

The Role of Artificial Intelligence in the Wars of U.S and Israel against the Resistance Front: A Case Study of Gaza War (2023-2024)

Ali Bagheri Dolatabadi 

Professor in International Relations, Department of Political Science, Yasouj University, Yasuj, Iran,
abagheri@yu.ac.ir

Abstract

Objective: Artificial intelligence is rapidly changing various fields of science. These fields started from statistics and computers sciences and have expanded to the military and security fields. In recent years, an important part of the military operations of the United States and Israel in the Middle East has been carried out by relying on this technology. The aim of the upcoming article is to analyze the use of this new technology in the American and Israeli wars against the resistance front.

Method: This research is descriptive-analytical in terms of method. The required data has been collected using the library method and referring to books, articles, interviews and reports published on websites and newspapers.

Results: The results of the research showed that Israel and U.S have used artificial intelligence in two military and economic dimensions against the resistance front: the military dimension include data collection and analysis, identification of military targets, assassination of military commanders, monitoring of communications of the resistance front forces, and cyber war. In the economic aspect, this technology has helped identification and blocking of assets and financial resources of the resistance front members and their supporting states.

Conclusion: It seems that artificial intelligence will play a much more effective role in the future wars than what it currently plays. For this reason, the states and groups that are members of the resistance front, which are constantly facing various threats from the US and Israel, will have an important duty to prepare for the dangers caused by the use of artificial intelligence technology in future wars.

Keywords: Artificial Intelligence, Resistance Front, U.S, Israel, Al-Aqsa Storm Operation.

Article type: Research

* Received on: 6 August 2024 Accepted on: 27 April 2025

Cite this article: Bagheri Dolatabadi, Ali (2025) The Role of Artificial Intelligence in the Wars of U.S and Israel against the Resistance Front: A Case Study of Gaza War (2023-2024), Summer 2025, Vol.14, NO.2, 89-111.

DOI: 10.30479/psiw.2025.20738.3353

© The Author(s).



Publisher: Imam Khomeini International University.

Corresponding Author: Ali Bagheri Dolatabadi (abagheri@yu.ac.ir)

نقش هوش مصنوعی در جنگ‌های آمریکا و اسرائیل علیه جبهه مقاومت: نمونه موردی جنگ غزه (۲۰۲۳-۲۰۲۴)

علی باقری دولت‌آبادی 

استاد روابط بین‌الملل، عضو هیات علمی گروه علوم سیاسی دانشگاه یاسوج، یاسوج، ایران. abagheri@yu.ac.ir

چکیده

هدف: هوش مصنوعی به سرعت در حال تغییر دادن عرصه‌های مختلف علم و دانش است. این عرصه‌ها از آمار و رایانه شروع گردیده و تا حوزه نظامی و امنیتی گسترده شده است. طی سال‌های اخیر بخش مهمی از عملیات نظامی آمریکا و اسرائیل در غرب آسیا با اتکا به این فناوری انجام شده است. هدف مقاله پیش رو تحلیل کاربست این فناوری جدید در جنگ‌های آمریکا و اسرائیل علیه جبهه مقاومت است.

روش: برای انجام پژوهش حاضر از روش تحلیلی-تبیینی استفاده شده است و داده‌ها به روش فیش‌برداری با مراجعه به کتب، مقالات، مصاحبه‌ها و گزارش‌های منتشرشده در وبسایت‌ها و روزنامه‌ها گردآوری شده است.

یافته‌ها: یافته‌های پژوهش نشان دادند که اسرائیل و آمریکا از هوش مصنوعی در دو بعد نظامی و اقتصادی علیه جبهه مقاومت استفاده نموده‌اند: بعد نظامی شامل جمع‌آوری و تحلیل داده‌ها، شناسایی اهداف نظامی، ترور فرماندهان نظامی، رصد ارتباطات نیروهای جبهه مقاومت و جنگ سایبری بوده است. در بعد اقتصادی این فناوری به شناسایی و مسدودسازی دارایی‌ها و منابع مالی اعضای جبهه مقاومت و دولت‌های حامی آنها کمک کرده است. **نتیجه‌گیری:** به نظر می‌رسد هوش مصنوعی در آینده نزدیک نقش به‌مراتب مؤثرتری نسبت به آنچه در حال حاضر ایفا می‌کند در جنگ‌ها بر عهده خواهد گرفت. به همین خاطر کشورها و گروه‌های عضو جبهه مقاومت که پیوسته با تهدیدات مختلف آمریکا و اسرائیل مواجه هستند وظیفه سنگینی در خصوص کسب آمادگی برای خطرات ناشی از کاربرد فناوری هوش مصنوعی در جنگ‌های آتی خواهند داشت.

واژگان کلیدی: هوش مصنوعی، جبهه مقاومت، آمریکا، اسرائیل، طوفان الاقصی.

نوع مقاله: پژوهشی

تاریخ دریافت مقاله: ۱۴۰۳/۰۵/۱۶ تاریخ پذیرش نهایی: ۱۴۰۴/۰۲/۰۷
استناد: باقری دولت‌آبادی، علی (۱۴۰۴)، نقش هوش مصنوعی در جنگ‌های آمریکا و اسرائیل علیه جبهه مقاومت: نمونه موردی جنگ غزه (۲۰۲۳-۲۰۲۴)، تابستان ۱۴۰۴، دوره ۱۴، شماره ۲، پیاپی ۵۴-۸۹: ۱۱۱.



ناشر: دانشگاه بین‌المللی امام خمینی (ره) © حق مؤلف

۱- مقدمه

در قرن ۲۱ هوش مصنوعی^۱ به نیروی دگرگون‌کننده همه حوزه‌ها تبدیل شده است. در واقع قابلیت‌های هوش مصنوعی و یادگیری ماشین در برنامه‌های هوش مصنوعی جوری تعبیه شده‌اند که بتوانند عملکردهایی مانند اتوماسیون یا قابلیت‌های پیش‌بینی را در اختیار کاربران قرار دهند. امروزه این برنامه‌های کاربردی هوشمند، فرآیندهای تجاری را ساده‌تر و آسان‌تر می‌کنند. این تنها حوزه صنعت و خدمات نیست که تحت تأثیر هوش مصنوعی است بلکه حوزه نظامی و امنیت نیز به شدت از این دانش تأثیر پذیرفته است. جذابیت جنگ نیمه‌خودکار که زمانی در قرن بیستم رویای رهبران بود، در حال رخ نمودن و واقعی شدن است. نیروهای نظامی، مانند سایر سازمان‌های بزرگ، باید به سرعت خود را با این عصر جدید - از لحاظ فناوری پیشرفته و عمدتاً دیجیتالی شده - وفق دهد. موفقیت در جنگ‌های آینده ممکن است تا حد زیادی به مهارت و دانش در این عرصه بستگی داشته باشد. ممکن است نیاز باشد که امنیت با تلاش‌های مشترک بین انسان و ماشین تأمین شود و ادغام هوش مصنوعی در بخش‌های نظامی مطمئناً کارایی را در برنامه‌ریزی و اجرای عملیات زمینی، دریایی و هوایی بیشتر خواهد کرد. از جمله رژیم‌هایی که تاکنون از این فناوری علیه مخالفان خود استفاده نموده‌اند می‌توان از آمریکا و اسرائیل نام برد (Szuba, 2023:1). پس از شروع عملیات طوفان الاقصی در ۷ اکتبر ۲۰۲۳ (۱۶ مهرماه ۱۴۰۲) و پیامدهای جدی که بر غرب آسیا گذاشت بحث و گفتگوهای بسیاری در رسانه‌ها در خصوص به‌کارگیری این فناوری از سوی اسرائیل با همراهی آمریکا علیه حماس و سایر اعضای جبهه مقاومت مطرح شده است؛ اما جزئیات و نحوه کاربست این فناوری هیچ‌گاه با جزئیات و به صورت دقیق تشریح نشده است. این ابهام و فقدان دانش و اطلاعات موجب گردیده تا گاه خسارت‌های جبران‌ناپذیری از بعد نیروی انسانی (شهادت فرماندهان نظامی) و منابع مادی برای جبهه مقاومت رقم بخورد. بر این اساس مقاله حاضر قصد دارد تا این خلأ را برطرف نموده و تا حد امکان چگونگی به‌کارگیری این فناوری در جنگ‌های آمریکا و اسرائیل را تشریح نماید. پرسش اصلی مقاله این است که آمریکا و اسرائیل چگونه از هوش مصنوعی در جنگ‌های خود علیه جبهه مقاومت استفاده کرده‌اند؟ طبق فرضیه پژوهش، هوش مصنوعی ابزارهای جدیدی در اختیار دشمنان مقاومت قرار داده است تا با سرعت بیشتر و کیفیت بالاتر اهداف خود را دنبال نمایند. برای انجام پژوهش حاضر از روش تحلیلی-تبیینی و شیوه گردآوری داده به صورت فیش‌برداری استفاده شده است. برای به دست آوردن داده‌ها بخش اعظم گزارش‌های خبری، تحلیلی، رسانه‌ای و مصاحبه‌های منتشرشده از سوی مقامات آمریکایی و اسرائیلی پس از شروع عملیات طوفان الاقصی مورد رصد و مطالعه قرار گرفته است.

