فصلنامه علمی مطالعات روابط بین‌الملل
دوره ۱۷، شماره ۳، شماره پیاپی (۶۷)، پاییز ۱۴۰۳، ص ۲۳۷ ـ ۲۱۷

مقاله پژوهشی

بررسی تهدیدها و فرصت‌های نظامی و سیاسی هوش مصنوعی بر امنیت ملی ایران

گارینه کشیشیان سیرکی[۱] جواد ایزدی[۲] طاهره نظافتی[۳]

تاریخ دریافت: ۱۴۰۳/۰۳/۲۹ تاریخ پذیرش: ۱۴۰۳/۰۹/۱۵

چکیده:

هوش مصنوعی از فناوری‌هایی است که قابلیت تأثیر بر ابعاد سیاسی و نظامی امنیت ملی دولت‌ها را دارد. بنابر یک تعریف کاربردی، هوش مصنوعی دانش ساخت ماشین‌هایی است که کارهایی را انجام می‌دهند که اگر توسط انسان انجام شود نیاز به هوش دارد. این پژوهش در قالب روش توصیفی – تحلیلی و سطوح امنیت در پی پاسخ به این سوال است که هوش مصنوعی چه تهدید و فرصت‌هایی در ابعاد نظامی و سیاسی امنیت ملی ایران دارد؟ نتایج نشان می‌دهد که هوش مصنوعی تهدیدها و فرصت‌های سیاسی و نظامی بر امنیت ملی ایران به همراه داشته است. مهم‌ترین تهدیدهای نظامی شامل افزایش حمله سایبری به تأسیسات هسته‌ای، حملات سایبری به نهادهای داخلی، جاسوسی و ترور افراد با سلاح‌های خودران است. فرصت‌های هوش مصنوعی در حوزه نظامی شامل تجهیز سلاح‌های موشکی و پهپادی، دستیابی به سلاح‌های رباتیک و قدرت بازدارندگی سایبری است. مهم‌ترین تهدیدهای هوش مصنوعی در حوزه سیاسی شامل حملات سایبری به صداوسیما و طراحی اخبار دروغ برای فریب افکار عمومی می‌شود. مهم‌ترین فرصت‌های بهره‌گیری از هوش مصنوعی در این حوزه نیز شامل تلاش برای تأثیر بر انتخابات و تقابل‌های راهبردی در سیاست خارجی است.

واژگان اصلی: هوش مصنوعی، امنیت ملی، تهدید، امنیت نظامی، امنیت سیاسی.

۱. دانشیار گروه علوم سیاسی و روابط بین الملل، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول)
g.keshishyan71@gmail.com
۲. دانش آموخته گروه علوم سیاسی و روابط بین الملل، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.
۳. دانشجوی گروه علوم سیاسی و روابط بین الملل، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.

مقدمه

ظهور فناوری هوش مصنوعی در چند دهه گذشته تغییرات بسیاری را به وجود آورده است. سیستم‌های مبتنی بر هوش مصنوعی خودمختار هستند و می‌توانند بدون مداخله انسانی به فعالیت بپردازند و با آموختن الگوهای تصمیم‌گیری هوشمند و بر اساس تحلیل موقعیت به نتیجه‌گیری متفاوتی برسند. سرمایه‌گذاری در فناوری‌های جدید هوش مصنوعی از راهبردهای مهم دولت‌ها است. استفاده از این سیستم‌ها با قابلیت منحصر به فرد در ابعاد امنیتی و تجاری به سرعت در حال گسترش است. موج جدید سیستم‌های هوش مصنوعی توانایی سازمان برای استفاده از داده‌ها را برای پیش‌بینی آینده سازمان و تصمیم‌گیری بهبود داده و هزینه پیش‌بینی را کاهش داده است (روشن و دیگران، ۱۴۰۰: ۱۱۸).

هوش مصنوعی در حوزه شخصی موضوعاتی مانند حفظ حریم خصوصی شهروندان، امنیت ملی و انسانی و در حوزه شرکت‌ها حفظ منافع، حقوق شخص ثالث، مالکیت فکری و حفاظت از داده‌های عمومی و تحلیل آنها، در حوزه نظامی توسعه سیستم‌های سلاح خودکار، از کاربردهای سیستم‌های مبتنی بر هوش مصنوعی است. سیستم نظامی هوش مصنوعی از این قابلیت برخوردارند که رویکردهای موجود برای حل مسالمت‌آمیز مناقشه را به حاشیه ببرند. قرار گرفتن پهپادهای هوشمند در اختیار گروه‌های تروریستی قابلیت تهاجمی آنها علیه دولت‌ها را افزایش می‌دهند.

هدف اصلی این پژوهش بررسی تهدیدها و فرصت‌های سیاسی هوش مصنوعی بر امنیت ملی ایران است. هوش مصنوعی در ایران از دو دهه گذشته مطرح بوده و در سال‌های اخیر استفاده از آن در حوزه‌های سیاسی، نظامی، امنیتی، سایبری و ... گسترش یافته است. بر این اساس می‌توان گفت که این فناوری در ایران نیز مانند سایر کشورها با تهدیدها و فرصت‌هایی همراه بوده است. تهدیدهای هوش مصنوعی علیه امنیت ملی بیشتر از همه مربوط به مقابله با دولت و ارکان آن است و همچنین ریشه در منازعات سیاسی و نظامی بین ایران و سایر کشورها دارد. حملات سایبری و هدف قرار دادن دانشمندان با استفاده از سلاح‌های متکی بر هوش مصنوعی نمونه‌هایی از این تهدیدهاست. در عین حال فرصت‌های ناشی از هوش مصنوعی قابلیت‌های جدیدی در حوزه بازدارندگی نظامی و همچنین پیش‌بینی‌پذیری در حوزه سیاسی در اختیار دولت قرار داده است. انجام پیش‌بینی نتایج انتخابات و بهره‌گیری از این فناوری برای تبیین اهداف و راهبردهای رقبا از این جمله است.

۲. ادبیات نظری و پیشینهٔ پژوهش

امنیت از مفهوم Secure اخذ گردیده است که در زبان فارسی معادل‌هایی چون امن، محفوظ، آسایش و ... برای آن آورده شده است. امنیت در برداشت عینی به معنای فقدان تهدید در کسب ارزش‌ها و در برداشت ذهنی به معنای فقدان ترس از مورد تهدید قرار گرفتن این ارزش‌ها تعریف می‌شود (کلودزیچ، ۱۳۸۷). امنیت ملی مفهومی است که تا اواخر قرن نوزدهم میلادی تعریف جامعی از آن در دسترس نبود. با ایجاد ملت – کشور، امنیت ملی به عنوان مفهومی نوظهور در قالب بقای ملی مطرح شد. پس از فروپاشی شوروی، امنیت ملی شکل جامع‌تری یافت و علاوه بر تهدید نظامی، تهدیدهای اقتصادی، اجتماعی، زیست محیطی و سیاسی را هم شامل شد (سیف، ۱۳۸۹: ۸). امنیت ملی در نگاه سلبی به معنای فقدان تهدید خارجی است. اما در نگاه ایجابی، امنیت شکل درون‌نگر دارد که طبق آن، ابعاد تهدید افزایش می‌یابد که در درون خود نوع جدیدی از مدیریت امنیت را نیز به همراه داشته است (عبدالله‌خانی، ۱۳۸۹: ٦٦-٦٤).

