هوش مصنوعی و کاربردهای نظامی در فضای سایبری

فریده محمدعلی‌پور[۱]، میرامیر پور موسوی[۲]

[۱]استادیار گروه روابط بین‌الملل دانشگاه خوارزمی
fm.alipour@khu.ac.ir
[۲]دانش‌آموخته کارشناسی ارشد روابط بین‌الملل دانشگاه خوارزمی
amir.p.m.7@gmail.com

چکیده

مهمترین تغییرات در جنگ‌ها در پی تحولات فناوری رخ داده‌اند و سه واژه‌ی بقا، امنیت و منافع ملی توجیه‌گر استفاده و توسعه انواع تسلیحات نظامی در جنگ بوده‌اند. جهان، مستمراً با پدیده‌ها و جهش‌های خارق‌العاده فناوری‌های نوین روبه‌رو می‌شود که بر زندگی و زیست مردمان و جوامع و جوامع بین‌المللی تأثیر بسیار داشته است. از مهم‌ترین دستاوردهای فنّاورانه‌ی بشر در طول تاریخ، هوش مصنوعی است. استفاده‌ی گسترده از هوش مصنوعی در جنگ سایبری از جنگ دوم خلیج فارس در قرن بیست و یکم آغاز و به صورت امری رقابتی موجب پیشرفت و توسعه نسل جدید تسلیحات و تجهیزات نظامی شده است. لذا در این پژوهش به این سؤال پاسخ داده شده است که کاربرد هوش مصنوعی در سامانه‌های نظامی چیست. یافته‌های پژوهش نشان می‌دهند هوش مصنوعی از طریق جنگ سایبری و تغییر اشکال پدافند نوین بر سامانه‌های نظامی تأثیر گذاشته و نسل جدیدی از آن‌ها ایجاد کرده است. سامانه‌های هوش مصنوعی می‌توانند با بهره‌گیری از سامانه‌های خبره و یادگیری ماشینی و بیگ دیتا باعث افزایش سرعت و دقت و هوشمندی پدافند شوند لذا با هوشمندتر و سریع‌تر شدن جنگ‌افزارها، فناوری پدافند نیاز روزافزونی به تشخیص‌دهنده و عوامل هوشمند دارد تا قبل از بروز هرگونه مخاطره‌ای، اقدامات پیشگیرانه صورت پذیرد.

کلمات کلیدی: هوش مصنوعی، فضای سایبری، جنگ سایبری، تسلیحات نظامی نوین، جنگ نامتقارن.

۱ مقدمه

استفاده کشورها از قدرت اقتصادی، سیاسی، فرهنگی و اجتماعی و رسانه‌ای در کنار قدرت امنیتی و نظامی برای پیشبرد اهداف و تأمین منافع ملی موجب گردیده که واژه‌ی «جنگ» صرفاً نظامی‌گری را به اذهان متبادر نسازد. در قرن حاضر با پیچیده شدن نظام بین الملل، جنگ ابعاد مختلفی تحت عنوان جنگ ترکیبی به خود گرفته و در این میان، جنگ سایبری با استفاده از هوش مصنوعی جایگاه ویژه‌ای دارد. این نوع از جنگ در چارچوب جنگ نامتقارن قرار می‌گیرد. جنگ نامتقارن به چند عنصر اصلی از جمله بهره‌گیری از نقاط ضعف

و آسیب‌پذیری دشمن، استفاده از فناوری‌های پیشرفته و غیر قابل انتظار و بهره‌گیری از روش‌های مبتکرانه اشاره داشته و عدم تقارن در فناوری، تاکتیک و استراتژی را نشان می‌دهد. جنگ نامتقارن را می‌توان در ابعاد هسته‌ای، شیمیایی، بیولوژیکی، الکترومغناطیسی، سایبری و... بکار بست. با عنایت به این موضوع، مطالعه ابعاد جدید جنگ مانند کاربرد هوش مصنوعی در فضای سایبری ضروری می‌نماید. در مورد جنگ سایبری یک سؤال بسیار مهم پدید می‌آید و آن این است که: در جهانی که هرکسی می‌تواند دشمن باشد و یا یک دشمن می‌تواند در هر جایی باشد، عملکرد باید چگونه باشد و چطور باید فکر کرد. اندیشه در خصوص این سؤال، انگیزه‌ی لازم برای پژوهش فراهم می‌کند.

