین‌ها باید در این الگوی خاص با آن مقابله کنند. مشکل می‌تواند پیمایش در پیچ و خم، ساده کردن زنجیره تأمین یا به حداقل رساندن زمان بیکاری و مسیرهای سفر باشد. صرفنظر از نیاز دقیق، قدرتی که ما به دنبال آن هستیم، کشف بزرگ‌ترین راه حل از طریق آزمون و خطا است، حتی اگر آشکار نباشد. مفهوم منحصر به فرد هوش مصنوعی، خودمختاری مبتنی بر هدف[۳۵] است که به عوامل خودمختار استقلال کامل می‌دهد. عامل به جای تشخیص تصادفی ناهنجاری‌ها، مشکلات را در چهارچوب اهداف و هدف فعلی خود جست‌وجو می‌کند. معماری چرخه یکپارچه فراشناختی کوتاه[۳۶]، که به‌عنوان چرخه‌های عمل-ادراک

34- Goal-Driven Systems Pattern
35- GDA
36- MIDCA

شناخته می‌شود، در هر دو سطح شناختی و فراشناختی رخ می‌دهد (۴۸).

به چند دلیل، فرایند مهندسی نیازمندی‌ها باید به صراحت اهداف را در هوش مصنوعی بیان کند. اهداف مبنایی را ارائه می‌دهند که با شناسایی شرایطی که از پیشنهاد آن‌ها پشتیبانی می‌کند، توجیهات پشت آن الزامات را برای مشتریان روشن می‌کند، تضادهای نیازمندی‌ها را شناسایی، در نهایت حل می‌کند، معیارهایی را برای کامل بودن مشخصات نیازمندی‌ها ارائه می‌کند و معمولاً به‌عنوان قابل اعتمادترین داده در مشخصات عمل می‌کند. بنابراین، واضح است که هدف اصلی این سیستم، عمل خود به خود با ظرفیت بیشتر در یک محیط پویا و مدیریت هر رویداد غیرمنتظره‌ای است که در میدان جنگ بسیار رایج است. این سیستم‌ها براساس الگوهای سیستم هدف‌محور کار را برای نیروهای مسلح آسان‌تر می‌کنند (۴۹).

روش «کسب دانش در مشخصات خودکار»[۳۷]، یکی از برجسته‌ترین نمونه‌های الگوهای سیستم هدف محور در حوزه معاصر هوش مصنوعی در دنیای مدرن است. تکنیک کسب دانش در مشخصات خودکار به توضیح کامل فرایند نیازمندی‌ها کمک می‌کند، از اهداف سطح بالایی که سیستم ترکیبی باید به آن دست یابد تا اقدامات، اشیاء و محدودیت‌هایی که جزء نرم افزار باید به آن‌ها پایبند باشد. این روشی برای مهندسی نیازمندی‌ها است که بر دریافت نیازمندی‌های نرم‌افزاری هدف‌گرا تمرکز دارد. یک سیستم ترکیبی شامل برنامه مورد نظر و محیط اطراف آن در این زمینه است. بنابراین، برای دید بهتر از محیط میدان جنگ یا درک مناطق مهاجمان، این کمک بزرگی است. نسبت به سایر برنامه‌های معمولی در ارتش، تصویربرداری بهتری از رویکرد دشمن ارائه می‌دهد. حتی می‌تواند اطلاعات را در میان تعداد زیادی از تیم‌های مختلف به اشتراک بگذارد. این تکنیک شامل زبانی برای مشخصات آن است تا رویه و اطلاعات سطح بالایی را که در اجرای مشاوره محلی رویه ارائه می‌شود، توضیح دهد (۵۰).

هوش مصنوعی توزیع شده[۳۸] برای به تصویر کشیدن یک محیط مشترک، شبیه به کسب دانش در مشخصات خودکار، متشکل از گروه‌هایی از عوامل مرتبط و شرایط رفتاری استفاده شده است. اثربخشی پردازش فهرست[۳۹] از نظر اجرای مکان و زمان هنگام تلاش برای عملکرد به‌عنوان یک سیستم خودمختار هدف گرا هنوز مورد بحث است (۵۱). صنایع و کسب‌وکارها مشتاقانه منتظر هستند تا با کمک این نرم‌افزار الگوی سیستم هدف‌محور، تأثیری سریع داشته باشند. در بخش نظامی، سیستم الگوی هدف

37- KAOS
38- DAI
39- LISP

محور با کمک هوش مصنوعی[۴۰] برای جمع‌آوری، بایگانی، بازیابی، تجزیه و تحلیل و تجسم داده‌های مکانی به منظور افزایش تصمیم‌گیری از منظر اهداف میدان جنگ استفاده شده است.

یادگیری تقویتی یکی از هیجان انگیزترین اما کم استفاده‌ترین انواع یادگیری ماشینی است. با این حال، ارتش مدت‌ها است که از این تکنیک استفاده می‌کند. یک رویکرد مفید برای حل مسئله برای آموزش سیستم‌های خودمختار برای انجام وظایف نظامی چالش برانگیز، یادگیری تقویتی است. یادگیری تقویتی سعی می‌کند از طریق آزمون و خطا یاد بگیرد، با استفاده از بازخورد محیطی و اهداف کلی برای تکرار به سمت موفقیت، برخلاف رویکردهای یادگیری نظارت شده، که در آن ماشین‌ها با آموزش توسط انسان‌ها با داده‌های دارای برچسب خوب، یا رویکردهای یادگیری بدون نظارت، یاد می‌گیرند. ماشین‌ها سعی می‌کنند از طریق کشف خوشه‌های اطلاعات و گروه بندی‌های دیگر یاد بگیرند (۵۲). بدون هوش مصنوعی، کسب‌وکارها برای توسعه برنامه‌ها و سیستم‌های مبتنی بر قوانین که به نرم‌افزار و سخت‌افزار در مورد نحوه عملکرد آموزش می‌دهند، به افراد متکی هستند. اگرچه سیاست‌ها و رویه‌ها می‌توانند شکننده و محدودکننده باشند، اما می‌توانند در مدیریت امور مالی، پرسنل، زمان و سایر منابع مفید باشند. سیستم‌ها فقط به اندازه قوانینی که انسان‌ها طراحی می‌کنند قوی هستند. در عوض، آنچه سیستم را به کار می‌اندازد، هوش انسانی است که در قوانین گنجانده شده است.

۱-۶- الگوی سیستم‌های خودمختار[۴۱]

هوش خودمختار یا الگوی سیستم خودمختار، پیچیده‌ترین نوع هوش مصنوعی است که در آن رویه‌ها برای تولید هوشمندی خودکار می‌شوند که رایانه‌ها، ربات‌ها و سیستم‌ها را قادر می‌سازد مستقل از تعامل انسانی رفتار کنند. این کلاس هوش مصنوعی ممکن است بیشترین استفاده را در بخش نظامی در سراسر جهان داشته باشد. سیستم‌های خودمختار قادر به انجام یک کار، دستیابی به یک هدف یا تعامل با محیط اطراف خود با دخالت اندک انسان هستند. این سیستم‌ها همچنین باید بتوانند رویدادها را پیش‌بینی کنند، برنامه‌ریزی کنند و از محیط اطراف خود آگاه باشند، که دلیل استفاده از آن‌ها برای تحقق اهداف و مقاصد نظامی منطقی‌تر است. این هم سخت افزار فیزیکی و هم سیستم‌های نرم افزاری مستقل را پوشش می‌دهد. کاهش یا لغو کار انسانی هدف اصلی الگوی نظام خودمختار است. کاربران باید اطمینان حاصل

40- DAI
41- Autonomous Systems Pattern

کنند که وقتی یک انسان از معادله حذف می‌شود، سیستم خودمختار تا حد امکان در سطح انسانی عمل می‌کند. درنتیجه، واضح است که چرا این یکی از الگوهای پیچیده‌تر برای اعمال است. ازآنجایی که سیستم‌های خودمختار برای کاهش نیاز به کار انسانی طراحی شده‌اند، باید قابل اعتماد، سازگار و دارای کالیبر فوق‌العاده بالا باشند (۵۳).

یکی از مهم‌ترین کاربردهای هوش مصنوعی در سیستم‌های خودمختار بدون سرنشین باهوش است. توسعه چنین سیستم‌هایی به طور قابل توجهی باعث پیشرفت در فناوری هوش مصنوعی می‌شود. ماشین‌های هوشمند طراحی شده توسط انسان که می‌توانند با استفاده از فناوری پیشرفته برای انجام وظایف یا مدیریت بدون دخالت انسان حمل شوند، به‌عنوان سیستم‌های خودمختار بدون سرنشین[۴۲] شناخته می‌شوند (۵۴). این نمونه بارز الگوی سیستم خودمختار در دنیای مدرن است. همچنین، این سریع‌ترین الگوی پیشرفته و سرمایه‌گذاری شده هوش مصنوعی در بخش نظامی در سراسر جهان است.

پیشرفت‌ها در مطالعه سیستم‌های خودمختار بدون سرنشین منجر به توسعه کاربردهای چشمگیر متعددی شده است. جامعه تحقیقاتی از پیشرفت‌های غیرمنتظره در وسایل نقلیه زمینی و هوایی خودمختار برای مقاصد تجاری و امنیتی شگفت زده شده‌اند که حتی برخی از آن‌ها محقق شده‌اند. به‌عنوان مثال، گوگل وسیله نقلیه بدون راننده خود را برای خرید در کالیفرنیا در دسترس قرار داده است، حتی زمانی که محصولات تسلا[۴۳] و سایر تولیدکنندگان هنوز در حال آزمایش هستند. وسایل نقلیه هوایی بدون سرنشین (پهپاد) اغلب در میدان نبرد برای اهداف مختلف و در عملیات جست‌وجو و نجات استفاده می‌شوند. در این سیستم‌ها الگوریتم‌های هوش مصنوعی در مقیاس وسیع اعمال می‌شوند. برای کارهایی مانند برنامه‌ریزی مسیر، شناسایی سیگنال رادیویی، راداری، بینایی، پیاده‌سازی در مقیاس بزرگ مدل‌هایی مانند حافظه کوتاه مدت[۴۴] و توجه در شبکه داخلی توسعه یافته است (۲). این پیشرفت‌ها هم اقتصاد و هم زندگی را نجات می‌دهند.

تقریباً هر شرکتی در سرتاسر جهان جذب رونق پهپادها شده است، به ویژه در بخش نظامی. وسایل نقلیه هوایی بدون سرنشین نظامی (پهپاد) عموماً برای ارزیابی حمله، آسیب، نظارت و شناسایی نبرد،

42- UAS

۴۳- شرکت تسلا شرکت خودروسازی چندملیتی آمریکایی است که طراح، فناور و تولیدکننده خودروهای برقی و قطعات موردنیاز خودروها و قطارهای برقی می‌باشد.

44- LSTM

اقدامات متقابل الکترونیکی و ارزیابی آسیب استفاده می‌شوند. در مقایسه با همتایان نظامی خود، پهپادهای غیرنظامی را می‌توان برای طیف وسیعتری از مشاغل، ازجمله جست‌وجو و نجات بلایا، بازرسی راه آهن و خطوط انتقال، اکتشاف منابع، نقشه‌برداری کشاورزی، کنترل ترافیک، پیش‌بینی آب و هوا، عکاسی هوایی و نظارت بر محیط زیست استفاده کرد. با این حال، این حلقه‌های کنترل یک سیستم برای حرکت، رفتار مناسب و عملکرد در زمینه‌های مختلف دنیای واقعی کافی نیستند. [۵۶، ۵۷].

کوبات‌ها که به ربات‌های مشارکتی نیز معروف هستند، نوع دیگری از سیستم‌های مستقل هستند. در صورتی که بسیاری با این ایده آشنا نباشند، کوبات‌ها ماشین‌هایی هستند که در کنار و نزدیک افراد برای تکمیل کارها کار می‌کنند. از سوی دیگر، ربات‌های صنعتی از نظر فیزیکی از مردم جدا شده و در قفس قرار می‌گیرند. کوبات‌ها به گونه‌ای طراحی شده‌اند که حتی در زمانی که نزدیک هستند، مستقل از انسان عمل کنند، حتی اگر می‌توانند در ظرفیت هوشی تقویت شده عمل کنند (۵۹). حتی اگر سیستم الگوهای خودمختار هوش مصنوعی بدون توجه به این که در مورد بخش نظامی یا صنعت و تجارت باشد، احتمالاً سخت‌ترین سیستم را ایجاد می‌کند، زمانی که با توسعه و ارتقای مناسب به خوبی انجام شود، ممکن است تأثیر قابل‌توجهی داشته باشد. هر اقدامی که ممکن است مستلزم استقلال باشد باید به دقت مورد بررسی قرار گیرد.

۱-۷- شناسایی الگوها و ناهنجاری ها[۴۵]

الگوها و ناهنجاری‌ها یکی از هفت الگوی هوش مصنوعی است که بیشتر در صنایع مختلف در سراسر جهان استفاده می‌شود و بخش نظامی نیز تفاوتی ندارد. تشخیص ناهنجاری برای هواپیماهای نظامی پیشرفته با کمک شبکه‌های عصبی تقویت شده با هوش مصنوعی و یادگیری ماشینی در حال حاضر بسیار رایج است. یادگیری ماشینی به ویژه در جابه‌جایی سریع حجم عظیمی از داده‌ها برای شناسایی الگوها، ناهنجاری‌ها یا موارد پرت ماهر است. یکی از آن استفاده‌های هوش مصنوعی، که به «تطابق الگو» معروف است، به طور مکرر ظاهر می‌شود و با دلایل خوب، طیف وسیعی از کاربردها را دارد. هدف اصلی الگوها و الگوهای ناهنجاری هوش مصنوعی درک الگوهای موجود در داده‌ها و یافتن ارتباطات سطح بالاتر بین آن داده‌ها با استفاده از یادگیری ماشینی و سایر رویکردهای شناختی است. یافتن این که چه چیزی با داده‌های فعلی مطابقت دارد و چه چیزی نیازی به تعیین این که آیا یک نقطه داده معین با الگوی موجود مطابقت دارد یا یک نقطه پرت یا ناهنجاری است، نیاز دارد. راه‌های زیادی برای اعمال این طرح وجود

45- Identifying Patterns and Anomalies

دارد که یکی از محبوب‌ترین الگوها است (۶۰).

کاربردهای این الگو شامل تقلب و تشخیص ریسک برای تعیین این که آیا رویدادها غیرعادی هستند یا مطابق با انتظارات است. یافتن راه‌هایی برای داده‌ها و کمک به کاهش یا تصحیح خطای انسانی از کاربردهای دیگر است. متن پیشگو نمونه دیگری از این الگو است. می‌تواند به الگوهای گفتار و زبان نگاه کند تا کلماتی را برای نوشتن کارآمدتر پیشنهاد کند. این به نیروهای مسلح کمک زیادی می‌کند تا درک بهتری از میدان جنگ و این که محیط میدان نبرد ممکن است چگونه باشد. اکنون اکثر کشورها این تکنیک هوش مصنوعی را در بخش نظامی خود اجرا می‌کنند تا به سربازان و دانشجویان کارآموز خود آموزش تاکتیکی و استراتژیک بیاموزند. برخی از آن‌ها حتی در مورد تشخیص الگو و شناسایی ناهنجاری‌ها یادگیری متمایز دارند.