۲- پیشینه پژوهش

هوش مصنوعی یکی از موضوعات جذاب پژوهشی طی سال‌های اخیر بوده و مقالات مختلفی به زبان انگلیسی در این خصوص نگاشته شده است. رابرت اچ. لطیف (2017) در کتاب «جنگ-های آینده: آمادگی برای میدان‌های جنگی جهانی جدید» جنبه‌های دگرگون‌کننده فناوری‌های نوظهور، از جمله هوش مصنوعی، و تأثیرات آنها بر اخلاق نظامی، قابلیت‌ها و جنگ‌های آینده را مورد بحث قرار داده است (Latiff, 2017) در همین رابطه کامینگز^۱ با بررسی «هوش مصنوعی و آینده جنگ‌ها» به این جمع‌بندی می‌رسد که «یک مسابقه تسلیحاتی استعاری^۲ در حوزه تجاری توسعه سامانه‌های خودمختار در حال انجام است» و تلاش می‌کند توضیح دهد چه تحولات نظامی جدیدی پیش رو خواهد بود (Cummings, 2018: 14). ماروالا و لاگازو^۳ دست به «مدل‌سازی نظامی با استفاده از هوش محاسباتی» زده و هفت متغیری که منجر به منازعات بین دولتی می‌شود را ارزیابی نموده‌اند (Marwala and Lagazio, 2011). کومار و بتارش^۴ در مقاله «استفاده از ربات‌ها و هوش مصنوعی در جنگ» اشاره می‌کنند «یکی از مزایایی که پهپادها و ماشین‌ها ارائه می‌دهند، فاصله و دوری در عملیات است. به جای کنترل دقیق آنها از سیگنال‌های رادیویی نزدیک، آنها را می‌توان از طریق ماهواره‌ها از هر مکانی بر روی کره زمین کنترل کرد.» بااین حال، علیرغم پیشرفت قابل توجه در ساخت ربات‌های باهوش‌تر، ربات‌های خودمختار همچنان فاقد «انعطاف‌پذیری برای واکنش مناسب در موقعیت‌های پیش‌بینی‌نشده» هستند (Kumar and Batarseh, 2020). سونگو جو^۵ در مقاله «قدرت نرم در شمال شرق آسیا: استفاده از هوش مصنوعی در جنگ اطلاعاتی» به نقش هوش مصنوعی در جنگ‌های اطلاعاتی با استفاده از قدرت نرم آژانس‌های اطلاعاتی-امنیتی پرداخته است. نرن چیتی و سابینا دیاس^۶ (2017) در مقاله «هوش مصنوعی، قدرت نرم و تغییرات اجتماعی» به بررسی این مسئله پرداخته‌اند که چگونه فناوری‌های جدید، فضایی برای تعامل و نفوذ اجتماعی مبتنی بر قدرت سخت و نرم ایجاد کرده‌اند. این آثار علیرغم تقویت ادبیات هوش مصنوعی عموماً فاقد بررسی میدانی و ارائه شواهد هستند.

در حوزه هوش مصنوعی و تأثیر آن بر امنیت مقالات منتشرشده به زبان فارسی کمتر از انگشتان یک دست است. احسان موحدیان (۱۳۹۸) در مقاله «هوش مصنوعی و تأثیر آن بر امنیت و روابط بین‌الملل» به این موضوع می‌پردازد که هوش مصنوعی موجب می‌گردد که جنگ‌های آینده خشونت‌بارتر و پیچیده‌تر گردد و نسلی جدید از تسلیحات خودران وارد میدان

1- Cummings

2- Metaphorical Arms Race

3- Marwala and Lagazio

4- Marwala and Lagazio

5- Sunggu Jo

6- Naren Chitty Sabina Dias

نبرد شوند. همچنین نویسنده به ناکارآمدی برخی نهادهای بین‌المللی در زمینه کنترل تسلیحات و میانجیگری بین‌المللی با حضور هوش مصنوعی اشاره می‌کند. سید جلال دهقانی فیروزآبادی و سعید چهرآزاد (۱۴۰۲) در مقاله «هوش مصنوعی و مسئله‌دار کردن درون‌مایه‌های امنیت ملی» به این پرسش پاسخ داده‌اند که هوش مصنوعی را چگونه می‌توان در قالب تروریسم، جنگ، تنازع و دفاع مسئله‌دار کرد؟ همان‌گونه که مرور آثار فوق نشان می‌دهد موضوع این مقاله از هر لحاظ دارای نوآوری و ابتکار است و می‌تواند سرآغازی برای پژوهش‌های بعدی باشد.

۳- تعریف مفاهیم

۳-۱- هوش مصنوعی

هوش مصنوعی شامل استفاده از سامانه‌های رایانه‌ای برای انجام وظایفی است که معمولاً به شناخت، برنامه‌ریزی یا استدلال انسانی نیاز دارند. هوش مصنوعی^۱ حاصل در کنار هم قرار گرفتن علوم مختلف شامل ریاضی، آمار، احتمالات، عصب‌شناسی محاسباتی و علوم رایانه و مجموعه‌ای از فناوری و روش‌های رایانه‌ای برای رسیدن به توانایی‌های شناختی و عملی انسان توسط ماشین است (McKinsey, 2023). یک مثال شناخته‌شده و پرکاربرد هوش مصنوعی چت جی.بی.تی^۲ است که خدمات مختلفی را به کاربر ارائه می‌دهد.

۳-۲- جبهه مقاومت

جبهه مقاومت یک ائتلاف ژئوپلیتیک منطقه‌ای، مرکب از مجموعه بازیگران دولتی (ایران و عراق) و غیردولتی (حزب‌الله لبنان، حماس، حشدالشعبی، انصارالله و...) است که منافع مشترک ملی، اسلامی و ایدئولوژیک دارند و تلاش می‌کنند با اتخاذ سیاست‌های مستقل و مقاومتی، نظام سلطه با محوریت آمریکا را نقد و تضعیف کنند (محمودی رجا، باقری دولت‌آبادی و راوش، ۱۳۹۷: ۹).

۴- چارچوب نظری

قدرت‌های بزرگ برای تضمین جایگاه خود در عرصه نظام بین‌الملل، خود را ملزم می‌دانند که به جدیدترین اشکال قدرت و نیرومندترین آنها مجهز سازند. امروزه «در سیاست خارجی، تنها قدرت نظامی یا اقتصادی تعیین‌کننده نهایی نخواهد بود، بلکه در کنار این منابع قدرت، منابع دیگری هم مورد استفاده قرار می‌گیرند، منابعی که هرچند در نگاه اول بیشتر جنبه فرهنگی یا هنری را تداعی می‌کنند اما در واقع می‌توان از آنها به‌عنوان منبع قدرت یاد کرد» (دارابی و

1- Artificial Intelligence

2- ChatGPT

ابراهیمی، ۱۳۹۹: ۳۲۸). این منابع امروزه در علم و دانش و فناوری بیشتر متمرکز شده است. به همین خاطر قدرت‌های بزرگ پیوسته بودجه‌های تحقیقاتی خود را افزایش داده و از عرصه‌های جدید علم و فناوری استقبال می‌نمایند.

مورگنتا، به عنوان پدر معنوی واقع‌گرایان، در بحث عناصر قدرت ملی در کنار عوامل جغرافیا، منابع طبیعی، توان صنعتی، جمعیت، منش ملی، روحیه ملی، آمادگی نظامی را یکی از ابعاد مهم قدرت برمی‌شمرد. برای دسترسی به این نوع از قدرت او بر سه عامل رهبری، کمیّت و کیفیت نیروهای مسلح و فناوری تأکید می‌نماید. وی در توضیح فناوری می‌نویسد: «سرنوشت ملت‌ها و تمدن‌ها را غالباً تفاوت در آن فناوری جنگی تعیین می‌کند، که طرف ضعیف‌تر قادر به جبران آن از هیچ طریق دیگری نیست. قدرت اروپا، در دوره توسعه آن از قرن پانزدهم تا نوزدهم، وابسته به فناوری جنگی برتر این قاره نسبت به نیمکره غربی، آفریقا، خاور نزدیک و خاور دور بود» (مورگنتا، ۱۳۸۹: ۲۱۵-۲۱۶). همچنین دسترسی آلمان‌ها به زیردریایی و بریتانیا به تانک‌های بسیار و پیشرفته، در جنگ جهانی اول برتری قابل توجهی به آنها نسبت به رقبا در مراحل از جنگ بخشید. کما اینکه آلمانی‌ها و ژاپنی‌ها در مرحله اول جنگ جهانی دوم به واسطه نیروی هوایی و هماهنگی استراتژیک و تاکتیکی آن با نیروی زمینی و دریایی به پیروزی‌های مهمی دست یافتند و نهایتاً این فناوری ساخت سلاح هسته‌ای توسط آمریکا بود که به جنگ پایان بخشید. مورگنتا پدیده سیاست را به سه الگوی اساسی تقسیم می‌کند: حفظ قدرت، افزایش قدرت و نمایش قدرت (مورگنتا، ۱۳۸۹: ۸۰). آنچه بیشتر با افزایش قدرت و نمایش آن گره خورده است، بحث فناوری و دانش است. دولت‌هایی که بتوانند جدیدترین و کارآمدترین تسلیحات را بسازند؛ قادر به دستیابی به اهداف خود در کوتاه‌ترین زمان و کمترین هزینه ممکن خواهند بود. به همین خاطر، تمرکز اصلی آمریکا و چین بر هوش مصنوعی قرار گرفته است. آمریکا در سال ۲۰۲۲، ۳۰۲۸ میلیارد دلار در هوش مصنوعی سرمایه‌گذاری کرد (AIPRM, 2024). در بودجه فدرال سال ۲۰۲۵، این رقم به ۳۰۳ میلیارد دلار افزایش پیدا کرده است. علاوه بر این، کنگره آمریکا در حال بررسی یک بسته حمایتی برای سرمایه‌گذاری ۳۲ میلیارد دلار در پروژه‌های نوآوری هوش مصنوعی در آژانس‌های غیرنظامی است (Dantes, 2024: 1). همچنین گفته می‌شود شرکت‌های متا^۱، آمازون^۲، آلفابت^۳ و مایکروسافت^۴ قصد دارند در سال ۲۰۲۵ تا ۳۲۰ میلیارد دلار در زمینه هوش مصنوعی سرمایه‌گذاری کنند (Subin, 2025: 1). هم‌زمان با افزایش بودجه‌ی آمریکا در حوزه هوش مصنوعی، بودجه‌های تخصیص داده شده از سوی وزارت دفاع آمریکا در این خصوص نیز روند افزایشی را تجربه کرده است. به نحوی که این وزارتخانه اکنون