استفاده از فضای سایبری در سازمان‌های نظامی، توانایی یگان‌ها برای رسیدن به بهترین درجه از تصمیم‌گیری، تحرک و عملکرد بر اساس وقایع میدان نبرد و پیش‌بینی تفکر و رفتار دشمن را افزایش می‌دهد. در عوض، توانایی دستکاری همان اطلاعات می‌تواند منجر به تصمیم‌گیری غلط یا سبب دگرگونی نتایج عملیات نظامی شود. ارائه اطلاعات قابل اعتماد به فرماندهان نظامی سنگ بنای عملیات اخیر بوده و منجر به پیشرفت‌های بسیاری در کاربرد فناوری شده است. سایبر داده‌ها به‌عنوان یک سلاح در میدان نبرد معرفی شده‌اند؛ پالس‌های الکترونیکی از یک ماشین به ماشین دیگر از طریق حوزه سایبر ارسال می‌شوند. هنگامی‌که این داده‌ها در نقطه انتها بازیافت می‌شوند، اطلاعات استخراج می‌گردد. ارزش قابل اطمینان‌ترین داده‌ها با توانایی جمع‌آوری قابل اعتمادترین اطلاعات مساوی است. از این رو، هدف، واکاوی کاربرد هوش مصنوعی در فضای سایبری به عنوان یک سلاح با کاربرد نظامی است. بررسی ادبیات موضوع، خلأ پژوهش در ابعاد مختلف این موضوع را آشکار می‌کند. لذا در این پژوهش به این سؤال پاسخ داده شده است که کاربرد هوش مصنوعی در سامانه‌های نظامی چیست. در پاسخ، با مروری بر مفهوم فضای سایبری و جنگ سایبری، در مقاله حاضر به کاربردهای نظامی هفت‌گانه هوش مصنوعی در فضای سایبری پرداخته می‌شود.

۲ ادبیات موضوع

در میان مکتوبات زبان فارسی کتب یا مقالات مربوط به موضوع پژوهش حاضر اندک هستند. در مقاله «هوش مصنوعی، نحوه عملکرد آن در امنیت دفاعی کشورهای پیشرفته و کاربرد و ضرورت آن در امور نظامی» [۱] با اشاره گذرا به تاریخچه‌ی هوش مصنوعی، به استفاده سربازان آمریکایی از هوش مصنوعی در افغانستان و عراق و تلاش چین و کره جنوبی برای ارتقا این فناوری پرداخته شده است. در مقاله «هوش مصنوعی و آینده حملات گروه‌های تروریستی تکفیری» [۲] نویسندگان رابطه این فناوری و گروه‌های تروریستی را در چهار عرصه بهره‌برداری از فضای مجازی، استفاده از رسانه‌های دیجیتالی به عنوان اسلحه، ارتباطات به شدت محافظت‌شده، و مهار و کنترل فناوری‌های خودکار با بیان تجربه موفق داعش مطرح کرده‌اند. مقاله «واکاوی تأثیر سلاح‌های خودکار بر صلح و امنیت بین‌المللی» [۳] به تأثیرگذاری هوش مصنوعی در تسلیحات نظامی و صلح و امنیت بین‌المللی اختصاص یافته است. در زبان انگلیسی، تعداد منابع بسیار بیشتر از زبان فارسی است. البته بیشتر آن‌ها به ابعاد حقوق بشردوستانه و خطرات ناشی از توسعه این فناوری بر زیست مردم پرداخته‌اند. در کتاب «ربات‌های قاتل: قانونی بودن و اخلاقی بودن سلاح‌های خودمختار» [۴] نویسنده به

بررسی ابعاد قانونی و فنی و اخلاقی ربات‌ها و تبیین فرصت‌ها و چالش‌های این تجهیزات اشاره می‌کند. در مقاله «برای متوقف کردن مسابقه تسلیحاتی هوش مصنوعی خیلی دیر شده است؛ در عوض باید آن را مدیریت کنیم» [۵] مؤلف با اشاره به خطرات موجود از لزوم همکاری جهانی و استفاده از دیپلماسی برای مدیریت این فرایند سخن می‌گوید.