برای یافتن روندها و ناهنجاری‌ها، اجرای برنامه‌های کاربردی در ماشین‌های مجازی به جای دستگاه‌های مبتنی بر سخت‌افزار به‌سرعت در همه صنایع محبوبیت پیدا می‌کند. این باعث کاهش هزینه می‌شود و در عین حال دسترسی به سرویس را آسان‌تر می‌کند. بسیاری از قدرت‌های نظامی در سرتاسر جهان این تکنیک‌ها را برای بیش از یک دهه برای کسب امتیاز بهتر در منطقه جنگی پذیرفته‌اند و به‌کار گرفته‌اند. پذیرش محیط ابری[۴۶] در دانشگاه و صنعت در حال گسترش است زیرا خدمات ابر منبع باز را برای اجرای برنامه در محیط‌های تحقیق و تولید ارائه می‌دهد. نسل بعدی جنگجویان سایبری با استفاده از این پلتفرم ابری در کشورهای متعددی آموزش می‌بینند. حتی قدرتمندترین نیروهای نظامی در سرتاسر جهان مدل آموزشی قدیمی خود را برای این آموزش ساخته شده با هوش مصنوعی کنار گذاشته‌اند. یکی از مسائل مربوط به سیستم ابری، مکان‌یابی ناهنجاری‌ها و پیش‌بینی آن‌ها پیش از وقوع است. هر قدرت نظامی که بتواند با شناسایی الگوها و ناهنجاری‌ها به رفع این موضوع بپردازد، غیرقابل توقف خواهد بود (۶۱).

رویکرد سنتی شامل بررسی دستی برای ناهنجاری‌ها با نظارت بر ضربان قلب و سطوح آستانه است. استفاده از الگوریتم‌های یادگیری ماشین برای تشخیص مشکلات پیش از وقوع، موضوع تحقیقات اخیر بوده است. مجازی‌سازی تابع شبکه، فرایند مجازی‌سازی خدمات شبکه بر روی سخت افزار اختصاصی است. دانشگاهیان و متخصصان کسب و کار از نزدیک نحوه اعمال مجازی‌سازی عملکرد شبکه [۴۷] را مشاهده می‌کنند. ارائه دهندگان خدمات می‌توانند به راحتی خدمات شبکه را در نرم افزارهایی که

46- OpenStack
47- NFV

می‌توانند روی سرورهای معمولی با استفاده از مجازی‌سازی عملکرد شبکه کار کنند، ترکیب کنند. با کمک مجازی‌سازی عملکرد شبکه، سوئیچ‌ها و روترها می‌توانند به‌عنوان خدمات شبکه مجازی روی یک سرور واحد عمل کنند. نیروهای نظامی توانسته‌اند هزینه سخت افزار را کاهش دهند. در نتیجه، سایر صنایع نیز سود می‌برند (۶۲).

برخی از روش‌های پیش‌بینی، مانند میانگین متحرک یکپارچه اتورگرسیو[۴۸]، برای تولید پیش‌بینی به داده‌های تاریخی متکی هستند. با این حال، اگر داده‌ها فاقد الگوهای قابل تشخیص باشند و سطوح بالایی از نوسانات تصادفی را نشان دهند، این تاکتیک‌ها بی‌اثر هستند (۶۳). الگوریتم‌های یادگیری ماشین و یادگیری عمیق بسیار کارآمدتر و قابل اعتمادتر از رویکردهای قبلی هستند. در پیش‌بینی الگو در افق‌های زمانی کوتاه‌تر برتری دارد، اما در افق‌های طولانی‌تر شکست می‌خورد. پیش‌بینی یک سلاح عالی از منظر نظامی است. همه چیز در مورد دقت و سرعت است. هرچه این دو موضوع بهتر باشد، پیشرفته‌تر در نظر گرفته می‌شوند. در بسیاری از کشورها، میانگین متحرک یکپارچه اتورگرسیو به‌عنوان دقیق‌ترین و سریع‌ترین برنامه پیش‌بینی تلقی می‌شود و بخش نظامی تاکنون به اجرای آن ادامه می‌دهد. به‌عنوان مثال کشورهایی مانند چین هزینه‌های نظامی خود را براساس این برنامه پیش‌بینی می‌کنند.

تکنیک‌های متعددی برای مشاهده الگوها و موارد عجیب هوش مصنوعی در عمل وجود دارد. هوش مصنوعی برای مشاهده الگوها، ازجمله نظارت هوشمند، تشخیص عیوب یا خطاها و ایجاد تغییرات در صورت لزوم، کاربردهای امنیت سایبری و تحلیل بازار سهام استفاده می‌شود. با این حال، مهم است که در مورد داده‌هایی که این الگوی هوش مصنوعی بر روی آن‌ها آموزش داده شده است، احتیاط کنیم. پس از این که چند سال پیش مشخص شد که ابزار استخدام هوش مصنوعی مردان را برای مشاغل فنی ترجیح می‌دهد، آمازون[۴۹] مورد انتقاد قرار گرفت. مجموعه داده‌های مغرضانه می‌توانند به ویژه بر الگوها و ناهنجاری‌های هوش مصنوعی، مانند الگوهای بیش‌شخصی‌سازی و شناسایی تأثیر بگذارند. اگر از داده‌های سوءگیری برای آموزش سیستم‌ها استفاده شود، نباید تعجب آور باشد که سیستم‌های تشخیص الگو همان نوع سوءگیری را با داده‌های آموزشی نشان می‌دهند. مهم نیست که سیستم در بخش نظامی یا

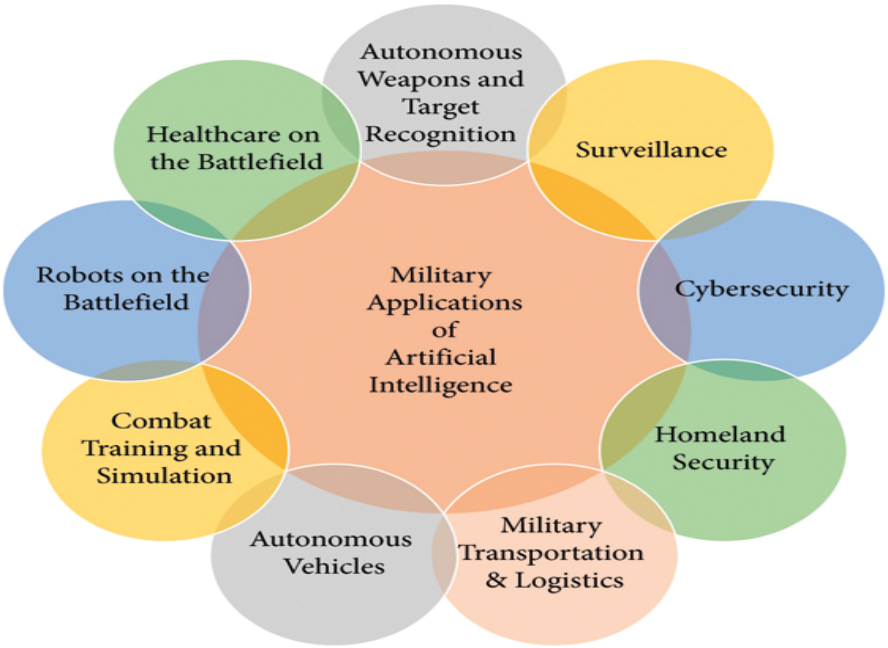
48- ARIMA

۴۹- آمازون شرکت تجارت الکترونیک چندملیتی آمریکایی است، که در سال ۱۹۹۴ میلادی توسط جف بیزوس، در شهر سیاتل واقع در ایالت واشینگتن تأسیس شد.

برای اهداف صنعتی استفاده می‌شود. اگر مجموعه داده‌های مغرضانه در طول شروع برنامه آموزشی نظامی رخ دهد، کل برنامه آموزشی و ایجاد استراتژی می‌تواند غیرقابل قبول باشد.

۲- کاربردهای هوش مصنوعی در بخش دفاعی[۵۰]

هوش مصنوعی در میدان‌های جنگ رواج بیشتری می‌یابد. مانند صنایع و مشاغل، ارتش نیز روز به روز شروع به تمرکز بیشتر بر هوش مصنوعی در هنگام پیشرفت و توسعه می‌کند. سیستم‌های نظامی مجهز به هوش مصنوعی می‌توانند حجم زیادی از داده‌ها را کارآمدتر از سیستم‌های معمولی پردازش کنند. علاوه بر این، هوش مصنوعی از طریق توانایی‌های محاسبه و تصمیم‌گیری ذاتی، خودکنترلی، خودتنظیمی و خودگردانی سیستم‌ها را افزایش می‌دهد. عملاً هر برنامه نظامی مستلزم هوش مصنوعی است و پیش‌بینی می‌شود که پشتیبانی نظامی رو به رشد از فناوری‌های خلاقانه و پیشرفته هوش مصنوعی باعث افزایش تقاضا برای سیستم‌های مبتنی بر هوش مصنوعی در ارتش شود (۶۵).



50- Applications of Artificial Intelligence in the Defense Sector

۲-۱- سلاح‌های خودمختار و شناسایی هدف[۵۱]

بحران موشکی کوبا در طول جنگ سرد[۵۲]، که تقریباً منجر به جنگ هسته‌ای شد، بهترین تصویر را از تأثیر و اهمیت استثنایی سیستم‌های تسلیحاتی خودمختار[۵۳] و شناسایی هدف ارائه می‌دهد (۶۶). این یک تکه فناوری (سیستم تسلیحات خودمختار نیروی دریایی ایالات متحده آمریکا[۵۴] و شناسایی هدف) می‌توانست از این سناریو جلوگیری کند. ایالات متحده آمریکا و اتحاد جماهیر شوروی[۵۵] پس از آموختن از نتیجه درگیری، مانند کاهش پیش‌بینی تصمیمات نظامی تحت کنترل هوش مصنوعی و دستیابی به دقت ماشین مانند، بیشتر بر بازدارندگی و ثبات در زمان جنگ تمرکز کردند. در این فناوری‌ها، سیستم حسگر خلبان

51- Autonomous Weapons and Target Recognition

۵۲- جنگ سرد به دوره‌ای از رقابت، تنش و کشمکش ژئوپلیتیکی بین اتحاد جماهیر شوروی و متحدانش (بلوک شرق) و ایالات متحده آمریکا و متحدانش (بلوک غرب) بعد از جنگ جهانی دوم گفته می‌شود. به‌طور کلی دوره زمانی جنگ سرد از ۱۹۴۷ میلادی و آغاز دکترین ترومن تا فروپاشی اتحاد جماهیر شوروی در ۱۹۹۱ میلادی در نظر گرفته می‌شود. به دلیل آن‌که در این دوران هرگز درگیری نظامی مستقیم میان نیروهای ایالات متحده آمریکا و اتحاد جماهیر شوروی به وجود نیامد اما گسترش قدرت نظامی و کشمکش‌های سیاسی منجر به جنگ‌های نیابتی و درگیری‌های مهم بین کشورهای پیرو و هم‌پیمانان این دو ابرقدرت شد، از واژه سرد برای توصیف این جنگ استفاده می‌شود. ریشه‌های جنگ سرد به پیروزی متفقین در جنگ جهانی دوم و پایان اتحاد موقت ایالات متحده آمریکا و اتحاد جماهیر شوروی علیه آلمان نازی و در ادامه درگیری ایدئولوژیک و ژئوپلتیک دو کشور برای گسترش نفوذ جهانی بازمی‌گردد. ترس از دکترین نابودی حتمی طرفین باعث شد تا هیچ‌یک از دو طرف حمله پیشگیرانه اتمی را آغاز نکنند. به غیر از مسابقه تسلیحات هسته‌ای و استقرارهای مرسوم نیروهای نظامی دو طرف از راه‌های دیگر همچون جنگ روانی، کارزارهای تبلیغات سیاسی، جاسوسی، تحریم‌های اقتصادی گسترده، رقابت در مسابقات ورزشی و فناوری مثل رقابت فضایی برای اثبات برتری خود استفاده کردند.

53- AWS

54- United States Navy (USN)

۵۵- اتحاد جماهیر شوروی سوسیالیستی یا به‌طور خلاصه شوروی یک حکومت سوسیالیستی فدرال بود که در سال ۱۹۲۲ میلادی به‌وجود آمد و در ۱۹۹۱ میلادی فرو پاشید. این حکومت اتحادیه‌ای متشکل از روسیه و چندین جمهوری دیگر در شمال اوراسیا بود که تحت حاکمیت یک نظام تک‌حزبی به نام حزب کمونیست شوروی بودند. پایتخت آن مسکو در جمهوری فدراتیو سوسیالیستی روسیه شوروی، بزرگ‌ترین جمهوری شوروی قرار داشت. از دیگر مراکز مهم این اتحادیه می‌توان به لنینگراد (روسیه شوروی)، کی‌یف (اوکراین شوروی)، مینسک (بلاروس شوروی)، تاشکند (ازبکستان شوروی) و آلماتی (قزاقستان شوروی) اشاره کرد. بیشتر اروپای شرقی، مناطقی از اروپای شمالی و تقریباً تمامی آسیای شمالی و مرکزی تحت حاکمیت این حکومت بودند. مناطق آب‌وهوایی زیادی ازجمله تونـدرایی، تایگـایی، استپی، بیابانی و کوهستانی شامل این کشور بود و جمعیت گوناگون آن در مجموع با عنوان «مردمان شوروی» شناخته می‌شدند.

هواپیمای بدون سرنشین برای شناسایی و پرتاب سلاح حتی ممکن است مانند سیستم حسگر خلبان در کابین خلبان یک هواپیمای مسکونی باشد (۷۱).

به عقیده برخی، بهترین سلاح‌های خودمختار با بیشترین ظرفیت برای شناسایی اهداف با دقت ماشین، سامانه موشکی پاتریوت، سیستم تسلیحاتی دریایی[۵۶] و چند مورد دیگر است (۸۴). با این حال، مؤلفه تشخیص این سیستم هنوز به فضای زیادی برای بهبود نیاز دارد. با این حال، به دلیل استفاده گسترده از هوش مصنوعی در بخش نظامی، یک مورد رو به افزایش وجود دارد. بیشتر چشم اندازهای سیستم‌های تسلیحاتی خودمختار مبتنی بر هوش مصنوعی خطرناک و تحت کنترل دولت آن‌ها در نظر گرفته می‌شوند. بسیاری از آن‌ها به‌عنوان دارای اهمیت عمومی شناخته می‌شوند. بیش از صد استدلال به نفع ممنوعیت سیستم‌های تسلیحاتی خودمختار خطرناک مبتنی بر هوش مصنوعی وجود دارد. با این حال، هیچ کشوری قصد ندارد استفاده از این فناوری قابل توجه را متوقف کند یا آن را کنار بگذارد. برعکس، به طور مداوم در حال توسعه و پیشرفت است. در آن صورت، سازمان‌های جهانی محدودیت‌های سیستم‌های تسلیحاتی خودمختار را تشدید کردند، زیرا نوآوری و پیشرفت را نمی‌توان متوقف کرد و آن‌ها این کار را انجام دادند تا قوانین را تا حد ممکن اخلاقی کنند. استانداردهای اخلاقی سیستم‌های تسلیحاتی خودمختار را برای سیستم تسلیحات خودمختار مرگبار[۵۷] ساختند (۸۵).