1- Meta

2- Amazon

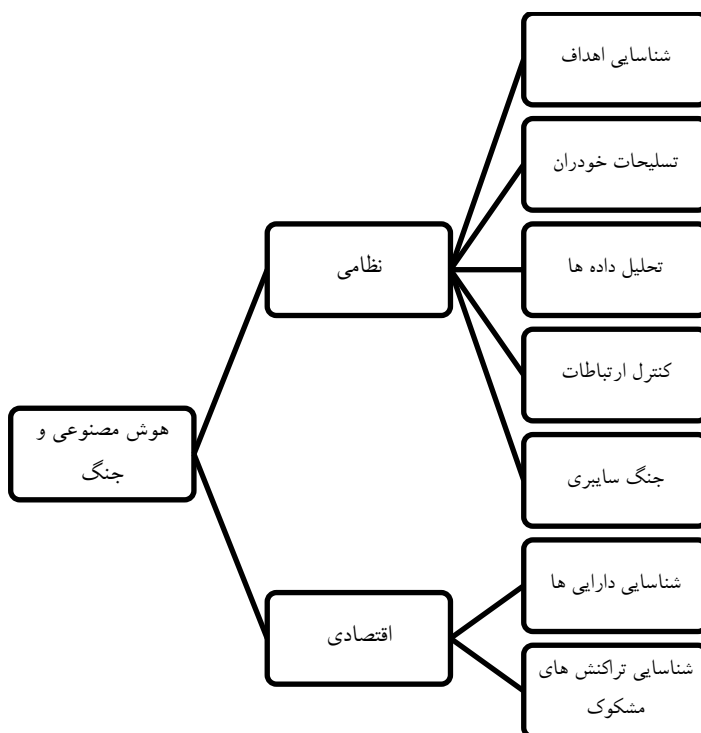
3- Alphabet

4- Microsoft

با رقمی حدود ۴۰۰ میلیون دلار بر ۶۸۵ پروژه مرتبط با هوش مصنوعی نظارت دارد (Miskelley, 2025: 2).

افزایش بودجه تحقیقات نظامی در زمینه هوش مصنوعی تا زمانی ادامه می‌یابد که آمریکا با به‌روزرسانی سخت‌افزاری و نرم‌افزاری تسلیحات خود به این اطمینان دست پیدا کند که همچنان دست برتر را در حوزه نظامی دارد و امنیت آن تضمین است. اساساً در نگاه رهبران کشورها «علم و فناوری زمانی می‌تواند نافع، اثرگذار و تحول‌آفرین باشد که خروجی و محصولات سیاسی حاصل از آن کاربردی باشد و توان اجتماعی ایجاد نماید» (آرایی، ۱۴۰۲: ۱۰۰). در واقع در نظام سیاسی آمریکا دانش در خدمت قدرت برای تضمین جایگاه جهانی آمریکا قرار گرفته است. آنها چندان به پیامدهای اخلاقی و حقوقی ناشی از کاربرد تسلیحات جدید به‌ویژه از نوع هوش مصنوعی آن توجهی ندارند. به همین خاطر ما شاهد به‌کارگیری انواع مختلفی از این تسلیحات در جنگ‌های جدید هستیم (Marr, 2018: 1-2). این کاربرد علاوه بر حوزه نظامی، حوزه اقتصادی را نیز در بر گرفته است (ر.ک: نمودار شماره ۱).

نمودار شماره ۱: چارچوب مفهومی پژوهش



۵- نقش هوش مصنوعی در جنگ سخت

در ادبیات نظامی مقصود از جنگ سخت دو بعد نظامی و اقتصادی است که در برابر جنگ نرم (فرهنگ، ارزش‌ها و هنجارها و سیاست خارجی) قرار می‌گیرد. در ادامه تأثیری که هوش مصنوعی بر این جنگ‌ها می‌گذارد بررسی می‌گردد:

۵-۱- جنگ سخت از نوع نظامی

در گذشته جنگ سخت صرفاً متکی بر تجهیزات میدانی و میزان مهارت کاربران در استفاده از این تسلیحات بود؛ اما امروزه نبرد از حالت انسانی خارج گردیده و بر تجهیزاتی تکیه دارد که با هوش مصنوعی کار می‌کنند. استفاده اسرائیل از هوش مصنوعی در جنگ، موضوع جدیدی نیست. برای دهه‌ها، اسرائیل از نوار غزه به‌عنوان آزمایشگاهی برای سنجش کارایی فناوری‌ها و تسلیحات جدید استفاده کرده و پس از این آزمایش‌ها، آن‌ها را به سایر کشورها فروخته است. بمباران نظامی ۱۱ روزه غزه در ماه می ۲۰۲۱ توسط نظامیان اسرائیل از سوی کارشناسان حوزه نظامی به‌عنوان نخستین جنگ هوش مصنوعی در جهان شناسایی شده است (Fatafta & Leufer, 2024). در ادامه به بررسی مهم‌ترین موارد کاربرد این تسلیحات از سوی اسرائیل اشاره می‌گردد.

۵-۱-۱- شناسایی اهداف نظامی

در گذشته کار شناسایی اهداف نظامی توسط نیروی انسانی و به اشکال مختلف از جاسوسی گرفته تا بهره‌مندی از انواع دوربین‌ها انجام می‌گرفت. اما امروزه هوش مصنوعی این نقش را بر عهده گرفته است. «هوش مصنوعی در تصویربرداری برای شناسایی افراد، وسایل نقلیه، اشیاء و رویدادها با تجزیه و تحلیل صدا و تصاویر گرفته‌شده توسط دوربین‌های امنیتی، استفاده می‌شود. فناوری‌های تشخیص چهره، به شناسایی مجرمان یا افراد مشکوک در بررسی‌های امنیتی کمک می‌کنند. بخش‌های دفاعی کشورها دارای سامانه‌های تشخیص چهره یا نرم‌افزارهای ردیابی افراد مشکوک با سوابق جنایی هستند» (Kaushik, 2023: 2).

پنتاگون از سال ۲۰۱۷ پروژه‌ای تحت عنوان میون 1 طراحی و اجرا کرده است که به این نهاد در یافتن اهداف نظامی کمک می‌نماید. به گفته شویلر مور 2، افسر ارشد فناوری فرماندهی مرکزی ایالات متحده (سنتکام)، «نیروهای آمریکایی در خاورمیانه با الگوریتم‌های دید رایانه‌ای به این تجربه رسیدند که این ابزار می‌تواند اهداف خود را از تصاویر گرفته‌شده توسط ماهواره‌ها و دیگر منابع داده، به‌خوبی مکان‌یابی و شناسایی نموده و هدف قرار دهد.» آنچه موجب گردید استفاده از این فناوری شتاب گیرد عملیات طوفان الاقصی در ۷ اکتبر توسط حماس بود. به گفته وی پس از این عملیات «ما به اقدامات خود نسبت به آنچه قبل از آن وجود داشت سرعت بیشتری دادیم... ما از قدرت بینایی رایانه برای شناسایی جایی که ممکن است تهدید وجود داشته باشد

1- Project Maven

2- Schuyler Moore

استفاده کردیم. ما مطمئناً در ۶۰ تا ۹۰ روز گذشته فرصت‌های بیشتری برای هدف‌گیری داشته‌ایم». او همچنین اشاره می‌کند که سامانه‌های هوش مصنوعی به شناسایی پرتابگرهای موشک در یمن و شناورهای سطحی در دریای سرخ کمک قابل توجهی کرده‌اند در نتیجه کار هدف‌گیری و دفع خطر آسان‌تر شده است (Manson, 2024: 1-3).

گزارش‌های منتشرشده در خصوص جنگ غزه نشان می‌دهد اسرائیل از یک سامانه تشخیص چهره حرفه‌ای برای کنترل و نظارت بر غزه، جمع‌آوری اطلاعات و تشخیص چهره فلسطینیان استفاده می‌کند. این سامانه از فناوری شرکت اسرائیلی کورسایت^۱ و گوگل فوتوز^۲ برای تشخیص چهره رزمندگان در میان انبوه جمعیت استفاده می‌کند (Fatafta & Leufer, 2024).

این سامانه و سامانه لاوند^۳ پایگاه گسترده‌ای از داده‌ها را در اختیار سربازان اسرائیل قرار داده است که با کمک آن توانسته‌اند ۳۷۰۰۰ هدف بالقوه را بر اساس ارتباط آشکار آنها با حماس شناسایی کنند. آنها با استفاده از اطلاعات این پایگاه، حجم زیادی کشتار بدون تفکیک نظامیان از غیرنظامیان در فلسطین انجام داده‌اند و اذعان داشته‌اند این سامانه «نقش اصلی را در جنگ ایفا کرده است و انبوهی از داده‌ها را پردازش می‌کند تا به سرعت به شناسایی جوانان [مظنون به همکاری با حماس] برای هدف قرار گرفتن کمک کند» (McKernan & Davise, 2024).