آشکار شدن ابعاد مختلف امنیت ملی از ابتدای دهه ۱۹۹۰ ناشی از مطالعات بوزان[1] ویور[2] و دوویلد[3] بود که به مکتب کپنهاگ معروف شدند. این مکتب به ویژه بعد از انتشار کتاب «مردم، دولت و هراس» اولین رهیافتی است که در راستای پایه‌گذاری جایگاهی مستقل برای مطالعات امنیتی تلاش نمود. امنیت در مکتب کپنهاگ با فقدان تهدید رابطه‌ای این همانی دارد و در آن بیش از همه به مرجع امنیت توجه شده است. در بخش سیاسی، حاکمیت و در بخش اجتماعی، هویت مرجع امنیت است. مفاهیم انتزاعی چون موازنه قوا، جامعه بین‌الملل، عدم گسترش جنگ‌افزارهای هسته‌ای و میکروبی و حقوق بین‌الملل نیز به عنوان مرجع امنیت مطرح است (قرشی، ۱۳۹۳: ۳٦-۳۵). اندیشمندان مکتب کپنهاگ با فاصله گرفتن از دیدگاه سنتی امنیت، امنیت ملی را در سطح دولت مطرح کردند. محوریت دولت سبب شد تا نظریه‌پردازان این مکتب، امنیت ملی را به عنوان مهم‌ترین بعد در میان ابعاد مختلف امنیت در نظر بگیرند و برای آن ابعاد نظامی، سیاسی، اقتصادی، اجتماعی و زیست محیطی را ذکر کنند (عبدالله‌خانی، ۱۳۸۹).

امنیت نظامی در تعریف امروزی به معنای نبود تهدیدات نظامی خارجی و داخلی علیه ارزش‌های

1. Bary Buzan
2. Weaver
3. Jop DoWild

مکتسب مادی و معنوی کشور و عدم احساس ترس از تهدید آن است (دهقانی فیروزآبادی، ۱۳۹٦: ۲۲). امنیت نظامی از نظر بوزان تنها به انگیزه‌های سیاسی دولت‌ها مربوط نیست، بلکه با مسائل ناشی از تاثیر تدابیر نظامی آنها نیز مرتبط است (بوزان، ۱۳۹۰: ۳۲۷). امنیت سیاسی عبارت است از ثبات سازمانی و ساختاری کشور، نظام حکومتی و ایدئولوژی مشروعیت‌بخش به دولت و نظام حکومتی آن. ناامنی در حوزه امر سیاسی، هم امنیت تک‌تک افراد جامعه را دچار خدشه می‌سازد و هم امنیت کشور (دولت ـ ملت) را تحت تاثیر قرار می‌دهد (رحمت‌اللهی و دیگران، ۱۳۹٤: ۱۱٦). به نظر می‌رسد که مکتب کپنهاگ موفق شد تا مطالعات امنیت ملی را از شکل سنتی نظامی خارج ساخته و ابعاد و زوایایی دیگری را نیز همچون ابعاد سیاسی، محیط زیستی، اقتصادی و اجتماعی برای آن مطرح کند.

پیشینه تحقیق

در مورد تأثیرات نظامی و سیاسی هوش مصنوعی بر امنیت ملی ایران آثار چندی تاکنون منتشر شده است که در زیر برخی از آنها بررسی شده است.

محقق	عنوان	روش	نتایج
علینقیان و همکاران، (۱٤۰۱)	اهداف و ابزارهای سیاستی توسعه هوش مصنوعی؛ جستاری در برنامه‌های سیاستی کشورهای منتخب	کیفی و تحلیل مضمون	توسعه هوش مصنوعی علاوه بر کسب منافع اقتصادی و رفاه، چالش‌های اخلاقی و امنیتی پیرامون توسعه این فناوری را در نظر دارد.
احمدی و همکاران، (۱٤۰۱)	نقش فناوری‌های نوظهور در امنیت و قدرت ملی کشورها: فرصت ها و تهدیدها	توصیفی – تبیینی	فناوری نوظهور به عنوان یک ابزار نوین در اختیار کنش‌گران دارای تهدیدها و فرصت‌هایی است که کارگزاران سپهر بین‌الملل باید بر اساس نیاز و با بهره‌مندی از ظرفیت‌های موجود، تمامی تهدیدها را به فرصت تبدیل نموده و در راستای منافع ملی بکار

			گیرند.
محمدحسینی و همکاران، (۱۳۹۹)	پیشران‌های ارائه خدمات سایبری پایدار در دولت با تاکید بر حفظ امنیت از طریق هوش مصنوعی	توصیفی – تحلیلی	۱۲ پیشران که دارای بیشترین پتانسیل ارائه خدمت در حوزه سایبری هستند، شناسایی شد. لازم است دولت در ارائه خدمات سایبری، میزان تاثیر سازمان از هم را در نظر گرفته و از اخذ تصمیم پراکنده بدون اولویت‌بندی مشخص، اجتناب کند و در تحقق خدمات سایبری بر رعایت بعد امنیت اهتمام نماید.
پورعزت و همکاران، (۱۳۹۷)	بازگشت عقلانیت؛ کاربست هوش مصنوعی	توصیفی – تحلیلی	به وسیله هوش مصنوعی تلاش می‌شود تا ظرفیت پردازش و تحلیل داده‌ها و با سرعت شگرف در خدمت حل مسائل عمومی قرار گرفته و زمینه‌سازی برای بازگشت عقلانیت به خط‌مشی گذاری عمومی انجام شود.
سیلر و همکاران، (۲۰۲۰)	هوش مصنوعی و امنیت ملی	توصیفی – تحلیلی	هوش مصنوعی در اطلاعات دفاعی، نظارت و جاسوسی، لجستیک، فضای سایبری، اطلاعات – عملیات و فرماندهی و کنترل سیستم‌های تسلیحاتی خودکار و نیمه‌خودکار کاربرد دارد و یکپارچه‌سازی فناوری نظامی را به چالش می‌کشد.

دافوی، (۲۰۱۸)	درآمدی بر حکمرانی هوش مصنوعی	توصیفی – تحلیلی	هوش مصنوعی در حوزه‌های پزشکی، حمل‌ونقل، انرژی، آموزش، رشد اقتصادی و پایداری محیط فرصت‌ساز است. مخاطرات آن نیز در زمینه حکمرانی عبارتند از: جابجایی نیروی کار، نابرابری، دگرگونی در قدرت ملی و بی‌ثباتی راهبردی

در مجموع با بررسی پژوهش‌های بالا مشخص شد که این پژوهش‌ها عمدتاً به هوش مصنوعی و چیستی آن، یا هوش مصنوعی را به مثابه ساختاری در نظر می‌گیرند که می‌توان علوم مختلف طبیعی و اجتماعی را در ضمن آن بررسی و مطالعه کرد. برخی نیز هوش مصنوعی را در چارچوب تهدیدات سایبری و تأثیر آن بر امنیت ملی بررسی کرده‌اند. این در حالی است پژوهش حاضر ابتدا به دنبال بررسی چیستی و مؤلفه‌های تاثیرگذار بر هوش مصنوعی در حوزه‌های سیاسی و نظامی و بعد از آن تهدیدها و فرصت‌های این فناوری برای امنیت ملی ایران است.

