

کاربست فناوری‌های هوش مصنوعی در

درگیری‌های مسلحانه نوین

مطالعه موردی جنگ غزه و پیامدهای راهبردی آن

سیدجلال دهقانی فیروزآبادی^۱

فهیمة مغفرت^۲

نوع مقاله: علمی-پژوهشی

تاریخ پذیرش: ۱۴۰۴/۰۸/۰۸

تاریخ دریافت: ۱۴۰۴/۰۴/۱۰

^۱. استاد گروه روابط بین‌الملل دانشگاه علامه طباطبائی، تهران، ایران. dehghani@atu.ac.ir

^۲. کارشناس ارشد روابط بین‌الملل، دانشگاه علامه طباطبائی، تهران، ایران. (نویسنده مسئول)

fahimemaghferat1993@gmail.com

چکیده

در دهه‌های اخیر، هوش مصنوعی به‌عنوان یکی از تأثیرگذارترین فناوری‌های تحول‌ساز در عرصه نبردهای نظامی شناخته شده است. توسعه سامانه‌های تصمیم‌یار، تحلیل‌گر داده‌های کلان و ابزارهای هدف‌گیری دقیق، منجر به شکل‌گیری نوعی از درگیری‌های مسلحانه شده که در آن فناوری‌های نوین نقشی محوری در راهبردهای نظامی ایفا می‌کنند. در این میان، جنگ غزه به‌عنوان یکی از جدیدترین نمونه‌ها، صحنه آزمون گسترده بهره‌گیری از هوش مصنوعی توسط ارتش رژیم صهیونیستی بوده است. این پژوهش با بهره‌گیری از رویکردی تحلیلی، انتقادی به مطالعه کاربست سیستم‌های هوشمند نظیر «لوندرا» (Lavender) و «گاسپل» (The Gospel) در عملیات‌های نظامی ارتش رژیم اسرائیل می‌پردازد. یافته‌های مقاله نشان می‌دهد که هرچند استفاده از هوش مصنوعی منجر به افزایش سرعت در شناسایی و حذف اهداف دشمن شده، اما هم‌زمان موجب بروز چالش‌های جدی در حوزه حقوق بشری، مسئولیت‌پذیری اخلاقی و مشروعیت سیاسی کنش‌های نظامی شده است. تحلیل داده‌های میدانی و گزارش‌های سازمان‌های بین‌المللی نیز حاکی از آن است که سطح خطای سامانه‌های مورد استفاده، احتمال آسیب به غیرنظامیان را افزایش داده و ضرورت بازنگری در چارچوب‌های حقوقی بین‌المللی را آشکار ساخته است. در نهایت، این مقاله ضمن بررسی پیامدهای راهبردی و ژئوپلیتیکی استفاده از هوش مصنوعی در جنگ غزه، بر لزوم تدوین پروتکل‌های شفاف بین‌المللی برای نظارت، کنترل و مسئولیت‌پذیری در به‌کارگیری این فناوری‌ها در منازعات آینده تأکید می‌کند.

• واژگان کلیدی

هوش مصنوعی، جنگ غزه، هدف‌گیری هوشمند، حقوق بشر، امنیت بین‌المللی.

۱- مقدمه

هوش مصنوعی در نظامی گری به کار بست الگوریتم‌ها، سامانه‌های یادگیری ماشینی و پردازش خودکار داده‌ها در فرآیند تصمیم‌گیری‌های رزمی اطلاق می‌شود. این فناوری‌ها در قالب‌هایی چون سامانه‌های هدف‌گیری خودکار، تحلیل بلادرنگ داده‌های میدانی و پهنادهای خودران، در پی افزایش دقت، سرعت و کارایی عملیات‌های نظامی طراحی و به کار گرفته شده‌اند. از جمله کاربردهای پیشرفته آن می‌توان به پهنادهایی اشاره کرد که قادرند به طور مستقل اهداف انسانی را شناسایی، ردیابی و حتی بدون دخالت مستقیم انسان، عملیات هدف‌گیری و حمله را اجرا کنند.