حال چرا این کدهای اخلاقی ضروری است؟ به‌عنوان مثال، پهپاد اسرائیلی هارپی یکی از کشنده‌ترین و پیچیده‌ترین سیستم‌های تسلیحاتی خودمختار خودران است که امروزه مورد استفاده قرار می‌گیرد. آن‌ها برای حرکت و تفکر در یک منطقه خاص برای اهداف مشخص آموزش دیده‌اند. این سیستم‌های تسلیحاتی خودمختار مبتنی بر هوش مصنوعی از کلاهک انفجاری قوی[۵۸] استفاده می‌کنند که در سناریوهای خاصی می‌تواند خطرناک باشد. اگر به جای حمله به دشمن، این ربات‌های هوش مصنوعی شروع به حمله به غیرنظامیان کنند یا نتوانند هدف دقیق را به دست آورند، چه؟ (۶۶).

با این حال، توسعه و استقرار سیستم‌های تسلیحاتی خودمختار در عملیات نظامی چندین نگرانی اخلاقی را ایجاد می‌کند. برخی از خطرات بالقوه سیستم‌های تسلیحاتی خودمختار شامل موارد زیر است: نقص- سیستم‌های تسلیحاتی خودمختار برای تصمیم‌گیری به الگوریتم‌های هوش مصنوعی متکی هستند و

56- AEGIS
57- LAWS
58- Fire and Forget

اگر نقصی وجود داشته باشد، سیستم ممکن است افراد یا گروه‌های اشتباهی را هدف قرار دهد. این می‌تواند منجر به تلفات ناخواسته و نقض حقوق بشر شود. عدم پاسخگویی- ازآنجایی که سیستم‌های تسلیحاتی خودمختار طوری طراحی شده است که بدون دخالت انسان عمل کند، تعیین مسئولیت برای هر گونه خطا یا تخلف در طول عملیات آن چالش برانگیز می‌شود. این عدم پاسخگویی می‌تواند منجر به مصونیت از مجازات برای افراد مسئول خطاها یا تخلفات شود. هک کردن- سیستم‌های تسلیحاتی خودمختار ممکن است هک شود و در برابر استفاده غیرمجاز آسیب پذیر شود. این می‌تواند منجر به استفاده از سیستم علیه کشوری شود که آن‌ها را ایجاد کرده است یا سایر اهداف ناخواسته. فقدان کنترل انسانی- سیستم‌های تسلیحاتی خودمختار برای کار کردن نیازی به مداخله انسانی ندارد و این نگرانی‌ها را در مورد از دست دادن کنترل انسانی بر نیروی نظامی افزایش می‌دهد. این عدم کنترل می‌تواند پیامدهای قابل توجهی برای اجرای جنگ داشته باشد.

۲-۲- نظارت[۵۹]

روز به روز، استفاده از هوش مصنوعی در بخش نظارت در حال بهبود است و احتمال استفاده از آن در هر صنعتی بیشتر می‌شود. بیش از بیست و سه هزار پتنت[۶۰] جدید مرتبط با هوش مصنوعی در سال ۲۰۰۸ میلادی وجود داشت. تا سال ۲۰۱۸ میلادی، حدود هفتادوهشت هزار نفر تحت نظارت با کمک هوش مصنوعی بودند (۸۶). بخش دفاعی به تنهایی سهم زیادی در به کارگیری و اجرای سیستم‌های نظارتی تقویت شده با هوش مصنوعی دارد. بسیاری از برنامه‌ها در حال حاضر در این بخش در سراسر جهان در حال اجرا هستند و احتمالاً به زودی برنامه‌های بیشتری رخ خواهند داد. انتظار می‌رود هر کشوری که این روند را دنبال نمی‌کند تحت سلطه قرار گیرد و از کیفیت سایر نیروهای نظامی که با کمک هوش مصنوعی از نظارت استفاده می‌کنند، پایین‌تر بماند. این نوآوری‌ها در این بخش سودمندتر هستند و قابلیت نظامی را پایدارتر و دقیق‌تر می‌کنند. به‌عنوان مثال، مکان مین‌های زیر آب یکی از حوزه‌های حیاتی

59- Surveillance

۶۰- سند ثبت اختراع، حق امتیاز یا اندیشه‌گواه یا پتنت حق انحصاری است که در قبال اختراع یا ایده ثبت شده به مخترع یا نماینده قانونی او اعطاء می‌شود. انحصار مجموعه‌ای از حقوق منحصر به فردی است که از طرف دولت‌ها برای مدتی معین در عوض تنظیم و افشاء عمومی جزئیات معین از یک روش، جریان عمل یا ترکیب خاصی از ماهیت که به‌عنوان اختراع شناخته می‌شود در اختیار شخص خاصی قرار می‌گیرد. به‌طوری‌که آن مفهوم، اختراعی جدید، مفید یا مورد استفاده صنعت شناخته شود.

تشخیص اشیاء در کاربردهای نظامی است که بر احساس امنیت برای غیرنظامیان و نظامیان تأثیر می‌گذارد.

بخش هوش مصنوعی روش‌های مختلفی را برای مکان‌یابی مشکلات دشواری که نیاز به عقل انسانی دارد ایجاد کرده است. برخی از این روش‌ها به بلوغ رسیده‌اند تا الگوریتم‌های دقیق بتوانند از آن‌ها پشتیبانی کنند. برخی از روش‌ها آنقدر معروف و گسترده شده‌اند که دیگر برای کمک به انسان‌ها در نظر گرفته نمی‌شوند. در عوض، هوش مصنوعی کار را با کیفیت و کارایی بسیار بهتر انجام می‌دهد (۸۷).

به لطف الگوریتم‌های پیشرفته هوش مصنوعی، انسان‌ها اکنون می‌توانند از قابلیت‌های جدیدی مانند رانندگی خودکار و تشخیص خودکار موقعیت‌های خطرناک بهره‌مند شوند. یادگیری عمیق[۶۱]، یک فناوری بسیار پیچیده که می‌تواند جایگزین الگوریتم‌های مرسوم برای افزایش تشخیص و تشخیص اشیاء بصری شود، یکی از این رویکردهای مبتنی بر هوش مصنوعی است. کارهای اخیر متعددی پیچیدگی‌های پیچیده مدل‌های یادگیری عمیق را بررسی کرده‌اند (۸۹). این تحقیق بر ترکیب روش‌های یادگیری عمیق برای تشخیص اشیاء و پردازش تصویر در سیستم‌های تشخیص و نظارت مستقل نصب شده در تقاطع‌های راه‌آهن با استفاده از ارائه‌هایی از حسگرها تمرکز دارد. در حال حاضر، بسیاری از گذرگاه‌های راه‌آهن از تدابیر امنیتی معمولی، ازجمله حسگرها، دوربین‌ها، علائم جاده‌ای، علائم راهنمایی و رانندگی و موانع فیزیکی استفاده می‌کنند تا از شرایط ناامن و مخاطره‌آمیز ناشی از دسترسی افراد به منطقه گذرگاه راه‌آهن در هنگام عبور قطار جلوگیری کنند (۹۰).

مطالعات و مقاله‌های تحقیقاتی متعددی بحث می‌کنند که چگونه فناوری نظارت مخابراتی مدرن می‌تواند ایمنی را در گذرگاه‌های راه آهن افزایش دهد. به‌عنوان مثال، سینگ برای هشدار دادن به رانندگان با استفاده از رابط انسان و ماشین[۶۲]، از طریق افکار و تئوری‌های خود، یک سیستم همکاری[۶۳] را برای گذرگاه‌های راه آهن پیشنهاد کرد که مبتنی بر فناوری‌های موجود مانند سیستم موقعیت‌یابی جهانی[۶۴] و ارتباط اختصاصی برد کوتاه[۶۵] می‌باشد زنگ تشخیص پلاک خودرو را با استفاده از یادگیری عمیق و مدل توجه بصری نشان می‌دهد. کیم برنامه‌های شبکه عصبی کانولوشنال عمیق[۶۶] را برای تشخیص پلاک‌ها مطالعه می‌کند (۹۰).

61- DL
62- HMI
63- ITS
64- GPS
65- DSRC
66- DCNN

با توجه به این فرایندها، شبکه‌ها را می‌توان به صورت ایستا با محدودیت‌های قابل توجهی حفظ کرد. شبکه‌های مورد استفاده برای نظارت نظامی و سایر اهدافی که به صورت ایستا توسط دستورات یا اسکریپت‌های ایستا اداره می‌شوند، مؤثرتر بوده و دارای منابع خودکار کمتری هستند. استفاده از شبکه‌های نرم افزاری تعریف شده برای بهبود مدیریت شبکه در هر نوع جنبه نظامی پیشنهاد شده است که اخیراً در تعداد زیادی از تحقیقات[۶۷] انجام شده است (۹۲). ارتباط داده‌ها و برآورد وضعیت هدف دو جزء اصلی یک برنامه کاربردی ردیابی هدف معمولی برای نظارت هستند. بنابراین، اتصال اندازه‌گیری به اندازه‌گیری، ارتباط اندازه‌گیری به مسیر، ارزیابی مسیر و ردیابی فرضیه‌های متعدد، بخش‌های اضافی ارتباط داده[۶۸] هستند. هر یک از این اجزا و اجزای فرعی این پتانسیل را دارد که به طور کامل یا جزئی توسط هوش مصنوعی در بخش نظامی انجام شود (۸۶).

۲-۳- امنیت سایبری[۶۹]

تحقیقات امنیت[۷۰] سایبری کل جهان را تحت تأثیر قرار داده است، درحالی‌که ایالات متحده آمریکا، چین، آلمان، هند، ژاپن، استرالیا و اکثر کشورهای اروپایی بیشترین پیشرفت را داشته‌اند. آن‌ها از فناوری

67- SDN
68- MHT
69- Cybersecurity

۷۰- امنیت دوری از هرگونه تهدید مقتدا و نیز آمادگی برای رویارویی با مقتدا است. مفهوم امنیت نسبی و دارای شدت و ضعف است، به این معنا که در برخی موقعیت‌ها (زمان و مکان‌های مختلف) در ذهن افراد ارتقاء یا کاهش می‌یابد. امنیت از ضروری‌ترین نیازهای یک جامعه است. مفهوم‌های مرتبط با امنیت در فارسی کلاسیک با واژه‌های زنهار و زینهاری ادا می‌شد. مفهوم امنیت از یک سو بسیط است بدین معنا که هر انسانی امنیت یا ناامنی را درک می‌کند؛ ولی از سوی دیگر پیچیده است و تعاریف متعدد و متنوعی از آن ارائه می‌شود. برای درک بهتر مفهوم امنیت، در مطالعات امنیتی تلاش می‌شود که این مفهوم را به اجزاء کوچک‌تر و قابل درک‌تری بشکنند. من جمله؛ تجزیه مفهوم امنیت به ارکان آن. ارکان امنیت عبارتند از: مرجع امنیت، تهدید امنیت، تولیدکننده امنیت، ابزار و روش تولید امنیت و غایت امنیت. مهم‌ترین رکن امنیت مرجع امنیت است. مرجع امنیت ناظر بر این سؤال اساسی است: که امنیت چه کسی؟ یا چه چیزی؟ قسمت دیگری از شکستن مفهوم امنیت، برای درک بهتر مفهوم امنیت شکستن این مفهوم به سطوح امنیت است. این سطوح عبارتند از امنیت جهانی، امنیت بین‌المللی، امنیت منطقه‌ای، امنیت ملی، امنیت داخلی و خارجی، امنیت عمومی، امنیت اجتماعی و امنیت فردی. ابعاد امنیت نیز تلاشی برای فهم بهتر مفهوم امنیت است. این ابعاد امروزه شامل نظامی، سیاسی، اقتصادی، فرهنگی، اجتماعی و زیست‌محیطی است.

هوش مصنوعی در قالب عوامل هوشمند برای دفاع در برابر سایر حملات سایبری و توقف حملات انکار سرویس توزیع شده[۷۱] استفاده می کنند (۵۶). همچنین، این چشم انداز تنها برای مشاغل و صنایع نیست. در بخش دفاعی بسیار بیشتر توسعه یافته و ارتقاء یافته است. استفاده پیشگامانه فرانک روزنبلت از شبکه‌های عصبی برای تشخیص الگو به دلیل کارایی آن مشهور است. می‌تواند به‌سرعت اطلاعات جدید را از داده‌های نظامی دریافت کند، با مشکلات چالش برانگیز مقابله کند و در برابر تعداد محدودی از حملات سایبری دشمن دفاع کند. برای شناسایی و جلوگیری از هرگونه نفوذ، شبکه‌های عصبی از نصب نرم افزار و سخت افزار پشتیبانی می کنند (۸۲).

در واقع، هوش مصنوعی راکد ماند و تنها به زیرمجموعه‌ای از حوزه‌های کاربردی خاص بخش دفاعی، مانند الگوریتم‌های پردازش داده، تبدیل شد. ارائه یک تجزیه و تحلیل کامل یا جزئی از همه انتخاب‌ها ممکن است امکان پذیر نباشد. اثربخشی تکنیک‌های هوش مصنوعی در یک ارزیابی نسبتاً سریع نشان داده شد. در عوض، مسیرها و معماری را به دسته‌های مختلف تقسیم کرد. قابلیت کشف در سطح جهانی برای شبکه‌های عصبی، سیستم‌های دانستن، عوامل هوشمند، جست‌وجو، یادگیری ماشین و سایر حوزه‌ها محدود است (۸۴).

پتانسیل هوش مصنوعی در امنیت سایبری بسیار زیاد و گسترده است. مهندسی اجتماعی با تأثیرگذاری بر رفتار افراد، از افراد برای دسترسی به یک سیستم استفاده می کند. درنتیجه، ضعیف‌ترین حلقه یک محیط امنیتی، ذهن انسان است که مهاجم به راحتی می‌تواند از آن سوءاستفاده کند. کشورهای مختلف نظامی از هوش مصنوعی برای افزایش امنیت و کارایی سیستم‌های خود برای جلوگیری از این امر استفاده می کنند. جنگ جهانی سوم یک حمله سایبری در نظر گرفته می‌شود، نه هر جنگ میدانی. این نشان می‌دهد که برای هر کشوری چقدر مهم است که امنیت سایبری خود را با کمک هوش مصنوعی بهبود بخشد. امنیت سیستم هر نظامی از هر کشوری را می‌توان با استفاده از سیستم‌های خبره، شبکه‌های عصبی و روش‌های دیگر افزایش داد. یک سیستم هوش مصنوعی خوب می‌تواند ماهیت حملات آتی را پیش‌بینی کند و با استفاده از سوابق حملات قبلی از آن‌ها جلوگیری کند. ممکن است رسیدن به درجه‌ای از امنیت در آینده امکان پذیر باشد و هک کردن را بسیار چالش برانگیز کند (۸۵).