۳. بحث و بررسی

مفهوم‌شناسی هوش مصنوعی[1]

ظهور پدیده هوش مصنوعی موجب اقبال پژوهشگران به آن در حوزه سیاست و امنیت شد. هوش مصنوعی به عنوان شاخه‌ای از علوم رایانه‌ای برای شبیه‌سازی هوش طبیعی در ماشین است و با علوم فلسفه، زبان‌شناسی، ریاضی، روانشناسی، فیزیولوژی ارتباط دارد. سیستم‌های مبتنی بر هوش مصنوعی می‌توانند واکنش‌هایی مشابه رفتار هوشمند انسان مانند درک شرایط پیچیده، شبیه‌سازی فرایندهای تفکر و شیوه‌های استدلال انسانی و پاسخ موفق به آنها، یادگیری و توان کسب دانش و استدلال برای حل مسائل داشته باشند. جان مکارتی که واژه هوش مصنوعی را در ۱۹۵۶ استفاده نمود، آن را دانش ساخت ماشین‌های هوشمند به ویژه برنامه‌های رایانه‌ای هوشمند، معرفی نمود (Horowitz and et

1. Artificial Intelligence

.(al, 2018

چهار نوع تعریف از هوش مصنوعی وجود دارد شامل سامانه‌هایی که شبیه انسان می‌اندیشند؛ سامانه‌هایی که به گونه‌ای عقلانی می‌اندیشند؛ سامانه‌هایی که شبیه انسان رفتار می‌کنند و سامانه‌هایی که به گونه‌ای عقلانی رفتار می‌کنند (مقدس، ۱۳۹۹: ۱۶۳). در تعریف گروه تخصصی هوش مصنوعی کمیسیون اروپا[1]«سیستم‌های هوش مصنوعی، سیستم‌هایی هستند که توسط انسان طراحی شده‌اند تا در صورتی که یک تکلیف پیچیده به عهده آنان قرار گیرد آنان به صورت فیزیکی یا در ابعاد دیجیتالی با درک محیط اطراف خود از طریق به دست آوردن داده‌ها و تحلیل و تفسیر داده‌های به دست آورده ساختاریافته یا ساختارنیافته، استدلال کردن بر اساس یافته‌ها، یا با تحلیل اطلاعاتی که از این داده‌ها به دست آورده‌اند عمل کنند و برای انجام دادن بهترین عمل با هدف انجام دادن تکلیف اولیه تصمیم بگیرند.» سیستم‌های هوش مصنوعی می‌توانند قواعد نمادین یا مدل‌های اعدادی را یاد بگیرند و رفتار خود را بر اساس تحلیل تأثیر اعمال قبلی خود بر محیط وفق دهند. به رغم این، تعاریف هوش مصنوعی یکسان نیست و طی زمان تغییر کرده است (تخشید، ۱۴۰۰: ۲۳۲–۲۳۱). از مهم‌ترین زبان‌های برنامه‌نویسی هوش مصنوعی نیز لیسپ[2]، پرولوگ[3]، کلیپس[4] و ویپی اکسپرت[5] است (Allen and Chan, 2017).

هوش مصنوعی در شکل ابتدایی در دهه ۱۹۴۰ با پژوهش‌های آلن تورینگ[6] و کلود شانون[7] متولد شد. در جنگ جهانی دوم، اهمیت شکستن پیام‌های رمز باعث شد تا تورینگ که به پدر هوش مصنوعی جهان معروف شد، ساخت ماشین رمزشکن را آغاز کرد. او آزمونی برای سنجش هوشمندی ماشین‌ها طراحی کرد که به آزمون تورینگ مشهور است (محمدعلی خلج، ۱۳۹۳: ۱۰۴). در دهه ۱۹۵۰ میلادی دانشگاه دارتموث آمریکا یک پروژه تحقیقاتی را به هوش مصنوعی اختصاص داد. هوش مصنوعی بعد از معرفی سوپرکامپیوتر «دیپ بلو»[8] توسط کمپانی IBM بیشتر توجه جهان

1. European Commission’s High-Level Expert Group on Artificial Intelligence
2. Lisp
3. Prolog
4. Clips
5. VIP Expert
6. Alan Mathison Turing
7. Claude Shannon
8. Deep Blue

جلب کرد (Hauser, 2019: 2). دهـه ۱۹۶۰ دهـه پیشـرفت تحقیقـات هـوش مصـنوعی بـود کـه برنامه‌های بازی شطرنج و ربات‌های هوشمند ساخته شـدند. از دهـه ۱۹۸۰ بـا سـاخت اولـین سـامانه خبره تجاری، به نام R1 در شـرکت Digital Equipment Corporation و تولیـدات مشـابه آن در دهه ۱۹۹۰ باعث شد تا هوش مصنوعی در مسیر پیشرفت‌های جدید و سریع قرار گیرد.

امروزه کشورها سعی دارند با بکارگیری هوش مصنوعی در سیاست، امنیت، اقتصاد و ... بـه مقابلـه بـا تهدیدات بپردازد. پیش‌بینی می‌شود هوش مصنوعی تا سال ۲۰۳۰ میلادی حدود ۱۵ تریلیـون دلار بـه اقتصاد جهانی تزریق کند. چین، آمریکا، بریتانیا، کانادا، روسیه، آلمان، نـروژ، سـوئد، فرانسـه و هنـد بـه ترتیب ۱۰ کشور برتر در این عرصه هستند (شـیرودی و همکـاران، ۱۳۹۹: ۲). پیشـرفت‌های اخیـر در قدرت محاسباتی و الگوریتم‌های بهبودیافته منجر به پیشرفت زیادی در قابلیت هـوش مصـنوعی شـده است. ارزش سیستم‌های هوش مصنوعی بیش از همه ناشی از ارزان‌تر، سریع‌تر یا آسـان‌تر اسـتقرار در مقیاس نسبت به تخصص انسانی است (Scharre and et al, 2018: 8-9).

یک سند پایه‌ای توسعه برنامه‌های هوش مصنوعی «توصیه‌های سازمان همکـاری و توسـعه اقتصـادی»[1] در سـال ۲۰۱۹ اسـت کـه از آن بـه نقشـه راه انتخـاب اهـداف و ابزارهـای لازم بـرای رویـارویی بـا چالش‌های گسترش هوش مصـنوعی و افـزایش مزیت‌هـای آن در اختیـار سیاسـت‌گذاری نـام بـرده می‌شود. این توصیه‌ها عبارتند از: ۱- تسهیل سرمایه‌گذاری عمومی و خصوصـی در تحقیـق و توسـعه هوش مصنوعی، ۲- پرورش اکوسیستمی دیجیتال برای توسعه هوش مصنوعی بـا حمایـت از تمـامی ذی‌نفعان و تسهیل فعالیت آنها در اکوسیستم، ۳- شکل دادن فضای سیاسـتی امکان‌پـذیر بـرای هـوش مصنوعی که در آن در عین وجود قوانین و استانداردهای لازم از خفـه شـدن نـوآوری نیـز جلـوگیری شود، ٤- فراهم کردن شرایط برای مردم به منظور کسب مهارت‌های لازم برای موفقیت در شـغل‌هایی که با افزایش استفاده از هوش مصنوعی به وجود می‌آیند و ۵- ایجاد شـرایط شبکه‌سـازی و همکـاری بین‌المللی برای بهره‌مندی از هوش مصنوعی قابل اعتماد (علی نقیان و همکاران، ۱٤۰۱: ٦).

کاربردهای هوش مصنوعی در عرصه نظامی

امنیت نظامی یک بخش اصلی را در امنیت ملی تمام کشورها تشکیل می‌دهد. سیسـتم‌های خودمختـار که از حسگر برای راه‌اندازی یک اقدام نظامی خودکار استفاده می‌کنند مانند مین‌های زمینـی حـداقل از

1 OECD

زمان جنگ جهانی دوم در جنگ استفاده شده‌اند. رایانه‌ها از آن زمان مسئولیت بیشتری در استفاده از زور به عهده گرفته‌اند. با اختراع بمب‌های Norden BombsightD و V-1 buzz در جنگ جهانی دوم، سیستم‌های رایانه‌ای برای اولین‌بار به حسگرهایی مرتبط شدند که در کنترل و کاربرد دینامیکی دخیل بودند. برای مثال، موشک‌های موسوم به آتش و فراموش[1] به حسگرهای داخلی اجازه می‌دهند تا موشک را بدون ارتباط بیشتر با اپراتور پس از انتخاب هدف اولیه و مجوز شلیک، به سمت هدف هدایت کنند (Allen and Chan, 2017).

