هوش مصنوعی و امنیت ملی در اسرائیل

(بخش اول)

لیران عانتبی

فوریه ۲۰۲۱

سوریان
مرکز مطالعات

فهرست مطالب:

هوش مصنوعی و امنیت ملی در اسرائیل

بخش اول

لیران عانتبی
فوریه ۲۰۲۱

هوش مصنوعی و امنیت ملی در اسرائیل: نکات اصلی

هوش مصنوعی (AI) نام جامعی برای اطلاعات و سیستم های رایانه ای است که رفتارهای هوشمندانه ای از خود نشان می دهند یا بینش ها و اطلاعات جدیدی ایجاد می کنند. این یک زمینه تکنولوژیکی پیشگامانه است که می تواند در برنامه های مختلف با کارایی نسبی ، با هزینه مناسب و در مقیاس وسیع اجرا شود. این پیشرفت تکنولوژیکی بر بسیاری از زمینه ها از جمله امنیت ملی تأثیر می گذارد.

برای اسرائیل هوش مصنوعی یک حوزه بسیار مهم است، زیرا اسرائیل در حال حاضر یکی از کشورهای پیشرو در توسعه خویش بوده و با توجه به قدرت اقتصادی تا حد زیادی متکی به صنعت فناوری پیشرفته است؛ با توجه به اینکه این فناوری پتانسیل کمک به مقابله با بسیاری از چالش ها را دارد. AI شامل بسیاری از مناطق ادراکی–تکنولوژیکی از جمله یادگیری ماشینی ، یادگیری عمیق ، بینایی کامپیوتری ، پردازش زبان طبیعی و تعدادی فناوری جانبی به هم پیوسته است. در حوزه امنیت ، هوش مصنوعی در موارد زیر استفاده می شود:

این قابلیت ها و برنامه ها توضیح می دهد که چرا فناوری هوش مصنوعی به طور کلی با امنیت ملی و به طور خاص با امنیت ملی اسرائیل ارتباط دارد.

درک اینکه این فناوری برای قدرت اقتصادی ، انعطاف پذیری امنیتی و توانمندسازی کشورها دارای اهمیت بسیار مهمی است و منجر به یک "رقابت تسلیحاتی" واقعی بین قدرتهای بزرگ یعنی ایالات متحده، چین و روسیه شده است. اکثر کشورهای پیشرو در این زمینه برنامه های ملی را حول هوش

مصنوعی بنا کرده اند و منابع را به رسمیت شناخته اند و اهمیت آن را مورد توجه قرار داده اند. این موضوع می تواند عرصه بین المللی و میدان های نبرد آینده را تحت تأثیر قرار دهد. علاوه بر این نگرانی هایی وجود دارد که پدیده های جدیدی که مانند "آبرجنگ" با هوش مصنوعی پدیدار شده اند، می تواند ثبات عرصه بین المللی را تضعیف کند. علیرغم مزایا و فرصت‌های تکنولوژیک فراوان، هوش مصنوعی چالش‌های مختلفی را برای اسرائیل ایجاد می کند

این مطالعه توصیه های کلیدی زیر را ارائه می دهد:

۱ – اسرائیل باید یک استراتژی ملی برای AI تنظیم و نهادی ایجاد نماید که آن را در سطح ملی مدیریت کند.

۲ – اسرائیل باید یک برنامه چند ساله برای هوش مصنوعی، مانند برنامه موجود در زمینه سایبری ایجاد کند تا بتواند این حوزه را به طور گسترده و عمیق تجزیه و تحلیل، سیاست ملی تخصیص منابع را رهبری و در مورد تحقیق و توسعه، منابع انسانی و سایر موارد تصمیم گیری کند.

۳ – اسرائیل باید یک راه حل ملی برای مسائل زیرساختی (سخت افزار، ابر، اتصال به اینترنت) ایجاد کند و یک بودجه جاری تخصیص دهد، زیرا جامعه امنیتی بر خلاف صنعت غیرنظامی، نیازهایی دارد به عنوان مثال به دلیل مسائل مربوط به اطلاعات طبقه بندی شده و سایر محدودیت های امنیتی که معمولاً اجازه استفاده از زیرساخت‌های تجاری را نمی‌دهد.

۴ – اسرائیل باید فوراً ادغام هوش مصنوعی را در فناوری امنیتی که در آن اسرائیل اکنون از مزیت نسبی برخوردار است (به عنوان مثال میدان هواپیماهای بدون سرنشین)، به منظور تولید چند برابر قدرت، در نظر بگیرد.

۵ – بخش دفاع باید کارکنان غیرفناوری از جمله در سطوح ارشد را برای آشنایی با AI، محدودیت‌ها و توانایی‌های آن آموزش دهد تا پرسنل آن بتوانند در تصمیم‌گیری در حوزه AI مشارکت و فعالیت بیشتری داشته باشند.

۶– سازمان‌های امنیتی مختلف باید مدیریت پرسنل را در سطح سیستم، از جمله تعیین نقش‌ها، استانداردها و آموزش‌های مشترک، انتقال پرسنل بین سازمان‌ها، علاوه بر ارائه انگیزه‌ها و بودجه برای جذب و نگهداری افراد مستعد به منظور از دست ندادن آنها با جذب صنعت غیرنظامی، در نظر بگیرند.

۷– اسرائیل باید حوزه های تحقیقاتی را که نیاز به تامین مالی دارند در بودجه دولتی–امنیتی تعریف کند، با توجه به اینکه برای امنیت ملی مهم هستند و در غیر این صورت در نظر گرفته نمی شوند.

۸– اسرائیل باید به جای تکیه بر مطالعات آکادمیک که فقط در سطح نظری هستند و در زمینه های مورد نیاز نهاد امنیتی ناکافی هستند یا در مناطق مورد نیاز سازمان امنیتی آزمایش نشده اند باید مطالعات جامعی را توسط نهاد امنیت ملی انجام دهد.

۹– اشتراک دانش در تشکیلات امنیتی اسرائیل بسیار مهم است. بنابراین، اسرائیل باید مکانیسم‌هایی را بین سازمان‌های امنیتی مختلف ایجاد کند تا از کارهای تکراری جلوگیری نماید، شکاف‌های بین سازمان‌ها را پر و راه‌حل‌ها را هماهنگ کند.

۱۰– اسرائیل باید ترکیبی از مکانیسم‌ها را برای تشویق سرمایه‌گذاری در مناطق هوش مصنوعی که تأثیر مثبتی بر امنیت ملی دارد، در نظر بگیرد. به موازات آن، دولت باید برای پیشبرد اقتصاد در این زمینه، هزینه های خود را برای هوش مصنوعی در مناطق غیرنظامی افزایش دهد.

۱۱– اسرائیل باید سرمایه‌گذاری‌های خود را در تحقیق و توسعه در زمینه تیم‌سازی انسان و ماشین برای تأسیسات امنیتی افزایش دهد، با این درک که علی‌رغم ماهیت بسیار خودمختار سیستم‌ها، برخی از عناصر کنترل انسانی پابرجا خواهند ماند.

در این زمینه، پیشنهاد می‌شود تا زمانی که اعتبار و ایمنی فناوری به خوبی تثبیت شده و به جنبه‌های اجرایی و قانونی پرداخته شود، تحقیق و توسعه AI در حوزه‌هایی که افراد را حمایت می‌کنند به جای آن‌هایی که جایگزین آن‌ها هستند، در اولویت قرار گیرد.

۱۲– زمینه پردازش زبان عبری باید از جمله در برنامه هایی مانند پردازش زبان طبیعی (NLP)، گفتار به متن، متن به سرعت و غیره توسعه یابد.

۱۳– اسرائیل باید هنجارها و اصولی را برای تضمین ایمنی و مسئولیت در استفاده از هوش مصنوعی در داخل تشکیلات امنیتی با هدف اتخاذ همان تصمیمات در نهادهای غیر نضامی ایجاد کند.

۱۴– اسرائیل باید یک کد اخلاقی برای استفاده از AI در تشکیلات امنیتی به طور کلی و در چارچوب تیم های انسانی–ماشین به طور خاص ایجاد کند.

۱۵– برای مقاصد قانونی، اخلاقی، ایمنی و فراوانی، اسرائیل باید تصمیم بگیرد که کدام سیستم ها باید مکانیسم های نظارت و کنترل انسانی را حفظ کنند.

۱۶– اسرائیل باید در سطح ملی آنچه را که در زمینه‌های AI و علوم داده در سطح بین‌المللی رخ می‌دهد، از جمله همه آنچه که به کنوانسیون‌ها و استانداردها مربوط می‌شود، نظارت کند تا مزیت اسرائیل حفظ شود.

۱۷– اسرائیل باید برای تقویت تحقیقات و همکاری مشترک با سایر کشورها اقدام کند. اسراییل باید با ائتلافی از کشورها در میدان هوش مصنوعی همکاری و حتی آن را رهبری کند، همانطور که در زمینه اطلاعات نظامی، دفاع هوایی و سایر زمینه ها این کار را می کند.

۱۸– اسرائیل باید به ابتکارات بین‌المللی اعم از امنیتی یا غیرنظامی بپیوندد و حتی رهبری آن را بر عهده بگیرد تا عناصر سرکش را از دستیابی به دستاوردها در زمینههوش مصنوعی محروم کند.

۱۹– اسرائیل باید استانداردها و فرآیندهای صادرات سیستم های AI، از جمله مجوزهای صادراتی مرتبط با امنیت را بررسی کند.

۲۰– اسرائیل باید تصمیماتی اتخاذ کند که قدرت صنعت و توانایی آن را برای عمل حفظ نماید و همچنین صادراتی را که می تواند به امنیت اسرائیل آسیب برساند محدود سازد.

خلاصه جامع

هوش مصنوعی و اهمیت آن برای امنیت ملی اسرائیل

هوش مصنوعی (AI) نامی کلی برای سیستم‌های رایانه‌ای مبتنی بر داده است که قادر به تولید دانش و بینش‌های جدید از طریق توانایی‌هایی مانند درک، استدلال و ادراک هستند که تاکنون به عنوان توانایی‌های منحصر به فرد انسان تلقی می‌شد. هوش مصنوعی این قابلیت ها را از طریق برنامه های متنوعی که نسبتا کارآمد، دارای قیمت مناسب و در مقیاس وسیع هستند ممکن می سازد.

اتوماسیون این توانایی‌های انسانی فرصت‌های جدیدی ایجاد می‌کند که بر بسیاری از حوزه‌ها از جمله امنیت ملی تأثیر می‌گذارد. هدف از این یادداشت، ارائه موضوع پیچیده هوش مصنوعی به عموم مردم و به طور خاص تصمیم گیرندگان است. با توجه به چالش‌ها و فرصت‌هایی که هوش مصنوعی تجسم می‌کند، این یادداشت توصیه‌هایی برای سیاست مورد نظر اسرائیل در این زمینه ارائه می‌کند.

هوش مصنوعی یک حوزه فناوری بسیار مهم برای اسرائیل به شمار می رود، زیرا اسرائیل در حال حاضر یکی از کشورهای پیشرو در توسعه آن است. هوش مصنوعی همچنین این پتانسیل را دارد که به اسرائیل کمک کند تا با چالش های زیاد پیش روی خود کنار بیاید. لازم به ذکر است اسرائیل تقریباً به طور کامل فاقد منابع طبیعی بوده و قدرت اقتصادی آن به شدت به صنعت فناوری پیشرفته متکی است.

اهمیت هوش مصنوعی افزایش یافته است زیرا هوش مصنوعی قادر به کمک به رشد اقتصادی، یافتن درمان برای بیماری ها و بهبود سیستم های بهداشتی، بهبود کارایی و ایمنی حمل و نقل، تشویق بهره‌وری انرژی، بهبود درک پدیده های آب و هوایی و شاید حتی از طریق بازدارندگی به ثبات مبتنی بر صلح در عرصه بین المللی منجر شود. بنابراین، ضروری است که تصمیم گیرندگان اسرائیل با این حوزه آشنا باشند و فرصت ها و چالش های آن را مطالعه کنند و در نتیجه قادر به تدوین یک سیاست مناسب و اطمینان از اجرای آن با سرعتی باشد که با رویدادهای منطقه ای و بین المللی همگام باشد؛ ضمن اینکه رقابت فزاینده در عرصه بین المللی را نیز در نظر می گیرد.