درگیری‌های مسلحانه نوین با بهره‌گیری از فناوری‌های پیشرفته‌ای مانند سامانه‌های سایبری، رباتیک و هوش مصنوعی، مرزهای کلاسیک جنگ را دگرگون کرده‌اند. در این نوع منازعات، تمایز میان جبهه جنگ و فضای غیرنظامی کاهش یافته و ابزارهای جنگی وارد عرصه‌های جدیدی از تصمیم‌گیری خودکار شده‌اند. به گفته پی. دبلیو. سینگر، ورود سیستم‌های رباتیک و هوشمند به میدان نبرد باعث انتقال بسیاری از وظایف انسانی به ماشین‌ها شده و ما را به آستانه انقلابی فناورانه در حوزه جنگ رسانده است (Singer, 2009: 356-374).

مفهوم «هدف‌گیری هوشمند» در این زمینه، به فرایندی اشاره دارد که در آن با استفاده از تحلیل داده‌های چندمنبعی و الگوریتم‌های یادگیری ماشینی، اهداف نظامی به صورت خودکار شناسایی شده و در صورت تأیید، عملیات علیه آن‌ها انجام می‌شود. این سامانه‌ها با ترکیب داده‌هایی نظیر تصاویر ماهواره‌ای، اطلاعات انسانی^۱، سیگنال‌های الکترونیکی^۲ و داده‌های مکانی، اهداف را تحلیل و طبقه‌بندی می‌کنند. سینگر به پروژه‌هایی اشاره می‌کند که بدون مداخله انسانی، فرایند شناسایی و انهدام اهداف را از ابتدا تا انتها انجام می‌دهند و از چک‌لیست‌های خودکار برای عبور یا رد اهداف استفاده می‌کنند، مگر آن که حضور غیرنظامیان تشخیص داده شود (Singer, 2009: 390-395).

یکی از چالش‌های اساسی این فناوری‌ها، مسئله «مسئولیت‌پذیری»^۳ در صورت بروز خطا است. هنگامی که تصمیم به شلیک توسط یک الگوریتم گرفته می‌شود، پرسش‌های مهمی در خصوص مسئولیت حقوقی مطرح می‌شود: آیا مسئولیت برعهده طراح الگوریتم است؟ فرمانده نظامی؟ یا شرکت سازنده؟ سینگر نشان می‌دهد که چارچوب‌های فعلی حقوق بین‌الملل پاسخ شفافی به این

^۱. HUMINT

^۲. SIGINT

^۳. Accountability

مسائل ندارند و احتمال دارد جامعه جهانی ناچار شود مانند مورد سلاح‌های لیزری کورکننده، استفاده از سامانه‌های کاملاً خودمختار را ممنوع اعلام کند.

پیشرفت سریع فناوری‌های نوین، به‌ویژه در حوزه هوش مصنوعی، طی سال‌های اخیر موجب تحول چشم‌گیری در شیوه‌های جنگ‌افزارسازی و تاکتیک‌های نظامی شده است. این تحولات در حوزه‌هایی مانند شناسایی اهداف، تصمیم‌گیری لحظه‌ای، و استفاده از پهپادهای تهاجمی به‌روشنی قابل مشاهده‌اند. یکی از برجسته‌ترین نمونه‌های این روند، بهره‌گیری ارتش رژیم صهیونیستی از سامانه‌های هوش مصنوعی در جنگ غزه است. سامانه‌هایی نظیر لوندرو و گاسپیل با پردازش داده‌های چندمنبعی، سرعت و دقت شناسایی اهداف را افزایش داده‌اند و به ارتش این رژیم امکان داده‌اند تا با واکنش سریع‌تری عملیات انجام دهد. (Morgan et al., 2020: 16)