بعد از دهه ۱۹۹۰ و پایان جنگ سرد به تدریج با پیشرفت و ورود هوش مصنوعی در عرصه نظامی، کشورها با تهدیدات جدیدی در امنیت ملی روبرو شدند. استفاده نظامی از هوش مصنوعی بین دولت‌ها به صورت رقابت درآمده و باعث پیشرفت نسل جدید بمب‌های هوشمند با هدایت لیزر یا پهپادها و هواپیماهای رادار گریز شده است (شیرودی و همکاران، ۱۳۹۹: ۱). کشورهای چین، روسیه، انگلستان و آمریکا بیشترین زرادخانه روبات‌های نظامی را دارند. تنها کشور چین تا سال ۲۰۱۲ بیش از ۲۷ مدل مختلف ربات‌های نظامی را رونمایی کرد. این دولت‌ها از هوش مصنوعی به منزله ابزار قدرت و صعود خود در رقابت با سایر دولت‌ها بهره می‌گیرند.

سیستم‌های رباتیک نظامی مبتنی بر هوش مصنوعی با توجه به میزان خودمختاری؛ به کنترل از راه دور (انسان ـ حاضر)، نیمه‌خودمختار (انسان ـ ناظر) و کاملا خودمختار (انسان ـ غایب) تقسیم می‌شوند. نمونه‌های اولیه پهپاد شاهد ۱۲۹ یک سامانه انسان ـ حاضر است و پهپاد MQ-9 Reaper نمونه سلاح انسان – ناظر می‌باشد. تسلیحات خودمختار نیز هر چند بااحتیاط به کار می‌روند اما ارتش‌های کشورهای قدرتمند برای بکارگیری گسترده آن در آینده نزدیک برنامه‌ریزی می‌کنند (اسلامی و انصاری، ۱۳۹۶: ۱۴۲–۱۴۰).

مهم‌ترین کاربردهای هوش مصنوعی در صنایع نظامی شامل نیز عبارتند از: سیستم‌های هدف‌گیری، نظارت مخفیانه و جاسوسی، تصویربرداری ماهواره‌ای که به اپراتور اجازه ردیابی هدف را می‌دهد، پیش‌بینی احتمال و زمان وقوع وقایع، کارایی در حوزه امنیت سایبری، امداد و تدارکات دریافت هشدار، تولید گزارش و تعمیر و نگهداری وسایل نظامی، ربات‌های هوشمند بدون سرنشین مانند مین‌یاب‌ها و نارنجک‌اندازها، میکرو پهپادها و چاپگرهای سه‌بعدی (Roth, 2019).

1. Fire-and-forget

کاربردهای هوش مصنوعی در عرصه سیاسی

امنیت سیاسی از مهم‌ترین چهره‌های امنیتی ملی است. هوش مصنوعی در ابعاد مختلف این عرصه از قبیل سیاست تطبیقی، تأثیر هوش مصنوعی بر آینده روابط بین‌الملل، رفتار سیاسی، نهادهای سیاسی و کارکردهای نظامی و امنیتی تأثیرگذار است (Granados and Pena, 2021). ولادیمیر پوتین[1] رئیس جمهور روسیه در سال ۲۰۱۷ اظهار کرد که «هوش مصنوعی آینده نه تنها برای روسیه، بلکه برای تمام بشریت است. این با فرصت‌های عظیم همراه است، اما همچنین تهدیدهایی است که پیش‌بینی آنها دشوار است. هر کسی رهبری این عرصه را به دست آورد، فرمانروای جهان خواهد شد» (Moggio, 2017). در آمریکا نیز دونالد ترامپ[2] رئیس جمهور سابق این کشور در فوریه ۲۰۱۹ ابتکار عمل هوش مصنوعی در حوزه‌های تحقیق و توسعه، زیرساخت، زمامداری و سیاست، نیروی کار و تعاملات بین‌المللی را اعلام کرد (The Withe House, 2019). برخی کاربردهای هوش مصنوعی در عرصه سیاسی شامل موارد زیر است:

۱- هوش مصنوعی طراحی و تولید ویدیوهای جعلی را امکان‌پذیر می‌کند که برای مثال در آن، رئیس جمهور کشوری حملاتی تند را علیه کشور دیگر ترتیب می‌دهد و با ادبیات نامناسب علیه مقامات آن اظهارنظر می‌کند. نمونه آن نیز در ماه‌های منتهی به انتخابات ریاست جمهوری ۲۰۱۶ آمریکا بود که انبوه اخبار جعلی با هدف تخریب هیلاری کلینتون در شبکه‌های اجتماعی منتشر شد.

۲- فریب شخصیت‌های مشهور سیاسی و جاسوسی و تخلیه اطلاعاتی آنها؛ در سال ۲۰۱۹ آمریکا مدعی شناسایی یک نمایه کاربری متعلق به زنی به نام کتی جونز در شبکه اجتماعی لینکداین[3] با اطلاعات جعلی شد. طراحان این نمایه با ارسال پیام به شخصیت‌های سیاسی آمریکا و اعضای برجسته اندیشکده‌های بروکینگز[4] و بنیاد هریتج[5] برای دوستی و تخلیه اطلاعاتی آنها تلاش می‌کردند.

۳- جذب تروریست برای گروه‌های تروریستی؛ برای مثال داعش در سال ۲۰۱٤ یک بسته جامع رسانه‌ای را ایجاد کرد که به طرز چشم‌گیری مسلمانان ناراضی را حتی از کشورهای پیشرفته جهان همچون آمریکا، بریتانیا، فرانسه و روسیه جذب کرد. گروه‌های تروریستی از این طریق، دیدگاه‌های

1. Vladimir Putin
2. Donald Trump
3. LinkedIn
4. Brookings Institution
5. The Heritage Foundation

خود را به مردم افراطی می‌رسانند و تلاش می‌کنند که مشروعیت و اقتدار دولت‌ها را تضعیف کنند. در سال ۲۰۱٤ حدود ۵۰ هزار حساب کاربری طرفدار داعش در توئیتر فعال بود (شیرودی و همکاران، ۱۳۹۹: ۲۵-۱٤).

٤- در مبارزات انتخاباتی نیز هوش مصنوعی می‌تواند انواع الگوریتم‌های کامپیوتری را برای مشخص کردن میزان رأی دهندگان و همچنین گروه‌های تجزیه و تحلیل که رفتار رای دهندگان را می‌سنجد. برای مثال در سال ۲۰۱۹ حزب محافظه‌کار که در بریتانیا قدرت را در دست داشت، از فناوری هوش مصنوعی Chat-Gpt در مبارزات انتخاباتی خود استفاده کرد (Alfiani, 2023: 247).

تهدیدات نظامی ناشی از هوش مصنوعی بر امنیت ملی ایران

امنیت ملی ایران علاوه بر تهدیدهای سخت مانند تهدیدات تروریستی و تهدید به حمله نظامی و وضع تحریم با پیشرفت علم و فناوری و هزینه‌مندی به کارگیری قدرت سخت، با تهدیدهای مبتنی بر هوش مصنوعی نیز مواجه بوده است.