دامنه های مختلف هوش مصنوعی و کاربردهای امنیتی آن

هوش مصنوعی شامل تعداد زیادی زیر دامنه، از جمله یادگیری ماشینی، یادگیری عمیق، بینایی کامپیوتر، پردازش زبان طبیعی (NLP) است؛ و همچنین تعدادی از فناوری های به هم پیوسته مانند اینترنت اشیاء (اشیای مختلفی با اتصال به اینترنت و توانایی انتقال و دریافت اطلاعات و کمک در انجام برخی اقدامات کار می کنند. به ترکیب اینترنت با چنین ابزاری که قابلیت استفاده از آن را دارد اینترنت اشیاء می گویند)

و فن آوری های دوگانه، که هم در عرصه های غیرنظامی و هم در عرصه های امنیتی خدمت می کنند. این حوزه‌ها و سایر حوزه‌ها، پایه‌هایی برای کاربردهای متنوع در زمینه‌های مختلف، از جمله تجارت، پزشکی، دانشگاه و حمل‌ونقل و همچنین بخش امنیتی هستند.

در بخش امنیتی، فناوری‌های هوش مصنوعی (AI) توسط اطلاعات نظامی در سیستم‌هایی استفاده می‌شوند که قادر به بررسی حجم عظیمی از داده‌های ویدیویی و شناسایی اهداف هستند. برنامه های لجستیکی که باعث بهبود و صرفه جویی در منابع می شوند. رانندگی خودکار که در بخش امنیتی نیز پتانسیل دارد، همانطور که در حوزه غیرنظامی این پتانسیل وجود دارد. سیستم های تسلیحاتی تمام اتوماتیک که امکان افزایش دقت و کاهش خطر را برای سربازانی که از آنها استفاده می کنند را فراهم می کند. سیستم‌های برنامه‌ریزی و پشتیبانی برای تصمیم‌گیری و شبیه‌سازی‌ها که فرآیندهای برنامه‌ریزی و تصمیم‌گیری را قبل از انجام مأموریت‌ها، بر اساس مقادیر فراوانی از داده‌ها که قبلاً قابل تجزیه و تحلیل نبود، بهبود و کاهش می‌دهند. سیستم های فرماندهی و کنترلی که با ارجاع متقابل و تجزیه و تحلیل آنها در حین انجام مأموریت ها در زمان واقعی و بهبود نتایج با هدایت و تغییر تصمیمات در یک حلقه مداوم، با داده های بزرگ از منابع مختلف مقابله می کنند. جنگ سایبری، حفاظت سایبری، و طیف الکترومغناطیسی – که در حال حاضر در استفاده از هوش مصنوعی پیشرو است – برای مدیریت حجم زیادی از داده ها و سرعت های فراتر از توانایی انسان برای اهداف حمله و حفاظت؛ پیش‌بینی، هشدار، و پیشگیری یا مدیریت بلایا که به استفاده از پایگاه‌های اطلاعاتی عظیم یا حسگرهای مختلف برای جمع‌آوری اطلاعات و دستیابی به بینش‌هایی بستگی دارد که با روش‌های دیگر به دست نمی‌آیند. علاوه بر این، هوش مصنوعی به فناوری های دیگری برای توسعه و استفاده از آن نیاز دارد. برای مثال، هوش مصنوعی برای آموزش برنامه‌های هوش مصنوعی به داده‌های بزرگ وابسته است. سپس برنامه‌ها می‌توانند عملیات مستقلی را روی فایل‌های داده‌های جدیدی که قبلاً در معرض آن قرار نگرفته‌اند، انجام دهند. نمونه‌های دیگر شامل فناوری‌هایی هستند که به عنوان زیرساخت برای فعال‌سازی برنامه‌های هوش مصنوعی، مانند محاسبات ابری، محاسبات ابری و کوانتومی، یا شبکه‌های نسل پنجم، که برای انتقال سریع داده‌ها و بهبود عملکرد سیستم‌های مبتنی بر هوش مصنوعی مورد نیاز هستند، عمل می‌کنند.

هوش مصنوعی از فناوری های مختلفی نیز پشتیبانی می کند. به عنوان مثال، از "Swarms(گروه ها)" پشتیبانی می نماید که از هماهنگی پیشرفته برای راه اندازی سیستم ها یا فناوری ها و کاربردهای مختلف در زمینه انسان استفاده می کند مانند تعامل ماشین و همچنین مغز و رابط ماشین، که برای کوتاه کردن زمان بین دریافت اطلاعات و تصمیم گیری یک فرد و انتقال آن به ماشین طراحی شده است.

هوش مصنوعی از فناوری های مختلفی نیز پشتیبانی می کند. به عنوان مثال، از " گروه ها " پشتیبانی می کند که از هماهنگی پیشرفته برای راه اندازی سیستم ها یا فناوری ها و کاربردهای مختلف در زمینه انسان مانند تعامل ماشین و همچنین مغز استفاده می کند؛ رابط ماشین، که برای کوتاه کردن زمان بین دریافت اطلاعات و تصمیم گیری شخص و انتقال آن به ماشین طراحی شده است.

این قابلیت‌ها و برنامه‌های کاربردی، رابطه بین فناوری هوش مصنوعی و امنیت ملی به طور کلی و امنیت ملی اسرائیل را به طور خاص، با توجه به مفهوم امنیت ملی و فراتر از آن و استراتژی ارتش اسرائیل که در سال ۲۰۱۵ صادر شد، تقویت می‌کند. بنابراین، مدیریت صحیح حوزه هوش مصنوعی پتانسیل بالایی برای حفظ و ارتقای امنیت ملی اسرائیل دارد و با توجه به رقابت بین المللی این حوزه در حال رشد از اهمیت بیشتری برخوردار است.

مسابقه تسلیحاتی و رقابت فناوری در هوش مصنوعی بین قدرت های جهانی

از سال ۲۰۱۴، رهبران بسیاری از کشورها از جمله قدرت های بزرگ فناوری و اقتصادی به اهمیت هوش مصنوعی برای تقویت کشورهای خود در کنار پیشرفت های صنعتی و فناوری پی برده اند. به عنوان مثال، چین، ایالات متحده و برخی از کشورهای اتحادیه اروپا قبلاً برنامه های ملی در زمینه هوش مصنوعی ایجاد کرده اند و منابع و توجه خود را به این حوزه اختصاص داده اند. بیشتر استراتژی‌ها بر اهمیت هوش مصنوعی برای رشد اقتصادی و علاوه بر این، برای حفظ امنیت ملی، از جمله کاربردهای نظامی تأکید می کنند.

یکی از حوزه‌های در حال توسعه در این مسابقه تسلیحاتی، سیستم‌های تسلیحاتی خودکار (AWS) است که قادر به مکان‌یابی، شناسایی و حمله به یک هدف بدون دخالت انسان است و ایالات متحده در این زمینه و همچنین حوزه «Swarms» رهبری را در دست دارد. به طور مشابه، چین در بسیاری از صنایع غیرنظامی مرتبط با هوش مصنوعی تا حدی به دلیل مدیریت متمرکز آن و به دلیل کنترل دولت بر شرکت های غیرنظامی پیشرو است.

علاوه بر این، چین همچنین دارای پایگاه‌های اطلاعاتی پر از اطلاعات در مورد جمعیت خود است که در یک دوره طولانی جمع‌آوری کرده است. چین توانست به دلیل نادیده گرفتن حقوق بشر و حقوق شهروندی این اطلاعات را جمع آوری کند. متقابلا در نتیجه چین در جذب کارشناسان و شرکت‌هایی که از سرقت الگوریتم‌ها می‌ترسند و نگران پیامدهای اخلاقی استفاده از فناوری هوش مصنوعی هستند، مشکل دارد. اتحادیه اروپا، بریتانیا و روسیه در زمینه هوش مصنوعی نسبتاً از چین و ایالات متحده عقبتر هستند

علاوه بر این، هوش مصنوعی می‌تواند از راه‌های دیگری بر عرصه بین‌المللی تأثیر بگذارد و این باید هنگام تدوین سیاست در این زمینه مورد توجه قرار گیرد. اینها شامل خطرات مربوط به ایمنی هوش مصنوعی است: اثرات نامطلوب بر سایر زمینه های تسلیحاتی از جمله : سلاح های هسته ای، خطر "هایپروار(آبَر جنگ) "، تأثیر بر موازنه قوا و احتمال یا خطر یک نظم جدید جهانی؛ شکاف فزاینده بین کشورهای در حال توسعه و توسعه یافته یا به جای آن، بهبود کیفیت زندگی و ثبات در عرصه بین المللی از طریق بازدارندگی.

نمونه‌های آزمایشی تاریخی مسابقات تسلیحاتی این موضوعات را روشن می‌کنند، از جمله مورد نسبتاً جدید سیستم‌های تسلیحاتی خودکار (AWS)، که نشان می‌دهد سرعت قوانین بین‌المللی محدود کننده فناوری‌های نوآورانه بسیار کند است. توسعه فناوری در این زمینه در نهایت تصمیم گیرندگان کشورهای مختلف را با چالش های اخلاقی، قانونی و مقرراتی مواجه خواهد کرد و احتمال حل به موقع آنها از طریق دادگاه های بین المللی و همکاری بین کشورها بسیار اندک است.

چالش ها در زمینه هوش مصنوعی و توصیه هایی برای مدیریت آنها

با توجه به رقابت بین المللی در توسعه هوش مصنوعی و با وجود مزایا و فرصت های فراوان آن، این فناوری چالش های مختلفی را برای اسرائیل ایجاد می کند که توجه تصمیم گیرندگان در این زمینه را می طلبد:

- **مسائل فنی،** از جمله مسائل توسعه، مشکل در تطبیق فناوری غیرنظامی با استفاده نظامی، چالش های استانداردسازی در سخت افزار و انرژی، کمبود داده های خام؛ مشکل در توضیح نتایج یک سیستم هوش مصنوعی، چرا که این سیستم یک "جعبه سیاه" است.
- **سازمانی،** شامل نیاز به بودجه های تعیین شده، سرمایه گذاری و مدیریت منابع انسانی، اسرائیل یک کشور کوچک با منابع محدود است.
- **استفاده،** از جمله مشکلات در تطبیق سرعت محیط یا افرادی که از این سیستم ها استفاده می کنند با قابلیت های بالای آن، مشکل سیستم های هوش مصنوعی برای انطباق با محیط های جدید که در آن آموزش ندیده اند، نگرانی های ایمنی و قابلیت اطمینان؛ چالش های اخلاقی؛ سوگیری بر اساس اطلاعات ارائه شده و استفاده از هوش مصنوعی برای تولید «اخبار جعلی» (fake news) که معتبر به نظر می رسد.
- **امنیتی و سیاسی؛** که شامل مسابقه تسلیحاتی بین المللی می شود، مشکل در موافقت و به کارگیری رویه های کنترل تسلیحات در این زمینه، وابستگی به هوش مصنوعی که ایجاد خواهد شد،

علاوه بر این که آنها در معرض حملات سایبری یا دستکاری های دیگر قرار خواهند گرفت. چالش‌های «نرم» که با این وجود به طور قابل‌توجهی گاه به‌طور غیرمستقیم بر امنیت ملی تأثیر می‌گذارند نیز به این دسته تعلق دارند. اینها شامل مسائل اخلاقی و قانونی است. اثرات بر بازار کار و اشتغال؛ پتانسیل نابرابری شدید در توزیع منابع یک کشور، که می تواند ثبات یک کشور را تضعیف کند.