با این حال، این پیشرفت‌ها در کنار کارایی نظامی، پیامدهای نگران‌کننده‌ای نیز در حوزه‌های اخلاقی و حقوق بشری داشته‌اند. استفاده از الگوریتم‌ها برای تصمیم‌گیری‌های مرگ‌بار، بدون نظارت انسانی کافی، خطر نقض اصول بنیادین حقوق بین‌الملل بشردوستانه^۱ را افزایش داده است. نهادهای بین‌المللی از جمله دیده‌بان حقوق بشر هشدار داده‌اند که این فناوری‌ها، در عین تسهیل عملیات نظامی، مسئولیت تصمیم‌گیرندگان را نیز چند برابر می‌کنند. (Human Rights Watch, 2024: 2)

این مقاله، با هدف بررسی ابعاد مختلف کاربرد هوش مصنوعی در جنگ غزه، به تحلیل تأثیرات آن بر عملکرد نظامی، پیامدهای حقوق بشری و چالش‌های اخلاقی ناشی از آن می‌پردازد. در نهایت، بر لزوم تدوین پروتکل‌های بین‌المللی برای نظارت و کنترل استفاده از این فناوری‌ها در درگیری‌های مسلحانه تأکید خواهد شد.

۲. پیشینه پژوهش

تحقیقات پیرامون کاربست فناوری‌های هوش مصنوعی در منازعات مسلحانه در سال‌های اخیر عمدتاً در سه محور اصلی متمرکز بوده‌اند: تحولات فناوریانه و نظامی، پیامدهای اخلاقی و حقوقی، و تأثیرات راهبردی و ژئوپلیتیکی این فناوری بر نظم بین‌المللی.

در حوزه‌ی تحولات فناوریانه و نظامی، آثار پی. دابلیو. سینگر (۲۰۰۹)، پل شار (۲۰۱۸) و آلن و چان (۲۰۱۷) از نخستین پژوهش‌هایی به شمار می‌روند که به نقش هوش مصنوعی در دگرگونی جنگ‌های مدرن پرداخته‌اند. سینگر در کتاب خود با عنوان سیم‌کشی برای جنگ، ظهور ربات‌ها و

^۱. International Humanitarian Law – IHL

سامانه‌های خودکار را آغازگر «انقلاب سوم در جنگ» دانسته و بر تأثیر این فناوری بر ساختار نیروهای مسلح و فرآیند تصمیم‌گیری نظامی تأکید کرده است. به‌طور مشابه، شار در اثر خود با عنوان ارتش بدون انسان هشدار می‌دهد که گسترش سامانه‌های خودمختار می‌تواند چرخه‌ی تصمیم‌انسانی را از فرآیند درگیری حذف کرده و خطر بروز خطاهای فاجعه‌بار را افزایش دهد.

پژوهش‌های جان جانسون (۲۰۱۹) و گزارش‌های اندیشکده رَند (۲۰۲۱؛ ۲۰۲۴) نیز نشان داده‌اند که ادغام فناوری‌های هوش مصنوعی در حوزه‌هایی چون شناسایی، تحلیل داده و کنترل میدان نبرد، ضمن افزایش سرعت واکنش و کارایی عملیاتی، موجب تغییرات بنیادین در الگوهای فرماندهی، کنترل و بازدارندگی نظامی شده است. با این حال، این آثار عمدتاً بر روندهای کلان فناورانه تمرکز داشته و از بررسی مصادیق عینی و میدانی، از جمله جنگ غزه، غفلت کرده‌اند.

در بُعد اخلاقی و حقوقی، پژوهش‌های ربکا کروتوف (۲۰۱۸؛ ۲۰۲۱)، س. کیسی، ماسلن (۲۰۱۸)، توماس گوتزه (۲۰۲۲) و هلن نیسن‌بام (۱۹۹۴) به مسئله‌ی «شکاف مسئولیت» و چالش پاسخ‌گویی در استفاده از سلاح‌های خودمختار پرداخته‌اند. این پژوهش‌ها نشان می‌دهند که انتقال تصمیم‌گیری از انسان به الگوریتم، سبب بروز ابهام در نسبت‌دادن مسئولیت اخلاقی و حقوقی می‌شود و نظام کنونی حقوق بین‌الملل بشردوستانه برای پاسخ‌گویی به این وضعیت کفایت لازم را ندارد.