حملات سایبری به تاسیسات هسته‌ای ایران

یکی از مهم‌ترین تأثیرات هوش مصنوعی به منظور مقابله با صنعت هسته‌ای ایران بوده است. ویروس Stuxnet که در ژوئیه ۲۰۱۰ شناسایی شد، برای خرابکاری سامانه‌های هدایت‌گر هسته‌ای انتشار یافت. در مه سال ۲۰۱۲ رسانه‌های آمریکا اعلام کردند که این ویروس با دستور اوباما[1] راه‌اندازی شده است. در سال ۲۰۱۳ ادوارد اسنودن[2] در مصاحبه با اشپیگل[3] اظهار کرد: «این بدافزار با همکاری آژانس امنیت ملی آمریکا و اسرائیل ساخته شده است» (جواهری، ۱۳۹٤: ۵۳-۵۲). مورد دیگر ویروس Narilam بود که در سال ۲۰۰۹ شناسایی شد. هدف این ویروس از یک طرف ایجاد اختلال در برنامه هسته‌ای بود تا ضمن کندن کردن سرعت پیشرفت‌ها، هزینه‌های آن افزایش یابد. از سوی دیگر خرابکاری سایبری در سیستم‌ها و برنامه هسته‌ای ایران می‌تواند خطر اشاعه هسته‌ای را نیز افزایش دهد (Walker, 2012).

حملات سایبری به نهادهای داخلی

1. Barak Obama
2. Edward Snowden
3. Spiegel

حملات به نهادهای داخلی ایران از جمله سیستم بانکی، تأسیسات نفتی و سامانه سوخت در دهه‌های اخیر، تهدید دیگر هوش مصنوعی است. سیستم بانکی ایران در سال ۱۳۹۱ هدف حمله ویروس Gauss«گاوس» قرار گرفت. سیستم هدف این ویروس، از خانواده ویندوز بود و مشخصات سیستم استفاده شده و اطلاعات بانکی و اینترنتی مرورگر را به سرقت می‌برد. تأسیسات نفتی ایران نیز در همان سال‌ها هدف ویروس Flame قرار گرفت. چند روز پس از انتشار اخبار مربوط به این بدافزار، مرکز ماهر ایران مدعی شد که برای نخستین بار در دنیا ابزار پاک‌سازی آن را تولید کرده است (Utinkova, 2021).

از سال ۲۰۱۵ پروژه نیتروزئوس علیه ایران در دستور کار قرار گرفت که هدف آن از کار انداختن نیروگاه‌های برق، خطوط ارتباطی تلفن و تجهیزات دفاع هوایی بود. این پروژه به عنوان یک نقشه احتمالی در صورت به نتیجه نرسیدن مذاکرات هسته‌ای نیز مطرح شد. روزنامه نیویورک‌تایمز در گزارشی درباره این پروژه اشاره کرد که آمریکا نقشه‌ای محدودتر برای از کار انداختن تاسیسات هسته‌ای فردو پیاده کرده و این موضوع از زمانی که استاکس‌نت بیش از هزار سانتریفیوژ[1] را در نطنز از کار انداخت در دست بوده است. اما از آنجا که نفوذ به سایت مشکل بود، این پروژه با استفاده از بدافزار برای از کار انداختن تجهیزات و سیستم‌های رایانه‌ای، طراحی شد (Sanger and Mazzetti, 2016).

در سال ۲۰۱۸ گروه هکری موسوم به «تپندگان» تابلوهای الکترونیکی فرودگاه‌های مشهد و تبریز را هک کرد. در جولای ۲۰۲۱ راه‌آهن ایران و سایت وزارت راه و شهرسازی از دسترس خارج شد. گروه ناشناخته‌ای به نام گنجشک درنده مسئولیت این حملات را بر عهده گرفت. گروه هکری عدالت علی در آگوست ۲۰۲۱ تصاویر دوربین‌های زندان اوین را منتشر کرد. در اکتبر ۲۰۲۱ فرایند پرداخت الکترونیکی سوخت در جایگاه‌های عرضه سوخت مختل شد. در نوامبر ۲۰۲۱ حمله‌ای ناموفق به سیستم‌های داخلی شرکت هواپیمایی ماهان توسط گروه «هوشیاران وطن» انجام شد. در فوریه ۲۰۲۲ نیز گروه عدالت علی فیلم دوربین‌های مداربسته زندان قزل حصار را منتشر کرد (Check Point Research, 2022).

مهم‌ترین پیامد حملات به نهادهای داخلی ایران، ایجاد نارضایتی در بین مردم بود. حملات به بانک‌ها

1. Centrifuge

می‌تواند سیستم اقتصادی کشور را زمین‌گیر نموده و نقش مهمی در بحران‌ها ایفا کند. در زمینه نفتی از آنجا که مهم‌ترین منبع تأمین درآمدها در ایران فروش نفت است، این گونه حملات می‌تواند در تولید و عرضه فرآورده‌های نفتی اختلال ایجاد نماید. پیامد حمله سایبری به سامانه سوخت پمپ بنزین‌ها نیز در ایجاد خسارات مادی و ایجاد نارضایتی در جامعه مؤثر است و تهدید علیه امنیت ملی محسوب می‌شود.

جاسوسی از ایران

هوش مصنوعی به وسیله دسته‌بندی، تحلیل اطلاعات و تصمیم‌گیری مناسب ابزاری نوین در جاسوسی محسوب می‌شود. جرمی فلمینگ مدیر ستاد ارتباطات دولت انگلیس در سال ۲۰۲۰ اظهار کرد که «هوش مصنوعی در آینده روند فعالیت‌های سازمان‌های جاسوسی را در جهان متحول می‌کند و برای حفاظت از کشورها، ارتقای امنیت ملی و ارتقای امنیت سایبری موثر خواهد بود.» در ایران در سال ۲۰۱۱ بدافزار مادی[1] حدود ۸۰۰ رایانه را آلوده نمود. ثبت اطلاعات صفحه کلید، عکس از صفحه مانیتور در فواصل مشخص، عکس در صورت استفاده از فیس بوک، اسکایپ یا جی‌میل، ضبط، ذخیره و ارسال فایل‌های صوتی کارکردهای این بدافزار بود (جواهری، ۱۳۹٤: ٥٦). پیامد جاسوسی به وسیله هوش مصنوعی، مواجه کشور با تهدیداتی نوین است که به وسیله ناشناختگی و تأخیر در بررسی حملات، آسیب‌پذیری امنیتی را افزایش می‌دهد.

ترور توسط سلاح‌های خودران

ترور دانشمندان از مهم‌ترین تهدیدهایی است که امنیت ملی ایران بیش از یک دهه با آن مواجه است. مئیر داگان رئیس اسبق موساد معتقد است: «ترور بسیار کارآمدتر و ارتکاب آن بسیار اخلاقی‌تر است تا ایجاد یک جنگ گسترده؛ زیرا جنگ شاید به اندازه کافی در تأسیسات هسته‌ای ایران خرابی به بار نیاورد. جایگزین نمودن افراد حذف شده به راحتی امکان‌پذیر نیست و ترور موجب تضعیف روحیه مقابل می‌شود» در سال‌های ۱۳۹۹–۱۳۸۸ پنج نفر از دانشمندان هسته‌ای ایران با روش بمب‌گذاری و شلیک گلوله ترور شدند. اما در آذر ۱۳۹۹ محسن فخری‌زاده تنها دانشمندی بود که با استفاده از سلاح مبتنی بر هوش مصنوعی ترور شد (صالحی و سلمانی فرهمند، ۱٤۰۰: ٤۱۲–٤۱۰).