این عوامل به توصیه های ارائه شده در اینجا کمک کرده اند. هدف از این توصیه‌ها حفظ و افزایش توانایی‌های اسرائیل در زمینه هوش مصنوعی، استفاده از این قابلیت‌ها در میان نهادهای مختلف امنیتی و آمادگی برای مقابله با چالش‌های ناشی از این فناوری، مانند استفاده از هوش مصنوعی توسط دشمنان اسراییل و یا در قالب یک مسابقه تسلیحاتی بین المللی است. توصیه های اصلی عبارتند از:

- **سازمانی:** تدوین استراتژی ملی هوش مصنوعی و ایجاد ارگانی که آن را در سطح ملی مدیریت کند، با تشخیص اهمیت آن و ضرورت داشتن مدیریت ملی در این زمینه ضروری است. این علاوه بر تشکیل یک برنامه چند ساله در زمینه هوش مصنوعی است، ایجاد و تقویت مدل‌های ساختاری در تأسیسات امنیتی، که پاسخگویی و انعطاف‌پذیری را ممکن می‌سازد. تشکیل ارگان‌های مشترک، روش‌های عمل و فضاهای کاری مشترک برای متخصصان سازمان‌های امنیتی مختلف که در این زمینه دخیل هستند و سایر نهادهایی که بر امنیت ملی اسرائیل تأثیر می‌گذارند.
- **تحقیق و توسعه:** لازم است ادغام فوری هوش مصنوعی در فناوری های مرتبط با امنیت آزمایش شود(مانند هواپیماهای بدون سرنشین) برای تولید افزایش ضریب قدرت بر اساس دانش و سرمایه گذاری های موجود مناطقی که اسرائیل در آنها مزیت نسبی دارد. اسرائیل باید در تحقیقات جامع توسط نهادهای دفاعی سرمایه گذاری و از تکیه انحصاری به بخش دانشگاهی در این زمینه خودداری کند. دولت اسرائیل باید تحقیق و توسعه هوش مصنوعی را در مناطقی که مزیت دائمی ایجاد می کند، در اولویت قرار دهد. دولت همچنین باید توسعه برنامه‌های امنیتی مبتنی بر فناوری‌های هوش مصنوعی غیرنظامی موجود، توسعه قابلیت‌های دفاعی هوش مصنوعی برای محافظت و حمله و موارد دیگر را ارتقاء دهد.
- **بودجه بندی و ایجاد زیرساخت ملی:** اسرائیل باید راه حلی جامع برای فقدان آشکار زیرساخت ملی در زمینه هوش مصنوعی ایجاد کند. دولت باید برای هر چیزی که مربوط به این رشته است بودجه مشخصی را تخصیص دهد و حوزه های تحقیقاتی را که توسط دولت تامین مالی می شود، تعریف کند.
- **منابع انسانی:** مدیریت منابع انسانی باید در سطح سیستمی مورد بررسی قرار گیرد و نه در سطح درون سازمانی که در حال حاضر مدیریت می شود. اسرائیل باید ادغام تأسیسات امنیتی در برنامه های

آموزشی موجود و ایجاد برنامه های آموزشی جدید را بررسی کند. دولت باید پرسنل غیرفناوری را تربیت کند تا با این رشته، توانایی ها و محدودیت های آن آشنا باشند.

- **اخلاق، قوانین، استانداردها و رویه‌های ایمنی:** اسرائیل باید ظرفیت ایجاد استانداردها و کنترل‌های ایمنی هوش مصنوعی را قویاً ایجاد کند. توسعه هنجارها و اصول ایمنی و مسئولیت در استفاده از هوش مصنوعی در تأسیسات امنیتی؛ باید یک کد اخلاقی در رابطه با هوش مصنوعی و به ویژه برای تیم‌های انسان و ماشین در سازمان امنیتی تعریف شود. تعریف طبقه‌بندی و استانداردهای سیستم‌های هوش مصنوعی برای اهداف مشترک، ایمنی و ظرفیت انجام بحث‌های مشترک بین ارگان‌ها و سازمان‌های مختلف، علاوه بر فرآیندهای سازمان‌یافته در مقابل صنعت؛ و برای تعریف استانداردهای مربوط به تحقیقات در زمینه انسان و ماشین.
- **اشتراک دانش:** توصیه اصلی افزایش اشتراک دانش در نهاد امنیتی اسرائیل با ایجاد مکانیسم های ثابت برای جلوگیری از تکرار و ایجاد راه حل های هماهنگ است که به دلیل بودجه و پرسنل محدود در این زمینه ضروری است. فرآیندهای تسهیم دانش در حال انجام با سایر سازمان ها نیز باید ایجاد شود.
- **جنبه های بین المللی، دیپلماتیک و اطلاعاتی:** پیگیری تحولات بین المللی در زمینه هوش مصنوعی برای تطبیق با سیاست اسرائیل و حفظ مزیت موجود در این زمینه ضروری است. تقویت تحقیقات و همکاری مشترک بین اسرائیل و سایر کشورها؛ و بررسی اینکه آیا، چگونه و کدام کاربردهای هوش مصنوعی اسرائیل باید از طریق کنوانسیون های بین المللی محدود شود.

در پایان، اسرائیل باید سیاستی در زمینه هوش مصنوعی تدوین کند تا بتواند به دستاوردهای قابل توجهی در این زمینه دست یابد و اجازه ندهد چنین حوزه مهم و چالش برانگیزی تنها تحت تأثیر نیروهای بازار قرار گیرد.

با توجه به سرعت بالای توسعه و رقابت بین المللی، سرعت تصمیم گیری، میزان منابع تخصیص یافته برای اجرای تصمیمات و کنترل و مدیریت بسیاری از وظایف در این زمینه، همگی مهم هستند. مدیریت این مسائل با هم تأثیر مهمی بر قدرت آینده اسرائیل از جمله اقتصاد و توانایی آن برای حفظ و بهبود امنیت ملی آن خواهد داشت.

پیشگفتار:

هوش مصنوعی – چرا حالا؟

هوش مصنوعی (AI) نام گسترده ای برای شبیه سازی رفتار هوشمند انسان با استفاده از اطلاعات و سیستم های رایانه ای یا ایجاد دانش و بینش هایی است که قبلاً هرگز وجود نداشته است. این فناوری مهم و پیشگامانه است. برای اولین بار در تاریخ، نرم‌افزار می‌تواند توانایی‌هایی مانند درک، استدلال، ادراک یا برقراری ارتباط را که به طور سنتی منحصراً انسانی در نظر گرفته می‌شد با هزینه کم و در مقیاس وسیع، با استفاده از برنامه‌های کاربردی مختلف و استفاده‌های متفاوت انجام دهد. مکانیزه شدن این توانایی‌های انسانی فرصت‌های جدیدی را ایجاد می‌کند و بر بسیاری از حوزه‌ها از جمله امنیت ملی تأثیر می‌گذارد.

قلمرو هوش مصنوعی بدون شک یک انقلاب واقعی است، پس از آن که برای چندین دهه به کندی توسعه یافته و گاهی اوقات حتی در مسیر خود متوقف شده است قابلیت‌های سخت‌افزاری جدید و همچنین در دسترس بودن پایگاه‌های اطلاعاتی، خدمات رایانش ابری و سایر قابلیت‌ها، این انقلاب را ممکن ساخته است و چیزی را که زمانی فقط تئوری یا حتی غیرممکن تلقی می‌شد، امکان‌پذیر کرده است. این فناوری محصولات و خدماتی مانند وسایل نقلیه خودران، تشخیص‌های پزشکی رایانه‌ای، تعامل صوتی به زبان طبیعی بین رایانه‌ها و افراد، سیستم‌های برنامه‌ریزی و بهینه‌سازی و توصیه‌هایی برای خدمات و محصولات بر اساس اقدامات قبلی را امکان‌پذیر کرده است.

کارشناسان ارزیابی می کنند که هوش مصنوعی می تواند نرخ رشد اقتصادی را افزایش دهد. یافتن درمان برای بیماری ها و بهبود سیستم های بهداشتی؛ افزایش کارایی و ایمنی حمل و نقل؛ تشویق بهره وری انرژی و بهبود درک پدیده های آب و هوایی؛ و شاید حتی از طریق بازدارندگی به ثبات مبتنی بر صلح در عرصه بین المللی منجر شود. کارشناسان تخمین می زنند که هوش مصنوعی زمانی که کنترل انواع اقدامات آشنا را به دست گرفته و طیف گسترده ای از قابلیت ها و برنامه های کاربردی جدید را فعال کند، زندگی ما را غیرقابل تشخیص تغییر خواهد داد. کسانی که امکان سنجی هوش مصنوعی عمومی را ارزیابی می کنند، معتقدند که قابلیت های آن در همه زمینه ها از توانایی های انسان ها فراتر خواهد رفت. بنابراین، شرکت‌ها و کشورها برای دستیابی به قابلیت‌هایی در زمینه هوش مصنوعی رقابت می‌کنند که هم در حوزه‌های اقتصادی و هم در حوزه بین‌المللی تأثیرگذار است.

همانطور که هوش مصنوعی به حوزه‌ها و دامنه های جدید حرکت می‌کند و پتانسیل آن رشد می کند، شکاف بین کسانی که در مسابقه پیشرو هستند و کسانی که عقب مانده‌اند بیشتر می‌شود. علاوه بر این، این رشته باعث مبارزه برای استعداد، دانش و توانایی تولید ارزش یا شکستن مرزهای جدید شده است.

هوش مصنوعی در کنار اینترنت اشیا و کلان داده، انقلاب صنعتی جدیدی را در بزرگترین مقیاس تاریخ ایجاد خواهد کرد. این انقلاب جدید در خدمات و محصولات مختلفی قابل مشاهده است که با استفاده از هوش مصنوعی تغییر اساسی کرده اند.

بسیاری از کشورها و سازمان‌ها متوجه شده‌اند که هوش مصنوعی دیگر یک فناوری آینده یا آینده‌نگر نیست. بلکه اکنون یک نیاز اساسی است. رهبران سازمان ها و کشورها سرمایه گذاری، توسعه و اجرای استفاده از هوش مصنوعی را تشویق می کنند.

این توسعه در برخی موارد باعث رقابت و در برخی دیگر به یک مسابقه تسلیحاتی واقعی منجر شده است. حوزه امنیت تأثیر برنامه های کاربردی هوش مصنوعی را احساس کرده است. هوش مصنوعی به طور گسترده در کاربردهای نظامی استفاده می شود و بر توانایی تولید یا حفظ برتری نظامی تأثیر می گذارد. این امر در استفاده از فناوری‌های هوش مصنوعی در هوش نظامی، رباتیک پیشرفته، جنگ سایبری و حفاظت سایبری مشهود است که اکنون در استفاده از هوش مصنوعی پیشگام هستند. اسرائیل یکی از کشورهای پیشرو در توسعه هوش مصنوعی در جهان است. این موقعیت با تعداد شرکت‌های نوپا در اسرائیل و شرکت‌های بین‌المللی که مراکز توسعه را در اسرائیل ایجاد می‌کنند، آشکار می‌شود.هوش مصنوعی نه تنها بر جنبه های اقتصاد اسرائیل بلکه بر امنیت ملی آن نیز تأثیر می گذارد.اسرائیل که با طیف گسترده ای از چالش های امنیتی دست و پنجه نرم می کند، چندین دهه است که برای تضمین و حفظ امنیت ملی خود به فناوری پیشرفته متکی بوده است.

علاوه بر این، با توجه به اینکه اسرائیل منابع طبیعی زیادی (به جز مقدار معینی گاز) ندارد، اقتصاد آن بر پایه صنعت فناوری پیشرفته، صادرات نظامی و سایر مناطق باریک استوار است. هوش مصنوعی توانایی مقابله با این چالش‌ها و چالش‌های آینده را ارائه می‌کند، در حالی که اسرائیل را قادر می‌سازد تا وضعیت اقتصادی، بین‌المللی و امنیتی خود را حفظ کند و شاید حتی آن را بهبود بخشد.

بنابراین اسرائیل باید برای دستیابی به این دستاوردها سیاستی در زمینه هوش مصنوعی تدوین کند و نباید چنین حوزه مهم و چالش برانگیزی را تنها تحت تأثیر نیروهای بازار قرار دهد. سرعت تصمیم گیری در مورد موضوع، از جمله دامنه منابع تخصیص یافته و نحوه نظارت و مدیریت این حوزه، با توجه به توسعه سریع فناوری، نفوذ آن و رقابت بین المللی، حیاتی است. بنابراین، دولت اسرائیل نمی تواند تأخیر را تحمل کند، زیرا شکست در این زمینه ممکن است منجر به عواقب شدید و هزینه های زیادی شود.