71- DDoS

۲-۴- امنیت داخلی[۷۲]

اگرچه چندین آژانس غیرنظامی عموماً مسئول واکنش به فجایع داخلی مانند حملات تروریستی هستند، نیروهای مسلح ایالات متحده آمریکا[۷۳] همیشه در پر کردن شکاف‌ها در توانایی غیرنظامیان نقش داشته است. برای بهبود این گزینه، هوش مصنوعی به طور گسترده به کمک می‌آید. صدها کشور نرم افزاری با کمک هوش مصنوعی را ترجیح می‌دهند تا مناطقی را که بیشتر به حمایت نظامی نیاز دارند، منطقه‌بندی کنند. جمع آوری داده‌ها و تجزیه و تحلیل داده‌ها با کمک نرم افزار مناسب نقش مهمی در این مورد دارد. سه هدف مهم امنیت ملی را می‌توان با استفاده از هوش مصنوعی در بخش دفاع ملی در شش حوزه ماموریتی حیاتی امنیت داخلی شکست داد (۸۸).

رهبران امنیت داخلی و نیروهای مسلح ملی همه کشورها با کمک هوش مصنوعی شانس بی‌پایانی برای حمایت بهتر از جوامع خود و اداره سازمان‌های خود خواهند داشت. برخی از رقبای استراتژیک بزرگ در سراسر جهان هزینه‌های قابل توجهی را در زمینه هوش مصنوعی برای امنیت کشورهای خود انجام داده‌اند. به طور مشابه، وزارت دفاع ایالات متحده آمریکا میلیاردها دلار برای ایجاد و ترکیب هوش مصنوعی در سیستم‌های دفاعی برای ارتقای قابلیت‌های نظامی هزینه می‌کند. انواع هوش مصنوعی که وزارت دفاع ایالات متحده آمریکا به کار می‌برد، از خودکارسازی فرایندهای تجاری ساده و پیش‌بینی مشکلات مکانیکی در سیستم‌های تسلیحاتی تا انجام تحلیل‌های پیچیده برای حمایت از مأموریت خود در جنگ‌ها را شامل می‌شود.

ماموریت جنگی وزارت دفاع بسیاری از کشورها به چندین قابلیت هوش مصنوعی بستگی دارد که هنوز در حال توسعه است. مثال‌ها عبارتند از بهبود سیستم‌های نظامی، ارزیابی داده‌های اطلاعاتی و ارائه پیشنهادات در میدان نبرد (۸۶). صورت و راه رفتن انسان، ویژگی‌های بیومتریک اصلی و غالب هستند که می‌توانند در سیستم‌های نظارت بصری در صنعت امنیت داخلی مدرن مورد بهره‌برداری قرار گیرند. از طریق تشخیص حرکت، ردیابی و درک رفتار، یک سیستم نظارت بصری تک دوربینی برای شناسایی و

72- Homeland Security

۷۳- نیروهای مسلح ایالات متحده آمریکا، نیروهای نظامی کشور ایالات متحده آمریکا هستند که از شش شاخه اصلی؛ نیروی زمینی، نیروی دریایی، نیروی هوایی، نیروی فضایی، سپاه تفنگداران دریایی و گارد ساحلی تشکیل می‌شوند. نیروهای مسلح ایالات متحده آمریکا بزرگ‌ترین نیروی‌های نظامی در جهان می‌باشد. شکل‌گیری آن به جنگ‌های استقلال آمریکا از بریتانیای کبیر باز می‌گردد.

شناسایی افراد کافی است. با این حال، دوربین‌های متعدد مبتنی بر هوش مصنوعی هنگام در نظر گرفتن امنیت داخلی سودمندتر هستند.

اکثر تکنیک‌های تقسیم‌بندی در امنیت داخلی شامل اطلاعات مکانی یا زمانی در طول پردازش تصویر است. پرکاربردترین تکنیک‌ها به این شرح است: تفاوت زمانی، تفریق پس زمینه و جریان نوری (۸۷). تست تحقیقاتی و علم و فناوری مبدل[۷۴] یک جزء ضروری و توصیه شده در محیط کار معاصر و ممکن است راه‌حلی یکپارچه برای رسیدگی به مسائل مرتبط در این زمینه‌ها باشد. متخصصان فناوری اطلاعات[۷۵] می‌توانند دسترسی به اطلاعات، تبادل و ظرفیت افسران مجری قانون شهرداری، ایالتی و فدرال را برای تجزیه و تحلیل جرم بهبود بخشند. متخصصان فناوری اطلاعات می‌توانند به ایجاد قابلیت‌های جدید جمع آوری اطلاعات، جمع آوری اطلاعات و تجزیه و تحلیل برای شناسایی حملات تروریستی در آینده کمک کنند. ایجاد ابزارهای تحلیلی، مدل‌سازی و شبیه‌سازی برای زیرساخت‌های حیاتی، آسیب‌پذیری فضای سایبری و ارزیابی ریسک و حفاظت می‌تواند توسط محققان فناوری اطلاعات کمک شود. محققان فناوری اطلاعات می‌توانند با توسعه مدیریت هویت و تکنیک‌های تشخیص فریب به ایجاد مرزهای هوشمند کمک کنند. محققان فناوری اطلاعات می‌توانند به افزایش امنیت کشتیرانی بین‌المللی و توسعه مدل‌های استراتژیک و عملیاتی مؤثر و کارآمد برای حفاظت از زیرساخت‌های مرتبط با حمل و نقل کمک کنند. محققان فناوری اطلاعات می‌توانند در توسعه روش‌های شبیه‌سازی، شناسایی و هشدار برای تهدیدات فاجعه‌بار بالقوه، مانند حملات شیمیایی و بیولوژیکی، کمک کنند. با تمرکز بر نیازهای حمل و نقل برای انجام چنین حملاتی، محققان فناوری اطلاعات می‌توانند به این تلاش‌ها کمک کنند. محققان فناوری اطلاعات می‌توانند با افزایش اشتراک اطلاعات و قابلیت همکاری ارتباطات قبل و بعد از بلایا به اولین پاسخ دهندگان کمک کنند. محققان فناوری اطلاعات می‌توانند با ایجاد ابزارهایی برای کمک به تصمیم‌گیری لجستیکی که اثربخشی عملیات پاسخ را افزایش می‌دهد، کمک کنند (۸۸).

با استفاده از هوش مصنوعی که بر اساس مطالعات محققان فناوری اطلاعات توسعه یافته بود، دویست و بیست و چهار سازمان تروریستی داخلی در ایالات متحده آمریکا و همچنین چهارصدوچهل سازمان تروریستی خارجی پیدا شدند که نشان‌دهنده پیشرفت و تأثیر قابل توجه هوش مصنوعی در این بخش است.

74- TST
75- IT

این فناوری برای نیروهای مسلح در دستگیری تروریست‌ها در سراسر جهان تفاوت ایجاد کرد. اخیراً مسائل امنیت داخلی در تحقیقات بین‌المللی در مورد فناوری‌های ضدتروریستی و ضدجنایت مطرح شده است.

ابزارها و روش‌های توسعه‌یافته توسط محققان فناوری اطلاعات برای امنیت ساخته شده با هوش مصنوعی شامل یکپارچه‌سازی داده‌ها، تجزیه و تحلیل داده‌ها، متن کاوی، پردازش تصویر و ویدئو و ترکیب شواهد می‌شود. با این حال، هنوز باید به مسائلی در مورد کاربرد مناسب آن‌ها در حوزه‌های اطلاعاتی و امنیتی با کمک داده‌های اولیه و کاربرد کارآمد آن‌ها در حوزه‌های ماموریت امنیت ملی پرداخته شود (۸۹). بسیاری از زیرشاخه‌های هوش مصنوعی باید به طور کامل مورد بررسی و بهبود قرار گیرند تا داده‌های خام امنیت داخلی را به هوش قابل اجرا تبدیل کنند. این زیرشاخه‌ها شامل داده کاوی، متن کاوی، وب کاوی، پردازش زبان طبیعی، برنامه ریزی، استدلال، حل اختلاف، تجزیه و تحلیل لینک و الگوریتم‌های جست‌وجو هستند.

۲-۵- حمل و نقل نظامی و لجستیک[۷۶]

هواپیماهای نظامی از سیستم‌های هوش مصنوعی استفاده می‌کنند، که می‌تواند بهترین نتایج ممکن را در تصمیم‌گیری ایجاد کند. این طرح‌های خاص هوش مصنوعی فقط برای خروجی بهتر در جبهه ساخته شده‌اند که نمی‌توان آن‌ها را به روش‌های دیگر جمع کرد. عملیات و عملکرد آن‌ها متفاوت است و از داده‌های بزرگ برای خروجی سریع نتیجه استفاده می‌کنند. این فناوری‌های تقویت شده با هوش مصنوعی با فعال کردن فرایند انواع متعدد و متنوعی از سیستم‌های هوایی بدون سرنشین[۷۷] و سایر سکوهای اطلاعاتی، نظارتی و شناسایی[۷۸] در قرن بیست و یکم به ارتش کمک می‌کنند (۴). واقعیت مجازی و شبیه‌سازی‌های جنگ هوایی محبوب‌ترین برنامه‌های آموزشی برای سربازان تازه‌کار هستند. تفنگداران دریایی ایالات متحده آمریکا[۷۹] تقریباً هفت میلیون دلار برای سیستم‌های هشداردهنده بدون سرنشین

76- Military Transportation and Logistics
77- UAV
78- ISR

۷۹- سپاه تفنگداران دریایی ایالات متحده شاخه‌ای از نیروهای مسلح ایالات متحده آمریکا است، که به‌عنوان زیرمجموعه‌ای از وزارت نیروی دریایی ایالات متحده آمریکا، وظیفه طراحی و اجرای عملیات آبی خاکی، همچنین انجام جنگ نامتقارن، جنگ کلاسیک و جنگ ترکیبی را با مشارکت نیروهای دریایی، زمینی و هوایی، برعهده دارد. سپاه تفنگداران دریایی مسئول اعمال قدرت ایالات متحده آمریکا است و از تحرک نیروی دریایی ایالات متحده آمریکا، به الزام

اختصاص دادند که می‌توانند چشم‌انداز بیشتری را در میدان نبرد به فرماندهان ارائه دهند، درحالی‌که نیروی هوایی ایالات متحده آمریکا[۸۰] بیش از هشتادوهفت دلار برای توسعه بازی‌های جنگی هوش مصنوعی سرمایه‌گذاری کرد (۴).

استفاده از شبکه‌های عصبی هوش مصنوعی در کاربردها و پیامدهای نظامی نویدبخش و پتانسیل زیادی برای باز کردن چندین درب در تقریباً هر صنعت، ازجمله لجستیک[۸۱] و حمل و نقل است. سیستم شناسایی خودکار[۸۲]، که داده‌های زیادی را در مورد ترافیک دریایی ارائه می‌دهد، اما به حجم قابل از داده‌های پردازش شده نیاز دارد، اخیراً نفوذ نظامی قابل توجهی پیدا کرده است (۹۲). مین‌های آبی حرکت و حمل و نقل کشتی‌های جنگی را به طور جدی به خطر می‌اندازد. با کمک وسایل نقلیه بدون سرنشین هوابرد[۸۳] و وسایل نقلیه زیرآبی بدون سرنشین[۸۴]، همچنین به‌عنوان وسایل نقلیه زیردریایی خودمختار[۸۵] شناخته می‌شوند، که به طور خاص برای این منظور ایجاد شده‌اند، این تهدید ممکن است تقریباً از بین برود و به بهبود حمل و نقل برای دریایی کمک کند (۹۳).

نیروی دریایی هر کشوری تنها با کمک هوش مصنوعی می‌تواند پاسخگوتر، سازگارتر، متحرک‌تر و

کنگره، برای انجام مأموریت‌های زمینی مشترک قوا، در هوا، خشکی و دریا استفاده می‌کند.

۸۰- نیروی هوایی ایالات متحده آمریکا، یکی از شاخه‌های اصلی نیروهای مسلح ایالات متحده آمریکا است که در ابتدا در سال ۱۹۰۷ میلادی به‌عنوان بخشی از نیروی زمینی ایالات متحده آمریکا شکل گرفت و سپس با تصویب قانون امنیت ملی ۱۹۴۷ میلادی توسط شورای امنیت ملی ایالات متحده آمریکا به‌عنوان شاخه مستقلی از نیروهای مسلح در هجدهم سپتامبر ۱۹۴۷ میلادی تأسیس شد. در سال ۱۹۴۹ میلادی نیز نیروی هوایی در کنار نیروهای دیگر، زیر فرماندهی وزارت دفاع ایالات متحده آمریکا قرار گرفت.

۸۱- لجستیک یا آماد به حرکت مواد، خدمات، پول و اطلاعات در داخل یک زنجیره تأمین گفته می‌شود. همچنین لجستیک شامل حرکت در داخل یک مجموعه، نظارت بر ورود و خروج محموله‌ها و کالاها، و جریان اطلاعات در سرتاسر زنجیره تأمین می‌شود. در علوم نظامی، آماد و لجستیک یعنی حفظ زنجیره تأمین با نیروهای نظامی، با وجودی که دشمن به دنبال به هم زدن آن است. در تدارکات نظامی، افسران تدارکات نحوه و زمان انتقال منابع به مکان‌های مورد نیاز را مدیریت می‌کنند. لجستیک شامل یکپارچه‌سازی اطلاعات، حمل و نقل، موجودی کالا، انبارداری، جابه‌جایی کالا و بسته‌بندی و در مواردی شامل امنیت نیز می‌شود. لجستیک قسمتی از زنجیره تأمین است که ارزش زمان و مکان را به آن می‌افزاید.

82- AIS
83- UAV
84- UUV
85- AUV

درنهایت کشنده‌تر از همیشه شود. تعداد افراد مورد نیاز، یک نقطه ضعف قابل توجه برای قدرت دریایی است. بدون چنین چیزی، یک تیم نمی‌تواند حریف خود را حتی با تجهیزات مناسب شکست دهد. با این حال، به نظر می‌رسد که هوش مصنوعی می‌تواند در این زمینه مفید باشد. سیستم‌های هوش مصنوعی اکنون برای پشتیبانی از مدیریت، رله اطلاعات سریع، برنامه‌ریزی، تدارکات، پاسخ به بحران، حفاظت از نیرو، زیرساخت نیرو، آموزش، هدایت و هوشمندی در حرکت استفاده می‌شوند. هوش مصنوعی همه گزینه‌ها را در نظر می‌گیرد و بهترین گزینه را برای هر کدام انتخاب می‌کند (۶).

بسیاری از بزرگ‌ترین شهرهای جهان با مشکلات لجستیک، ترافیک و حمل و نقل دست و پنجه نرم می‌کنند. این به دلیل رشد سریع جمعیت انسانی و افزایش تعداد وسایل نقلیه در جاده‌ها است. استفاده از فناوری در برنامه‌ریزی و مدیریت یک سیستم حمل و نقل پایدار می‌تواند بسیار سودمند باشد. شهرها در حال مبارزه با تراکم ترافیک هستند. بنابراین، راه‌حل‌های هوش مصنوعی که از یک رابط کاربری واحد برای دریافت داده‌های بلادرنگ از وسایل نقلیه در حال حرکت برای کنترل ترافیک و استفاده از قابلیت تحرک در صورت تقاضا برای برنامه‌ریزی سفر استفاده می‌کنند، پدیدار شده‌اند. ادغام ایمن تصمیم‌گیری مبتنی بر هوش مصنوعی، مدیریت ترافیک، مسیریابی، خدمات شبکه حمل و نقل و سایر ابزارهای بهینه‌سازی تحرک، امکاناتی برای مدیریت ترافیک کارآمد هستند. برخی از فناوری‌های هوش مصنوعی که به حمل و نقل کمک می‌کنند عبارتند از: شبکه‌های عصبی مصنوعی[۸۶]، الگوریتم‌های ژنتیک[۸۷]، بازپخت شبیه‌سازی شده[۸۸]، مدل منطق فازی[۸۹] و بهینه‌ساز کلونی مورچه‌ها[۹۰]. هدف از اجرای این تاکتیک‌ها در مدیریت حمل و نقل در ارتش و سایر بخش‌ها در سرتاسر جهان کاهش ازدحام، افزایش قابلیت پیش‌بینی زمان سفر مسافران، افزایش اقتصادی و بهره‌وری سیستم به‌عنوان یک کل است (۹۳).