در مقاله «مسابقه تا پرتگاه: مدلی از هوش مصنوعی» [۶] نویسندگان با ارائه مدلی برای توسعه کم‌خطر این فناوری به بررسی خطرات توسعه نظامی هوش مصنوعی می‌پردازند. این مقاله مدل ساده‌ای از یک مسابقه تسلیحاتی هوش مصنوعی را ارائه می‌دهد. نتایج مدل‌سازی نشان می‌دهد افزایش اطلاعات، خطرات را افزایش می‌دهد: هرچه گروه‌ها بیشتر از توانایی‌های دیگران (در مورد خود) بدانند، خطر بیشتر می‌شود.

مروری بر ادبیات نشان می‌دهد بیشتر پژوهشگران به تنگناهای حقوقی و اخلاقی، لزوم بکارگیری دیپلماسی و یا ارتباط موضوع با حقوق بشردوستانه توجه کرده‌اند. ازاین‌رو، پژوهش حاضر درصدد رفع بخشی از این خلأ علمی با بیان کاربرد و تأثیرات هوش مصنوعی بر نسل جدید جنگ‌ها است.

۳ فضای سایبری

فضای سایبری از سه لایه‌ی فیزیکی، اطلاعاتی و اجتماعی به وجود می‌آید که متشکل از پنج جزء (جغرافیایی، شبکه فیزیکی، شبکه منطقی، شخصیت سایبری و شخص) است. لایه‌ی فیزیکی شامل جزء جغرافیایی و جزء شبکه فیزیکی است. جزء جغرافیایی موقعیت فیزیکی عناصر شبکه است؛ در حالی که مرزهای ژئوپلیتیکی را می‌توان به راحتی در فضای مجازی با سرعتی نزدیک به سرعت نور عبور داد، هنوز جنبه فیزیکی به سایر حوزه‌ها گره خورده است. جزء فیزیکی شبکه شامل تمام سخت‌افزار و زیرساخت (سیمی، بی‌سیم و نوری) است که از شبکه و اتصالات فیزیکی (سیم، کابل، فرکانس رادیویی، روترها، سرورها و کامپیوترها) پشتیبانی می‌کند. لایه‌ی منطقی شامل مولفه شبکه منطقی است که ماهیت فنی دارد و از اتصالات منطقی بین گره‌های شبکه تشکیل شده است. گره‌ها هر وسیله متصل به یک شبکه کامپیوتری مانند لپ‌تاپ‌ها و تلفن‌های همراه هستند. لایه‌ی اجتماعی شامل جنبه‌های انسانی و شناختی است و شامل مولفه‌های شخصیت سایبری و شخص می‌شود. مؤلفه شخصیت سایبری شامل هویت یا شخصیت یک شخص در شبکه (آدرس ایمیل، آدرس IP رایانه، شماره‌ی تلفن همراه و موارد دیگر) است. جزء شخص به افراد واقعی در شبکه اشاره دارد. یک فرد می‌تواند چندین شخصیت سایبری داشته باشد (به عنوان مثال، حساب‌های ایمیل مختلف در رایانه‌های مختلف) و یک شخصیت سایبری می‌تواند چندین کاربر داشته باشد [۷].

شبکه پروتکل فضای سایبری به این حقیقت تأکید دارد که محدوده عملیاتی به یک مکان فیزیکی محدود نمی‌شود. میدان‌های نبرد سنتی به فضای فیزیکی محدود می‌شوند اما گنجایش و ظرفیت فضای سایبری تا حد زیادی گسترده‌تر است و محدوده عملیات آن نیز پیچیده است. به عنوان مثال یک ویروس اجرا شده در فضای سایبری قادر است علاوه بر ضربه زدن به هدف تعیین‌شده به طور غیر مشخص به سامانه‌های موجود در دیگر کشورها از جمله خود کشور حمله‌کننده نیز لطمه بزند. خسارت‌های عظیم حملات معمولاً قابل پیش‌بینی نیست.