بسیاری در تدوین مواد، دانش و توصیه هایی که در این مطالعه ظاهر می شوند، شرکت کرده اند. با این حال، تنها من به عنوان نویسنده، مسئول هر ادعا یا خطایی هستم که در اینجا دیده می شود. به همین مناسبت، مایلم از موسسه مطالعات امنیت ملی (INSS) که این تحقیق را تسهیل و منابع لازم

را تخصیص داد، و به ویژه رئیس ژنرال اودی دکل به دلیل کمک و حمایت گسترده او از این تحقیق و انتشار آن، به دلیل درک اهمیت موضوع تشکر کنم. از اعضای کمیته تخصصی حرفه ای که برای هدف این مطالعه گرد هم آمدند و دانش، زمان و انرژی خود را در این تحقیق سهیم کردند، تشکر می کنم: آقای اوری الیابایف، مشاور در زمینه هوش مصنوعی و بنیانگذار Machine & Deep Learning، اسرائیل؛ سرتیپ ژنرال ایتای برون، معاون مدیر INSS; الیشا استوین، رئیس بخش اسکن هورایزون در وزارت اطلاعات؛ خانم گیل برام، مدیر تحقیقات در کارگاه علمی، فناوری و امنیت، یووال نعمان، دانشگاه تل آویو؛ سرهنگ دوم چن ویتز، افسر ارشد داده، شعبه مخابرات ارتش اسرائیل، آقای تال، رئیس گروه علم داده، دفتر نخست وزیری؛ سرهنگ دوم اران دهان، رئیس بخش هوش مصنوعی، اداره توسعه تسلیحات و زیرساخت های فناوری؛ دکتر شموئیل اون، پژوهشگر ارشد، INSS; ژنرال دکتر ساسون حداد، پژوهشگر ارشد، رئیس برنامه اقتصاد و امنیت ملی، INSS. و اوری فریدمن، کارآموز در برنامه فناوری های پیشرفته و امنیت ملی، که در بررسی و ادغام مطالب این یادداشت کمک کردند.

تشکر ویژه از اعضای کمیته سرهنگ بواز زالمانوویچ، رئیس سابق شاخه برنامه درسی پایه بخش عملیات ارتش اسرائیل و درور بن داوید، رئیس AI در Matrix, Ltd.، که علاوه بر همه موارد دیگر، در مورد نسخه‌های یادداشت اظهار نظر کردند و کمک زیادی به بهبود سند نهایی کردند.

همچنین از دکتر انات کورز، محقق ارشد و مدیر تحقیقات INSS و دکتر گالیا لیندن استراوس، محقق ارشد INSS که تلاش زیادی برای ویرایش و بهبود این سند انجام دادند و دکتر الا گرینبرگ برای ویرایش زبانی به زبان انگلیسی و خانم نوام ران، مسئول انتشارات INSS تشکر می کنم.

لیران عانتبی

اکتبر ۲۰۲۰

معرفی

در این مرحله، تغییرات تکنولوژیک با سریعترین روند در تاریخ اتفاق افتاده و برخی از آنها تأثیر بسیار مهمی بر کشورها، جوامع و افراد داشته است. در میان این تغییرات، هوش مصنوعی (AI) یک حوزه فناوری در حال رشد است که تقریباً بر تمام جنبه های زندگی تأثیر انقلابی داشته است. هوش مصنوعی مفهومی است که به طور کلی به سخت افزار یا نرم افزار یا یکپارچه سازی اشاره دارد که می تواند رفتاری را ارائه دهد که هوشمندانه به نظر می رسد.

این رشته از فناوری – که در ابتدا شاخه ای از علوم کامپیوتر بود – به طور فزاینده ای جایگاه افتخاری در عرصه بین المللی به خود اختصاص داده است و اکنون به کانون رقابت بین شرکت ها و کشورها تبدیل شده است. توسعه هوش مصنوعی همراه با پیشرفت‌هایی در زمینه‌های فناوری و علمی دیگر مانند محاسبات ابری، داده‌های بزرگ، روباتیک پیشرفته و خودروهای خودکار رخ داده است و به نظر می‌رسد این پیشرفت‌ها در آینده نزدیک دنیای ما را تغییر خواهند داد.

استفاده از سیستم ها، اپلیکیشن ها و خدمات پیشرفته افزایش یافته است و بسیاری از کشورها، شرکت ها و مقامات امنیتی بر اساس نیاز خود از آنها استفاده می کنند. کاربردهای غیرنظامی هوش مصنوعی شامل برنامه‌های ناوبری، الگوریتم‌هایی که کالاها یا خدمات سفارشی را ارائه می‌دهند، برنامه‌های کاربردی در تجارت بانکی و مالی و سیستم‌هایی در زمینه‌های تعمیر و نگهداری و تدارکات است. سیستم‌های مبتنی بر هوش مصنوعی نیز در عرصه امنیتی، مانند اطلاعات نظامی، لجستیک، سیستم های فرماندهی، کنترل و ارتباطات، سیستم های نظامی خودمختار از جمله سیستم های تسلیحاتی و جنگ سایبری رایج هستند

هوش مصنوعی دیگر یک فناوری آینده نگر نیست. بلکه یک نیاز اساسی را در زمان حاضر فراهم می

کند. بسیاری از رهبران سازمان ها یا کشورها این مفهوم را درونی کرده اند و سیاست هایی را برای تشویق توسعه و سرمایه گذاری در هوش مصنوعی اتخاذ کرده اند. با این حال، علاوه بر مزایای هوش مصنوعی، چالش‌های زیادی را در توسعه، استفاده و اثرات همراه آن نیز شامل می‌شود. رهبران در زمینه های مختلف و در دنیایی که ما در آن زندگی می کنیم باید نگران این چالش ها باشند.

این یادداشت دو هدف اساسی دارد:

اول، در نظر گرفته شده است که به عنوان یک راهنمای کلی برای فرماندهان، مدیران و تصمیم گیرندگان عمل کند تا آنها را با موضوعات و اصطلاحات اصلی مرتبط با هوش مصنوعی و امنیت ملی آشنا سازد. برای این منظور در چندین فصل سعی شده است تا مسائل پیچیده از جمله مسائل فنی قابل درک باشد.

دومین هدف این یادداشت، توصیه یک سیاست هوش مصنوعی در زمینه امنیت ملی است، با این فرض که هوش مصنوعی یک قابلیت اساسی است که اسرائیل به آن نیاز دارد و اسرائیل باید توانایی‌ها و جایگاه خود را در برابر رقابت جهانی هوش مصنوعی و چالش های منطقه ای و سایر چالش ها حفظ و تقویت کند.

بخش اول این یادداشت، فناوری هوش مصنوعی و کاربردهای امنیتی آن را با بحث در مورد پیشینه تاریخی، حوزه‌های فناوری مرتبط با هوش مصنوعی، و کاربردهای امنیتی آن و همچنین موضوع هوش مصنوعی عمومی ارائه می کند.

بخش دوم به مسائل مربوط به هوش مصنوعی و عرصه بین المللی می پردازد. این شامل مروری بر وضعیت توسعه و استفاده از هوش مصنوعی در کشورهای پیشرو، اثرات احتمالی فناوری در عرصه بین‌المللی، و همچنین مطالعه موردی استفاده از سیستم‌های تسلیحات خودکار مرگبار (LAWS) و درس‌های آموخته شده در مورد هوش مصنوعی و عرصه بین المللی است.

بخش سوم به هوش مصنوعی در زمینه امنیت ملی اسرائیل مربوط می شود و شامل بررسی وضعیت، بررسی مفهوم امنیت ملی اسرائیل، و ارتباط بین هوش مصنوعی و امنیت ملی و استراتژی ارتش آن است. این بخش همچنین به طور مفصل به چالش‌های بسیاری در توسعه، پیاده‌سازی و استفاده از هوش مصنوعی در اسرائیل و همچنین چالش‌های امنیتی، سیاسی و غیرمستقیم برای امنیت ملی اسرائیل می‌پردازد. نتیجه‌گیری این یادداشت، بر اساس هوش مصنوعی، توصیه‌هایی برای تقویت و حفظ امنیت ملی اسرائیل ارائه می کند.

این مطالعه بر انواع منابع اولیه و ثانویه، از جمله اسناد راهبردی، تحقیقات دانشگاهی، مصاحبه با کارشناسان و متخصصان و نتیجه‌گیری‌هایی که در جلسات کمیته تخصصی حرفه‌ای برای این مطالعه

فرموله شده است، تکیه داشت. این کمیته در مورد موضوعات مختلفی که این یادداشت را شامل می شود بحث و گفتگو کرد. محتویات بحث ها به درک دقیق تری از بسیاری از جنبه های هوش مصنوعی در رابطه با سازمان های امنیتی مختلف، صنایع و شرکت های غیرنظامی و همچنین درک عمیقی از فناوری و قابلیت های آن و با توصیف مفهومی این یادداشت، تهیه فهرستی از چالش‌ها و ترسیم توصیه‌های راهبردی کمک کرد.

توصیه‌های راهبردی برای تعدادی از حوزه‌های کلیدی را نشان می‌دهد که در آنها اسرائیل باید برای حفظ و بهبود امنیت ملی خود از طریق هوش مصنوعی اقدام کند: قلمرو سازمانی، بودجه، تامین مالی و زیرساخت ملی، ایمنی، قانون و اخلاق، قانون گذاری و استانداردسازی، اشتراک دانش، جنبه های بین المللی، دیپلماتیک، اطلاعات نظامی و همکاری و منابع انسانی از جمله آموزش و پرورش. برخی از این توصیه ها به بودجه قابل توجه و تغییرات سازمانی قابل توجهی نیاز دارند، در حالی که برخی دیگر نیاز ندارند و در مدت زمان کوتاهی می توانند اجرا شوند.

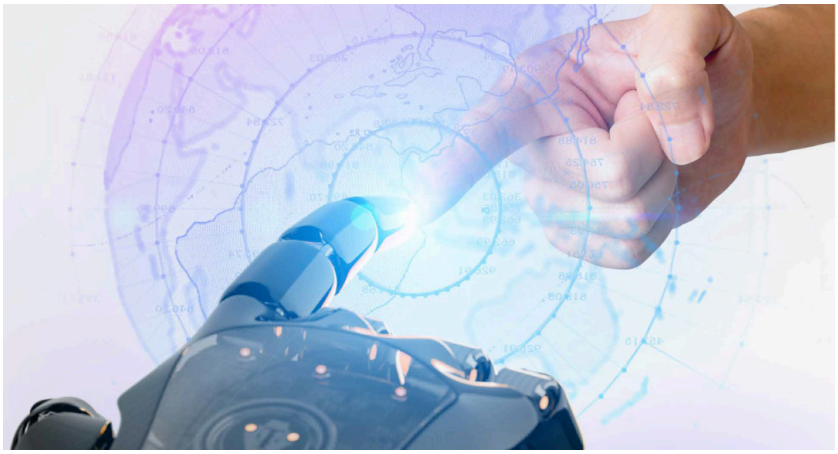
با این وجود، در زمینه ای بسیار مهم که با توسعه سریع و نفوذ متنوع مشخص می شود، لازم است یک نهاد فراگیر داشته باشیم که فعالیت ها را در سطح ملی هماهنگ، بودجه بندی و هدایت کند، همانطور که اسرائیل به عنوان مثال در حوزه سایبری انجام می دهد. این امر اسرائیل را قادر می‌سازد تا وضعیت خود را به عنوان یک رهبر فناوری جهانی حفظ کرده و بهبود بخشد و در عین حال از مزیت نسبی خود برای تأثیرگذاری مثبت بر امنیت ملی خود استفاده کند.

بخش اول:

هوش مصنوعی و کاربردهای امنیتی آن

تا کنون، بزرگترین خطر هوش مصنوعی این است که مردم خیلی زود به این نتیجه می رسند که آن را درک می کنند.