با وجود اهمیت نظری این مطالعات، تمرکز آن‌ها عمدتاً مفهومی بوده و فاقد تحلیل‌های تجربی از کاربرد واقعی سامانه‌های هوش مصنوعی در محیط‌های عملیاتی است. در مقابل، گزارش‌های اخیر سازمان عفو بین‌الملل (۲۰۲۴) و دیدبان حقوق بشر (۲۰۲۴) با بررسی عملکرد سامانه‌های «لوندر» و «گاسپل» در جنگ غزه، برای نخستین‌بار ابعاد عینی این چالش‌ها را نمایان کرده‌اند. یافته‌های این گزارش‌ها نشان می‌دهد که استفاده از سامانه‌های مزبور، به‌دلیل خطاهای الگوریتمی و فقدان کنترل انسانی مؤثر، منجر به نقض اصول بنیادین حقوق بشردوستانه؛ از جمله اصول تمایز و تناسب، و افزایش چشمگیر تلفات غیرنظامیان شده است.

از منظر راهبردی و ژئوپلیتیکی نیز، مطالعات مایکل هوروویتز (۲۰۱۸) و ویتز و اسلون (۲۰۲۰) و همچنین گزارش‌های اندیشکده رَند، بر نقش هوش مصنوعی در رقابت میان قدرت‌های بزرگ و شکل‌گیری نوعی «موازنه‌ی الگوریتمی قوا» تأکید دارند. در همین چارچوب، پژوهش بلک و همکاران (۲۰۲۴) نشان می‌دهد که کشورهایی با منابع محدود؛ از جمله رژیم اسرائیل، با بهره‌گیری از چابکی فناورانه و پیوند میان دولت، صنعت و دانشگاه، قادرند به ضریب قدرتی فراتر از وزن

ژئوپلیتیکی خود دست یابند. این یافته‌ها حاکی از آن است که کاربرت هوش مصنوعی در منازعات معاصر نه تنها یک تحول فناورانه، بلکه ابزاری راهبردی برای بازتعریف موازنه‌ی قوا و تثبیت برتری اطلاعاتی در سطح منطقه‌ای و بین‌المللی به شمار می‌رود. نیز نشان داده‌اند که این قبیل دولتها می‌توانند با بهره‌گیری از چابکی فناورانه و تمرکز بر نوآوری‌های داده‌محور، به سطحی از قدرت نظامی و اطلاعاتی دست یابند که فراتر از وزن ژئوپلیتیکی واقعی‌شان است. این دیدگاه‌ها توضیح می‌دهد که استفاده‌ی رژیم اسرائیل از سامانه‌های هوش مصنوعی در جنگ غزه نه تنها بعدی نظامی، بلکه کارکردی راهبردی در تثبیت برتری فناورانه و بازدارندگی اطلاعاتی داشته است.

در ادبیات فارسی، پژوهش‌های مرتبط با کاربرت هوش مصنوعی در جنگ‌های مدرن هنوز در مراحل ابتدایی قرار دارند و بیشتر بر ابعاد حقوقی و هنجاری متمرکز بوده‌اند تا تحلیلی، عملیاتی. به‌رغم اهمیت موضوع، تحقیقات اندکی به‌صورت مستقیم به کاربرد میدانی هوش مصنوعی در درگیری‌های معاصر پرداخته‌اند.