روزنامه نیویورک تایمز در گزارشی از این ترور به قلم رونین برگمن تحلیلگر نظامی اسرائیلی نوشت:

1. Madi

«این اولین آزمایش میدانی یک تک‌تیرانداز کامپیوتری پیشرفته و مجهز بـه هـوش مصـنوعی و چشـم چنددوربینه بود که به ماهواره وصل بود و در هر دقیقه ۶۰۰ گلوله شلیک می‌کرد ... وزن این مسلسـل، ربات، اجزا و لوازم جانبی‌اش حدود یک تن است. بنابراین تجهیزات آن بـه قطعـات کـوچکتر تقسـیم شده و قطعه قطعه از مسیرها و در زمان‌های مختلـف وارد کشـور شـدند و سـپس مخفیانـه در ایـران مونتاژ گردیدند. ربات به گونه‌ای ساخته شد تا در وانت زامیاد جـا شـود ... هـوش مصـنوعی دسـتگاه طوری تنظیم شد تا تأخیر، لرزش و سرعت خودرو را جبران کند. کـل عملیـات کمتـر از یـک دقیقـه طول کشید. ۱۵ گلولـه شـلیک شـدند. (Bergman and Fassihi, 2021). کـاربرد ایـن فنـاوری هوش مصنوعی، روش‌های سنتی ترور را متحول نمود. همچنـین عملیات‌هـایی از ایـن نـوع، نیـاز بـه انتقال تجهیزات به صورت قطعات کوچک در یـک بـازه زمـانی بلنـد مـدت دارد کـه شناسـایی آن را سخت‌تر می‌کند. مهم‌ترین پیامد این موضوع این است که شناسایی آن با روش‌هـای سـنتی، سـخت و غیرممکن است و کشف و خنثی‌سازی آن نیز نیاز به هوش مصنوعی دارد.

فرصت‌های نظامی هوش مصنوعی بر امنیت ملی ایران

تجهیز سلاح‌های موشکی و پهپادی

متخصصین نظامی ایرانی در سال‌های اخیر سعی کرده‌اند تا هوش مصنوعی را نیـروی هـوایی بـه کـار گیرند. موشک‌ها بخش زیادی از راهبرد بازدارندگی ایران را به خود اختصـاص داده‌انـد. مجهـز کـردن موشک‌ها به هوش مصنوعی قابلیت پرتاب از چند سامانه به یک هـدف را در اختیـار ایـران قـرار داده است. سردار تنگسیری از فرماندهان سپاه پاسداران اظهار داشت: «ما توانستیم پهپادها را هـم بـه هـوش مصنوعی مجهز کنیم و این فناوری روی برد و دقـت هـدف زنـی و رادارگریـزی آنهـا مـؤثر اسـت و افتخار می‌کنیم که پهپاد را در یک مدت بسیار کوتاه با تبدیل تهدیـدات بـه فرصـت‌ها و بهره‌گیـری از فناوری های نوپدید و با دانش بومی تولید کردیم و تمامی تجهیـزات ایـن پهپادهـا شـامل بـال، بدنـه، موتور، سیستم هدایت آنها و ... ساخت داخـل اسـت». همچنـین سـردار حـاجی‌زاده فرمانـده نیـروی هوافضای سپاه در رزمایش پیامبر اعظـم در ژانویـه ۲۰۲۱ اظهـار کـرد: «ترکیـب قابلیت‌هـای موشـکی جدید، عملیات هواپیماهای بدون سرنشین و فناوری هوش مصنوعی امکانـات و قـدرت جدیـدی را در این زمینه برای سپاه به وجود آورده است» (Lisman, 2021: 2-5).

دستیابی به سلاح‌های رباتیک

ایران در حوزه نظامی در یک دهه اخیر تلاش زیادی برای دستیابی به سلاح‌های خودمختار رباتیک انجام داده است. نیروهای ایرانی با آموزش فنی و بدون محدودیت در آزمایش دقیق سلاح، منابع لازم را برای دستیابی به سلاح‌های رباتیک دارند. نیروهای نظامی ایران اعم از ارتش، نیروی هوایی و سپاه پاسداران با استقرار سیستم‌های تحت هدایت هوش مصنوعی در میدان جنگ در اسرع وقت هر چند که ابتدایی و غیرقابل اعتماد باشد، به دنبال بهره‌گیری از مزیت آنها ایجاد توانایی برای حملات سریع‌تر در برد بیشتر هستند. هوش مصنوعی و سیستم خودمختار با توجه به پیگیری طولانی مدت آنها برای افزایش توان و قابلیت‌های نامتقارن ایران مناسب است (Lisman, 2021: 2-5).

قدرت بازدارندگی سایبری

یکی از مهم‌ترین فرصت‌های هوش مصنوعی برای ایران، ایجاد قدرت بازدارندگی در پدافند سایبری است. هوش مصنوعی در این زمینه بدون رقیب است و ایران در صدد است تا همانند حوزه موشکی، در سایبری نیز از قدرت بازدارندگی این فناوری استفاده کند (رستمی، ۱٤۰۱: ۵۹). سردار غلامرضا جلالی فرمانده پدافند غیرعامل ایران در این باره اظهار کرد: «جمع‌بندی سازمان پدافند غیرعامل کشور این است که در سال ۱٤۰۲ هوش مصنوعی وارد دفاع سایبری شود. در همین زمینه، شرکت‌های دانش بنیان داخلی بسیاری مشغول فعالیت هستند که به دنبال بهره‌مندی از توان آنها هستیم. رصد و پایش، کشف و برطرف کردن و امن‌سازی تهدید سایبری و پایدارسازی و تداوم کارکرد از جمله زمینه‌هایی است که می‌توان از هوش مصنوعی بهره برد (جلالی، ۱٤۰۲: ۳).

تهدیدهای سیاسی هوش مصنوعی بر امنیت ملی ایران

طراحی اخبار دروغین برای دست‌کاری افکار عمومی

طراحی و انتشار اخبار دروغین و جعلی از مهم‌ترین تهدیدات هوش مصنوعی علیه امنیت ملی ایران است. بخش زیادی از ناآرامی‌های ۱٤۰۱ به دنبال فوت مهسا امینی متأثر از نقش شبکه‌های اجتماعی اینستاگرام، تلگرام و توئیتر در نشر تصاویر غیرواقعی از افراد دستگیر یا کشته شده بود. نمایش بیشتر فیلم‌ها و تصاویر این وقایع این گونه القاء کرد که مردم زیادی معطوف به این وقایع هستند. داغ شدن (#مهسا-امینی) در توئیتر و بازنشر آن بیش از ۳۰۰ میلیون، نمونه تاثیر هوش مصنوعی بود. هر چند بسیاری از چهره‌های شناخته شده در ایران و جهان این هشتگ را بازنشر کردند، اما تعداد کاربران توئیتر فارسی و وجود ربات‌ها و حساب‌های جعلی نشان از غیرواقعی بودن این آمار داد.