الیازر یودکووسکی، محقق و نویسنده آمریکایی در حوزه هوش مصنوعی



فصل اول:
هوش مصنوعی چیست؟

ایده هوش مصنوعی اولین بار در سال ۱۹۴۵ زمانی که وانوار بوش، یکی از بنیانگذاران اولیه، سیستمی را برای افزایش دانش و درک انسان پیشنهاد کرد، توسعه یافت. پس از او آلن تورینگ، که در سال ۱۹۵۰ مقاله ای در مورد قابلیت های ماشین ها برای شبیه سازی انسان ها و توانایی آنها در انجام اقدامات هوشمندانه مانند بازی شطرنج نوشت.

اصطلاح هوش مصنوعی (AI) چند سال بعد تکامل یافت و به جان مک کارتی، دانشمند کامپیوتر و محقق در زمینه علوم شناختی، که اولین کنفرانس آکادمیک در این زمینه را در سال ۱۹۵۶ سازماندهی و همینطور به ماروین لی مینسکی که به عنوان یک ریاضیدان آموزش دیده بود و در تحقیقات، اختراعات و بسیاری فعالیت کرد نسبت داده شد. این مینسکی بود که تعریف رایج هوش مصنوعی را ابداع و خاطرنشان کرد: «هوش مصنوعی علم ساخت ماشین‌ها برای انجام کارهایی است که اگر توسط مردان انجام شود نیاز به هوش دارد».

در آغاز مطالعه هوش مصنوعی، پارادایم غالب الگوی "نمادین" بود که به دنبال تکرار افکار سطح بالای انسانی بود. با گذشت سالها، پارادایم «پیوندگرا» جایگزین شد، که تلاش می کرد از طریق نورون های مصنوعی از اساس بیولوژیکی شناخت انسان تقلید کند. با این حال، این پارادایم‌ها نتوانستند انتظارات فراتر از نمایش‌های نظری یا آزمایشگاهی را برآورده کنند و به «زمستان هوش مصنوعی» منجر شدند، زمانی که تحقیقات و سرمایه‌گذاری‌ها در هوش مصنوعی برای دوره‌های زمانی طولانی حداقل بود.

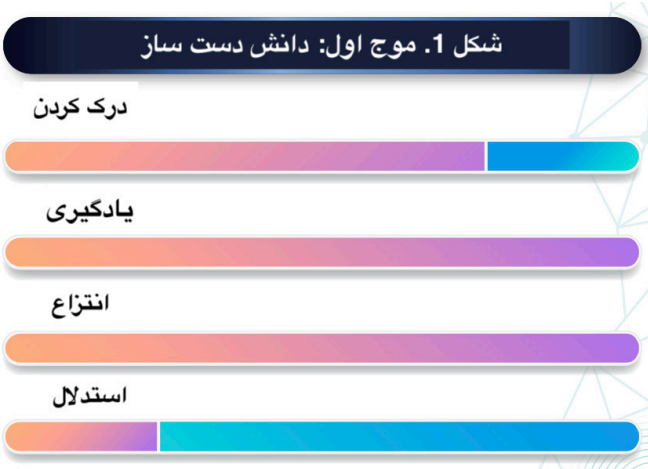
در دهه گذشته، با توجه به پیشرفت در تحقیقات علوم کامپیوتر، توسعه سخت افزار و نرم افزار در محاسبات و ارتباطات و همچنین محاسبات ابری و داده های بزرگ، هوش مصنوعی پیشرفت چشمگیری داشته

است، از جمله در حوزه های فرعی مانند یادگیری ماشین و شبکه های عصبی مصنوعی. این مفاهیم بعداً به تفصیل بررسی خواهد شد). برخی از مطالعات ادعا کرده اند که پیشرفت در زمینه شبکه های عصبی به قدری عمیق است که تقریباً مترادف با هوش مصنوعی تلقی می شود.

بیشتر کاربردهای رایج در هوش مصنوعی متعلق به زیر دامنه‌ای به نام یادگیری ماشینی است که شامل الگوریتم‌های آماری است که با تجزیه و تحلیل حجم زیادی از داده‌ها و ایجاد قوانینی در مورد آنها به دنبال تقلید از وظایف شناختی انسان هستند.

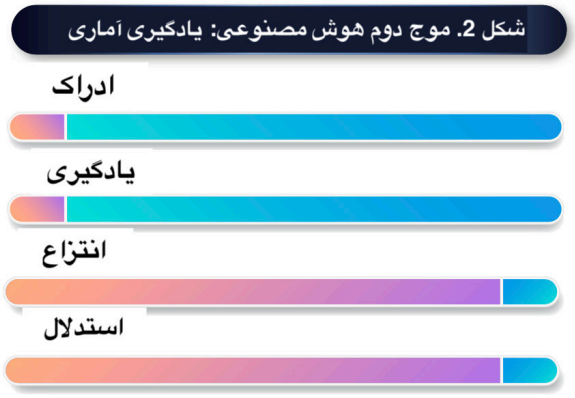
الگوریتم در واقع بر روی اطلاعات موجود «آموزش» می‌دهد و نوعی مدل آماری برای خود ایجاد می‌کند تا در آینده همان کار را بر روی داده‌های جدیدی که قبلاً با آن‌ها مواجه نشده است، انجام دهد.

هوش مصنوعی به حوزه وسیع‌تری از علم داده تعلق دارد و در واقع، برای عملکرد مؤثر به داده‌های زیادی نیاز دارد، به‌ویژه داده‌های بزرگ، که برای ایجاد بینش مهم با کمک الگوریتم‌های یادگیری مورد نیاز است. با این حال، هوش مصنوعی تنها به داده‌های بزرگ وابسته نیست، که تنها یکی از ابزارهای کارآمد برای تولید ارزش و دانش از چنین حجمی از داده‌ها است که به الگوریتم‌های قوی برای تجزیه و تحلیل آنها نیاز دارد.



شکل 1. موج اول: دانش دست ساز

استدلال را در مورد مسائل با تعریف محدود فعال می کند.
عدم توانایی یادگیری و مدیریت ضعیف عدم قطعیت.
منبع:
Launchbury، "A A DARPA Perspective on Artificial Intelligence.



طبقه بندی و قابلیت های پیش بینی دقیق.
بدون قابلیت زمینه ای و حداقل توانایی استدلال.

منبع: Launchbury، "یک دیدگاه دارپا در مورد هوش مصنوعی".

بخش قابل توجهی از کار بنیانگذاران هوش مصنوعی مبنای نظری الگوریتم‌های یادگیری ماشینی بود که در بسیاری از سیستم‌های معاصر استفاده می‌شوند و اقداماتی مانند شناسایی تصویر و رانندگی مستقل را امکان‌پذیر می‌سازند.

این سیستم ها متعلق به آنچه به عنوان هوش مصنوعی محدود یا هوش مصنوعی ضعیف شناخته می شود، تعلق دارند، اگرچه گاهی اوقات اینها می توانند برنامه های پیشرفته ای باشند.

این مفهوم به الگوریتم‌هایی اشاره دارد که برای مقابله با مجموعه‌ای از مشکلات خاص، مانند بازی‌ها، شناسایی تصویر، یا ناوبری طراحی شده‌اند. این مفهوم با هوش مصنوعی عمومی، که مربوط به سیستمی است که قادر به استفاده از هوش در سطح انسانی برای طیف وسیعی از وظایف است، متفاوت است. تا زمان نگارش این مقاله، هوش مصنوعی عمومی هنوز وجود ندارد، و نظرات در مورد اینکه آیا حداقل در دو دهه آینده ایجاد خواهد شد یا خیر، متفاوت است. هوش مصنوعی توسعه یافته عمدتاً به برنامه های یادگیری عمیق تعلق دارد. این فناوری را در واقع می‌توان به عنوان هوش مصنوعی محدود طبقه‌بندی کرد، اما شکل دقیق‌تری از یادگیری رایانه‌ای و همچنین استفاده تجاری گسترده‌تر از برنامه‌های هوش مصنوعی را ممکن می‌سازد.

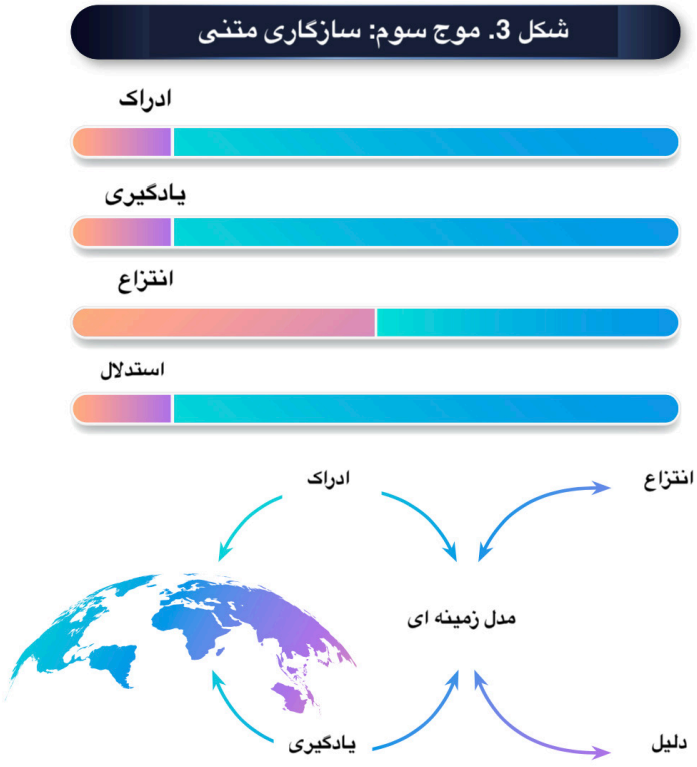
پیشینه تاریخی: سه موج اول هوش مصنوعی

توسعه هوش مصنوعی را می توان بر اساس توسعه قابلیت های هوش مصنوعی به سه موج مجزا تقسیم کرد. آژانس پروژه های تحقیقاتی پیشرفته دفاعی (دارپا) وزارت دفاع ایالات متحده یکی از نهادهای پیشرو در جهان در توسعه هوش مصنوعی برای اهداف امنیتی است. دارپا هوش مصنوعی را به عنوان «توانایی برنامه‌ریزی‌شده برای پردازش اطلاعات» تعریف می‌کند. در کنار این تعریف ساده، دارپا هوش مصنوعی را به سه موج تقسیم کرده است که با مقیاس هوش مفهومی مشخص می‌شود که در آن چهار قابلیت زیر اندازه‌گیری می‌شوند، مشابه ابعاد هوش انسانی:

۱. ادراک: توانایی تشخیص رویدادهای جهانی
۲. یادگیری: توانایی یادگیری چیزها و سازگاری با موقعیت های مختلف
۳. انتزاع: توانایی گرفتن دانش کشف شده در سطح معین و استنتاج از آن یا به کار بردن آن در سطحی دیگر.
٤. استدلال: توانایی توضیح منطقی، یا تصمیم گیری منطقی.

موج اول هوش مصنوعی مبتنی بر «دانش دست ساز» بود که در آن متخصصان دانش موجود را در مورد یک موضوع خاص جمع‌آوری کردند و آن را در چارچوب قوانینی که می‌توانستند برای رایانه اعمال کنند، توصیف می‌کردند که به نوبه خود می‌توانست مفاهیم آنها را یاد بگیرد.
این نسل از هوش مصنوعی شامل نرم‌افزار لجستیک برای برنامه‌ریزی عملیاتی مانند محموله‌ها، نرم افزار محاسبه مالیات و نرم افزاری که می تواند با مردم شطرنج بازی کند، می شود. بسیاری از برنامه ها و اپلیکیشن های کامپیوتری در گوشی های هوشمند یا نرم افزارهایی مانند مایکروسافت آفیس بر اساس این موج هوش مصنوعی ساخته شده اند. به گفته دارپا، محصولات موج اول توانایی حسی متوسطی دارند و می توانند علیت را در جنبه های بسیار محدود توضیح دهند، اما فاقد توانایی یادگیری هستند و نمی توانند با عدم قطعیت کنار بیایند. با این حال، دارپا ادعا می کند که این موج دستاوردهای زیادی مانند

دفـاع سـایبری داشـته و توسـعه آن همچنـان ادامـه دارد و امـروز نیـز مطـرح اسـت.