۴ جنگ سایبری

تغییر فناوری تسلیحات همواره بر جنگ تأثیرات ژرف گذاشته است. در قرن نوزدهم، نیروی زمینی و دریایی با قدرت توپخانه حرف اول را می‌زد، در قرن بیستم نیروی هوایی به عنوان بعد سوم توان نظامی و سپس در بعد چهارم فضا اضافه شد. در قرن بیست و یکم سایبر است که با چهار بعد دیگر آمیخته می‌شود. با پیشرفت فناوری و راهیابی هوش مصنوعی به این زمینه مخصوصاً در خصوص حمله بدافزارها و امنیت داده و امنیت سیستم با سلاحی مواجه هستیم که قابلیت کشتن انسان را دارد زیرا دیگر حمله فقط در فضای سایبر اتفاق نمی‌افتد؛ بلکه توانایی آسیب‌رساندن به تجهیزات فیزیکی نیروگاه‌ها، ایستگاه‌های راه‌آهن، فرودگاه‌ها، بیمارستان‌ها و ...وجود دارد که کشتن مستقیم هزاران انسان را ممکن می‌کند. جنگ سایبری در فضای سایبری انجام می‌شود و دستیابی به توانمندی‌های جنگ سایبری به حمله‌کننده، قدرت تخریب جبران‌ناپذیری حتی بدون شلیک یک گلوله می‌دهد. با تمرکز بر سامانه‌های الکترونیکی و ارتباطی طرف متخاصم، نیازی به اعزام لشکرها یا ناوهای جنگی نیست و به جای آن از ویروس‌های رایانه‌ای و بمب‌های پالس الکترومغناطیسی استفاده می‌شود که قادر است خرابی‌های وسیعی را در مدارات الکترونیکی به وجود آورد.

توان فوق‌العاده‌ای که یک کشور از این طریق کسب می‌کند می‌تواند دشمن را همچون یک بمب اتم منفعل کند بدون اینکه نیاز به بکارگیری ارتش متعارف باشد. در جنگ‌های متعارف معاصر همچون جنگ‌های خلیج فارس، بالکان، افغانستان و عراق، همواره حمله‌های پیشگیرانه و ویران‌کننده علیه مراکز فرماندهی، سایت‌ها و سامانه‌های راداری دفاع هوایی، مراکز ارتباطی فرماندهی و کنترل، انجام و متعاقب آن یورش به کارخانه‌های برق، دپوهای مهمات، سوخت و مراکز اصلی نیروهای آفندی نظامی کشورهای هدف واقع شده است. در جنگ سایبری نیز چنین سناریویی با اولویت‌بندی مشابه طرح‌ریزی می‌شود تا با زمین‌گیر ساختن دشمن بدون هرگونه برخورد فیزیکی و تحمیل خسارت پیروزی حاصل شود. از این رو، در این‌گونه جنگ‌ها، هدف نهایی فلج کردن و از کار انداختن سامانه‌ها و سازمان‌های معمول نظامی کشور هدف بوده تا نتوانند به فعالیت ادامه بدهند.

توجه به شبکه جنگ زمینی و آمیخته شدن آن با قدرت سایبری به روشن شدن بحث کمک می‌کند. شبکه جنگ زمینی، شبکه‌ای فنی است که شامل تمام سامانه‌های مدیریت اطلاعات ارتش و سامانه‌های اطلاعاتی است که جمع‌آوری، پردازش، ذخیره، نمایش، انتشار و محافظت از اطلاعات در سراسر جهان را انجام می‌دهد؛ بنابراین یک شبکه ساده نیست. این شبکه اطلاعات مورد نیاز فرماندهان در هر محیط و در هر زمان را برای تسهیل اقدامات اساسی تأمین می‌کند.

با توجه به افزایش وابستگی توانمندی شبکه عملیات زمینی یکپارچه به فضای سایبری، تهدیدات پالس‌های الکترونیک و هک اطلاعات حساسیت زیادی یافته است زیرا می‌توانند محرمانگی و یکپارچگی مأموریت سیستم فرماندهی و اطلاعات را به خطر اندازند. عملیات تهاجمی دشمن در فضای سایبری و طیف الکترومغناطیس در عملیات خودی نیز تأثیر می‌گذارد. توانایی دشمنان برای دستیابی به فضای سایبری نظامی منجر به دستکاری اطلاعات در سامانه‌های نظامی می‌شود؛ این تغییر می‌تواند اقدامات بعدی را تحت تأثیر قرار دهد و به بی‌اعتمادی در سیستم‌های خودی بینجامد. بی‌اعتمادی، کاهش درک موقعیت از محیط