۲-۶- وسایل نقلیه خودمختار[۹۱]

وسایل نقلیه خودران که گاهی اوقات به‌عنوان ربات‌های متحرک شناخته می‌شوند، هم در بخش نظامی و هم در بخش خصوصی به کار گرفته می‌شوند. وسایل نقلیه زمینی بدون سرنشین[۹۲]، فضاپیماهای بدون

86- ANN
87- GA
88- SA
89- FLM
90- ACO
91- Autonomous Vehicles
92- UGV

سرنشین، وسایل نقلیه هوایی بدون سرنشین[۹۳] و وسایل نقلیه زیرآبی بدون سرنشین[۹۴] برخی از این موارد هستند. بیشتر سیستم‌های کنونی فقط تا حدی مستقل هستند و به تعامل مکرر انسانی وابسته هستند. فراتر از این قابلیت، سیستم‌های نرم افزاری پیچیده و در عین حال سازگار مورد نیاز خواهند بود [۹۴]. براساس فناوری‌های نرم‌افزاری بسیار ساده و اساسی هوش مصنوعی مانند لاکهید مارتین یک وسیله نقلیه زمینی بدون سرنشین برای حمل تجهیزات، اسلحه‌ها، تجهیزات پزشکی و جیره‌های جوخه‌های بزرگ فراهم می‌کند. به همین ترتیب، نرم افزار سیستم[۹۵] نیز در ارتش ایالات متحده آریکا وجود دارد که هنوز یک پیشرفت است که بیش از یک سرباز مجروح را بر روی یک وسیله نقلیه بدون سرنشین مدیواک حمل می‌کند (۹۵). وسایل نقلیه خودران[۹۶] از تکنیک‌های هوش مصنوعی برای پاکسازی مسیر بهتر در موقعیت‌های مختلف استفاده می‌کنند. اگرچه توانایی آن‌ها در تشخیص اشیاء در سال‌های اخیر بسیار بهبود یافته است، اما اکنون آن‌ها کارهای بیشتری انجام می‌دهند.

۲-۷- آموزش رزمی و شبیه سازی[۹۷]

یکی از بهترین نمونه‌های افزودن هوش مصنوعی به آموزش و شبیه‌سازی رزمی، خلبانان هوشمند خودکار برای استفاده نظامی است. دو هواپیمای[۹۸] بهترین هواپیماهای مبتنی بر هوش مصنوعی هستند که هر دو در ایستگاه هوایی اقیانوس دریایی در ویرجینیا بیچ[۹۹] مستقر هستند (۹۸). این‌ها فناوری مربوطه و آزمایش زیرساخت شبکه در حال انجام را نشان داده و ارزیابی می‌کنند.

یک برنامه دفتر تحقیقات نیروی دریایی، آموزش مجازی و محیط[۱۰۰]، مربیان مجازی همه جانبه‌ای را برای عملیات نظامی در مناطق شهری[۱۰۱] ایجاد می‌کند. در این تمرین، جوخه‌های آتش‌نشانی چهار نفره تفنگداران دریایی ایالات متحده آمریکا در یک منطقه شهری شبیه‌سازی شده مستقر می‌شوند و وظیفه پاکسازی ساختمانی را دارند که می‌تواند سربازان دشمن را در خود جای دهد. مخالفان مجازی برای پر

93- UAV
94- UUV
95- BAE
96- AVs
97- Combat Training and Simulation
98- STOW 97 & Roadrunner 98
۹۹- ویرجینیا بیچ بزرگ‌ترین شهر ایالت ویرجینیا در ایالات متحده آمریکا است.
100- VIRTE
101- MOUT

کردن محیط و آزمایش کارآموزان ضروری هستند. یک سری بازی‌های رایانه‌ای تجاری[۱۰۲] تقویت‌شده با هوش مصنوعی، شبیه‌سازی‌هایی را در خود جای داده است که اکنون در نوآوری‌های نظامی به کار می‌روند. یک گزینه کاربردی‌تر و مؤثرتر برای آموزش رزمی نسبت به شروع بلادرنگ برای کشورهای دارای ارتش بسیار پیشرفته است (۹۹).

دستورالعمل‌های بازی و سناریوهای آموزشی برای آموزش بازی‌های پیچیده به بازیکنان جدید، مانند شبیه‌سازی‌های تاکتیکی بسیار واقعی از میدان‌های جنگ معاصر، کافی نیستند. افزودن گزارش‌های پس از بازی مفید است، اما آن‌ها به‌ندرت راهنمایی برای کل کار ارائه می‌دهند و اغلب بر انتقادات کمی تمرکز می‌کنند تا جزئیاتی در مورد کارهایی که بازیکن اشتباه انجام داده و نحوه بهبود آن. درجه بالاتری از تعامل و تجزیه و تحلیل کیفی عمیق‌تر توسط فناوری سیستم آموزش هوشمند[۱۰۳] برای کمک به بازیکنان در حین بازی ارائه می‌شود. فناوری هوش مصنوعی با ترکیب یک جزء سیستم آموزش هوشمند با نیروی ضربت زرهی شبیه‌سازی تاکتیکی[۱۰۴] و ایجاد مرکز آموزشی رزمی مجازی[۱۰۵] به کار می‌رود. محیط نظامی، ازجمله کلاس درس، میدان نبرد و استقرارهای تعبیه شده کانون اصلی توسعه مرکز آموزشی رزمی مجازی بود. از طرف دیگر، این بازیکنان ممکن است در حین یادگیری بازی‌های چالش برانگیز دچار ناامیدی شوند یا از جایگزین‌های تاکتیکی و عمق استراتژی قابل دسترسی در یک بازی خوب طراحی شده بی‌اطلاع باشند (۱۰۰).

۲-۸- ربات‌های به کمک هوش مصنوعی در میدان نبرد[۱۰۶]

حفظ سلامتی و جان سربازان در میدان نبرد یکی از اهداف اصلی فناوری مدرن است. یکی از استراتژی‌هایی که معمولاً در این زمینه مطرح می‌شود، «آوردن ماشین‌ها به میدان جنگ» است. استفاده از روبات‌های الهام‌گرفته از زیست‌محیطی در عملیات‌های نظامی ممکن است به‌سرعت جایگزین سلاح‌های متعارف در جنگ شود. ربات‌ها می‌توانند دمای شدید، کمبود غذا و نوشیدنی و خستگی‌های تهدیدکننده زندگی را تحمل کنند. یک شرکت آمریکایی[۱۰۷]، رهبر بازار روبات‌های متحرک است. ربات‌ها می‌توانند

102- MOUTbot
103- ITS
104- ATF
105- V-CTC
106- AI-Assisted Robots on the Battlefield
107- Boston dynamics

آزادانه حرکت کنند، موانع را بیابند و از آن اجتناب کنند، یک برنامه سفر از پیش تعیین‌شده را دنبال کنند و نشانه‌های اطراف خود را تشخیص دهند و براساس آن عمل کنند (۹۲).

۲-۹- مراقبت‌های بهداشتی در میدان نبرد[۱۰۸]

فناوری پوشیدنی با قابلیت‌های هوش مصنوعی اکنون ممکن است داده‌های پزشکی سربازان را ارزیابی کند و به تشخیص‌های دشوار کمک کند. برای پایش سلامت لحظه‌ای پارامترهای فیزیولوژیکی و زیست‌پزشکی، ازجمله دمای بدن و ضربان قلب، می‌توان از یک شبکه حسگر بدن[۱۰۹] متشکل از گره‌های حسگر فیزیولوژیکی و زیست‌پزشکی که نزدیک یا داخل بدن انسان قرار دارند، استفاده کرد (۱۰۲-۱۰۳).

یک سرباز نمی‌تواند موشک ورودی را به‌سرعت کلاه ایمنی در تصویر شناسایی کند. برای هشدار دادن به سربازان از نزدیک شدن به گلوله‌ها، بمب‌ها یا امواج آسیب رسان، با حسگرهای سربازان دیگر دستگاه‌های اینترنت اشیاء میدان جنگ ادغام می‌شود. درنتیجه، این کلاه‌ها و لباس‌های هوشمند می‌توانند از سربازان در برابر آسیب‌های مغزی تروماتیک[۱۱۰] محافظت کنند. کارشناسان بهداشت می‌توانند به اطلاعات مراقبت‌های بهداشتی سربازان دسترسی داشته باشند تا وضعیت سلامتی را به طور مداوم بررسی و مقایسه کنند تا پاسخ‌های بلادرنگ در صورت لزوم به لطف ادغام کلاه ایمنی هوشمند، لباس‌های فرم هوشمند و حسگرهای عینک هوشمند اعمال شوند (۱۰۴).

هوش مصنوعی را می‌توان با سیستم‌های جراحی رباتیک[۱۱۱] و سکوهای زمینی رباتیک[۱۱۲] ترکیب کرد تا عملیات پشتیبانی و نجات جراحی از راه دور در مناطق جنگی انجام شود. مشاوره تله رادیولوژی می‌تواند از طریق یک پلتفرم خودکار ارائه شود (۱۰). یک ربات کوچک در داخل حفره شکمی قرار می‌گیرد. مفهوم بی‌سیم در این مدل بیشتر اصلاح شد و یک ربات با استفاده از یک پلتفرم شبیه یک پورت لاپاروسکوپی[۱۱۳] تک برش قرار گرفته است. همانند لاپاراسکوپ‌های نوک انعطاف‌پذیر بر روی بازوهای رباتیک مدل داوینچی، بازوهای جراحی ربات دارای دامنه حرکتی وسیعی هستند (۱۰۷-۱۰۸).

108- Healthcare on the Battlefield
109- BSN
110- TBI
111- RSS
112- RGP
۱۱۳- لاپاراسکوپی عملیاتی است که با استفاده از یک دوربین و برش‌های کوچک در ناحیه شکم یا لگن انجام

۳- تأثیر و تأثیر هوش مصنوعی بر ثبات استراتژیک جهانی و خطر هسته ای[۱۱۴]

هوش مصنوعی صدای پرطرفداری است که اغراق در مزایا و به حداقل رساندن خطرات مرتبط با توسعه و کاربرد آن در ارتش را ساده می‌کند. ثبات استراتژیک ممکن است با اختلاط و در هم تنیدگی قابلیت‌های هسته‌ای و غیرهسته‌ای و سرعت فزاینده جنگ به خطر بیافتد. مواردی که توسط فناوری‌های جدید به جهان ارائه می‌شود، پیش‌بینی می‌کند و نشان می‌دهد که احتمال تشدید تنش نظامی، به‌ویژه تشدید غیرعمدی و ناخواسته، پیشرفت فناوری در قابلیت‌های معمولی با کمک هوش مصنوعی را افزایش می‌دهد. توانایی هوش مصنوعی نظامی برای افزایش این خطرات برجسته نشده است، حتی اگر نگرانی‌های تشدید غیرعمدی ناشی از پیشرفت‌های فناوری نظامی در ادبیات قبلی ذکر شده بود (۱۰۹).

قابلیت‌های هوش مصنوعی تأثیر قابل توجهی دارند زیرا مسئولیت ثبات استراتژیک بین‌المللی را بر عهده دارند. یک انتخاب واحد ممکن است این تعادل ظریف را بر هم بزند و بر ثبات استراتژیک بین قدرت‌های بزرگ نظامی جهان تأثیر بگذارد. برخی از تسلیحات مبتنی بر هوش مصنوعی و فناوری‌های اخیراً توسعه یافته آنقدر مؤثر و پیشرفته هستند که ممکن است بتوانند اثرات آن‌ها را خنثی کنند. نبود سلاح‌های زیادی که ثبات را تهدید می‌کند امر خوبی است. مهمات حمله سرگردان[۱۱۵] که گاهی اوقات به‌عنوان هواپیماهای بدون سرنشین انتحاری شناخته می‌شوند، سلاح‌هایی هستند که بدون تعامل انسانی با اهداف درگیر می‌شوند. آن‌ها با استفاده از حسگرهای از پیش برنامه‌ریزی شده برای تشخیص جسم و انجام حمله، اشیایی مانند کشتی‌ها، تانک‌ها و رادارهای دشمن را تعقیب می‌کنند. مهمات حمله سرگردان از موشک‌های کروز[۱۱۶] خطرناک‌تر و کشنده‌تر هستند، زیرا آن‌ها با هوش مصنوعی تقویت شده‌اند و به آن‌ها اجازه می‌دهند هر پرتابه‌ای را سریع‌تر از اپراتورهای انسانی شلیک کنند و بیشتر در هوا بمانند (۱۱۰).

قابلیت‌های متعارف تقویت‌شده با هوش مصنوعی ممکن است بر ثبات استراتژیک بین قدرت‌های نظامی بزرگ تأثیر بگذارد. فعل و انفعالات پیچیده و متنوع بین این فناوری جدید و تسلیحات پیچیده

114- Impact and Influence of Artificial Intelligence on Worldwide Strategic Stability and Nuclear Risk

115- LAM

۱۱۶- سامانه موشکی کروز گونه‌ای هواگرد بی‌سرنشین هدایت شونده و از گونه بالستیک است که مسیر آن تا رسیدن به هدف قابل تغییر و هدایت است. در بیشتر سامانه‌های کروز از گونه‌ای موتور جت استفاده می‌شود درحالی‌که موشک‌های دیگر از موتور راکتی استفاده می‌کنند.

مرسوم مختلف می‌تواند قابلیت‌های هسته‌ای را به خطر بیاندازد و تأثیرات مخرب احتمالی آن‌ها را چند برابر کند. حتی در مناطق به شدت مستحکم مانند شرق و سواحل چین، در یک سورتی[۱۱۷] پرازدحام، صدها پهپاد خودکار مجهز به هوش مصنوعی ممکن است بتوانند از دفاع بسیار پیشرفته دشمن اجتناب کنند و از تعداد آن‌ها بیشتر باشند (۱۱۲).