Source: Launchbury, "A DARPA Perspective on Artificial Intelligence."

موج دوم به عنوان "یادگیری آماری" شناخته می شود که با طبقه بندی مشخص می شود. در این موج، کارشناسان از قابلیت‌های پیشرفته‌تری که توسط یادگیری ماشینی تسهیل می‌شود، استفاده کردند، که در آن الگوریتم‌های یادگیری آماری بر داده‌های بزرگ متکی هستند. در این موج برخلاف موج قبلی، کارشناسان به جای قوانین ثابت، مدل‌های آماری مسائل مختلف را به رایانه‌ها آموزش دادند و سپس الگوریتم‌ها را بر روی بسیاری از مثال‌ها آموزش دادند تا اینکه به سطح دقت مطلوب رسیدند. محصولات این موج، تشخیص صدا یا تشخیص چهره را در تلفن‌های همراه و «ربات‌ها» که خدمات مشتریان را از طریق مکاتبات چت اینترنتی ارائه می‌دهند، فعال می‌کرد.

این نسل از هوش مصنوعی شامل سیستم هایی برای تجزیه و تحلیل یا ترجمه متن است. نرم افزار

دستیار شخصی در تلفن های هوشمند؛ و توانایی انجام بازی های چالش برانگیز مانند بازی استراتژی چینی Go. این موج هوش مصنوعی شامل رانندگی خودکار نیز می شود. با این حال، این نسل از هوش مصنوعی توانایی درک قوانین یا علیت در پشت اقداماتی که انجام می دهد را ندارد، بنابراین در معرض خطا یا دستکاری است. به گفته دارپا، موج دوم هوش مصنوعی می‌توانست چیزها را بر اساس تفاوت‌های ظریف و توانایی پیش‌بینی طبقه‌بندی کند، اما فاقد توانایی‌های زمینه‌ای و حداقل توانایی‌ها برای استدلال منطقی بود.

موج سوم که از آن به عنوان «انطباق متنی» یاد می شود، یک موج توضیحی است که در حال حاضر در حال توسعه است. الگوریتم ها یا سیستم های این موج مدل هایی را فرموله می کنند که موضوعات خاصی را توضیح می دهند. دارپا انتظار دارد که سیستم های ساخته شده حول مدل های زمینه ای به تنهایی یاد بگیرند که چگونه مدل های مختلف باید ساختار شوند. این توانایی ها به طور قابل توجهی با بسیاری از الگوریتم هایی که در حال حاضر به عنوان یک "جعبه سیاه" عمل می کنند متفاوت است و باعث ایجاد چالش در توضیح نحوه رسیدن آنها به نتیجه می شود (موضوعی که در بخش بعدی توضیح داده خواهد شد). بنابراین، این موج هوش مصنوعی از اطلاعات به صورت انتزاعی استفاده می کند و آن را یک گام به جلو می برد، اما در حال حاضر قابلیت های این سیستم ها هنوز محدود است.امید است که محصولات این موج بیشتر «انسانی» باشند و بتوانند به زبان طبیعی ارتباط برقرار کنند، بتوانند خود را آموزش و پرورش دهند (مانند نرم افزار Alpha-Go که خود را در هزاران بازی «Go» علیه خودش آموزش داده است.) و قادر خواهد بود داده ها را از چندین منبع مختلف جمع آوری کند و نتیجه گیری هایی را به خوبی توضیح دهد.به گفته دارپا، این موج می‌تواند قابلیت‌های هوش مصنوعی را در زمینه‌های حسی، یادگیری و استدلال بهبود بخشد، اگرچه محصولات هنوز هم فقط قابلیت‌های متوسطی در زمینه انتزاع خواهند داشت.

فناوری‌های موجود در زمینه این موج شامل «دستیارهای هوشمند» است که توانایی کمک به آنها فراتر از فناوری‌های نسل دوم مانند سیری و الکسا پیشرفت کرده است.مثال دیگر Google Duplex است که می‌تواند قرار ملاقات‌هایی (مانند رزرو در آرایشگاه یا رستوران) بگذارد و در عین حال مکالمه صوتی منسجمی را با نماینده خدمات انسانی مدیریت کند. علاوه بر وظایف عملیاتی مستقل این نرم افزار همچنین می داند که چگونه با شناسایی وظایفی که نمی تواند به تنهایی انجام دهد، به کاربر سیگنال دهد.

در حالی که سه موج هوش مصنوعی به راحتی قابل شناسایی هستند، اکثر تحقیقات مربوط به هوش مصنوعی در سال های اخیر، به ویژه در زمینه امنیت ملی، به این واقعیت پرداخته اند که هیچ تعریف

واحدی برای اصطلاح هوش مصنوعی وجود ندارد. تدوین یک تعریف پذیرفته شده از هوش مصنوعی به دو دلیل عمده مشکل ساز است: اول، رویکردهای متنوع و گوناگونی برای تحقیق در این زمینه وجود دارد. دوم، به دلیل محدودیت‌هایی که هنوز در مطالعه علوم اعصاب (و همچنین در فلسفه) نقض نشده‌اند، در تعریف یا توافق بر سر تعریف «هوش» مشکل اساسی وجود دارد. بنابراین توانایی بررسی این مفاهیم در رابطه با ماشین‌ها یا اعمال آن‌ها در ماشین‌ها محدود است. علیرغم این دشواری، این مطالعه تعاریف مختلف را بررسی می کند و تعریفی را برای بحث باقی مانده در این سند و توصیه های راهبردی که در ادامه می آید پیشنهاد می کند.

هوش مصنوعی – یک تعریف عملیاتی

یکی از تعاریف شناخته شده هوش مصنوعی که قبلاً ذکر شد، توسط ماروین لی مینسکی این گونه بیان شد: «دانش ساخت ماشین‌هایی است که کارهایی را انجام میدهند که اگر توسط مردان انجام شود نیاز به هوش دارد.» مزیت این تعریف گسترده بودن آن به اندازه ای است که ایده ها، روش ها و ابزارهای مختلف را شامل شود.

با این حال، فاقد استفاده از اصطلاح "هوشمند" در بافت انسانی است – اصطلاحی که هنوز تعریف نشده است و توسط رشته های علمی درگیر در این موضوع به طور واضح مشخص می شود. علاوه بر این، هنگام تعریف نظم و انضباط برای امنیت ملی و ارائه توصیه‌های راهبردی، تعریف ضروری دوگانه‌تری برای تعیین اینکه باید شامل چه چیزی شود و چه چیزی نامربوط است،کمک می کند.

دارل وست و جان آلن ادعا کرده اند که "هوش مصنوعی (AI) ابزار گسترده ای است که به مردم امکان می دهد درباره نحوه ادغام اطلاعات، تجزیه و تحلیل داده ها و استفاده از بینش های حاصل برای بهبود

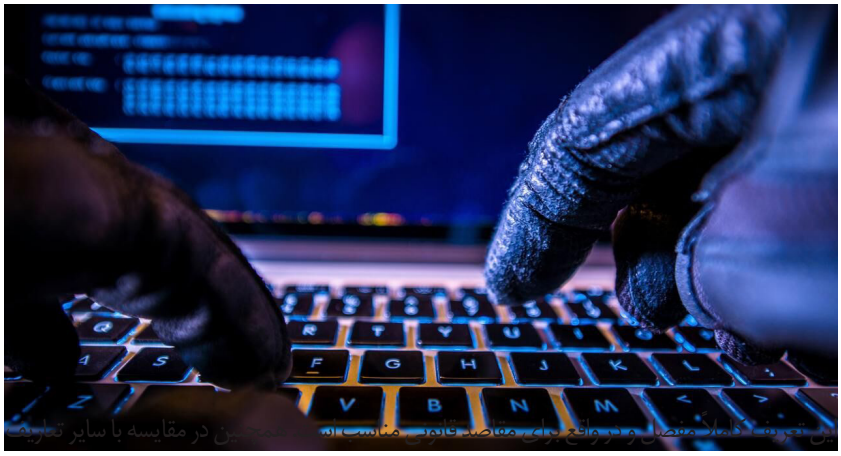
تصمیم گیری تجدید نظر کنند. وست و آلن معتقدند که با وجود اینکه هیچ تعریف پذیرفته شده یکسانی وجود ندارد، درست است که به هوش مصنوعی به عنوان «ماشین هایی که با توجه به ظرفیت انسان برای تفکر، قضاوت و نیت به تحریک سازگار با پاسخ های سنتی انسان پاسخ می دهند» اشاره کنیم.به گفته وست و آلن، «هوش مصنوعی به داده‌هایی بستگی دارد که می‌توان آن‌ها را در زمان واقعی تجزیه و تحلیل کرد و به مشکلات عینی رسیدگی کرد. داشتن داده هایی که در جامعه تحقیقاتی «در دسترس برای اکتشاف» باشد، پیش نیاز توسعه موفقیت آمیز هوش مصنوعی است.»

به گفته شابهندو شوکلا و ویجی جیسوال، برنامه‌های کاربردی هوش مصنوعی «تصمیم‌هایی را می‌گیرند که معمولاً به سطح انسانی تخصص نیاز دارند» و به افراد کمک می‌کنند تا مشکلات را پیش‌بینی کنند یا با مسائلی که به وجود می‌آیند مقابله نمایند. بنابراین، برنامه های کاربردی هوش مصنوعی هدفمند، هوشمندانه و سازگارانه عمل می کنند. پس از بحث در مورد برخی از تعاریف نظری، مناسب است بررسی کنیم که سازمان های درگیر در تحقیق و توسعه یا مقررات و قوانین هوش مصنوعی چگونه عملاً آن را تعریف می کنند. علیرغم تعریف کلی دارپا از هوش مصنوعی به عنوان «توانایی برنامه ریزی شده برای پردازش اطلاعات»، باید روشن شود که هر سیستم محاسباتی از هوش مصنوعی استفاده نمی کند. الگوریتم های هوش مصنوعی برای تصمیم گیری و انجام این کار با استفاده از داده های وارد شده در زمان واقعی طراحی شده اند.

هنگامی که آنها در سیستم های مختلف استفاده می شوند، این ماشین های غیرفعال نیستند که فقط قادر به واکنش های مکانیکی یا از پیش تعیین شده، مانند دوران اتوماسیون(مانند درب های اتوماتیک یا حتی عملکردهای اتوماتیک در ماشین لباسشویی)؛ هستند بلکه ماشین‌هایی با حسگرها، داده‌های دیجیتال و حتی ورودی‌های راه دور هستند که می‌توانند اطلاعات را از منابع مختلف یکپارچه کنند، بلافاصله آن‌ها را تجزیه و تحلیل و بر اساس بینش‌های مبتنی بر داده‌ها عمل کنند. این امر پیچیدگی و سرعتی را در پذیرش داده‌هایی که قبلاً ممکن نبود، ممکن می‌سازد تا جایی که به دولت ایالات متحده مربوط می شود، هیچ تعریف رسمی از هوش مصنوعی وجود ندارد و سازمان های مختلف ممکن است بنا به نیاز خود آن را به گونه ای متفاوت تعریف کنند. با این حال، مجموعه ای از قوانینی که بودجه وزارت دفاع ایالات متحده را تنظیم می کند (قانون مجوز دفاع ملی سال مالی ۲۰۱۹) تعریفی از هوش مصنوعی برای تصویب بخش ۲۳۸ ارائه می دهد که در تحقیق و توسعه این زمینه مشارکت دارد:

- هر سیستم مصنوعی که وظایفی را تحت شرایط مختلف و غیرقابل پیش بینی بدون نظارت قابل توجه انسان انجام می دهد، یا می تواند از تجربه درس گرفته و در صورت قرار گرفتن در معرض مجموعه داده ها، عملکرد خود را بهبود بخشد.