از دیگر کاربردهای هوش مصنوعی در جنگ اخیر اسرائیل علیه حماس، کشف و انهدام تونل‌های حماس در غزه بود. تونل‌هایی که مقامات اسرائیلی آن را «متروی غزه» می‌نامند و مطالعه اخیر آکادمی نظامی ایالات متحده وست پوینت^۴ نشان می‌دهد که ۱۳۰۰ تونل به طول بیش از ۵۰۰ کیلومتر (۳۱۰ مایل) در این باریکه وجود دارد. ارتش اسرائیل در جنگ اخیر برای نقشه‌برداری از تونل‌ها به پهپادهایی روی آورده است که از هوش مصنوعی برای یادگیری شناسایی انسان‌ها استفاده می‌کنند و می‌توانند زیرزمینی کار کنند. این قابلیت بر عملکرد نظامی گروه‌های مقاومت در آینده تأثیر جدی خواهد گذاشت. از جمله پهپادهایی که توسط استارت‌آپ اسرائیل رباتیک^۵ در این زمینه ساخته‌شده پهپادی محصور در یک جعبه رباتیک است که طبق اظهارات مقامات ارتش اسرائیل از آن برای ورود به تونل‌ها و فیلم‌برداری و مشاهده تا جایی که ارتباطات اجازه می‌دهد استفاده می‌شود (France 24, 2024).

گزارش‌های منتشرشده در خصوص سایر متحدان آمریکا نشان می‌دهد این کشورها با در اختیار گرفتن پهپادهای دوربرد مجهز به هوش مصنوعی از آنها در عملیات نظامی خود استفاده می‌کنند. به طور مشخص اوکراین به صورت گسترده این پهپادها را علیه اهداف نظامی و غیرنظامی در روسیه استفاده کرده است (Cotovio et al., 2024: 1-5). در حال حاضر آمریکا، انگلیس و

1- Corsight

2- Google Photos

3- Lavender

4- US military academy West Point

5- Robotican

اسرائیل بزرگ‌ترین کاربران هواپیماهای بدون سرنشین در جهان هستند و زرادخانه‌های آنها روزبه‌روز در حال گسترش است (Humble, 2024: 2).

۵-۱-۲- نسل جدید سلاح‌های خودران و خودکار

در جنگ‌های هوشمند تسلیحات خودران و خودکار به تدریج جای نیروی انسانی را خواهند گرفت. به موازات توسعه سامانه‌های هوش مصنوعی، مرحله بعد حضور بیشتر سربازان انسان‌نما در عرصه عملیات است. ربات‌های توسعه‌یافته با فناوری فعلی می‌توانند استفاده محدودی داشته باشند، زیرا بر اساس الگوریتم‌های قبلی هستند که دقت کمتری دارند. اما گروه‌های کاری مختلط که با حضور ربات‌ها و انسان‌ها تشکیل شده‌اند، کارایی عملیاتی ارتش‌ها را افزایش داده و تلفات جانی انسان‌ها را کاهش می‌دهند. ربات‌ها در موقعیت‌هایی که انسان‌ها کارایی چندانی ندارند، نقش مکمل را ایفا خواهند کرد (Zender, 2019: 1).

وقتی توسعه‌دهندگان هوش مصنوعی محصولات جدیدی را معرفی می‌کنند که می‌توانند در خدمت نیروهای مسلح قرار گیرند، به لحاظ نظری می‌توانند روند جنگ و نحوه مبارزه با آن را در بسیاری از جبهه‌های مختلف تغییر دهند. مزیت اصلی ربات‌های خودکار و خودمختار در بخش جنگ سخت این است که می‌توانند جان بسیاری از سربازان را با رفع نیاز به نبرد تن‌به‌تن در جنگ نجات دهند. اکثر ربات‌های نظامی امروزی مجهز به سلاح نیستند، آنها ربات‌های تاکتیکی هستند که عمدتاً برای خنثی کردن مواد منفجره، شناسایی، مراقبت و شناسایی تک‌تیراندازها در میدان استفاده می‌شوند. بسیار محتمل است که معرفی ربات‌های جنگنده نسل جدید، توانایی پیروزی در جنگ‌ها بدون دادن تلفات زیاد را افزایش دهد. هوش مصنوعی این توانایی و چابکی را دارد که با افزایش دقت و سرعت همه‌چیز، از مانورهای تاکتیکی در میدان نبرد گرفته تا تدارکات و انتقال نیروهای نظامی به مناطق جنگی، روند جنگ را واقعاً تغییر دهد. پنتاگون قصد دارد تا سال ۲۰۲۶ هزاران وسیله نقلیه خودمختار نسبتاً ارزان‌قیمت و قابل مصرف با هوش مصنوعی را به میدان بیاورد تا خود را هم‌تراز با چین قرار دهد. این ابتکار بلندپروازانه - که رپلیکیتور 1 نام دارد - به دنبال ایجاد پیشرفت در نوآوری نظامی ایالات متحده برای استفاده از پلتفرم‌هایی است که کوچک، هوشمند، ارزان و در دسترس هستند (Bajak, 2023: 1-4).

وزارت دفاع آمریکا در تلاش است تا پیشرفت‌های هوش مصنوعی خود را بر اساس آخرین پیشرفت یادگیری ماشینی ارتقا بخشد. مجموعه پنتاگون دارای بیش از ۸۰۰ پروژه طبقه‌بندی نشده مرتبط با هوش مصنوعی است که هنوز در مرحله آزمایش هستند. به‌طور معمول، یادگیری ماشینی و شبکه‌های عصبی به انسان کمک می‌کنند تا به سطح شناخت و کارایی بالاتری برسد.

میسی کامینگز^۱، مدیر مرکز رباتیک دانشگاه جورج میسون، می‌گوید: «هوش مصنوعی که در حال حاضر در وزارت دفاع داریم کاملاً کاربردی است و به تقویت توانمندی نیروها کمک می‌کند. هوش مصنوعی خودش به تنهایی نمی‌تواند کاری انجام دهد بلکه نظامیان از آن برای درک بهتر شرایط گنگ و مبهم صحنه جنگ استفاده می‌کنند.» به گفته تام سیبل^۲، مدیرعامل هوش مصنوعی C3 AI مستقر در سیلیکون ولی، فناوری C3 مسیر موشک‌ها را برای آژانس دفاع موشکی ایالات متحده مدل‌سازی می‌کند و درباره تهدیدات امنیتی هشدار می‌دهد (Bajak, 2023: 1-2). این فناوری که در سیستم پدافند گنبد آهنین^۳ مورد استفاده قرار گرفته است به آمریکا و اسرائیل کمک می‌کند جلوی پرتاب بسیاری از راکت‌ها و موشک‌ها از سوی جبهه مقاومت را در کل منطقه بگیرند (Amoroso & Tamburrini, 2017).

به‌طور کلی، جنگ غزه علیرغم اینکه تهدیدات امنیتی علیه اسرائیل را افزایش داده، فرصت‌هایی برای این رژیم فراهم کرده است تا دست به آزمایش‌های غیرقانونی فناوری‌های نظامی نو ظهور بزند (France 24, 2024). فن‌آوری‌های نظامی جدید از جمله دوربین‌های تفنگی مجهز به هوش مصنوعی و هواپیماهای بدون سرنشین رباتیک، برتری خاصی به صنایع نظامی اسرائیل داده‌اند. دوربین‌های اپتیکی مجهز به هوش مصنوعی ساخته‌شده توسط استارت‌آپ اسمارت شوتر^۴ که به سلاح‌هایی مانند تفنگ و مسلسل متصل می‌شود به سربازان اسرائیل کمک می‌کند تا هواپیماهای بدون سرنشین را رهگیری کنند. این امر به منزله تضعیف مهم‌ترین سلاح نظامی مورد استفاده حزب‌الله، حماس و حوثی‌ها در نبرد با اسرائیل است. به گفته یک مقام نظامی اسرائیل، «این فناوری از هر سرباز معمولی - حتی یک سرباز نابینا - یک تک‌تیرانداز ماهر می‌سازد». سامانه مورد استفاده دیگر نسل جدیدی از پهپادها به نام پرندگان خشمگین است که قادرند پهپادهای مهاجم حماس را از کار انداخته و سرنگون سازند» (France 24, 2024: 1).

همچنین ارتش اسرائیل در استفاده از ریزپرنده‌های کنترل از راه دور مجهز به مسلسل و موشک، برای نظارت، وحشت‌افکنی و کشتن غیرنظامیانی که در چادرها، مدارس پناه گرفته‌اند، پیشگام نقض قوانین بین‌المللی بوده است. در جریان جنگ غزه مسئولین بیمارستان‌ها، مناطق مسکونی و ساکنان کمپ آوارگان نصیرات گزارش دادند که برخی پهپادها صدای گریه نوزادان و زنان را پخش می‌کنند تا فلسطینیان را فریب دهند و هدف قرار دهند. چندین سال است که اسرائیل «پهپادهای انتحاری»، «تک‌تیراندازهای خودکار روبو» و برجک‌های مجهز به هوش مصنوعی را برای هدف قرار دادن غیرنظامیان در امتداد مرز غزه استفاده کرده است. «جگوار» یکی از اولین

1- Missy Cummings

2- Tom Siebel

3- Iron Dome

4- Smart Shooter

روبات‌های نظامی در جهان بود که در سال ۲۰۲۱ جایگزین سربازان این رژیم در مرزهایش گردید (Fatafta & Leufer, 2024).