در مقابل، یک جنگنده رادارگریز[۱۱۸] ایالات متحده آمریکا به طور جدی توسط یک هواپیمای بدون سرنشین نسبتاً ارزان و منفرد[۱۱۹] تهدید نخواهد شد. این پارازیت‌های الکترومغناطیسی کوچک و سلاح‌های سایبری می‌توانند با شبکه‌های ارتباطی و سنسورهای هدف‌گیری دشمن تداخل داشته باشند و سیستم دفاعی چندلایه دشمن را در آمادگی برای حملات تهاجمی بمب‌افکن پنهان‌کار دوربرد و ازدحام پهپادها از بین ببرند. در سال ۲۰۱۱ میلادی، در خاورمیانه، پهپادهای آسیب پذیری[۱۲۰] زیرمجموعه‌های سیستم‌های ایالات متحده آمریکا را در معرض حملات سایبری تهاجمی قرار دادند. برای جلوگیری (یا کاهش) این تهدید، نسل‌های آینده فناوری هوش مصنوعی ممکن است در هواپیماهای رادارگریز گنجانده شود. هوش مصنوعی به زودی قادر به کنترل گروه‌های پهپاد کوچکی خواهد بود که مأموریت‌های سنجش، شناسایی و هدف‌گیری نزدیک به هواپیماهای سرنشین‌دار را انجام می‌دهند، همراه با دفاع در برابر حملات ازدحام. در آینده، پهپادها و بهبود استقامت سکوی پشتیبانی ممکن است مقاومت گروه‌های پهپاد را در برابر چنین اقدامات متقابلی افزایش دهند (۱۱۱).

۳-۱- تشدید بی‌ثباتی جهانی از طریق جعل عمیق[۱۲۱]

موضوع مهمی که در طول استفاده از هوش مصنوعی پدیدار شد، ظرفیت اشخاص ثالث برای دستکاری سیستم‌های هشدار و درج اطلاعات گمراه‌کننده برای فریب دادن اپراتورهای فناوری انسانی بود. یک نهاد غیردولتی که قبلاً فاش نشده بود به نام «نگهبانان صلح جهانی» عکس‌ها و ویدیوهای جعلی را در شبکه‌های اجتماعی منتشر کرد تا این طور به نظر برسد که تعدادی از سربازان نیروهای ویژه آمریکایی در

۱۱۷- سورتی عبارت است از هر بار به مأموریت گسیل داشتن و بازگشتن یک هواپیما، کشتی یا واحد نظامی. با هر یک رفت‌وبرگشت اصطلاحاً یک سورتی برای آن شمارش می‌شود.

118- F-35
119- UAV
120- MQ-1 -MQ-9
121- Escalation of Global Instability via Deep Fakes

سوریه در جریان درگیری با مربیان نظامی روسی با گاز کشته شده‌اند. برخی از تحلیلگران آمریکایی استدلال کردند که استفاده از سلاح‌های هسته‌ای تاکتیکی به‌عنوان انتقام موجه است.

خانواده‌های چند تن از رهبران برجسته ایالات متحده آمریکا متعاقباً در فیلم‌های ضبط‌شده‌ای که در رسانه‌های آمریکایی و چینی منتشر شد، به‌سرعت واشنگتن را ترک کردند. گزارش‌های دیگر شاهدان عینی از طریق شبکه‌های اجتماعی می‌گویند که پایگاه‌های موشکی در غرب ایالات متحده آمریکا در حالت آماده‌باش قرار گرفته‌اند و اپراتورهای دو نفره آن‌ها قفل ورودی‌های سیستم‌های فرماندهی و کنترل هسته‌ای هوش مصنوعی سیلوها را باز کرده‌اند. با توجه به این علائم و چندین نشانه دیگر که در برنامه‌های آگاهی فضایی مبتنی بر هوش مصنوعی روسیه به کار می‌رود، سیستم‌های نظارت تاکتیکی مسکو به مقامات روسی اعلام کردند که احتمال وقوع حمله هوایی ایالات متحده آمریکا وجود دارد. رییس جمهور چین در گزارش اولیه وضعیت که توسط تیم کنترل تهیه شد به ایالات متحده آمریکا هشدار داد که علیه هیچ کشوری حمله هسته‌ای انجام ندهد. وی همچنین اظهار داشت که اگر ایالات متحده آمریکا مدرک قانع‌کننده‌ای مبنی بر آماده نبودن خود برای جنگ ارائه نکند، چین مجبور به اتخاذ اقدامات متقابل نامطمئن می‌شود که واقعاً نمونه تکان‌دهنده‌ای از تأثیر و تأثیر هوش مصنوعی بر ثبات استراتژیک در سراسر جهان است. این پرونده تصویر قابل قبولی از تشدید وضعیت توسط اشخاص ثالث ارائه کرد. یک نهاد غیردولتی یک جعلی عمیق و قانع‌کننده ایجاد کرد تا یک بحران هسته‌ای شامل دو کشور را تسریع کند (۱۱۴).

۳-۲- ارزیابی‌های هشدار اولیه تحریف شده[۱۲۲]

جعل‌های عمیقی که توسط نهادهای خارجی انجام می‌شود، می‌توانست با ابزارهای هوش مصنوعی که برای تولید موارد مثبت کاذب سوءاستفاده می‌شوند، تقویت شود. در این مورد، تنها سه ماه پیش از وضعیت اضطراری، پلتفورم یکپارچه سازمان سایبری ایالات متحده آمریکا، که بر اطلاعات یکپارچه، الکترونیکی و همچنین عملکردهای جنگ سایبری نظارت و هماهنگی می‌کند نتایج آماری غیرعادی در مورد ارزیابی‌های آگاهی فضایی در مورد نشانه‌های پیشرفته تولید می‌کرد. مجموعه‌های تهدید پیشرفته دائمی از داده‌های مرتبط با بازیگران سایبری روسیه را انتخاب کرد.

در طول تمرین، خدمه ایالات متحده آمریکا از انواع مسائل احتمالی ناشی از ارزیابی‌های مبتنی بر

122- Distorted Early Warning Assessments

هوش مصنوعی ارائه شده توسط پلتفرم یکپارچه سازمان سایبری ایالات متحده آمریکا آگاه بودند. سیستم‌های هشدار تاکتیکی روسیه نیز به همان شیوه مغرضانه خواهند بود، که آن‌ها را بسیار نگران می‌کرد. این می‌توانست به یک جنگ هسته‌ای مستقیم بین دو کشور قدرتمند نظامی منجر شود و به جنگ جهانی منجر شود (۱۱۵). حملات با استفاده از داده‌ها، توانایی سیستم هوش مصنوعی برای تشخیص داده‌های خوب و بد را می‌توان با افزودن ورودی‌های تحریف شده به نمونه‌های آموزشی برای چنین رویه هوش مصنوعی تضعیف کرد. ایجاد محتوا، تسلیحات بازخورد، حملات انسان در وسط و تزریق اختلال رایج‌ترین روش‌ها برای این عملیات هستند.

۳-۳- از طریق هشدارهای ایمنی مثبت کاذب[۱۲۳]

چند سال پیش، نرم افزار مدیریت مبتنی بر هوش مصنوعی در چهار راکتور تجاری انرژی هسته‌ای در مناطق پرجمعیت چین شروع به گزارش هشدارهای ایمنی جعلی کرد. در هر نمونه، حسگرها مسائل ساختاری را در کارخانه شناسایی کردند و بدنه‌های مدیریتی را بر آن داشت تا پروتکل‌های اضطراری را اجرا کنند که عملیات را متوقف می‌کرد، حتی اگر بررسی‌های مهندسی نه آسیب ساختاری و نه آسیب انسانی را نشان دهد. با این حال، وقفه‌های مکرر در تولید برق از طریق این نیروگاه‌های مهم به اقتصاد آسیب می‌رساند. در پاسخ، مقامات عامل از یک فروشنده نرم‌افزار هوش مصنوعی، خواستند تا عملکردهای تشخیص را تغییر دهد تا پیش از شروع اقدامات خودکار خرابی، تخریب پایداری ساختاری بیشتر مورد نیاز باشد. این باعث شد که هر نیروگاه آسیب دیده با ظرفیت کامل یا نزدیک به ظرفیت کامل کار کند. در طول دورهای اولیه، مشخص نبود که آیا نتایج مثبت کاذب به دلیل فعالیت‌های مخرب بوده است؟ (۱۱۴).

۳-۴- سیستم‌های ناوبری نادرست[۱۲۴]

یک تغییر جزئی در نحوه بازی می‌توانست منجر به جنگ قدرت قابل توجهی شود که ناشی از سنسورهای معیوب مختلف است. در مورد ساخت و ساز خیالی با سناریوی بحران، یک ناوشکن[۱۲۵] نیروی دریایی ایالات متحده آمریکا که در تمرینی به نام آزادی ناوبری در آب‌های سرزمینی دریای جنوبی چین[۱۲۶] که چین ادعای

123- Through False-Positive Safety Alerts

124- Malfunctioning Navigational Systems

۱۲۵- در نیروهای دریایی، ناوشکن گونه‌ای کشتی جنگی سریع با تحرک و برد عملیاتی بالا است که به همراهی و محافظت از شناورهای بزرگ‌تر در یک ناوگان، کاروان دریایی یا ناوگروه هواپیمابر نبرد می‌پردازد.

۱۲۶- دریای جنوبی چین دریایی حاشیه‌ای است که بخشی از اقیانوس آرام به شمار می‌آید و ناحیه‌ای در حدود سه و نیم میلیون

آن را دارد، به طور خطرناکی به برخورد خطرناک با کشتی دیگری نزدیک شد. این ورودی‌ها به طور بالقوه می‌توانند یک سیستم هوش مصنوعی را با تغییر جزئی پیکسل‌ها یا الگوهای تصویر به سمت طبقه‌بندی نادرست تصویر سوق دهند. تغییراتی که ممکن است برای دید انسان نامرئی باشد و منجر به شرایط ناگوار شود (۱۱۴).

۳-۵- ربودن فناوری بخش خصوصی[۱۲۷]

یکی از چشمگیرترین ایراداتی که این تمرین نشان داد، پتانسیل یک بازیگر غیردولتی دیگر برای سرقت پیشرفت‌های فناوری بخش خصوصی برای اهداف مخرب بود که پیامدهای فاجعه باری برای ثبات استراتژیک خواهد داشت. آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی قراردادهایی را با شرکت فناوری آمریکایی[۱۲۸] برای مغناطیس‌سنج‌ها و گرانش‌سنج‌های پیشرفته‌اش اعطاء کرد. این دو شرکت برای پرتاب ماهواره‌های سنجش کوانتومی در چهار منبع باز که از هوش مصنوعی برای اندازه‌گیری تغییرات جزئی در میدان‌های مغناطیسی و گرانشی زمین استفاده می‌کردند، همکاری کردند. مشترکان شروع به استفاده از فناوری جدید برای مکان‌یابی پساب‌های فلزی خطرناک از سایت‌های صنعتی، کشتی‌های غرق شده و چشم انداز معادن جدید کردند. ترتیبات واسنار و مقررات بین‌المللی حمل و نقل اسلحه ایالات متحده آمریکا، کنترل‌های صادراتی را بر روی فناوری[۱۲۹] اعمال می‌کنند که فقط به کشورهای ناتو[۱۳۰] که محققین مورد تأیید دولت هستند، مبادله می‌شود.

در دور اول، تصاویر ماهواره‌ای از دریای چین جنوبی به صورت آنلاین منتشر شد که آب را شفاف کرد و محل اختفای سه زیردریایی چینی را آشکار کرد. تیم ایالات متحده آمریکا نگران این بود که هر

کیلومتر مربع از سنگاپور تا تنگه تایوان را دربرمی‌گیرد. پس از پنج اقیانوس جهان این دریا بزرگ‌ترین ناحیه دریایی جهان است. جزیره‌های واقع بر دریای جنوبی چین که با هم یک مجمع‌الجزایر را تشکیل می‌دهند بالغ بر صدها عدد هستند. این جزیره‌ها که عمدتاً خالی از سکنه هستند و همچنین خود دریا مورد جدال کشورهای مختلف بوده‌اند. به همین علت حتی نام‌های متفاوتی برای اشاره به این دریا به کار می‌رود که البته «دریای جنوبی چین» نام پذیرفته شده بین‌المللی، حداقل در انگلیسی و زبان‌های اروپایی است و سازمان آب‌نگاری بین‌المللی و سازمان‌های بین‌المللی دیگر آن را دریای چین جنوبی می‌نامند.

127- Hijacking the Private-Sector Technology

128- QuantumAI

129- QuantumAI

۱۳۰- سازمان پیمان اطلس شمالی یا سازمان پیمان آتلانتیک شمالی یا به صورت مخفف ناتو در چهارم آوریل ۱۹۴۹ میلادی با هدف دفاع جمعی در واشینگتن، دی. سی. پایه‌گذاری شد و بزرگ‌ترین پیمان نظامی در جهان است که سی و دو کشور در آن عضویت دارند.

کسی این اطلاعات را به صورت آنلاین منتشر کند، ممکن است موقعیت زیردریایی‌های ایالات متحده آمریکا را نیز فاش کند، درحالی‌که تیم چینی معتقد بود که دولت ایالات متحده آمریکا مقصر است. اتفاقی که در دور دوم افتاد. همان وب‌سایتی که اطلاعات جغرافیایی زیردریایی‌های چینی را ارائه می‌کرد، اکنون یک نقشه جهانی با نشانگرهای اضافی برای زیردریایی‌های هسته‌ای از ایالات متحده آمریکا و روسیه دارد. تضعیف پتانسیل حمله دوم ارائه شده توسط زیردریایی‌های مجهز به سلاح هسته‌ای مخفی، خطری برای ثبات استراتژیک بود (۱۱۴).

راه‌های زیادی وجود دارد که هوش مصنوعی می‌تواند ثبات جهانی، به‌ویژه بین کشورهای قدرتمند در ارتش را نقض کند و منجر به خطرات هسته‌ای شدید شود. نسل جدیدی از قابلیت‌های متعارف پیشرفته تقویت شده با هوش مصنوعی، خطر تشدید تصادفی ناشی از ترکیب سلاح‌های هسته‌ای و استراتژیک غیرهسته‌ای، افزایش سرعت جنگ، تضعیف ثبات استراتژیک و افزایش احتمال هسته‌ای را تشدید خواهد کرد. تعارض. ازآنجایی که هیچ کس هوش مصنوعی را به طور کامل کنترل و درک نمی‌کند، نمی‌توان به طور کامل به آن اعتماد کرد.

۳-۶- عدم قطعیت‌ها، تهدیدها و چالش‌های کلی هوش مصنوعی[۱۳۱]

به طور کلی، جدا از چالش‌های خود، می‌تواند چالش‌هایی را نیز ایجاد کند که می‌توان آن را تهدید نامید. هوش مصنوعی در ارتش می‌تواند یک شمشیر دولبه باشد، اگر به طور ضمنی از اخلاق جهانی پیروی نکند و به طور مکرر توسط تعدیل کنندگان و ارزیاب‌های درست رعایت نشود. یک گمراهی و سهل انگاری جزئی می‌تواند ارتش هر کشوری را به آستانه فروپاشی برساند که منجر به بی‌ثباتی جهانی یا سناریوی هشداردهنده‌ای شود که هیچ کس انتظارش را نداشت. برای جمع‌بندی بهتر، اجازه دهید عدم قطعیت‌ها، تهدیدها و چالش‌های اصلی هوش مصنوعی در حوزه فعلی کاربردها و پیاده سازی‌های نظامی را بررسی و برجسته کنیم:

اول- نگرانی‌های اخلاقی: استفاده از هوش مصنوعی در ارتش چندین نگرانی اخلاقی را ایجاد می‌کند، ازجمله پتانسیل سیستم‌های تسلیحاتی خودمختار برای تصمیم‌گیری درباره مرگ یا زندگی بدون نظارت انسان. باید اطمینان حاصل شود که استفاده از هوش مصنوعی در کاربردهای نظامی با استانداردها و اصول اخلاقی همسو باشد.