اسلامی و انصاری در مقاله‌ای با عنوان «به‌کارگیری روبات‌های نظامی در میدان جنگ در پرتو اصول حقوق بین‌الملل بشردوستانه» (۱۳۹۶)، میزان انطباق سامانه‌های خودکار با اصول بنیادین حقوق جنگ، از جمله تمایز، تناسب و منع رنج غیرضروری را بررسی کرده‌اند. آنان هشدار می‌دهند که خودمختاری تسلیحات هوشمند و فقدان داده‌های منفی در فرآیند یادگیری ماشینی، می‌تواند به نقض حقوق غیرنظامیان بینجامد. همچنین با اشاره به خلأهای قانونی موجود، بر ضرورت تدوین سازوکارهای تازه برای تعیین مسئولیت دولتها در استفاده از سامانه‌های هوشمند تأکید دارند.

در همین راستا، لامع، امینی‌نیا و افشاری در مقاله‌ای با عنوان «مسئولیت بین‌المللی دولتها در کاربرد هوش مصنوعی در جنگ‌افزارها با تأکید بر نقض حقوق جنگ در غزه» (۱۴۰۳)، با رویکردی تحلیلی، اسنادی، به بررسی موردی نقض قواعد حقوق جنگ در نتیجه‌ی استفاده از سامانه‌های هوش مصنوعی در عملیات نظامی رژیم اسرائیل پرداخته‌اند. آنان با اشاره به سامانه‌هایی نظیر پهپادهای مسلح خودکار، ربات‌های کشنده و سیستم‌های هدف‌گیری مبتنی بر پردازش حسگر، از حمله سامانه‌ی اسرائیلی هارپی، استدلال می‌کنند که استفاده از این تسلیحات در غیاب چارچوب‌های حقوقی روشن، منجر به نقض اصول بنیادین حقوق بشردوستانه شده است. به باور آنان، مسئولیت دولتها در قبال این اعمال باید در قالب قواعد حقوق بین‌الملل بازتعریف شود و دولت رژیم صهیونیستی باید نسبت به خسارات جانی ناشی از استفاده از این تسلیحات پاسخ‌گو شناخته شود.

با وجود ارزش نظری پژوهش‌ها، تمرکز آن‌ها عمدتاً بر تحلیل حقوقی و مفهومی بوده و به جنبه‌های فناورانه و سازوکارهای فنی سامانه‌های هوش مصنوعی در میدان نبرد، مانند لوندرو و گاسپل، و اثرات راهبردی آن‌ها بر توازن قوا نپرداخته‌اند. از این‌رو، پژوهش حاضر با رویکردی میان‌رشته‌ای، در پی پر کردن این شکاف است و با اتکا به داده‌های میدانی، گزارش‌های بین‌المللی و تحلیل فنی سامانه‌ها، می‌کوشد تا تصویری جامع از نحوه‌ی کاربست هوش مصنوعی در تصمیم‌سازی‌های نظامی و پیامدهای آن بر اصول حقوق بشردوستانه و امنیت بین‌المللی ارائه دهد. برخلاف اغلب مطالعات پیشین که تمرکز خود را بر ابعاد نظری، فناورانه یا هنجاری محدود کرده‌اند، این مقاله با رویکردی ترکیبی از فناوری، حقوق و ژئوپلیتیک به بررسی موردی جنگ غزه می‌پردازد. پژوهش حاضر نخستین مطالعه‌ای است که نحوه‌ی عملکرد واقعی سامانه‌های هوش مصنوعی نظامی لوندرو و گاسپل را در پیوند با اصول بنیادین حقوق بین‌الملل بشردوستانه و موازنه‌ی قدرت منطقه‌ای تحلیل می‌کند. این پژوهش ضمن پر کردن خلأ موجود در ادبیات داخلی و خارجی، به ارائه‌ی چارچوبی تحلیلی برای ارزیابی مسئولیت، مشروعیت و پیامدهای راهبردی کاربست هوش مصنوعی در درگیری‌های آینده می‌پردازد.