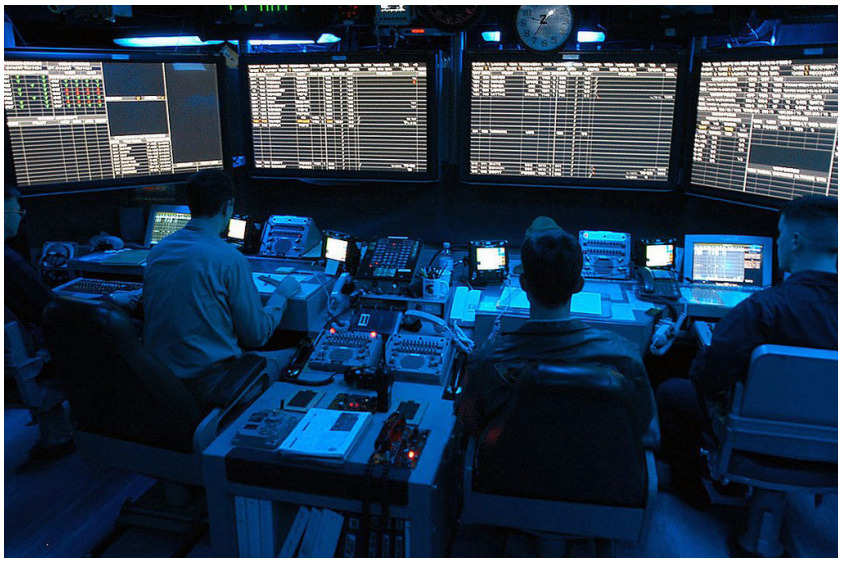
- یک سیستم مصنوعی توسعه یافته در نرم افزار کامپیوتر، سخت افزار فیزیکی، یا زمینه های دیگر که وظایفی را که نیاز به ادراک، شناخت، برنامه ریزی، یادگیری، ارتباط یا عمل فیزیکی شبه انسانی دارند را حل می کند.
- یک سیستم مصنوعی طراحی شده برای تفکر یا عمل مانند یک انسان، از جمله معماری های شناختی و شبکه های عصبی.
- مجموعه ای از تکنیک ها، از جمله یادگیری ماشینی که برای تقریب یک کار شناختی طراحی شده است.
- یک سیستم مصنوعی طراحی شده برای عمل منطقی، شامل یک عامل نرم افزاری هوشمند یا ربات تجسم یافته که با استفاده از ادراک، برنامه ریزی، استدلال، یادگیری، برقراری ارتباط، تصمیم گیری و عمل به اهداف می رسد.



به تصمیم گیری در مورد اینکه کدام حوزه های برنامه نویسی و محاسبات به رشته هوش مصنوعی تعلق ندارند کمک می کند. با این وجود، بسیار طولانی و فنی است. با توجه به هدف این سند – در دسترس قرار دادن دانش در مورد هوش مصنوعی برای تصمیم گیرندگان و توصیه راهبردی در بخش امنیت ملی – این مطالعه به تعریف کوتاه تر و ساده تری مانند دارپا نیاز دارد. تعریف دارپا برای اهداف این تحقیق مناسب تر از تعریف مینسکی است، برای مثال، زیرا به موضوع بحث برانگیز هوش انسانی مربوط نمی‌شود، و در واقع، انواع برنامه ها یا روش های پردازش پذیرفته شده در حال حاضر را امکان پذیر و حتی آن را ترک می کند. دریچه ای برای پیشرفت های آینده، بدون بار جزئیات فنی که برای درک آن نیاز به تخصص دارد. حتی اگر این تعریف به احتمال زیاد شامل قابلیت‌های محاسباتی و پردازشی «ضعیف»

باشد، همانطور که در بالا توضیح داده شد، برخی از روش‌ها و برداشت‌های موج اول هنوز در زمینه‌ها و کاربردهای مختلف مفید و بنابراین ارزشمند هستند.

با این حال، اما در مواردی که تصمیم گیرندگان برای بررسی باید تعریف را محدود کنند که آیا یک توسعه مطابق با تعریف هوش مصنوعی است یا خیر، هوش مصنوعی را می‌توان به عنوان توانایی ایجاد دانش و بینش‌هایی که قبلاً وجود نداشت، با استفاده از اطلاعات و تکیه بر ماشین‌ها و رایانه‌ها یاد کرد. با تمرکز بر توانایی برنامه ریزی شده برای پردازش اطلاعات، این تعریف بین بخش قابل توجهی از برنامه های کاربردی هوش مصنوعی و برنامه های کاربردی کامپیوتر عمومی تمایز قائل می شود و تعریف کلی را به گونه ای محدود می کند که هنوز تعداد زیادی از برنامه ها و طیف گسترده ای از رشته ها را پوشش می دهد در حالی که بر خلق دانش جدید تاکید می کند. بنابراین، تعریف راهنمای هوش مصنوعی که در اینجا استفاده می‌شود، استفاده از اطلاعات و سیستم‌های رایانه‌ای برای ارائه رفتاری است که هوشمندانه به نظر می‌رسد، یا ایجاد دانش و بینشی که قبلاً هرگز وجود نداشته است. این تعریف به اندازه‌ای گسترده است که فناوری‌ها و کاربردهای مختلف و نیازهای مختلف برای تحقق این توانایی‌ها را شامل می‌شود. در عین حال، این تعریف به اندازه‌ای محدود است که همه حوزه‌های محاسباتی را شامل نمی‌شود، بلکه فقط آن‌هایی را شامل می شود که ویژگی‌های هوش مصنوعی در آنها بیان می‌شود. این تعریف به تدوین فصول زیر کمک کرد.



فصل دوم:
زمینه های هوش مصنوعی

هوش مصنوعی شامل بسیاری از حوزه‌های ادراکی–فناوری از جمله یادگیری ماشینی، یادگیری عمیق، بینایی رایانه‌ای، پردازش زبان طبیعی و تعدادی از زمینه‌های به هم پیوسته کمکی است. این فصل بر روی زیر دامنه های مختلف هوش مصنوعی تمرکز دارد.

شکل 4: هوش مصنوعی و زیر دامنه های آن

فراگیری ماشینی

رایج‌ترین زیر دامنه هوش مصنوعی، یادگیری ماشینی است.یادگیری ماشینی به الگوریتم‌ها اجازه می‌دهد تا از اطلاعات یاد بگیرند و راه‌حل‌ها را به‌طور مستقل توسعه دهند، با استفاده از الگوریتم‌های مبتنی بر آمار که از پایگاه‌های داده بزرگ «یاد می‌گیرند» تا توانایی‌های شناختی انسان را بازسازی کنند و بنابراین وظایف مشخص را در موقعیت‌های ناآشنا انجام دهند. .یادگیری ماشینی به الگوریتم ها اجازه می دهد تا از طریق آموزش های مکرر یاد بگیرند و نتایجی را ایجاد کنند که با توجه به دامنه آموزش و تجربه الگوریتم بهبود یابد. این با نرم افزار نوشته شده توسط یک برنامه نویس انسانی متفاوت است. یک مثال یک برنامه هوش مصنوعی است که پایگاه داده ای از الفبای دست نویس را دریافت می کند و یاد می گیرد که بین حروف دست نویس تمایز قائل شود، حتی اگر دست خط شخص در مخزن موجود ظاهر نشود.چندین رویکرد برای یادگیری ماشین وجود دارد، از جمله یادگیری با نظارت، که در آن برنامه‌نویس یادگیری را بر اساس مدل اولیه موجود قرار می‌دهد که ماشین آن را بهبود می‌بخشد و یادگیری بدون نظارت، که در آن سیستم‌های یادگیری مدل خود را توسعه می‌دهند، که به مدل موجود بستگی ندارد. رویکرد دیگر یادگیری تقویتی است که در آن نرم‌افزار از آزمون و خطا یاد می‌گیرد، نه از یک مخزن اطلاعات موجود.

یادگیری عمیق

یادگیری عمیق زیرمجموعه ای از یادگیری ماشینی است که از شبکه های عصبی مصنوعی استفاده می کند. اینها الگوریتم هایی هستند که از رفتار شبکه عصبی در مغز انسان الهام گرفته شده اند.شبکه عصبی با انجام اصلاحات کوچک با بررسی مقدار زیادی از داده ها برای بهبود دقت آن، یاد می گیرد. بنابراین خروجی یک نورون ورودی نورون دیگر است. یادگیری عمیق به این دلیل نام خود را به دست آورد که بر اساس لایه های زیادی از نورون های مصنوعی است. شبکه‌های عصبی به دلیل موفقیت‌های قابل‌توجهی که دارند، به رایج‌ترین رویکردها برای یادگیری ماشین تبدیل شده‌اند و مسئول دستاوردهای مختلفی در زمینه هوش مصنوعی از جمله تشخیص چهره در سطحی بالاتر از توانایی انسان برای شناسایی چهره‌ها؛ شناسایی اشیاء در تصاویر؛ کنترل وسایل نقلیه خودران و هواپیماهای بدون سرنشین؛ رونویسی گفتار در سطحی فراتر از سطح یک رونویس کننده حرفه ای انسانی و ترجمه زبان، از جمله آن دسته از زبان هایی که فناوری به آنها آموزش داده نشده است ؛هستند.

شکل 5. فعالیت یک شبکه عصبی ساده در کاربرد شناسایی یک عکس

این رویکردهای مرکزی دارای قابلیت‌هایی در زمینه‌های مختلف زیر هستند:

پردازش تصویر: قابلیت پردازش تصویر از یادگیری عمیق استفاده می‌کند و نرم‌افزار را قادر می‌سازد تا اشیاء درون یک تصویر را تشخیص دهد و آنها را دسته‌بندی کند. این نرم افزار تصویر را به پیکسل تقسیم می کند و به هر پیکسل با توجه به رنگ آن مقادیری اضافه می کند. این تجزیه و تحلیل تصویر از سیستم عمیق شبکه های عصبی مصنوعی نرم افزار عبور می کند که بر روی پایگاه داده بزرگی از تصاویر آموزش داده شده و تصویر را بر اساس آن دسته بندی می کند. امروزه برخی از فناوری‌ها در این زمینه به عنوان یک محصول خارج از قفسه در دسترس عموم هستند، مانند نرم‌افزار Google AI Vision. بینایی کامپیوتر: بینایی کامپیوتری با فناوری‌های پردازش تصویر متفاوت است، زیرا نرم‌افزار را قادر می‌سازد تا اشیا را در زمان واقعی شناسایی کند و مشابه توانایی بینایی انسان، اما بدون نیاز به دسته‌بندی، به آنها پاسخ دهد. برای مثال، این فناوری‌ها در خودروهای خودران استفاده می‌شوند، زیرا می‌توانند فردی را که ناگهان به جاده برخورد می‌کند شناسایی کرده و به راننده هشدار دهند. بینایی رایانه ای همچنین تجسم سه بعدی، اندازه گیری توده استخوانی، ناوبری مستقل و کنترل تراکنش های نامنظم را فعال کرده است. پردازش زبان طبیعی: پردازش زبان طبیعی (NLP) زیردامنه ای از یادگیری