۵-۱-۳- تحلیل داده‌ها و کمک به کاربر نظامی

در سال‌های اخیر، بشر با توسعه سریع دانش و فناوری مواجه بوده است؛ فناوری‌هایی که ممکن است منجر به تغییرات اساسی در زمینه‌های اقتصادی، اجتماعی، فرهنگی، سیاسی و نظامی پس از انقلاب صنعتی شود. سامانه‌های هوش مصنوعی مرحله سوم مدل‌هایی را توسعه می‌دهند که درک می‌کنند ما در چه دنیایی زندگی می‌کنیم، چه موقعیتی داریم و با شکل‌دهی به فرآیندهای تصمیم‌گیری، قوانین منطقی را بررسی کرده و راه‌حل‌هایی را پیدا می‌کنند. علاوه بر این، این سامانه‌ها قادر خواهند بود داده‌ها را از منابع مختلف جمع‌آوری کنند، این داده‌ها را برای سامانه‌های خود در دسترس قرار دهند و حتی با برنامه‌ریزی خود، تفکر انتزاعی را توسعه دهند (Zender, 2019: 1).

رابرت اشلی^۱، رئیس سابق آژانس اطلاعات دفاعی ایالات متحده، در خصوص نقش و اهمیت به‌کارگیری هوش مصنوعی در جنگ‌ها می‌گوید: «الگوریتم‌ها می‌توانند حجم انبوه داده‌های اطلاعاتی را بسیار سریع‌تر از تحلیل‌گران انسانی غربال کنند. استفاده از هوش مصنوعی برای کمک به هدف‌گیری، این پتانسیل را دارد که به فرماندهان برتری میدانی بالایی بدهد. شما با داده‌های در دسترس سریع‌تر از حریف تصمیم می‌گیرید، و اصل داستان هم در جنگ همین است» (Brumfiel, 2023: 1-2). برنامه انجیل^۲ یکی از چندین برنامه هوش مصنوعی است که توسط بخش اطلاعات ارتش اسرائیل استفاده می‌شود. در کنار این برنامه، سایر سامانه‌های هوش مصنوعی قرار دارند که مقادیر زیادی از داده‌های اطلاعاتی را جمع‌آوری و طبقه‌بندی می‌کنند. سامانه انجیل این‌گونه است که گزینه‌ها و توصیه‌هایی ارزشمند به تحلیل‌گر انسانی عرضه می‌کند. این اهداف می‌توانند هر چیزی باشند، از جنگنده‌های انفرادی گرفته تا تجهیزاتی مانند پرتابگرهای راکت یا تأسیساتی مانند پست‌های فرماندهی حماس. اساساً انجیل از کاری که گروهی از افسران اطلاعاتی در گذشته انجام می‌دادند، تقلید می‌کند، اما انجیل بسیار کارآمدتر است. یک گروه ۲۰ نفره از افسران ممکن است ظرف ۵۰ تا ۱۰۰ روز بتوانند ۳۰۰ هدف را شناسایی کنند؛ اما انجیل و سامانه‌های هوش مصنوعی مرتبط با آن می‌توانند حدود ۲۰۰ هدف را ظرف ۱۰ تا ۱۲ روز پیشنهاد کنند — میزانی که حداقل ۵۰ برابر سریع‌تر از عملکرد انسان است (Brumfiel, 2023: 1-7). همچنین گفته می‌شود که اسرائیل از ابرداده واتس‌آپ که متعلق به شرکت متا است برای ارائه داده‌ها به سامانه هدف‌گیری هوش مصنوعی لاوندر استفاده می‌کند. سامانه لاوندر مشابه سامانه انجیل کاربرد گسترده‌ای در جنایات اسرائیل و کشتارهای این رژیم علیه مردم بی‌گناه غزه داشته است (Fatafta & Leufer, 2024).

1- Robert Ashley

2- Gospel

نتیجه به‌کارگیری این تجهیزات طی ۵ ماه منتهی به مارس ۲۰۲۴ آن‌گونه که از سوی اسرائیل گزارش شده است شهادت ۳۰۰ عضو حزب‌الله از جمله ۵ فرمانده ارشد، زخمی شدن بیش از ۷۵۰ نفر و هدف گرفتن حدود ۴۵۰۰ هدف بوده است. از این تعداد ۱۲۰۰ هدف از هوا و بیش از ۳۱۰۰ هدف از زمین مورد حمله قرار گرفته‌اند. در این گزارش به نابودی ۴۵۰ هدف زیرساختی، ۱۵۰ پست دیدبانی، ۷۰ مقر نظامی و ۵۰ زیرساخت پرتاب موشک‌های سنگین حزب‌الله لبنان اشاره شده و ادعا گردیده توانایی هوایی و زمینی حزب‌الله به‌شدت آسیب دیده است (کانال تلگرامی ارتش دفاعی اسرائیل، ۱۴۰۲/۱۲/۲۴).

اسرائیل اولین بار در سال ۲۰۲۱ از سامانه انجیل در نبرد با حماس برای شناسایی مکان‌های راکت‌اندازهای حماس استفاده کرد. گروه میستال^۱ که در آن زمان فعالیت‌های این سامانه را ثبت و رصد می‌نمود، گزارش کرده است که «این سامانه در آن زمان موفق به شناسایی ۲۰۰ هدف گردید؛ اما با این حال خالی از اشکال نیز نبود. چراکه گاه مواردی را گزارش می‌کرد که یک هدف واقعی نبودند. این سامانه در اصل یک توصیه هدف‌یابی برای یک تحلیلگر انسانی ارائه می‌کند و اوست که در نهایت تصمیم می‌گیرد که آیا آن را به سربازان در میدان نبرد بدهد یا خیر؟ اوست که این اهداف را به نیروی هوایی، نیروی دریایی و مستقیماً به نیروهای زمینی از طریق اپلیکیشنی موسوم به ستون آتش^۲ می‌فرستد که فرماندهان آن را روی گوشی‌های هوشمند نظامی و سایر دستگاه‌ها نصب کرده‌اند» (Brumfiel, 2023:1).

۵-۱-۴- شناسایی و کنترل ارتباطات افراد

یکی از مهم‌ترین خدمات هوش مصنوعی در جنگ‌های هوشمند به دولت‌ها رصد ارتباطات نیروهای دشمن و شناسایی این ارتباطات برای دستگیری یا کشتن آنها در آینده است. این کار بر اساس سابقه فکری و رفتاری افراد، رفتارهای احتمالی آنها برحسب اطلاعات برگرفته از فضای مجازی و حقیقی و شناسایی ارتباطات مختلف انجام می‌پذیرد. یک برنامه رایانه‌ای قادر است مانند یک انسان و شاید بهتر کار کند و حتی با تحقیق درباره سرنخ‌های موجود به تنظیم فرضیه بپردازد.

امروزه استفاده از تلفن‌های هوشمند و فعالیت افراد در فضاهای مجازی کار تشخیص صداها، تصاویر و ردیابی آنها بر اساس هوش مصنوعی را آسان‌تر از گذشته ساخته است. دولت انگلیس از این فناوری در ردیابی افراد وابسته به گروه داعش بارها استفاده نموده است. به گفته مقامات وزارت کشور انگلیس «استفاده از فناوری یادگیری ماشین می‌تواند ۹۴ درصد تبلیغات آنلاین تروریست‌ها را با دقت ۹۹.۹۹۵ درصد شناسایی کند. این بدان معناست که اگر یک پلتفرم روزانه پنج میلیون بار آپلود دریافت کند، این مدل تقریباً تمام ویدیوهای تبلیغاتی را می‌گیرد و تنها

1- Misztal's group

2- Pillar of Fire

حدود ۲۵۰ ویدیو را برای بررسی انسانی نشانه‌گذاری می‌کند. متیو کالینز^۱، معاون مشاور امنیت ملی انگلیس در این باره می‌گوید: «فناوری‌های نوین، استاندارد جدیدی را برای تشخیص خودکار تبلیغات ویدیویی مضر و نفرت‌انگیز تروریستی در زمانی که رهبران فناوری در سراسر جهان گفته بودند این کار امکان‌پذیر نیست، ایجاد کرد» (Tech UK, 2022: 1-2).