و اطلاعات نظامی را در پی دارد. فناوری حتی مرگ ناشی از سلاح‌های کلاسیک را افزایش می‌دهد؛ مثل استفاده از لینک‌های داده و شبکه‌های مبتنی بر سامانه‌های هدف‌دار، هدف قرار دادن و هدایت نهایی از طریق سامانه‌های لیزری. سامانه‌های تعیین موقعیت جهانی، سلاح‌های جستجوگر و سلاح‌های هوشمند، درک فرمانده از وضعیت و محیط را افزایش می‌دهند. به نظر می‌رسد در فاز اول جنگ‌های آینده، درگیری‌ها به صورت مستقیم و رو در رو نخواهند بود بلکه نبردها در حوزه پنجم و در فضای سایبر اتفاق خواهد افتاد و پس از آن شاهد جنگ‌های رو در رو خواهیم بود لذا درگیری در دو فاز نبرد سایبری و جنگ اتفاق خواهد افتاد در درگیری‌های عادی و برتری با نیرویی است که توانایی مدیریت صحنه نبرد در هر دو فاز را دارد.

قدرت‌های جهانی از هوش مصنوعی برای توسعه و استقرار سامانه‌های تسلیحاتی خودمختار مرگبار که به عنوان «ربات‌های سلاخ» یا «ربات‌های قاتل» نیز شناخته می‌شوند، بهره می‌گیرند. این ربات‌ها، سامانه‌های تسلیحاتی هستند که از هوش مصنوعی برای شناسایی، انتخاب و کشتن اهداف انسانی بدون دخالت انسان استفاده می‌کنند. لذا رقابت در این حوزه شدید است. باید توجه کرد که (۱) به‌طور گسترده‌تر، هر رقابت برای هوش مصنوعی برتر گاهی اوقات به‌عنوان یک «مسابقه تسلیحاتی» در نظر گرفته می‌شود؛ (۲) تلاش برای تسلط بر هوش مصنوعی نظامی با تلاش برای تسلط در بخش‌های دیگر همپوشانی دارد، به ویژه زمانی که کشوری به دنبال مزایای اقتصادی و نظامی است.

۵ هوش مصنوعی و کاربردهای نظامی در فضای سایبری

پیشرفت در هوش مصنوعی یادگیری عمیق و رباتیک قابلیت‌های جدیدی را امکان‌پذیر می‌کند که استراتژی‌های نظامی را به طور قطع تحت تأثیر قرار می‌دهد. پیامدهای این تحولات بر مجموعه‌ای از معیارهای نظامی شامل دانش، نظارت، شناسایی تا موازنه‌های حمله و دفاع و حتی خود برنامه‌های هسته‌ای اثر می‌گذارد. در ادامه به بررسی هفت کاربرد نظامی قابل توجه پرداخته می‌شود که با فناوری هوش مصنوعی در حال توسعه هستند [۸].

نیروهای رزمی و دفاعی در سراسر زمین در حال توسعه عنصر هوش مصنوعی در سلاح‌هایی هستند که در بخش‌های زمینی، هوایی، دریایی و فضایی استفاده می‌شوند. بهره‌گیری از هوش مصنوعی در سامانه‌های وابسته به این بخش‌ها پیشرفت‌های معمول جنگی را که کمتر به مداخله انسان وابسته هستند ممکن کرده است. همچنین هوش مصنوعی توانایی این را دارد که دسته یا گردان یا واحدی از سلاح‌های خودگردان و پرسرعت را مدیریت کرده و سرعت مدیریت و حملات را از چندین جهت افزایش داده و همچنین توانایی پدافند را بسیار کند نماید.