۳. چارچوب نظری و روش‌شناسی

۳-۱. چارچوب نظری: حقوق بین‌الملل بشردوستانه و مخاصمات مسلحانه

به‌کارگیری هوش مصنوعی در عملیات نظامی، به‌ویژه در جنگ غزه، پرسش‌های مهمی درباره مسئولیت‌پذیری، دقت تصمیم‌گیری و پیامدهای انسانی ایجاد کرده و نگرانی‌هایی نسبت به رعایت اصول حقوق بین‌الملل بشردوستانه برانگیخته است. چارچوب نظری مناسب برای تحلیل این موضوع، حقوق بین‌الملل بشردوستانه^۱ است که با هدف کاهش آثار مخرب جنگ بر غیرنظامیان و محدودسازی ابزار و روش‌های جنگی، بر اصول بنیادینی چون تمایز، تناسب، ضرورت نظامی و منع رنج غیرضروری استوار است (International Committee of the Red Cross, 2005).

بر اساس اصل تمایز^۲، طرف‌های مخاصمه باید میان نیروهای نظامی و غیرنظامیان تفکیک قائل شوند (International Committee of the Red Cross, 2005: Rule 1: 3). با این حال، گزارش‌ها درباره سامانه‌های هوش مصنوعی ارتش اسرائیل، از جمله «لوندرو» و «گاسپل»، از شناسایی گسترده

^۱. IHL

^۲. Distinction

اهداف انسانی و ساختمانی بدون تشخیص دقیق افراد مرتبط با گروه‌های مسلح حکایت دارد. سامانه لوندر تا ۳۷۰۰۰ فرد فلسطینی را به‌عنوان اهداف بالقوه شناسایی کرده و گاسپل نیز در شناسایی اهداف ساختمانی نقش پشتیبان تصمیم‌گیری ایفا می‌کند (Davies & McKernan, 2024; Guardian, 2024)؛ امری که اصل تمایز را با چالش مواجه می‌سازد.

اصل تناسب^۱ تصریح می‌کند که حتی در صورت مشروع بودن هدف نظامی، حمله نباید موجب تلفات غیرنظامی نامتناسب با مزیت نظامی مورد انتظار شود (International Committee of the Red Cross, 2005: Rule 14: 46). گزارش‌هایی مبنی بر کشته‌شدن ده‌ها غیرنظامی در حملاتی برای حذف اعضای پایین‌رتبه حماس، احتمال نقض این اصل را مطرح می‌کند (The New Arab, 2024). همچنین اصل ضرورت نظامی^۲، تخریب یا تصرف اموال دشمن را تنها در صورت وجود ضرورت قاطع مجاز می‌داند و بمباران اماکن فاقد دفاع و قابل اشغال را ممنوع می‌کند؛ بنابر این اصل: «تخریب یا تصرف اموال دشمن ممنوع است، مگر آنکه ضرورت نظامی قاطع آن را ایجاب کند». طبق حقوق عرفی: «مکان‌های فاقد دفاع که امکان اشغال آن‌ها وجود دارد، نمی‌توانند بمباران شوند» (International Committee of the Red Cross, 2005: 124, 175; Rule 50). از این منظر، استفاده از سامانه گاسپل برای شناسایی اهداف ساختمانی که در مواردی به کشته‌شدن حدود ۲۰ غیرنظامی برای هدف قرار دادن یک فرد پایین‌رتبه انجامیده، می‌تواند ناقض این اصل تلقی شود. اصل منع رنج غیرضروری^۳ از اصول بنیادین حقوق بین‌الملل بشردوستانه است که استفاده از وسایل و روش‌های جنگی ذاتاً موجب آسیب مفرط یا رنج بدون توجیه نظامی را ممنوع می‌کند. این ممنوعیت در اسناد کلاسیک بین‌المللی، از جمله اعلامیه سن‌پترزبورگ و مقررات لاهه، تصریح شده و بر محدودسازی ابزارهایی تأکید دارد که آثار آن‌ها فراتر از ضرورت نظامی است (International Committee of the Red Cross, 2005: Rule 70: 237-243). مصنوعی به توسعه یا استفاده از تسلیحاتی با پیامدهای غیرقابل پیش‌بینی، بی‌رویه یا خارج از کنترل منجر شود، می‌تواند ناقض این اصل تلقی گردد.