اسرائیل همانند انگلیس، در انجام ترورهای دولتی به شدت به چنین داده‌هایی وابسته است. این رژیم طی سال‌های گذشته بارها با استفاده از پهپاد و موشک مستشاران ایرانی و نیروهای جبهه مقاومت را در سوریه و لبنان هدف قرار داده است. دو تن از مهم‌ترین چهره‌ها در این خصوص شهید سید رضی موسوی، مسئول پشتیبانی جبهه مقاومت در سوریه (تاریخ شهادت ۶ دی ماه ۱۴۰۲) و صادق امیدزاده، فرمانده اطلاعات عملیات سپاه قدس در سوریه (تاریخ شهادت ۳۰ دی ماه ۱۴۰۲) بودند. همچنین جوخه‌های ترور اسرائیل موفق شدند در ۱۲ دی ماه ۱۴۰۲ صالح العاروری، معاون رئیس دفتر سیاسی حماس، را به همراه دو تن از همراهانش در لبنان با استفاده از همین فناوری ترور نمایند. اسرائیل مدعی است تاکنون بیش از ۴۰۰ حمله هوایی در سوریه و سایر بخش‌های غرب آسیا انجام داده است. آنها از این کارزار به عنوان «جنگی میان جنگ‌ها»^۲ یاد می‌کنند که هدف آن بازدارندگی در مقابل ایران و تضعیف توانایی آن برای ضربه زدن به اسرائیل است (Nissenbaum, 2021: 1-5). ارتش اسرائیل گفته است: «ما در حال حاضر بر روی تسلیحاتی که بیشترین خسارت را ایجاد می‌کند، تمرکز کرده‌ایم» (McKernan & Kierszenbaum, 2023). طبق گزارش‌های منتشرشده از غزه «سربازان اسرائیلی برای معرفی کردن اهداف بیشتر، برای بمباران‌های روزانه تحت فشار هستند و از بمب‌های موسوم به گنگ^۳ برای هدف قرار دادن شبه‌نظامیان در گروه‌ها و دسته‌های کوچک در خانه‌هایشان استفاده می‌کنند. گروه‌هایی که شناسایی آنها با سامانه هوش مصنوعی لاوندنر صورت می‌گیرد» (Abraham, 2024). یکی از افسران اطلاعاتی اسرائیل در این باره می‌گوید: «ما علاقه‌ای به کشتن افراد [حماس]، حتی وقتی که در یک ساختمان نظامی یا درگیر فعالیت‌های نظامی بودند، نداریم. برعکس، ارتش اسرائیل به عنوان اولین گزینه، بدون تردید و واهمه آنها را در خانه‌هایشان بمباران می‌کرد. [چراکه] بمباران خانه و یک خانواده بسیار ساده‌تر [از کشتن آنها به صورتی تک‌نفری] است. این سامانه اساساً برای جستجوی آنها در این شرایط ساخته شده است» (Abraham, 2024). افسر اطلاعاتی دیگری هدف از این بمباران‌های گسترده و بی‌هدف به ساختمان‌های مسکونی و بیمارستان‌ها را «صرفه‌جویی در زمان، بجای کار بیشتر و دقیق‌تر» و «وادارسازی غیرنظامیان برای اعمال فشار بر حماس» ذکر می‌کند (Abraham, 2023). این در حالی است که این اقدامات اسرائیل مصداق بارز جنایت جنگی و نسل‌کشی است و این حجم از کشتار دسته

1 Matthew Collins

2 War between the Wars

3 Dumb Bombs

جمعی فلسطینی‌ها و تخریب خانه‌ها و اماکن غیرنظامی از زمان جنگ جهانی دوم به بعد، امری بی‌سابقه بوده است.

۵-۱-۵ جنگ سایبری

هم‌زمان با پیشرفت و متنوع شدن تهدیدها، چالش‌های موجود در حوزه امنیت سایبری نیز شکلی پیچیده‌تر به خود گرفته است. مهاجمان با بهره‌برداری از امکانات مختلف و پنهان ساختن هویت خود، فرآیند شناسایی را تا حد امکان پیچیده می‌سازند. انتظار می‌رود هوش مصنوعی هم نحوه دفاع بازیگران در برابر حملات سایبری و هم راه‌اندازی آنها را تغییر دهد. به‌عنوان مثال، سامانه‌هایی با قابلیت‌های هوش مصنوعی و یادگیری ماشینی می‌توانند درحالی‌که نقاط ضعف را در سامانه‌های خودی شناسایی می‌کنند به‌طور خودکار نقاط آسیب‌پذیر را در سامانه‌های دشمن برای بهره‌برداری بیابند. هوش مصنوعی این توانایی را دارد که از برنامه‌ها، داده‌ها، شبکه‌ها و رایانه‌ها در برابر افرادی که مجاز به دسترسی به آنها نیستند محافظت کند. هوش مصنوعی همچنین مهارت مطالعه الگوهای حملات سایبری و شکل‌دهی استراتژی‌های حفاظتی برای مبارزه با آنها را دارد. این سیستم‌ها می‌توانند کوچک‌ترین رفتارهای حملات بدافزاری را خیلی سریع و قبل از ورود به شبکه تشخیص دهند (SDI, 2024: 3-4).

یکی از تهدیدات دنیای سایبری، از دسترس خارج شدن سرویس‌های مختلف به علت بروز مشکلات سخت‌افزاری است. هوش مصنوعی با ورود به این حوزه نیز کارایی خود را به نمایش گذاشته است. هوش مصنوعی سبب ارتقا کمی و کیفی روش‌های نگهداری و کاهش هزینه‌ها از یکسو و پیچیدگی حملات از سوی دیگر شده است. طی سال‌های گذشته نهادهای مختلف اسرائیل ازجمله دوربین‌های مداربسته چهارراه‌ها، شبکه برق و آب و صنایع این رژیم مورد حملات سایبری گروه عصای موسی، گروه نزدیک به جریان مقاومت قرار گرفته است. متقابلاً این رژیم از این قابلیت برای اخلاف در برنامه هسته‌ای ایران و نیز ضربه زدن به زیرساخت‌های ایران ازجمله پالایشگاه‌ها، پتروشیمی‌ها و ... استفاده کرده است. حمله با ویروس استاکس نت به تأسیسات هسته‌ای نطنز در سال ۲۰۱۰ خسارت‌بارترین اقدام علیه ایران بوده است (Farwell & Rohozinshki, 2011:28).

۵-۲- جنگ سخت از نوع اقتصادی

برای بیش از یک قرن، تحریم ابزار مطلوب سیاست خارجی دولت‌ها برای پیگیری منافع خود بوده است. تحریم‌های اقتصادی محدودیت‌هایی در خصوص حجم واردات و صادرات، مسدود کردن دارایی‌ها یا جلوگیری از سپرده‌گذاری بانکی و نقل‌وانتقال پول و سپرده را در بر می‌گیرد. در حال حاضر آمریکا با افزون بر تحریم ۱۰ هزار فرد و نهاد مختلف در جهان، در رأس تحریم-کنندگان بین‌المللی قرار گرفته است (Forbes, 2024: 1-2). هوش مصنوعی ازجمله فناوری‌هایی

است که نقش مهمی در شناسایی افراد و نهادها و دارایی‌های آنها ایفا می‌نماید. در ادامه به دو بعد از این نقش‌آفرینی‌ها اشاره می‌گردد:

۵-۲-۱- شناسایی دارایی‌ها

شرکت‌های فناوری و بانک‌ها فعالانه در حال طراحی راه‌حل‌ها و ابزارهای هوش مصنوعی برای ارزیابی بهتر حوزه‌های قضایی پرخطر، شناسایی حرکت‌های احتمالی مشکل‌ساز یا مشکوک مالی و اصلاح غربالگری افراد در معرض اتهام و افراد یا سازمان‌های تحریم‌شده هستند. این نوآوری‌ها شامل رباتیک، اتوماسیون شناختی، یادگیری ماشین^۱، تجزیه و تحلیل داده‌ها و هوش مصنوعی در چارچوب انطباق با قوانین ضد پولشویی است (Singh, 2018: 4). این اقدامات به گروه ویژه اقدام مالی که در سال ۱۹۸۹ در همین راستا تشکیل گردید کمک قابل توجهی می‌نماید. هدف ظاهری و اعلامی این گروه مبارزه با پولشویی، مبارزه با تأمین مالی تروریسم و تأمین مالی اشاعه سلاح‌های کشتار جمعی و سایر تهدیدات مرتبط با سلامت نظام مالی بین‌المللی است؛ اما ناگفته روشن است که سطح دسترسی‌هایی که این نهاد به تراکنش‌های مالی و اسامی دارندگان حساب‌ها پیدا خواهد کرد به اعمال تحریم‌های هوشمند و هدفمند علیه افراد و دولت‌ها کمک خواهد کرد (باقری دولت‌آبادی، ۱۳۹۹: ۱۷۳-۲۰۱). شاید به همین دلیل نیز هست که عضویت در این نهاد علی‌الظاهر داوطلبانه و در عمل برای گروهی از کشورها به‌ویژه دولت‌های حامی جبهه مقاومت الزامی شده است. وزارت خزانه‌داری آمریکا پیوسته لیست تحریم افراد و نهادهای مختلف را بر اساس چنین گزارش‌هایی به‌روزرسانی می‌نماید. این امر راه‌های انتقال وجه به حساب اعضای جبهه مقاومت، خرید و فروش تسلیحات از سوی آنها، دریافت کمک‌های مردمی و... را مسدود می‌سازد.

۵-۲-۲- شناسایی تراکنش‌های مشکوک

بانک‌ها می‌توانند از هوش مصنوعی برای شناسایی الگوهای غیرمعمول در تراکنش‌های مالی مشتریان استفاده کنند. به‌عنوان مثال، الگوریتم‌های مالی تشخیص می‌دهند که یک مشتری در یک بازه زمانی کوتاه چه میزان تراکنش انجام داده یا تراکنش‌های غیرعادی که در مکان‌های دور از محل زندگی مشتری رخ داده است، در کدام کشورها بوده است. این الگوریتم‌ها می‌توانند به بانک کمک کنند تا تراکنش‌های مشکوک را شناسایی کند و اقدامات لازم را برای جلوگیری از تخلف-های مالی انجام دهد. ساین آپتیک^۲ و دیتا روبات دو نمونه از این پلتفرم‌ها هستند. دیتا ربات این توانمندی را دارد که با بررسی شبکه‌های اجتماعی و سایر اطلاعات در دسترس، محتوای گمراه-کننده ربات‌ها و دیپ فیک‌ها را شناسایی کند؛ آن‌هم در محیطی که در آن افزایش اطلاعات غلط

1- Machine learning

2- Scienaptic AI

در پلتفرم‌هایی مانند توییتر و فیس بوک به یک چالش دردرساز برای بسیاری از افراد و حتی دولت‌ها تبدیل شده است (Data Robot, 2024: 3).