۱.۵ لجستیک و حمل و نقل

یکی از اجزای اساسی فعالیت‌های نظامی موفق شبکه حمل و نقل قوی، تدارکات تسلیحات، مهمات و مهم‌تر از همه نیروی انسانی است. یک مکانیسم دفاعی برای ایفای نقش محوری در لجستیک و حمل و نقل نظامی به کمک هوش مصنوعی نیاز زیادی دارد. ترکیب هوش مصنوعی با حمل و نقل نظامی می‌تواند هزینه‌های حمل

و نقل را به حداقل برساند و عملکرد انسان‌ها را بهبود بخشد. همچنین ناوگان‌های دریایی را قادر می‌سازد تا در مواجهه با مین‌های دریایی آن‌ها را راحت‌تر تشخیص دهند و سرعت خرابی اجزا را پیش‌بینی کنند و هزینه نگهداری آن را بسیار کاهش دهند. برای مثال ارتش ایالات متحده از پلتفرم هوش مصنوعی واتسون ساخت شرکت آی‌بی‌ام برای کمک به تعیین پیچیدگی‌های تعمیر و نگهداری در وسایل نقلیه جنگی Stryker استفاده می‌کند.

۲.۵ شناسایی اهداف

در موقعیت‌های نبرد چندگانه رویه‌های هوش مصنوعی برای افزایش دقت تشخیص هدف بسیار مفید بوده و این امکان با تجزیه و تحلیل اسناد و شواهد مستند، محتوای خبری و انواع منابع اطلاعاتی امکان‌پذیر است. تحلیل داده‌ها، مأموران امنیتی را قادر می‌سازد تا دانش گسترده‌ای از حوزه‌های مختلف عملیات به دست آورند. تکنیک‌های چارچوب تشخیص هدف مبتنی بر هوش مصنوعی قادر به تخمین استراتژی دشمن و مجموعه‌ای از شرایط اقلیمی و محیطی و حتی فرهنگی هستند.

۳.۵ مراقبت‌های بهداشت و درمانی منطقه رزمی

با ترکیب هوش مصنوعی و علم رباتیک می‌توان در مناطق جنگی به طور کلی از جراحی از راه دور و تخلیه از راه دور انجام داد. تحت شرایط جنگی سامانه‌های مجهز به هوش مصنوعی می‌تواند مسائل پزشکی مربوط به سربازان را بسیار سریع‌تر پوشش دهند و به تشخیص‌های پیچیده کمک کنند. برای مثال در ایالات متحده یک ماژول نمونه اولیه استدلال بالینی که به عنوان تحلیلگر پرونده الکترونیک پزشکی شناخته می‌شود (EMRA[1]) توسعه یافته است. در این فناوری، مکانیسم یادگیری ماشین برای پردازش تاریخچه‌ی پزشکی الکترونیکی بیماران و شناسایی و اولویت‌بندی اساسی‌ترین اختلالات آن‌ها به طور مؤثر به کار برده شده است. ناتو نیز با استفاده از هوش مصنوعی در پی ایجاد و توسعه سامانه گزارش‌دهی و ردیابی پزشکی دیجیتال برای وارد کردن مفهوم سلامت دیجیتال به میدان نبرد است [۹].

۴.۵ شبیه‌سازی رزمی و تمرین

شبیه‌سازی و یادگیری، طیفی چندوجهی است که شامل طراحی فرآیند و برنامه‌نویسی نرم‌افزار برای ایجاد برنامه‌های کاربردی نرم‌افزاری است که سربازان را با بسیاری از سامانه‌های جنگی که در طول عملیات نظامی به کار می‌روند آشنا کرده و به نوعی از آن‌ها مراقبت می‌کند. نیروی دریایی ایالات متحده سازمان‌هایی مانند SAIC, ATK را برای ارتقای پروژه‌های خود ثبت کرده است در حالی که طرح‌های ارتش ایالات متحده توسط نهادهایی مانند CACI, TORCH MILLENIUM ENGINEERING TECHNOLOGIES تقویت می‌شوند.