131- The Overall Uncertainties, Threats, and Challenges of AI

دوم- قابلیت اطمینان: یکی از چالش‌های اصلی استفاده از هوش مصنوعی در کاربردهای نظامی، اطمینان از قابلیت اطمینان آن است. دقت مدل‌های هوش مصنوعی به شدت به کیفیت و کمیت داده‌های مورد استفاده برای آموزش بستگی دارد و همیشه خطر خطا و سوءگیری در داده‌ها وجود دارد. هرگونه نادرستی در خروجی یک سیستم هوش مصنوعی می‌تواند عواقب شدیدی داشته باشد، به ویژه در عملیات نظامی.

سوم- امنیت سایبری: سیستم‌های هوش مصنوعی در ارتش اغلب با سیستم‌های دیگر مرتبط هستند و بنابراین در برابر حملات سایبری آسیب‌پذیر هستند. استفاده مخرب از هوش مصنوعی می‌تواند آسیب قابل توجهی به زیرساخت‌ها، پرسنل و عملیات ارتش وارد کند. علاوه بر این، شناسایی و پیشگیری از حملات سایبری مبتنی بر هوش مصنوعی دشوار است.

چهارم- حملات خصمانه: حملات خصمانه نوعی حمله است که می‌تواند باعث شود سیستم‌های هوش مصنوعی با دستکاری داده‌های ورودی نتایج نادرستی تولید کنند. در یک زمینه نظامی، حملات خصمانه می‌تواند باعث شود یک سیستم هوش مصنوعی اهداف را به اشتباه شناسایی کند یا اطلاعات گمراه‌کننده ارائه دهد.

پنجم- آموزش: توسعه و آموزش سیستم‌های هوش مصنوعی برای کاربردهای نظامی به منابع و تخصص قابل توجهی نیاز دارد. علاوه بر این، کیفیت و کمیت داده‌های موجود برای آموزش می‌تواند محدود باشد و ایجاد مدل‌های هوش مصنوعی دقیق و قابل اعتماد را دشوار می‌کند.

ششم- یکپارچه سازی: ادغام سیستم‌های هوش مصنوعی با زیرساخت‌ها و فرایندهای نظامی موجود می‌تواند چالش برانگیز باشد. این امر مستلزم تغییرات قابل توجهی در سیستم‌ها و فرایندهای موجود است که می‌تواند زمان بر و پرهزینه باشد.

هفتم- درک و تصور عمومی: استفاده از هوش مصنوعی در برنامه‌های نظامی نگرانی‌هایی را در میان مردم در مورد پتانسیل ماشین‌ها برای جایگزینی سربازان انسانی، کاهش پاسخگویی و افزایش خطر آسیب به غیرنظامیان ایجاد می‌کند.

آخرین اما نه کم‌اهمیت، درستی سیستم‌های تقویت و پردازش هوش مصنوعی به‌ویژه در معرض فریب هستند، حتی اگر این یک موضوع هوشمندانه و استراتژیک مداوم است که به دوران سایبری پیش از آن می‌رسد. اتکاء به هوش مصنوعی همراه با بهره‌برداری بازیگران مخرب از فناوری می‌تواند به طور قابل توجهی پیامدهای مخرب عملیات اطلاعات نادرست را تشدید کند. ایجاد چهارچوب‌های قانونی که

نحوه تعامل فناوری جدید با زرادخانه فعلی ابزارهای اطلاعات نادرست، مانند رسانه‌های اجتماعی را تعیین می‌کند باید مسئولیت حیاتی دولت‌ها باشد (۱۱۶-۱۱۷).

نتیجه

هدف این پژوهش نمایش بخش‌های اصلی استفاده و امکان استفاده از تقویت‌های هوش مصنوعی و الگوریتم‌های هوش مصنوعی در بخش نظامی، به‌ویژه در امنیت سایبری، تشخیص اشیاء، رباتیک و تدارکات است. به طور کلی، هفت الگوی هوش مصنوعی راه خود را برای ارتقای قابلیت‌های نظامی هموار می‌کنند. بحث تأثیر آن‌ها بر احساس امنیت مردم نیز به تصویر کشیده شده است. یکی از پیشرفت‌های کلیدی فناوری در آینده این است که هوش مصنوعی بهترین امکان را برای تأثیر قابل توجهی بر تحول و پیشرفت جامعه معاصر همراه با قابلیت نظامی دارد. مرحله جدید و هیجان انگیز توسعه سریع برای فناوری هوش مصنوعی آغاز شده است. اکنون پذیرفته شده است که بیشترین پتانسیل را برای تغییر چشم انداز فناوری مخرب در آینده دارد. همچنین، استفاده از آن‌ها برای بهبود استراتژی‌های ملی و دارایی‌ها مانند برنامه‌های کاربردی در ارتش بسیار رایج شده است. با این حال، ما باید در مورد نحوه استفاده از آن و شرایط کوتاه مدت مراقب باشیم. اگر تأثیر بدی بر نسل بعدی داشته باشد، بهتر است جلوی آن نوآوری‌های خاص گرفته شود.

امکانات و کاربردهای هوش مصنوعی در ارتش، مانند سلاح‌های خودمختار، شناسایی هدف، نظارت، امنیت سایبری، حمل و نقل، لجستیک نظامی، نظارت بر امنیت داخلی، امنیت سایبری، وسایل نقلیه خودمختار و آموزش رزمی و شبیه سازی، شرح، بحث و ارزیابی می‌شوند. در این پژوهش انجام شناسایی با استفاده از خودروهای نیمه خودمختار در نظامی، استفاده از سامانه‌های حسگر برای بهبود به همراه ارزیابی تهدید در سامانه‌های پدافند هوایی با نیازهای زمانی بالا، الگوهای نوظهور تحلیل اطلاعاتی، سامانه‌های فرماندهی و کنترل از دیدگاه نظامی کاربردهای بالقوه دیگری هستند.

اگر هوش مصنوعی در بخش نظامی به درستی پیاده‌سازی نشود، احتمالاً به شمشیر دولبه‌ای تبدیل می‌شود که می‌تواند به جای انجام کارهای خوب، هر دو انتها را بریده و یک ملت را نابود کند. با این وجود، تجزیه و تحلیل دقیق‌تر نیازمندی‌ها برای درک استفاده مورد نیاز است. با توجه به ریسک، کیفیت داده‌ها و محدودیت‌های نظارتی، نیازهای نظامی ممکن است به طور قابل توجهی متفاوت باشد و برخی از

اشکال باز بودن ممکن است حتی قابل اجرا نباشند.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

منابع

فارسی

ـ ناظمی اردکانی، نجات پور، مجید؛ محمدی، مصطفی، ۱۳۹۵، انقلاب اطلاعات و تأثیر آن بر جنگ نرم، **فصلنامه پژوهش‌های راهبردی سیاست**، شماره ۱۶.

ـ نجات پور، مجید؛ فرخی، مرتضی؛ سجادی، محسن؛ هادی پور، میثم، ۱۴۰۱، تحلیل جایگاه هوش مصنوعی در توسعه سازمان نظامی، **فصلنامه مدیریت و پژوهش‌های دفاعی**، شماره ۹۸.

لاتین

- S. Das, A. Dey, A. Pal, and N. Roy, Applications of artificial intelligence in machine learning: review and prospect, International Journal of Computer Application, vol. 115, no. 9, 2015.
- M. L. Cummings, Artificial Intelligence and the Future of Warfare, Institute of International Affairs London, London, UK, 2017.
- P. Sharma, K. K. Sarma, and N. E. Mastorakis, Artificial intelligence aided electronic warfare systems- recent trends and evolving applications, IEEE Access, vol. 8, 2020.
- C. H. Heller, The future navy-near-term applications of artificial intelligence, Naval War College Review, vol. 72, 2019.
- Y. Zhang, Z. Dai, L. Zhang, Z. Wang, L. Chen, and Y. Zhou, Application of artificial intelligence in military: from projects view, in Proceedings of the 2020 6th International Conference On Big Data And Information Analytics (BigDIA) , Shenzhen, China, December 2020.
- C. H. Heller, Near-term applications of artificial intelligence, Naval War College Review, vol. 72, 2022.
- R. Arkin, Governing Lethal Behavior in Autonomous Robots, CRC Press, Boca Raton, FL, USA, 2009.
- P. Scharre, Army of None: Autonomous Weapons and the Future of War, WW Norton & Company, New York, NY, USA, 2018.
- V. R. Vaidya, M. Lyle, W. R. Miranda et al. , Long-term survival of patients with left ventricular noncompaction, Journal of the American Heart Association, vol. 10, no.

2, Article ID e015563, 2021.
- O. Gillath, A. Ting, M. S. Branicky, S. Keshmiri, R. B. Davison, and S. Ryan, Attachment and trust in artificial intelligence, Computers in Human Behavior, vol. 115, 2021.
- P. Pradhan and A. Satapathy, Physico-mechanical characterization and thermal property evaluation of polyester composites filled with walnut shell powder, Polymers and Polymer Composites, vol. 30, 2019.
- D. Lee and S. Yeo, Developing an AI-based chatbot for practicing responsive teaching in mathematics, Computers & Education, vol. 191, 2018.
- J. Hu, J. Emile-Geay, J. Nusbaumer, and D. Noone, Impact of convective activity on precipitation δ18O in isotope-enabled general circulation models, Journal of Geophysical Research: Atmospheres, vol. 123, no. 23, 2018.
- J. Dalzochio, R. Kunst, J. L. V. Barbosa et al. , Predictive maintenance in the military domain: a systematic review of the literature, ACM Computing Surveys, vol. 55, 2023.
- A. Creswell, T. White, V. Dumoulin, K. Arulkumaran, B. Sengupta, and A. A. Bharath, Generative adversarial networks: an overview, IEEE Signal Processing Magazine, vol. 35, no. 1, 2018.
- R. Sharma, A. Kumar, and C. Chuah, Turning the blackbox into a glassbox: an explainable machine learning approach for understanding hospitality customer, International Journal of Information Management Data Insights, vol. 1, no. 2, 2021.
- A. S. Wicaksono and A. Afif, Hyper parameter optimization using genetic algorithm on machine learning methods for online news popularity prediction, International Journal of Advanced Computer Science and Applications, vol. 9, no. 12, 2018.
- K. Feng, H. Han, K. Tang, and J. Wang, Statistical tests for replacing human decision makers with algorithms, 2019.
- S. Dai, A. Bechtel, C. Eble et al. , Recognition of peat depositional environments in coal: a review, International Journal of Coal Geology, vol. 219, 2020.
- C. J. Chiu, J. C. Hu, Y. H. Lo, and E. Y. Chang, Health promotion and disease prevention interventions for the elderly: a scoping review from 2015–2019, International Journal of Environmental Research and Public Health, vol. 17, no. 15, 2020.
- H. -M. Chuang and D. -W. Cheng, Conversational AI over military scenarios using intent detection and response generation, Applied Sciences, vol. 12, no. 5, 2022.
- A. Brisson, G. Pereira, R. Prada et al. , Artificial intelligence and personalization opportunities for serious games, Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment, vol. 8, no. 5, 2021.
- P. Pataranutaporn, V. Danry, J. Leong et al. , AI-generated characters for supporting personalized learning and well-being, Nature Machine Intelligence, vol. 3, no. 12, 2021.
- J. M. Valdez Mendia and J. J. A. Flores-Cuautle, Toward customer hyper-personalization experience-a data-driven approach, Cogent Business & Management, vol. 9, no. 1, 2022.
- S. Barnes, Understanding virtual reality in marketing: nature, implications and potential, SSRN Electronic Journal, vol. 52, 2016.
- L. Gao, Y. Chen, B. Zhang, and Y. Gao, A real-time target detection and recognition system for UAVs based on improved YOLOv3 and ST-C3D, IEEE Access, vol. 7, 2019.
- K. Qian, C. Liu, B. Yang, and J. Wang, Hyperpersonalized UAV intelligence based on machine learning, IEEE Transactions on Intelligent Transportation Systems, vol.

12, 2021.
- J. Sha, Y. Chen, Y. Gao, and X. Li, Deep neural networks-based target detection and recognition for UAV, IEEE Access, vol. 9, 2021.
- L. Shamir, J. D. Delaney, N. Orlov, D. M. Eckley, and I. G. Goldberg, Pattern recognition software and techniques for biological image analysis, PLoS Computational Biology, Vol. 6, no. 11, 2010.
- F. Valafar, Pattern recognition techniques in microarray data analysis, Annals of the New York Academy of Sciences, vol. 980, no. 1, 2002.
- M. T. H. Chi, R. Glaser, and M. J. Farr, the Nature of Expertise, Psychology Press, London, UK, 2014.
- W. G. Chase and H. A. Simon, The MIND'S eye in chess, in Visual Information Processing, Elsevier, Amsterdam, The Netherlands, 1973.
- A. D. Groot, Perception and memory versus thought: some old ideas and recent findings, Problem Solving, vol. 30, 1966.
- D. E. Egan and B. J. Schwartz, Chunking in recall of symbolic drawings, Memory & Cognition, vol. 7, no. 2, 1979.
- A. Lesgold, H. Rubinson, P. Feltovich, R. Glaser, D. Klopfer, and Y. Wang, Expertise in a complex skill: diagnosing x-ray pictures, in The Nature of Expertise, pp. 311–342, Lawrence Erlbaum Associates, Inc, Mahwah, NY, USA, 1988.
- S. Hussain, O. Ameri Sianaki, and N. Ababneh, A survey on conversational agents/chatbots classification and design techniques, Web, Artificial Intelligence and Network Applications, vol. 927, 2019.
- H. Shum, X. He, and D. Li, From Eliza to XiaoIce: challenges and opportunities with social chatbots, Frontiers of Information Technology & Electronic Engineering, vol. 19, no. 1, 2018.
- V. L. Rubin, Y. Chen, and L. M. Thorimbert, Artificially intelligent conversational agents in libraries, Library Hi Technology, vol. 28, no. 4, 2010.
- V. Sharma, M. Goyal, and D. Malik, An intelligent behaviour shown by chatbot system, International Journal of New Technology and Research, vol. 3, no. 4, 2017.
- L. C. Klopfenstein, S. Delpriori, S. Malatini, and A. Bogliolo, The rise of bots: a survey of conversational interfaces, patterns, and paradigms, in Proceedings of the 2017 Conference on Designing Interactive Systems, Edinburgh, Scotland, June 2017.
- H. M. Chuang and D. W. Cheng, Conversational AI over military scenarios using intent detection and response generation, Applied Sciences, vol. 12, no. 5, 2022.
- S. Zulaikha, H. Mohamed, M. Kurniawati, S. Rusgianto, and S. A. Rusmita, Customer predictive analytics using artificial intelligence, Singapore Economic Review, vol. 12, 2020.
- F. T. Johnsen, Z. Zielinski, K. Wrona et al. , Application of IoT in military operations in a smart city, in Proceedings of the 2018 International Conference On Military Communications And Information Systems (ICMCIS) , Warsaw, Poland, May 2018.
- A. Akbar, A. Khan, F. Carrez, and K. Moessner, Predictive analytics for complex IoT data streams, IEEE Internet of Things Journal, vol. 4, no. 5, 2017.
- G. Shmueli and O. R. Koppius, Predictive analytics in information systems research, MIS quarterly, vol. 21, 2011.
- R. Saha, M. T. Tariq, and M. Hadi, Deep learning approach for predictive analytics to support diversion during freeway incidents, Transportation Research Record: Journal of the Transportation Research Board, vol. 2674, no. 6, 2020.