حملات سایبری به صداوسیما

سایت‌ها و شبکه‌های سازمان صداوسیما که مسئولیت کلیه خدمات رادیـویی و تلویزیـونی در ایـران را بر عهده دارد، از ابتدای سال ۲۰۲۲ چنـدین بـار هـک شـد. در بهمـن ۱۴۰۰ در بـین پخـش آنـونس برنامه‌ها به مدت ده ثانیه، تصاویری از سران سازمان منافقین پخـش شـد. شـبکه قـرآن، رادیـو پیـام و جوان هم با همین مشکل روبرو شدند. گزارش مؤسسه تحقیقات سایبری چک‌پوینـت نشـان می‌دهـد این حملات با روش ربایش سیگنال‌های پخش انجام شده و برای پخش فایل ویـدیویی، مهاجمـان از برنامه‌ای به نام SimplePlayout.exe اسـتفاده کردنـد (Check Point, 2022). چنـد روز بعـد، وب‌سایت تلوبیون نیز مورد حملـه قـرار گرفـت. پیامـد ایـن موضـوع بـا اسـتفاده از فنـاوری هـوش مصنوعی، اخلال در امنیت سیاسی کشور است. چه این که گروهک منافقین که سال‌هاسـت در جنـگ با دولت و ملت ایران قرار دارد این وسیله را به عنوان قدرت‌نمایی و ایجاد مشـروعیت بـرای خـود در نظر می‌گیرد.

فرصت‌های سیاسی هوش مصنوعی بر امنیت ملی ایران

پیش‌بینی نتایج انتخابات

انتخابات از مهم‌ترین جنبه سیاسی امنیت ملی است. با فناوری هوش مصنوعی می‌توان نتایج انتخابـات را پیش‌بینی و تخمین زد. نمونه این موضوع در ایران قبل از انتخابات ریاست جمهوری ۱۳۹۶ مسـابقه پیش‌بینی نتایج انتخابات با استفاده از الگوریتم‌های هوش مصنوعی و داده‌هـای موجـود در شـبکه‌های اجتماعی توسط دانشگاه صنعتی شریف برگزار شد. مجموعه داده این مسـابقه شـامل ۱,۵ میلیـون پیـام ارسال شده در حدود ۳۰ هزار کانال تلگرامی بود و نتایج نیز حکایت از پیش‌بینی انتخابات با اختلافـی کم نسبت به نتایج واقعی داشت.

تقابل‌های راهبردی در سیاست خارجی

در دوره‌ای که سیاست خارجی در حال حرکت به سمت الگوریتم‌هایی است که هدف آنهـا مشـورت دادن به دولت است، هوش مصنوعی می‌تواند در سیاست خارجی استفاده شود. برای مثال می‌تـوان بـا کاربست هوش مصنوعی تقابل ایران و آمریکا در رابطه با برنامه هسته‌ای ایـران و سـناریوهای محتمـل آن را تحلیل و پیش‌بینی کرد. یکی از سامانه‌ها بدین منظور، شبیه‌سازی بازی‌هـا و تقابل‌هـای راهبـردی است که از نرم‌افزارهای مختلفی از قبیل GMCR و نرم‌افزار تلفیقی ماسکیتا بهـره می‌گیـرد. نرم‌افـزار

GMCR که ابتدا در وزارت دفاع کانادا توسعه یافت، در زمینه‌های غیرنظامی مبتنی بر تقابل منافع استفاده می‌شود.

ماسکیتا از مشاوران سیاست خارجی ایالات‌متحده است که مدلی تلفیقی از بازی‌های بیزین برای تحلیل و تجویز در زمینه سیاست خارجی ارائه داد. هدف این مدل، پیش‌بینی فرایندها و نتایج منجر به مذاکرات یا موقعیت‌های سیاسی منجر به درگیری، جنگ، توافق یا تجزیه است. این مدل برای موقعیت‌های تهدید و مذاکره یا احتمال جنگ بین‌المللی، سیاست داخلی یا روابط متقابل اجتماعی و کسب‌وکار به کار می‌آید. لازم است تا بازیگران، کنش‌های محتمل آنها و ارزیابی‌های جاری، کوتاه‌مدت و بلندمدت از روندها، تاکتیک‌ها و باورهای ذی‌نفعان بازی تحلیل شوند. البته در کنار گرامر اصلی نظریه بازی‌ها، برخی قواعد ابتکاری و اکتشافی نیز برای محاسبات به کار گرفته می‌شوند. این قواعد ابتکاری با اصول نظریه بازی‌ها ترکیب می‌شوند تا تصویری واقعی‌تر از موقعیت تعامل به دست بیاید (مجیدزاده، ۱۳۹۹: ۲-۳).

نتیجه‌گیری

هوش مصنوعی از مهم‌ترین فناوری‌هایی است که امنیت ملی دولت را در ابعاد مختلف آن از جمله سیاسی و نظامی در معرض فرصت و تهدید قرار داده است. امنیت ملی ایران از دهه‌های گذشته با تهدیدهای سنتی مانند حملات نظامی، گروه‌های تروریستی و دروغ‌پردازی‌های رسانه‌ای مواجه بوده است. با این حال بعد از پیشرفت در فناوری‌های هوش مصنوعی، تهدیدات نظامی و سیاسی ناشی از آن علیه امنیت ملی افزایش یافته است. هوش مصنوعی در قالب سیستم‌های هدف‌گیری، تصویربرداری ماهواره‌ای، امنیت سایبری، پهپادها و تعمیر وسایل نقلیه نظامی، امنیت نظامی را متحول کرده است. این فناوری همچنین با ایجاد روش‌های مشارکت، مبارزه‌های انتخاباتی و طراحی ویدیوهای باورپذیر از سیاستمداران امنیت سیاسی دولت را تحت تأثیر قرار داده است. امنیت ملی ایران نیز در ابعاد نظامی و سیاسی تحت تأثیر این فناوری بوده است. در واقع دولت‌ها سعی می‌کنند از هر ابزاری برای مقابله با قدرت رقبا استفاده کنند. در این راه حملات بدافزاری علیه صنعت هسته‌ای ایران از سوی آمریکا و اسرائیل و ایجاد اخلال در سیستم‌های داخلی ایران از جمله در قالب بدافزارهای گاوس و فلیم، پروژه نیتروزئوس و حملات سایبری علیه بخش‌های مختلف کشور مانند راه‌آهن، وزارتخانه‌ها، زندان‌ها، سامانه سوخت در ایران انجام شده است. هوش مصنوعی به عنوان

ابزار جاسوسی علیه ایران نیز توسط بدافزار مادی استفاده شده است. در عین حال مهم‌ترین کاربرد هوش مصنوعی در حوزه نظامی ترور دکتر فخری‌زاده با سلاح تک‌تیرانداز کامپیوتری مجهز به چشم چند–دوربینه در سال ۱۳۹۹ بود. علاوه بر تهدید، هوش مصنوعی فرصت‌های متنوعی مانند مجهز کردن سامانه‌های موشکی و پهپادی، دستیابی به سلاح‌های رباتیک و بازدارندگی سایبری در اختیار ایران قرار داده است. در حوزه سیاسی بهره‌گیری از هوش مصنوعی تهدیدهایی نظیر حمله سایبری سازمان منافقین به صداوسیما و طراحی اخبار دروغین در ناآرامی‌ها و اغتشاشات سال ۱۴۰۱ را به همراه داشت. در عین حال این فناوری به وسیله پیش‌بینی نتایج انتخابات و انجام تقابل‌های راهبردی در سیاست خارجی به ویژه در موضوعات راهبردی همچون موضوع هسته‌ای که تقابل راهبردی بین ایران و قدرت‌های جهانی از جمله ایالات متحده وجود دارد فرصت‌هایی را نیز در اختیار کشور قرار داده است.