[1] Electronic Medical Record Analyst

۵.۵ نظارت بر تهدید و آگاهی از موقعیت

تشخیص تهدید و آگاهی از موقعیت به فعالیت‌های اطلاعاتی، نظارت و شناسایی (ISR[۲]) وابسته است. ISR عبارت است از کسب، پردازش و ارائه به موقع، دقیق، اطلاعات مرتبط، منسجم و مطمئن برای پشتیبانی از اجرای فعالیت‌های هماهنگی و یکپارچگی فرماندهی. در ترتیبات رباتیک مورد استفاده برای انجام مأموریت‌های ISR از راه دور اطلاعات ساخته و از طریق مسیرهای از پیش تعریف‌شده ارسال می‌شود. از طرفی، تکمیل مجدد این سامانه‌ها از طریق هوش مصنوعی به شناسایی تهدیدها کمک می‌کند و در نتیجه آگاهی آن‌ها را افزایش می‌دهد. از طرف دیگر پهپادها با ویژگی‌های یکپارچه هوش مصنوعی با تفسیر تهدیدات احتمالی و انتقال داده‌های مربوط به این خطرات به محافظت از مناطق حساس مرزی کمک می‌کنند؛ بنابر این استفاده از پهپادها می‌تواند ایمنی تأسیسات نظامی استراتژیک را تقویت کند و در عین حال امنیت و قدرت کنش و واکنش کارکنان نظامی را در میدان جنگ و بخش‌های دورافتاده بهبود بخشد.

۶.۵ هوش مصنوعی و پردازش داده‌ها

هوش مصنوعی برای سرعت زیاد و دقیق بودنش معروف است. این سرعت و دقت برای حجم زیادی از داده‌ها برای به دست آوردن اطلاعات ارزشمند مفید است. هوش مصنوعی می‌تواند به پردازش و تجمیع اطلاعات از پایگاه داده‌های متنوع و همچنین به دست آوردن اطلاعات از منابع مختلف خارجی کمک کند؛ این کار ارتش را برای تفسیر الگوها و استنتاج روابط بسیار توانمند می‌سازد.

۷.۵ هوش مصنوعی و پرنده هدایت‌پذیر

پرنده هدایت‌پذیر از دور یا به اختصار پَهپاد که به آن هواپیمای بدون سرنشین نیز می‌گویند، گونه‌ای هواگرد هدایت‌پذیر از راه دور و بی‌خلبان است. پرواز پهپادها ممکن است تحت کنترل از راه دور توسط یک اپراتور انسانی، یا با درجات مختلفی از خودمختاری، مانند کمک توسط خلبان خودکار تا هواپیماهای کاملاً خودمختار انجام شود که هیچ شرطی برای مداخله انسانی ندارند [۱۰].

از هوش مصنوعی در هواپیماهای بدون سرنشین برای هوشمندتر کردن این ماشین‌های پرنده استفاده می‌شود. این‌ها نوعی پهپاد هستند اما تنها یک ماشین پرنده مکانیکی ساده نیستند؛ آن‌ها محیط اطرافشان را آنالیز کرده و به محیط اطراف واکنش نشان می‌دهند یا به هر چیزی که در اطرافشان رخ می‌دهد. به طور همزمان الگوریتم‌ها به این ماشین‌های مستقل اجازه می‌دهند که در صف نزدیک به هم پرواز کرده و از وجود یکدیگر به مانند حضور انسان‌ها مطلع باشند. پهپادهای مختلفی شامل پهپادهای مجهز به هوش مصنوعی با قابلیت‌های پرواز ارتفاع بالا و انجام انواع مأموریت‌ها در ارتش‌های جهان در حال خدمت هستند.

[2]Intelligence Surveillance and Reconnaissance

۶ نتیجه‌گیری

جنگ سایبری برای تشریح نوع جدیدی از جنگ که بر سامانه‌های ارتباطی و الکترونیکی دشمن متمرکز می‌گردد، ابداع شده است. این جنگ یکی از ستون‌های اصلی جنگ نامتقارن است که عدم تقارن در فناوری، تاکتیک و استراتژی را آشکار می‌کند. نابرابری توان تجهیزاتی و قدرت نظامی کشورهای متخاصم منجر به بکارگیری تاکتیک‌های غیر کلاسیک ازسوی طرف ضعیف‌تر شده است. در این نوع از جنگ، نیازی به اعزام لشکرها یا ناوهای جنگی نبوده و به جای آن از ویروس‌های رایانه‌ای و بمب‌های پالس الکترومغناطیسی استفاده می‌شود که قادر است خرابی‌های وسیعی در مدارات الکترونیکی به وجود آورد.