شرکت کوانتکسا^۱ یکی از استارت‌آپ‌های مهم در حوزه مالی به شمار می‌رود که با به‌کارگیری هوش مصنوعی پروفایل‌هایی از مشتریان مورد اعتماد و بازیگران غیرقابل اعتماد ایجاد و روابط آنها را تجزیه و تحلیل می‌کند. این استارت‌آپ خطرات پیش‌فرض را شناسایی می‌کند و به طرز کارآمدی تقلب و پولشویی را تشخیص می‌دهد. بانک اچ. اس. بی. سی. برای پیگیری مبارزه با پولشویی از این استارت‌آپ بهره می‌گیرد (رستمی و خلیلی تیرتاشی، ۱۴۰۲: ۳۰).

فناوری‌های جدید در این حوزه عموماً در قالب فناوری‌های نظارتی^۲ شناخته می‌شوند، زیرا آنها به بهبود مبارزه با پولشویی، مقابله با تأمین مالی تروریسم و افزایش ارائه الزامات قانونی از طریق هوش مصنوعی و زیرمجموعه‌های مختلف آن، مانند یادگیری ماشین و پردازش کمک می‌کنند (McCarthy, 2023: 2). هوش مصنوعی می‌تواند با تجزیه و تحلیل حجم بالایی از داده‌های مالی و شناسایی سریع و دقیق فعالیت‌های مشکوک، به شناسایی و جلوگیری از پولشویی کمک کند. آمریکا، اتحادیه اروپا، انگلیس و اسرائیل از این فناوری برای جلوگیری از دسترسی گروه‌های جبهه مقاومت به منابع مالی استفاده می‌نمایند و تقریباً حساب‌های مالی تمامی افراد برجسته این گروه‌ها در لیست تحریم‌ها قرار گرفته است (Pavlidis, 2023: 156).

۶- نتیجه‌گیری

تأثیری که هوش مصنوعی می‌تواند در حوزه نظامی-امنیتی داشته باشد به سرعت نوآوری، ادغام و اجرای برنامه‌های فناورانه توسط کشورها بستگی دارد. همه برنامه‌های نظامی به‌طور مستقیم با توانمندی نرم‌افزارهای امنیتی، اطلاعاتی و مهندسان برنامه‌های کاربردی مرتبط هستند. درحالی‌که برنامه‌ها و سامانه‌های مورد استفاده در بخش‌های نظامی بیشتر خودکار هستند تا خودران، جهش قابل توجهی در بخش‌های تحقیق و توسعه نظامی برای پیشرفت در برنامه‌ها و سامانه‌های مستقل در بخش‌های هوش مصنوعی زمینی، هوایی، و دریایی درحال جریان است. تردیدی وجود ندارد که هوش مصنوعی در آینده نزدیک دستورالعمل بسیار بزرگی برای ارتش‌های سراسر جهان خواهد بود، کما اینکه هم‌اکنون به بخشی از دستور کار نظامی قدرت‌های بزرگ تبدیل شده است. پیش‌تاز بودن آمریکا و اسرائیل در حوزه دانش هوش مصنوعی باعث گردیده تا جهان شاهد کاربرد این فناوری از سوی آنها در جنگ باشند. آنها از این دانش هم در عملیات ترور و هم جنگ‌های کلاسیک مکرر استفاده کرده‌اند. ترور شهید فخری‌زاده، دانشمند هسته‌ای ایران، در ۷ آذر ۱۳۹۹ با استفاده از این فناوری انجام گردید و

1- Quantexa

2- RegTech

گذر زمان و نشر اطلاعات جدید، ابعاد تازه‌ای از عملیات صورت گرفته بر اساس این فناوری را روش خواهد ساخت. آنچه این مقاله تلاش نمود تشریح سازد این نکته بود که در جنگ غزه این فناوری به شکل گسترده مورد استفاده قرار گرفته است. بخشی از موارد کاربرد این فناوری در حوزه نظامی عبارت بودند از: جمع‌آوری و تحلیل داده‌ها، شناسایی اهداف نظامی، ترور فرماندهان نظامی، رصد ارتباطات نیروهای جبهه مقاومت و جنگ سایبری. همچنین هم‌راستا با بعد نظامی در بعد اقتصادی نیز این فناوری به شناسایی و مسدودسازی دارایی‌ها و منابع مالی اعضای جبهه مقاومت و دولت‌های حامی آنها از سوی آمریکا و اسرائیل کمک کرده است. اگرچه این برتری فناوری منجر به از بین بردن انگیزه و روحیه مقاومت در رزمندگان نشده؛ اما توانسته است قابلیت‌ها و توانمندی‌های اسرائیل را در میدان نبرد تقویت نماید.

پیشنهادهای عملی

به نظر می‌رسد هوش مصنوعی در آینده نزدیک نقش به‌مراتب مؤثرتری نسبت به آنچه در حال حاضر ایفا می‌کند، در جنگ‌ها بر عهده خواهد گرفت. به همین خاطر کشورها و گروه‌های عضو جبهه مقاومت که پیوسته با تهدیدات مختلف آمریکا و اسرائیل مواجه هستند وظیفه سنگینی در خصوص آمادگی برای خطرات ناشی از کاربرد فناوری هوش مصنوعی در جنگ‌های آتی خواهند داشت. بر این اساس توصیه می‌شود اقدامات زیر در دستور کار قرار گیرد: ۱- آموزش نیروهای جبهه مقاومت در خصوص نقش و کاربرد فناوری هوش مصنوعی در جنگ‌ها؛ ۲- تجهیز جبهه مقاومت به این تسلیحات جدید؛ ۳- استفاده متقابل از این فناوری‌ها علیه اسرائیل؛ ۴- انجام مطالعات میدانی در خصوص نحوه و تأثیرات کاربرد تسلیحات مبتنی بر هوش مصنوعی در جنایات‌های انجام‌شده در غزه به دست اسرائیل؛ ۵- شناسایی راه‌های مقابله و خنثی‌سازی تسلیحات جدید هوش مصنوعی؛ و ۶- حمایت از طرح‌های دانش‌بنیان در خصوص ساخت تسلیحات مبتنی بر هوش مصنوعی.

کتابنامه

- آرای، وحید، (۱۴۰۲)، دیپلماسی علم و فناوری و الهام بخشی اسلامی و منطقه‌ای جمهوری اسلامی ایران، فصلنامه مطالعات بیداری اسلامی، ۱۲(۲): ۹۵-۱۱۶.
- باقری دولت‌آبادی، علی، (۱۳۹۹)، سنجش و تحلیل میزان آگاهی سیاسی درباره گروه ویژه اقدام مالی، رهیافت‌های سیاسی و بین‌المللی، ۱۲(۱): ۱۷۳-۲۰۱.
- دارابی، علی؛ ابراهیمی، هادی، (۱۳۹۹)، نقش مکتب سلیمانی در بالندگی دیپلماسی رسانه‌ای، فصلنامه مطالعات بیداری اسلامی، ۹(۱۸): ۳۲۷-۳۵۳.

- دهقانی فیروزآبادی، سید جلال؛ چهرآزاد، سعید، (۱۴۰۲)، هوش مصنوعی و مسئله‌دار کردن درون‌مایه‌های امنیت ملی، پژوهش‌های راهبردی سیاست، ۱۲(۴۶): ۲۰۷-۲۴۲.
- رستمی، ایوب؛ خلیلی تیرتاشی، نصرالله، (۱۴۰۲)، کاربرد هوش مصنوعی در سامانه‌های مالی از دیدگاه اقتصاد اسلامی، مطالعات فقه اقتصادی، ۵(۲): ۳۴-۲۱.
- کانال تلگرامی ارتش دفاعی اسرائیل، (۱۴۰۲)، حملات ارتش اسرائیل به سازمان حزب‌الله، ۲۴ اسفند ماه.
- محمودی رجا، سید زکریا؛ باقری دولت‌آبادی، علی؛ راوش، بهنام، (۱۳۹۷)، بررسی محور مقاومت و آینده نظام سلطه با استفاده از نظریه نظام جهانی، فصلنامه مطالعات بیداری اسلامی، ۱۴(۷): ۷-۲۸.
- موحدیان، احسان، (۱۳۹۸)، هوش مصنوعی و تأثیر آن بر امنیت و روابط بین‌الملل، مجله امنیت بین‌الملل، ۱۷(۱): ۶۵-۷۵.
- مورگنتا، هانس ج.، (۱۳۸۹)، سیاست میان ملت‌ها: تلاش در راستای قدرت و صلح، ترجمه حمیرا مشیرزاده، چاپ چهارم، تهران، وزارت امور خارجه.