ماشینی است که نرم افزار را قادر می سازد تا رونویسی، ترجمه، و اعمال را بر اساس معانی گسترده یک زبان گفتاری و نوشتاری انجام دهد و کلمات و جملات جدیدی تولید کند که برای شخص معنادار باشد. از جمله برنامه های کاربردی پردازش زبان طبیعی، تولید زبان طبیعی (NLG) است که به پردازش مقادیر زیادی از اطلاعات و تولید روایت ها و بینش های ساده و قابل فهم و درک زبان طبیعی (NLU) که به پردازش متونی که اطلاعات آنها گم شده یا ساختاری ندارد کمک می کند. طیف گسترده ای از برنامه های کاربردی هوش مصنوعی اکنون از فناوری NLP استفاده می کنند، از جمله برنامه های دستیار شخصی مانند سیری، اکو و دستیار گوگل، برنامه های کاربردی ترجمه زبان، برنامه های کاربردی دولتی و تجاری که پایگاه داده های بزرگ مبتنی بر متن و حتی برنامه های امنیتی در زمینه نظامی را تجزیه و تحلیل می کنند.یک فناوری مرتبط، تحت تأثیر هوش مصنوعی و توسعه آن، اینترنت اشیا است. اینترنت اشیا (IoT) دنیایی را توصیف می کند که در آن رایانه ها و حسگرهای کوچک در اشیاء مختلف تعبیه شده اند. این اشیاء می توانند اطلاعات دیجیتالی را تولید و ذخیره کنند، در حالی که محیط خود را نظارت می کنند، اطلاعات ارائه می دهند و عملیات را در یک سطح مستقل یا حداقل خودکار انجام می دهند. این اشیاء همچنین به اینترنت متصل می شوند و به آنها اجازه می دهند با محیط، سایر دستگاه ها و افراد ارتباط برقرار کنند. از آنجایی که فناوری هوش مصنوعی به وجود داده های انبوه نیز متکی است که آن را قادر به نتیجه گیری می کند، فناوری اینترنت اشیا نقش مهمی در ارتقای هوش مصنوعی دارد. علاوه بر این، ادغام این فناوری در برنامه‌های هوش مصنوعی بلادرنگ به سیستم هوش مصنوعی اجازه می‌دهد تا ورودی‌های واقعیت زمان واقعی را دریافت کند و به طور منظم پاسخ خود را بهبود بخشد. این فناوری، برای مثال، خدمات شهرهای هوشمند را فعال می کند، همانطور که در شهر چینی هانگژو نشان داده شد. به طور مشابه، این فناوری دارای کاربردهای امنیتی بسیاری از جمله اینترنت ابزار میدان جنگ (IoBT) است.یکی از ویژگی های فناوری هوش مصنوعی این است که قابلیت استفاده دوگانه دارد. یعنی می توان از همان برنامه برای اهداف غیرنظامی، نظامی یا امنیتی استفاده کرد.این منحصر به هوش مصنوعی نیست و در سایر فناوری ها و زمینه های علمی وجود دارد. قابلیت استفاده دوگانه هوش مصنوعی مشهود است، به عنوان مثال، در یوتیوب نرم افزاری است که می تواند به طور مستقل اشیاء نامناسب را در ویدیوها شناسایی کرده و به کاربر هشدار دهد. این نرم افزار همچنین می تواند اسلحه ها یا شخصیت های مشکوک را در فیلم های امنیتی شناسایی کرده و در مورد آنها هشدار تولید کند. این قابلیت استفاده دوگانه فرصت ها و همچنین چالش هایی را ایجاد می کند. صنایع امنیتی را قادر می‌سازد تا با بخش تجاری همکاری کنند و فناوری‌هایی را با کاربردهای مختلف توسعه دهند که برای هر دو بخش مفید است. با استفاده از حداقل تنظیمات، فناوری توسعه یافته برای بخش تجاری می تواند برای

اهداف جنگی مورد استفاده قرار گیرد و می تواند قابلیت های پیشرفته ای را برای نیروهای متخاصم یا زیرسلطه دولتی فراهم کند. این چالش امنیتی علاوه بر محصولات یا اجزای تکنولوژیکی مختلف است که با تنظیمات ساده می توانند به راحتی برای کسانی که نمی توانند آنها را از صنایع امنیتی خریداری کنند به سلاح تبدیل شوند. انواع مختلف برنامه های کاربردی هوش مصنوعی که قابلیت های متفاوتی دارند و در حال حاضر در بسیاری از حوزه ها تعبیه شده اند، بر اساس یافته های مقالات و مطالعات سال‌های ۲۰۱۸–۲۰۱۹ در جدول ۱ زیر خلاصه شده است.

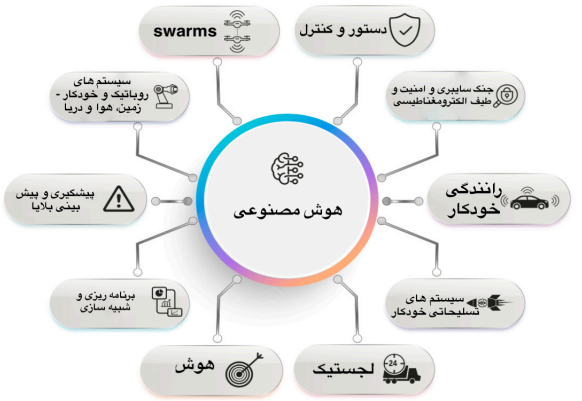
جدول 1. هوش مصنوعی: زمینه های استفاده

	تحلیل پایگاه داده ها	پردازش فیلم	پردازش زبان طبیعی	قابلیت های خودکار	بینایی کامپیوتری و پردازش تصویر	شخصی سازی خدمات
امنیت ملی	✓	✓	✓	✓	✓	
سایبری	✓			✓		
بانک و دارایی	✓					✓
حمل و نقل	✓	✓	✓	✓	✓	✓
آموزش	✓	✓	✓			✓
ارتباطات	✓		✓			✓
کار و تولید	✓	✓	✓	✓	✓	
مراقبت های بهداشتی	✓	✓	✓	✓	✓	✓

فصل سوم:
کاربردهای امنیتی گسترده

برنامه های کاربردی هوش مصنوعی در زمینه امنیتی گسترده شده اند و به سرعت در دسترس هستند. مؤسسات امنیتی در کشورهای مختلف، شرکت های امنیتی و حتی برخی از شرکت های غیرنظامی در توسعه این برنامه ها سهیم بوده اند. برای مثال، در ارتش اسرائیل، مرسوم است که بسیاری از برنامه‌ها را به دو گروه اصلی تقسیم کنیم: برنامه‌هایی که جایگزین «کارگران سخت» می‌شوند، مانند رمزگشایی خودکار، ترجمه‌های خودکار، و کارهای دیگر، که بیشتر آنها وظایف بی‌پایانی در نظر گرفته می‌شوند. آنهایی که به تصمیم گیری و در برخی موارد، تصمیمات مستقل در مورد وظایف مانند برنامه ریزی و پیش بینی کمک می کنند.

شکل 6. کاربردهای هوش مصنوعی در حوزه امنیتی



فهرست کردن تمام برنامه‌ها و زمینه‌هایی که هوش مصنوعی در آن‌ها برای مسائل امنیتی استفاده می‌شود، به دلیل تعداد زیاد برنامه‌ها و سرعت سریع تغییر، دشوار است. علاوه بر این، برخی از برنامه‌های غیرنظامی به طور بالقوه می‌توانند به برنامه‌های امنیتی تبدیل شوند، و برخی نیز بر امنیت تأثیر می‌گذارند (مانند برنامه‌های دیپ فیکینگ).

اطلاعات نظامی

انواع قابلیت‌های هوش مصنوعی برای نیازهای اطلاعاتی نظامی از پردازش تصویر گرفته تا بینایی کامپیوتری، پردازش زبان با روش‌های مختلف و قابلیت‌های دیگر مناسب است. پروژه های مختلف اطلاعات نظامی در سراسر جهان اکنون از الگوریتم ها استفاده می کنند. در عصری پر از داده ها، نیروی انسانی نمی تواند تمام داده های جمع آوری شده توسط بسیاری از حسگرهای سیستم های امنیتی را مدیریت کند. بنابراین، استفاده از هوش مصنوعی در اطلاعات نظامی ضروری نیست، زیرا به خودکارسازی فرآیندهای اطلاعاتی نظامی به ویژه در زمینه‌های اطلاعات بدون ساختار کمک می‌کند و تولید بینش و دانش جدیدی را امکان‌پذیر می‌سازد که با ابزارهای قبلی امکان‌پذیر نبود.در میان بسیاری از پروژه های اطلاعاتی نظامی که از هوش مصنوعی استفاده می کنند، پروژه Maven است که به دلیل مخالفت‌هایی که در میان کارمندان خود برانگیخته معروف است. گوگل و وزارت دفاع ایالات متحده این پروژه بینایی کامپیوتری را با هم انجام دادند و از هوش مصنوعی برای تجزیه و تحلیل ویدئوهای جمع آوری شده توسط پهپادها استفاده کردند. دارپا برنامه‌ای دارد که الگوریتم‌هایی را برای کمک به شناسایی اهداف در محیط‌های دشوار که می‌توان درکنار رادار در یک‌محل قرار داد و با مقایسه داده‌های تولید شده از آنها این برنامه را توسعه داد. الگوریتم‌ها همچنین در تجزیه و تحلیل متن یا صدا استفاده می‌شوند که به برنامه‌های تشخیص چهره کمک می‌کنند. در سال ۲۰۱۸، جایزه نخست وزیر برای خدمات امنیت عمومی برای یک پروژه مبتنی بر یادگیری ماشینی اعطا شد که با تجزیه و تحلیل داده ها از منابع مختلف به جلوگیری از صدها حمله تروریستی کمک کرد.

لجستیک

حوزه لجستیک دستخوش تغییرات قابل توجهی هم در کاربردهای غیرنظامی و هم در کاربردهای نظامی شده که در نتیجه قابلیت‌های پیش‌بینی و برنامه‌ریزی توسط هوش مصنوعی ممکن گردیده است. در واقع، ارتش ایالات متحده از دهه ۱۹۹۰ از سیستم های لجستیکی استفاده کرده است، که به ارتش کمک کرد تا انتقال نیروها را در طول جنگ اول خلیج فارس برنامه ریزی و بهینه سازی کند و سرمایه گذاری

در تحقیقات ۳۰ ساله هوش مصنوعی را جبران نماید. اخیرا، نیروی هوایی ایالات متحده از سیستم‌های هوش مصنوعی برای پیش‌بینی تعمیر و نگهداری هواپیما و ایجاد برنامه‌ریزی نگهداری هواپیما استفاده کرده است.فعالیت پشتیبانی لجستیکی ارتش ایالات متحده (LOGSA) در سیستم Watson IBM، بر اساس اطلاعات جمع‌آوری‌شده از حسگرهای آن، برنامه‌ای برای تعمیر و نگهداری ناوگان خودروهای زرهی جنگی Stryker ایجاد کرده است. در واقع، از بسیاری جهات، لجستیک نظامی مشابه لجستیک غیرنظامی است، زیرا هم شرکت‌های تجاری و هم سازمان‌های غیرنظامی نیز از خدمات لجستیک و تعمیر و نگهداری سیستم‌ها استفاده زیادی می‌کنند. طراحی و اجرای وظایف لجستیکی با کاربرد دوگانه به سیستم‌های مختلفی مانند روبات‌ها و نرم‌افزارهای خاص متکی است که برای مثال به مدیریت انبارهای آمازون کمک می‌کنند.

ادامه دارد...

درباره نویسنده:
لیران عانتبی

همکار مهمان مرکز مطالعات امنیت ملی اسراییل

لیران عانتبی یکی از اعضای پژوهش در INSS است و فن آوری های پیشرفته و برنامه امنیت ملی از جمله مطالعه هوش مصنوعی و امنیت ملی را مدیریت می کند. او برنامه تحقیقاتی پیش بینی و سیاست‌های تکنولوژیکی را مدیریت کرده است و در سال های ۲۰۱۳-۲۰۱۴ محقق عضو تحقیقات کالج نئوابوئر (Neubauer) بود. دکتر عانتبی همچنین مدرس دانشگاه بن گوریون در برنامه دانشگاهی آکادمی نیروی هوایی و در دانشکده دولت، دیپلماسی و استراتژی مرکز میان رشته ای هرتزلیا است.

پیش از این، او چندین سال به عنوان عضو IP aw (پانل بین المللی مقررات سیستم های سلاح های خودکار، مشاوره سازمان ملل متحد) خدمت کرد. او دکترایش را از دانشگاه تل آویو گرفت، پایان نامه او در زمینه تأثیر ربات های نظامی بر بکارگیری نیروهای دموکراسی در درگیری‌های نامتقارن بود.

دکتر عانتبی در چندین زمینه، در حوزه امنیت ملی و امور نظامی، از جمله:

فن آوری های پیشرفته مانند هواپیماهای بدون سرنشین، ربات ها، هوش مصنوعی و غیره؛ پیامدهای تکنولوژی بر امنیت؛ تکنولوژی نظامی و پیامدهای استفاده از آن؛ تأثیر فن آوری های پیشرفته در سیاست،


سورین
مرکز مطالعات
آبان
۱۴۰۰