دستیابی به توانمندی جنگ سایبری، به حمله‌کننده، قدرت تخریب جبران‌ناپذیری حتی بدون شلیک یک گلوله می‌دهد. میدان نبرد تغییر می‌یابد، فنون نظامی جدیدی ابداع و ابعاد جدیدی از ژئواستراتژی و ژئوپلیتیک نبرد آشکار میشود. چنین فناوری‌هایی به دلیل توانایی‌های برتر محاسبه و تصمیم‌گیری‌شان، خودتنظیمی[۳]، خودکنترلی[۴] و خودفعال‌سازی[۵] را تقویت کرده‌اند. توان فوق العاده‌ای که یک کشور از این طریق کسب می‌کند، می‌تواند دشمن را منفعل کرده و در عین حال ارتش کلاسیک، سازمان‌یافته و منظمی هم به کار گرفته نشده باشد.

نسل جدید جنگ در روابط بین الملل با کاربرد هوش مصنوعی آغاز شده است. بهره‌گیری از هوش مصنوعی به عنوان یک سلاح در میدان نبرد برای توفیق در عملیات نظامی قدرت برتر را به کشورهایی خواهد بخشید که قدرت‌های جهانی نیستند اما نسلی پیشرو از نخبگان علمی با ایده‌های جدید را در اختیار دارند که می‌توانند توازن قدرت در عرصه بین المللی را تغییر دهند. پژوهش فعلی با آشکار کردن ابعادی از کاربرد هوش مصنوعی در فضای سایبری، راه را برای گسترش بحث در خصوص آثار آن بر موازنه قدرت و موازنه تهدید، بازدارندگی و سایر موضوعات مهم روابط بین‌الملل باز می‌کند.

مراجع

[۱] قلیزاده، میثم؛ حقیقی، مهدی؛ رضایی، علیرضا؛ و قاسمی، ابراهیم. هوش مصنوعی، نحوه عملکرد آن در امنیت دفاعی کشورهای پیشرفته و کاربرد و ضرورت آن در امور نظامی. مجموعه مقالات کنفرانس بین‌المللی امنیت، پیشرفت و توسعه پایدار مناطق مرزی، سرزمینی و کلان‌شهرها، راهکارها و چالش‌ها با محوریت پدافند غیرعامل و مدیریت بحران، ۱۳۹۷.

[۲] شیرودی، محمدسجاد؛ همتی، مجید؛ و سیاه‌پوش، ابراهیم. هوش مصنوعی و آینده حملات گروه‌های تروریستی تکفیری. فصلنامه مطالعات آسیای جنوب غربی، ۱۳۹۹.

[۳] عزیزی‌بساطی، مجتبی؛ و سکوتی، مرضیه. واکاوی تأثیر سال‌های خودکار بر صلح و امنیت بین‌المللی. سیاست خارجی، ۱۳۹۴.

[4] Krishnan, A. *Killer Robots: Legality and Ethicality of Autonomous Weapons*. Rutledge, 2009.

[3] self-regulation
[4] self-control
[5] self-actuation

[5] Geist, E. M. It's already too late to stop the ai arms race, we must manage it instead. *Bulletin of the atomic scientists*, 2016.

[6] Armstrong, S, Nick Bostrom Carl Shulman. Racing to the precipice: a model of artificial intelligence development. tech. rep., Future of Humanity Institute, https://link.springer.com/article/10.1007/s00146-015-0590-yI, 2015.

[7] Crowther, G. Alexander. National defense and the cyber domain. *2018 Index of Military Strength*, https://www.heritage.org/sites/default/files/2017-10/2018_IndexOfUSMilitaryStrength-2.pdf, 2018.

[8] Abell, Nicholas. 7 key military applications of machine learning.

https://medium.com/@nqabell89/7-key-military-applications-of-machine-learning-9818dfa2ea86, 2020.

[9] Jänig, Ch. W., Koblenz B. Bringing digital health to the battlefield - a conceptional approach for a standardized nato digital medical reporting and tracking system. *Conference: Military Health System Research Symposium 2020 At: Kissimmee, Florida, July 2020*.

[10] Cary, L., Coyne J. *ICAO Unmanned Aircraft Systems (UAS)*, pp. 112 – 115. Blyenburgh and Co., Paris, France, 2011.