References

- Abraham, Yuval, (2023), "A Mass Assassination Factory": Inside Israel's Calculated Bombing of Gaza", +972 Magazine, 30 November, <https://www.972mag.com/mass-assassination-factory-israel-calculated-bombing-gaza/>
- Abraham, Yuval, (2024), 'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza, +972 Magazine, April 3, <https://www.972mag.com/lavender-ai-israeli-army-gaza/>
- AIPRM, (2024), "AI Statistics 2024", <https://www.aiprm.com/ai-statistics/>
- Amoroso, Daniele, Tamburrini, Guglielmo (2017), "The Ethical and Legal Case against Autonomy in Weapons Systems", *Global Jurist*, 22 September, <https://www.degruyter.com/document/doi/10.1515/gj-2017-0012/html?lang=de>
- Araei, Vahid, (2023), Science and technology diplomacy and Islamic and regional inspiration of the Islamic Republic of Iran, *Journal of Islamic Awakening Studies*, 12(2), 95-116. **(in Persian)**
- Arnikatarh, (2023), "A look at the impact of artificial intelligence in the future of cyber security", <https://arnika.ai/fa/mag/articles/ai-effect-on-cyber-security-future.> **(in Persian)**
- Bagheri Dolatabadi, Ali, (2020), Evaluation and Analysis of the Level of Political Awareness about FATF, *Political and International Approaches*, 12(1): 173-201. doi: 10.29252/piaj.2020.100633 **(in Persian)**
- Bajak, Frank, (2023), Pentagon's AI Initiatives Accelerate Hard Decisions on Lethal Autonomous Weapons, *Apnews*, 25 November,

<https://apnews.com/article/us-military-ai-projects-0773b4937801e7a0573f44b57a9a5942>

- Brumfiel, Geoff, (2023), "Israel is Using an AI System to Find Targets in Gaza, Experts Say it's Just the Start", *NPR*, 14 December, <https://www.npr.org/2023/12/14/1218643254/israel-is-using-an-ai-system-to-find-targets-in-gaza-experts-say-its-just-the-st>
- Chitty, Naren; Dias, Sabina, (2017), Artificial Intelligence, Soft Power and Social Transformation, *Journal of Content, Community & Communication Amity*, 6(3): 1-14.
- Cotovio, Vasco; Sebastian, Clare; Goodwin, Allegra, (2024), "Ukraine's AI-Enabled Drones Are Trying to Disrupt Russia's Energy Industry. So far, It's Working", *CNN Agency*, 2 April, <https://edition.cnn.com/2024/04/01/energy/ukrainian-drones-disrupting-russian-energy-industry-intl-cmd/index.html>
- Cummings, M. L. (2019), "Artificial Intelligence and the Future of Warfare", *Chatham House*, <https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf>.
- Dantes, Noah, (2024), "AI Set to Dominate US Federal Market Spending and Discourse in 2025", *Omdia*, 17 June, <https://www.canalys.com/insights/ai-set-to-dominate-us-federal-market-spending-and-discourse-in-2025>
- Darabi, Ali; Ebrahimi, Hadi, (2021), The Role of Soleimani School in the Growth of Media Diplomacy, *Journal of Islamic Awakening Studies*, 9(2): 327-353. **(in Persian)**
- Data Robot, (2024), "DataRobot Research and Innovation", *Data Robot*, <https://www.datarobot.com/innovation/>
- Dehghani Firozabadi, Seyed Jalal, & Chehrazad, Saeed, (2023), Artificial Intelligence and Problematisation of National Security Topics, *Political Strategic Studies*, 12(46): 207-242. doi: 10.22054/qpps.2022.70690.3130 **(in Persian)**
- Farwell, James P.; Rohozinshki, Rafal, (2011), Stuxnet and the Future of Cyber War, *Survival*, 53(1): 23-40
- Fatafta, Marva; Leufer, Daniel, (2024), "Artificial Genocidal Intelligence: how Israel is Automating Human Rights Abuses and War Crimes," *Access Now*, 9 May, <https://www.accessnow.org/publication/artificial-genocidal-intelligence-israel-gaza/>
- Forbes, (2024), "The Most Sanctioned Countries", *Forbes Georgia*, <https://forbes.ge/en/the-most-sanctioned-countries/>
- France 24 (2024), "Israel Deploys New Military AI in Gaza War", *France 24*, 10 February", <https://www.france24.com/en/live-news/20240210-israel-deploys-new-military-ai-in-gaza-war>
- Humble, Kristian, (2024), "War, Artificial Intelligence, and the Future of Conflict", *Georgetown Journal of International Affairs*, 12 July,

- <https://gjia.georgetown.edu/2024/07/12/war-artificial-intelligence-and-the-future-of-conflict/>
- IRNA News Agency, (2008). Using artificial intelligence to fight terrorism, *IRNA News Agency*, May 27, <https://www.irna.ir/news/10537990>(in Persian)
 - Israel Defense Forces Telegram Channel, (2024), Israeli Army Attacks on Hezbollah Organization, March 14. (in Persian)
 - Jo, Sunggu, (2023), Soft Power in Northeast Asia, Using AI in Information Warfare, *Robotics & AI Ethics*, 8(1): 23-36.
 - Kaushik, Khushhal, (2023), "How Does AI Help Defence Forces to Overcome Terrorism on the Ground?" 6 Jun, https://www.linkedin.com/pulse/how-does-ai-help-defence-forces-overcome-terrorism-groundkaushik?utm_source=rss&utm_campaign=articles_sitemaps&utm_medium=google_news
 - Kumar, Abhinav; Batarseh, Feras A. (2020), "The Use of Robots and Artificial Intelligence in War", *London School of Economics Business Review*, February 17, <https://blogs.lse.ac.uk/businessreview/2020/02/17/the-use-of-robots-and-artificial-intelligence-in-war/>.
 - Latiff, Robert H. (2017), *Future War: Preparing for the New Global Battlefield*, New York, Knopf.
 - Mahmoodi Raja, Seyyed Zakaria; Bagheri Dolatabadi, Ali; Ravesh, Behnam, (2019), The Axis of Resistance and the Future of Domination System Using the World-Systems Theory, *Journal of Islamic Awakening Studies*, 7(14): 7-28. (in Persian)
 - Manson, Katrina, (2024), "US Used AI to Help Find Middle East Targets for Airstrikes", *The Bloomberg*, 26 February, <https://www.bloomberg.com/news/articles/2024-02-26/us-says-it-used-ai-to-help-find-targets-it-hit-in-iraq-syria-and-yemen>
 - Marr, Bernard, (2018), "Weaponizing Artificial Intelligence: The Scary Prospect of AI-Enabled Terrorism", *Forbes*, Apr 23, <https://www.forbes.com/sites/bernardmarr/2018/04/23/weaponizingartificial-intelligence-the-scary-prospect-of-ai-enabled-terrorism>.
 - Marwala, Tshilidzi; Lagazio, Monica, (2011), *Militarized Conflict Modelling Using Computational Intelligence*, London: Springer-Verlag.
 - McCarthy, J. (2023), The Regulation of RegTech and SupTech in Finance: Ensuring Consistency in Principle and in Practice, *Journal of Financial Regulation and Compliance*, 31(2): 186-199.
 - McKernan, Bethan; Davise, Harry, (2024), 'The Machine did it Coldly': Israel Used AI to Identify 37,000 Hamas Targets, *The Gurdian*, 3 April, <https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes>
 - McKernan, Bethan; Kierszenbaum, Quique, (2023), 'We're Focused on Maximum Damage': Ground Offensive into Gaza Seems Imminent, *The Gurdian*, 10 October, <https://www.theguardian.com/world/2023/oct/10/right-now-it-is-one-day-at-a-time-life-on-israels-frontline-with-gaza>

- McKinsey, (2023), "What is AI?" Website of McKinsey, *McKinsey*, April 24, <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai>
- McKinsey and Company, (2022), "The fight against Money Laundering: Machine Learning is a Game Changer", *Insights*, www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer
- Miskelley, Anna, (2025), "Budget Trends and the Future of AI in U.S. Defense", *Defence and Security Monitor*, 11 March, <https://dsm.forecastinternational.com/2025/03/11/budget-trends-and-the-future-of-ai-in-u-s-defense/>
- Morgenthau, Hans J. (2010), *Politics among Nations: The Struggle for Power and Peace*, translated by Homeyra Moshirzadeh, 4th edition, Tehran, Ministry of Foreign Affairs. **(in Persian)**
- Movhedian, Ehsan, (2019), Artificial intelligence and Its Impact on Security and International Relations, *Journal of International Security*, 7(1): 65-75. **(in Persian)**
- Nissenbaum, D. (2022), "Israel's 'War between the Wars' With Iran Expands across Middle East", *Wall Street Journal*, 10 April, <https://www.wsj.com/articles/israels-war-between-the-wars-with-iran-expands-across-middle-east-11649595603>
- Pavlidis, Georgios, (2023), Deploying Artificial Intelligence for Anti-money Laundering and Asset Recovery: The Dawn of a New Era, *Journal of Money Laundering Control*, 26(7): 155-166.
- Rostami, Ayoub; Khalili Tirtashi, Nasrullah, (2023), Application of Artificial Intelligence in Financial Systems from the Perspective of Islamic Economics, *Strategic Studies of Jurisprudence and Law*, 5(2): 21-34. doi: 10.22034/ejs.2023.385433.1379 **(in Persian)**
- SDI, (2024), "The Most Useful Military Applications of AI in 2024 and Beyond", *SDI Sentient Digital*, <https://sdi.ai/blog/the-most-useful-military-applications-of-ai/>
- Singh, Radish et al., (2018), "The Case for Artificial Intelligence in Combating Money Laundering and Terrorist financing", *Deloitte*, <https://www2.deloitte.com/tr/en/pages/financial-advisory/articles/the-case-for-artificial-intelligence-in-combating-money-laundering-and-terrorist-financing.html>
- Subin, Samantha, (2025), "Tech Megacaps Plan to Spend More than \$300 Billion in 2025 as AI Race Intensifies", *CNBC Agency*, 8 February, <https://www.cnbc.com/2025/02/08/tech-megacaps-to-spend-more-than-300-billion-in-2025-to-win-in-ai.html>
- Szuba, Jared, (2023), "CENTCOM Eyeing Artificial Intelligence to Counter Iran's Drones, Says Kurilla Read more", *Al-Monitor*, April 12, <https://www.al-monitor.com/originals/2023/04/centcom-eyeing-artificial-intelligence-counter-irans-drones-says-kurilla>

- Tech UK, (2022), "Stopping the Spread of Online Daesh Propaganda", *Tech UK*, 4 May, <https://www.techuk.org/resource/stopping-the-spread-of-online-daesh-propaganda.html>
- Zender, Alexy, (2019), "How will Artificial Intelligence Change the Character of War?" *Beyond the Horizon*, Jan 3, <https://behorizon.org/how-will-artificial-intelligence-change-the-character-of-war/>