تهدیدها و فرصت‌های سیاسی و اجتماعی هوش مصنوعی بر امنیت ملی ایران

تهدیدهای نظامی	فرصت‌های نظامی	تهدیدهای سیاسی	فرصت‌های سیاسی
حملات سایبری به تأسیسات هسته‌ای ایران	تجهیز سلاح‌های موشکی و پهپادی	طراحی اخبار دروغین برای دست‌کاری افکار عمومی	پیش‌بینی نتایج انتخابات
حملات سایبری به نهادهای داخلی	دستیابی به سلاح‌های رباتیک	حملات سایبری به صداوسیما	تقابل‌های راهبردی در سیاست خارجی
جاسوسی از ایران	قدرت بازدارندگی سایبری		
ترور توسط سلاح‌های خودران			

منبع: (یافته‌های پژوهش)

منابع

احمدی، علی؛ زرگر، افشین و آدمی، علی. (۱٤۰۱). «نقش فناوری‌های نوظهور در امنیت و قدرت ملی کشورها؛ فرصت‌ها و تهدیدها». مطالعات بین المللی، ۱۸(٤)، ۱۳۹-۱۵۹.

اسلامی، رضا و انصاری، نرگس. (۱۳۹٦). «به کارگیری روبات های نظامی در میدان جنگ در پرتو اصول حقوق بشردوستانه». حقوقی بین المللی، ۳٤(٥٦)، ۱٤۱-۱٦٤.

تخشید، زهرا. (۱٤۰۰). «مقدمه‌ای بر چالش‌های هوش مصنوعی در حوزهٔ مسئولیت مدنی». حقوق خصوصی، ۱۸(۱)، ۲۲۷-۲۵۰.

جواهری، مهدی. (۱۳۹٤) «بررسی تروریسم از نظر گونه‌شناسی مورد مطالعه تروریسم سایبری در بحث فناوری هسته‌ای در ایران». مطالعات بین‌المللی پلیس، ۸ (۲٤)، ۳۱-٦٤

حسینی، حسین؛ مقدم فر، حمیدرضا و قنبرپور، مصطفی(۱۳۹۵). واکاوی نقش و کارکرد شبک ههای اجتماعی مجازی در حوادث انتخابات سال ۱۳۸۸ جمهوری اسلامی ایران. آفاق امنیت، ۷(۲٤)، ۱-۲٤.

دهقانی فیروزآبادی، جلال. (۱۳۹٦). اصول و مبانی روابط بین‌الملل، تهران: انتشارات سمت.

رحمت اللهی، حسین؛ لک زایی، نجف؛ ارسطا، محمدجواد و حاج زاده، هادی. (۱۳۹٤). «امنیت سیاسی افراد و مرجع آن در فقه امامیه». حقوق اسلامی، ۱۲(٤٤)، ۱۱۳-۱۵۲.

رستمی, محسن. (۱٤۰۱).«شناسایی و معرفی ظرفیت های کاربردی هوش مصنوعی در توسعه مضمون‌های راهبردی در سازمان های نظامی». راهبرد دفاعی، ۲۰(۷۸)، ۳٤-۷٤.

روشن, سید علیقلی؛ یعقوبی، نورمحمد و مومنی، امیررضا. (۱٤۰۰). «کاربست هوش مصنوعی در بخش دولتی (مطالعه ای فرا ترکیب)». علوم مدیریت ایران، ۱٦(٦۱)، ۱۱۷-۱٤۵.

شیرودی، محمدسجاد؛ همتی، مجید و سیاه پوش، ابراهیم. (۱۳۹۹). «هوش مصنوعی و آینده حملات گروه‌های تروریستی تکفیری». مطالعات آسیای جنوب غربی، ۳(۹)، ۱-۲۸.

صالحی، محمدخلیل وسلمانی فرهمند، محمد، (۱٤۰۰).«تحلیل ترور دانشمندان هسته‌ای ایران از منظر حقوق داخلی و بین‌الملل»، دو فصلنامه تمدن حقوقی، ٤(۹)، ٤۰۷-٤۳۲.

عبداللهخانی، علی. (۱۳۸۹). نظریه‌های امنیت. تهران: انتشارات ابرار معاصر

قرشی، یوسف. (۱۳۹۳). امنیتی شدن و سیاست خارجی جمهوری اسلامی ایران. تهران: نشر پژوهشکده مطالعات راهبردی

کلودزیچ، ادوارد. (۱۳۸۷). امنیت و روابط بین‌الملل. ترجمه محمود یزدان‌فام، تهران: اندیشکده مطالعات راهبردی.

محمدعلی خلج، محمدحسین. (۱۳۹۳). «دریفوس و تاریخ فلسفی هوش مصنوعی». غرب‌شناسی، ۵(۱)، ۱۰۳-۱۲۸.

مقدس، محمدمهدی، (۱۳۹۹)، «تحلیل و بررسی امکان هوش مصنوعی هیدگری در آرای هیوبرت دریفوس»، جستارهایی در فلسفه و کلام، سال ۵۲، شماره اول.

جلالی، غلامرضا، (۱۴۰۲/۰۲/۳۰)، «به کارگیری هوش مصنوعی در پدافند سایبری»، دسترسی در: https://www.isna.ir/news/1402023018878/.

مجیدزاده، رضا، (۱۳۹۹/۰۴/۱۸)، «کاربرد هوش مصنوعی در سیاست خارجی»، دسترسی در: https://www.scfr.ir/fa/300/30101/125202/.

Allen, Greg and Chan, Taniel, (2017), Artificial Intelligence and International Security, Belfer Center, July.

Alfiani, Sandra, (2023), the use of artificial intelligence technology in political digital marketing strategies, proceeding of The 3rd FUAD's International Conference on Strengthening Islamic Studies, Vol 3.

Bergman, Ronen and Fassihi, Farnaz, (2021), The Scientist and the A.I.-Assisted, Remote-Control Killing Machine, available at: https://www.nytimes.com/fa/2021/09/18/world/middleeast/fakhrizadeh-iran-assassination-robot-mossad.html

Check Point, (2022), EvilPlayout: Attack against Iran's State Broadcaster, februari 18, available at: https://research.checkpoint.com/2022/evilplayout-attack-against-irans-state-broadcaster/

Granados, Oscar and Pena, Nicolas, (2021), Artificial Intelligence and International System Stracture, Journal of Revista Brasileira de Política Internacional, Vol 64, No 1.

Hauser, Sarah, (2019), From Deep Blue to Alexa: The history of artificial intelligence, available at: https://blog.solvatio.com/en/from-deep-blue-to-alexa-the-history-of-artificial-intelligence.

Horowitz, Michael and et al, (2018), Artificial Intelligence and International Security, Center for a new American Security.

Lisman, Evan, (2021), Iran's bet on autonomous weapons, available at: https://warontherocks.com/2021/08/irans-bet-on-autonomous-weapons/

Maggio, Edoardo, (2017), Putin believes that whatever country has the best AI will be 'the ruler of the world, available at: https://www.businessinsider.com/putin-believes-country-with-best-ai-ruler-of-the-world-2017-9.

Roth, Marcus, (2019), Artificial Intelligence in the Military – An Overview of Capabilities, available at: https://emerj.com/ai-sector-overviews/artificial-intelligence-in-the-military-an-overview-of-capabilities/.

Sanger, David E and Mazzetti, Mark, (2016), U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict, available at: https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html

Scharre, Paul and et al, (2018), Artificial Intelligents, What Every Policymaker Needs to Know, Center for a New American Security.

Utinkova, Hana, (2021), Cyber-attacks Against Iran as Instruments of Hybrid Warfare, Charles University faculty of social Sciences Institute of Political Studies Department of Security Studies.

Walker, Danielle, (2012), Narilam virus targets Middle East, but isn't like others, available at: https://www.scmagazine.com/news/narilam-virus-targets-middle-east-but-isnt-like-others.

Withe House, (2019), the national artificial intelligence research and development strategic plan: 2019 update, a reported by the select committee on artificial intelligence of the national science & technology Council