- K. L. Rich and M. S. Salter, Bradley m2a3/m3a3 embedded training system (bets): initial user assessment: defense technical information center, Army Research Inst for the Behavioral and Social Sciences Alexandria VA, vol. 14, 2002.
- M. Paisner, M. T. Cox, M. Maynord, and D. Perlis, Goal-driven autonomy for cognitive systems, Proceedings of the Annual Meeting of the Cognitive Science Society, vol. 36, 2014.
- P. Deadman and R. H. Gimblett, A role for goal-oriented autonomous agents in modeling people-environment interactions in forest recreation, Mathematical and Computer Modelling, vol. 20, no. 8, 1994.
- R. Darimont and A. van Lamsweerde, Formal refinement patterns for goal-driven requirements elaboration, ACM SIGSOFT Software Engineering Notes, vol. 21, 1996.
- R. E. Stepp and R. S. Michalski, Conceptual clustering of structured objects: a goal-oriented approach, Artificial Intelligence, vol. 28, no. 1, 1986.
- Y. Li, Deep reinforcement learning: an overview, 2018.
- P. Bourgine, Towards a Practice of Autonomous Systems, towards a practice of autonomous systems. Proceedings of the first European conference on artificial life, vol. 7, 1992.
- T. Zhang, Q. Li, C. Zhang et al. , Current trends in the development of intelligent unmanned autonomous systems, Frontiers of Information Technology & Electronic Engineering, vol. 18, no. 1, 2017.
- D. Harel, A. Marron, and J. Sifakis, Autonomics: in search of a foundation for next-generation autonomous systems, Proceedings of the National Academy of Sciences, vol. 117, no. 30, 2020.
- H. Abbass, J. Harvey, and K. Yaxley, Lifelong testing of smart autonomous systems by shepherding a swarm of watchdog artificial intelligence agents, 2018.
- R. Haddal and N. Hayden, Autonomous Systems Artificial Intelligence and Safeguards, Sandia National Lab. (SNL-NM) , Albuquerque, NM, USA, 2018.
- P. Arcaini, E. Riccobene, and P. Scandurra, Modeling and analyzing MAPE-K feedback loops for self-adaptation, in Proceedings of the IEEE/ACM 10th International Symposium On Software Engineering For Adaptive And Self-Managing Systems, Florence, Italy, May 2015.
- M. Peshkin and J. E. Colgate, Cobots, Industrial Robot: International Journal, vol. 26, no. 5, 1999.
- M. Du, F. Li, G. Zheng, and V. Srikumar, DeepLog: anomaly detection and diagnosis from system logs through deep learning, in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, November 2017.
- Y. Himeur, K. Ghanem, A. Alsalemi, F. Bensaali, and A. Amira, Artificial intelligence based anomaly detection of energy consumption in buildings: a review, current trends and new perspectives, Applied Energy, vol. 287, Article ID 116601, 2021.
- L. Girish and S. K. N. Rao, Anomaly detection in cloud environment using artificial intelligence techniques, Computing, vol. 20, 2021.
- P. V. de Campos Souza, A. J. Guimarães, T. S. Rezende, V. J. Silva Araujo, and V. S. Araujo, Detection of anomalies in large-scale cyberattacks using fuzzy neural networks, AIDS, vol. 1, no. 1, 2020.
- A. Mishra and P. Yadav, Anomaly-based ids to detect attack using various artificial intelligence & machine learning algorithms: a review, in Proceedings of the 2nd

International Conference On Data, Engineering And Applications (IDEA) , Bhopal, India, February 2020.
- M. Taddeo, D. McNeish, A. Blanchard, and E. Edgar, Ethical principles for artificial intelligence in national defence, Philosophy & Technology, vol. 34, no. 4, 2021.
- M. C. Horowitz, when speed kills: lethal autonomous weapon systems, deterrence and stability, Journal of Strategic Studies, vol. 42, no. 6, 2019.
- M. Pestana, Flying unmanned aircraft: a pilot's perspective, Infotech@Aerospace 2011, St. Louis, MI, USA, 2011.
- D. J. K. Hawley, Automation And The Patriot Air And Missile Defense System, Center for a New American Security, Washington, DC, USA, 2017.
- M. R. Chaparro, An Analysis Of Spending Patterns Associated With the PHALANX Close-In Weapon System (CIWS) Program, Defense Technical Information Center, Fort Belvoir, VA, USA, 2003.
- R. Bogue, Robot ethics and law: Part one: ethics, Industrial Robot: International Journal, vol. 41, no. 4, 2014.
- M. C. Haas and S. -C. Fischer, The evolution of targeted killing practices: autonomous weapons, future conflict, and the international order, Contemporary Security Policy, vol. 38, no. 2, 2017.
- J. D. Flanagan and G. W. Luke, Aegis: newest line of navy defense, Johns Hopkins APL Technical DigestBhopal, India, vol. 2, no. 4, 1981.
- J. Haner and D. Garcia, The artificial intelligence arms race: trends and world leaders in autonomous weapons development, Global Policy, vol. 10, no. 3, 2019.
- A. Gomez de Agreda, Ethics of autonomous weapons systems and its applicability to any AI systems, Telecommunications Policy, vol. 44, no. 6, Article ID 101953, 2020.
- A. Wrabel, R. Graef, and T. Brosch, A survey of artificial intelligence approaches for target surveillance with radar sensors, IEEE Aerospace and Electronic Systems Magazine, vol. 36, no. 7, 2021.
- M. S. Hossain, G. Muhammad, and N. Guizani, Explainable AI and mass surveillance system-based healthcare framework to combat COVID-I9 like pandemics, IEEE Network, vol. 34, no. 4, 2020.
- E. Alajrami, H. Tabash, Y. Singer, and M. -T. E. Astal, On using ai-based human identification in improving surveillance system efficiency, in Proceedings of the 2019 International Conference On Promising Electronic Technologies (ICPET) , Gaza, Palestine, October 2019.
- M. T. Nguyen, L. H. Truong, T. T. Tran, and C. -F. Chien, Artificial intelligence based data processing algorithm for video surveillance to empower industry 3. 5, Computers & Industrial Engineering, vol. 148, Article ID 106671, 2020.
- P. Sikora, L. Malina, M. Kiac et al. , Artificial intelligence-based surveillance system for railway crossing traffic, IEEE Sensors Journal, vol. 21, no. 14, 2021.
- N. Aloysius and M. Geetha, A review on deep convolutional neural networks, in Proceedings of the International Conference on Communication and Signal Processing (ICCSP) , Chennai, India, April 2017.
- A. Rego, A. Canovas, J. M. Jimenez, and J. Lloret, An intelligent system for video surveillance in IoT environments, IEEE Access, Vol. 6, 2018.
- B. S. Sagar, S. Niranjan, N. Kashyap, and D. N. Sachin, Providing cyber security using artificial intelligence– a survey, in Proceedings of the 2019 3rd International Conference On Computing Methodologies And Communication (ICCMC) , Erode,

India, March 2019.
- J. Li, Y. Liu, and L. Gu, Ddos attack detection based on neural network, 2010 2nd international symposium on aware computing, vol. 4, 2010.
- D. P. Patil, Artificial Intelligence in Cyber Security, 2016.
- A. Anwar and S. I. Hassan, Applying artificial intelligence techniques to prevent cyber assaults, International Journal of Computational Intelligence Research, vol. 8, 2017.
- M. C. Horowitz, G. C. Allen, E. Saravalle, A. Cho, K. Frederick, and P. Scharre, Artificial Intelligence and International Security, Center for a New American Security, Washington, DC, USA, 2018.
- T. Ko. , A survey on behavior analysis in video surveillance for homeland security applications, in Proceedings of the 2008 37th IEEE Applied Imagery Pattern Recognition Workshop, Washington, DC, USA, October 2008.
- H. Chen and F. Y. Wang, Guest editors' introduction: artificial intelligence for homeland security, IEEE Intelligent Systems, vol. 20, no. 5, 2005.
- H. Chen, F. -Y. Wang, and D. Zeng, Intelligence and security informatics for homeland security: information, communication, and transportation, IEEE Transactions on Intelligent Transportation Systems, vol. 5, no. 4, 2004.
- L. F. Cranor, A Framework For Reasoning About the Human in The Loop, Carnegie Mellon University, Pittsburgh, PA, USA, 2008.
- C. Rhodes, J. Hagen, and M. Westergren, A Strategies-To-Tasks Framework for Planning and Executing Intelligence, Surveillance, and Reconnaissance (ISR) Operations, RAND, Santa Monica, CA, USA, 2007.
- M. Bistron and Z. Piotrowski, Artificial intelligence applications in military systems and their influence on sense of security of citizens, Electronics, vol. 10, no. 7, 2021.
- L. S. Iyer, AI enabled applications towards intelligent transportation, Transport Engineer, vol. 5, Article ID 100083, 2021.
- L. N. Long, S. D. Hanford, O. Janrathitikarn, G. L. Sinsley, and J. A. Miller, A review of intelligent systems software for autonomous vehicles, IEEE Symposium on Computational Intelligence in Security and Defense Applications, vol. 54, 2007.
- Y. Ma, Z. Wang, H. Yang, and L. Yang, Artificial intelligence applications in the development of autonomous vehicles: a survey, IEEE/CAA Journal of Automatica Sinica, vol. 7, no. 2, 2020.
- Z. Liu, H. Jiang, H. Tan, and F. Zhao, An overview of the latest progress and core challenge of autonomous vehicle technologies, MATEC Web of Conferences, vol. 308, 2020.
- X. Li and B. I. Epureanu, AI-based competition of autonomous vehicle fleets with application to fleet modularity, European Journal of Operational Research, vol. 287, no. 3, 2020.
- R. M. Jones, Automated intelligent pilots for combat flight simulation, AI magazine, vol. 16, 1999.
- R. E. Wray, J. E. Laird, A. Nuxoll, D. Stokes, and A. Kerfoot, Synthetic adversaries for urban combat training, AI magazine, vol. 16, 2004.
- W. R. Murray, Intelligent tutoring systems for commercial games: the virtual combat training center tutor and simulation, in Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment, Salt Lake City, Utah, October 2006.
- J. Rosen, B. Hannaford, and R. M. Satava, Surgical Robotics, Springer US, Berlin,

Germany, 2011.
- A. Gondalia, D. Dixit, S. Parashar, V. Raghava, A. Sengupta, and V. R. Sarobin, IoT-based healthcare monitoring system for war soldiers using machine learning, Procedia Computer Science, vol. 133, 2018.
- H. B. Lim, D. Ma, B. Wang, Z. Kalbarczyk, R. K. Iyer, and K. L. Watkin, A soldier health monitoring system for military applications, in Proceedings of the 2010 International Conference on Body Sensor Networks, Singapore, June 2010.
- J. Farroha and B. Farroha, Enabling intelligent battlefield healthcare through secure cyber medicine, Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation 2019, vol. 11015, 2019.
- T. Haidegger and Z. Benyo, Surgical robotic support for long duration space missions, Acta Astronautica, Vol. 63, no. 7–10, 2008.
- R. B. Lim and D. Oleynikov, Robotics in the military, in Robotic-Assisted Minimally Invasive Surgery, S. Tsuda and O. Y. Kudsi, Eds. , Springer International Publishing, Berlin, Germany, 2019.
- M. Reichenbach, T. Frederick, L. Cubrich et al. , Telesurgery with miniature robots to leverage surgical expertise in distributed expeditionary environments, Military Medicine, vol. 182, no. 1, 2017.
- M. E. Rentschler, S. R. Platt, K. R. Berg, J. Dumpert, D. R. Oleynikov, and S. M. Farritor, Miniature in vivo robots for remote and harsh environments, IEEE Transactions on Information Technology in Biomedicine, vol. 12, no. 1, 2008.
- J. Cox and H. Williams, The unavoidable technology: how artificial intelligence can strengthen nuclear stability, The Washington Quarterly, vol. 44, no. 1, 2021.
- J. Johnson, Artificial intelligence in nuclear warfare: a perfect storm of instability? The Washington Quarterly, vol. 43, no. 2, 2020.
- M. Voskuijl, Performance analysis and design of loitering munitions: a comprehensive technical survey of recent developments, Defence Technology, vol. 18, no. 3, 2022.
- J. S. Johnson, Artificial intelligence: a threat to strategic stability, Artificial Intelligence, vol. 24, 2020.
- C. Don, G. Josh, and I. Chris, Environmental Assessment for the MQ-1 Predator and MQ-9 Reaper Unmaned Aircraft System (UAS) Second Formal Training Unit (FTU-2) Beddown, 2009.
- M. Fitzpatrick, Artificial intelligence and nuclear command and control, Survival, Vol. 61, no. 3, 2019.
- L. M. Hough, N. K. Eaton, and M. D. Dunnette, Criterion-related widities of personality constructs and the effect of response distortion on those widities, Journal of applied psychology, vol. 75, 1990.
- A. Anastassov, Artificial intelligence and its possible use in international nuclear security law, BAS Humanities and Social Sciences, vol. 1, 2021.
- R. Legvold and C. F. Chyba, Introduction: the search for strategic stability in a new nuclear era, Dædalus, vol. 149, no. 2, 2020.

Legal Civilization

No.18- Winter 2024

ISSN: 2873-1841
ISSN: 2873-1922

The Place of Artificial Intelligence in the Validation of Arbitration Evidence

Homayoun Mafi, Fatemeh Ghanad, Mohammad Amin Esmaeilpour

Artificial Intelligence in the Criminal Justice System: Leading Trends and Possibilities

Salar Sadeghi

Challenges and Obstacles of Criminal Liability in Robots with Artificial Intelligence Capabilities

Amin Amirian Farsani, Sayyed Mohammad Hosseni

Artificial Intelligence and its Effect on the Judicial System

Amirreza Mahmoudi, Maryam Bahrekazemi

A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence

Amin Hajivand, Ali Khosh Manzar, Saber Sayari Zuhan

Artificial Intelligence in the Criminal Justice System: Leading Trends and Possibilities

Salar Sadeghi

Artificial Intelligence and Legal Liability

Sara Solhchi, Kian Biglarbeigi

Artificial Intelligence and Diplomacy Interaction for Environmental Sustainability

Sobhan Tayebi, Nader Tayebi

Artificial Intelligence Crime an Interdisciplinary Analysis of Foreseeable Threats and Solutions

Zahra Vahabi

Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting

Sara Solhchi

The Use of Artificial Intelligence in Crime Detection and Criminal Investigations; Case Study: Serial Murders

Hamidreza Heydarpour, Mohammad Shahanaghi, Zhila Mehrara

Ethical Permissibility of Using Artificial Intelligence through the Lens of Al-Farabi's Theory on Natural Rights and Prosperity

Mohamad Mahdi Davar

Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges

Yasser Shakeri