در کنار آن، اصل مسئولیت‌پذیری به‌عنوان یکی از چالش‌های نوظهور در حوزه سامانه‌های خودکار نظامی مطرح است. استفاده از هوش مصنوعی در شناسایی و هدف‌گیری مستقل، ابهاماتی جدی درباره انتساب مسئولیت حقوقی ایجاد می‌کند؛ به‌ویژه در مواردی که سامانه بدون تأیید

1. Proportionality

2. Military Necessity

3. Unnecessary Suffering

انسانی اقدام به حمله می‌کند و مشخص نیست مسئولیت متوجه فرمانده نظامی، طراح الگوریتم یا شرکت سازنده است. این وضعیت در ادبیات حقوقی معاصر با عنوان «خلاً مسئولیت‌پذیری قانونی» در جنگ‌افزارهای خودمختار^۱ مطرح شده است. هرچند عامل انسانی در مرحله به‌کارگیری دخیل است، ماهیت خودمختار این سامانه‌ها مرزهای مسئولیت را مبهم می‌سازد. با این حال، بر اساس قواعد مسئولیت دولت‌ها در حقوق بین‌الملل عمومی، کشورها در قبال نقض‌های ناشی از استفاده نیروهای مسلح‌شان از سامانه‌های خودمختار پاسخ‌گو هستند، از جمله در مواردی که سامانه پیش از استقرار به‌درستی آزمایش یا ارزیابی نشده باشد ((International Committee of the Red Cross, 2016: 16).
 کاربست سامانه‌های خودکار مبتنی بر هوش مصنوعی در عملیات نظامی، صرفاً تحول فنی در شیوه هدایت جنگ نیست، بلکه بازتابی از نابرابری‌های ساختاری در نظام بین‌الملل است؛ زیرا انحصار طراحی، پردازش و تفسیر داده‌ها در اختیار دولت‌های فناورمحور قرار دارد و غیرنظامیان در مناطق درگیری به داده‌های قابل حذف تقلیل می‌یابند. این روند اصول بنیادین حقوق بین‌الملل بشردوستانه، از جمله تمایز، تناسب و منع رنج غیرضروری را با چالش مواجه می‌کند و با تضعیف «کنترل انسانی معنادار»، ابهام در انتساب مسئولیت حقوقی میان طراح، فرمانده و دولت بهره‌بردار را تشدید می‌سازد؛ امری که ضرورت بازنگری در قواعد موجود درباره جنگ‌افزارهای خودمختار را برجسته می‌کند.

بر این اساس، پژوهش حاضر با اتکا به چارچوب حقوق بین‌الملل بشردوستانه، به ارزیابی مشروعیت به‌کارگیری هوش مصنوعی در جنگ غزه و سنجش میزان انطباق آن با تعهدات دولت‌ها ذیل معاهدات بین‌المللی، از جمله کنوانسیون‌های ژنو ۱۹۴۹ و پروتکل‌های الحاقی و نیز قواعد عرفی حقوق جنگ می‌پردازد و سازوکارهای پاسخ‌گویی و جبران در صورت تخلف را بررسی می‌کند. در مورد ارتش اسرائیل و گزارش‌های مربوط به استفاده از سامانه‌هایی نظیر «لوندرا» بدون حضور مستقیم انسانی، پرسش‌هایی جدی درباره رعایت چارچوب حقوقی موجود و مسئولیت بین‌المللی دولت و فرماندهان نظامی در قبال تلفات غیرنظامی مطرح می‌شود. این تحلیل با داده‌های میدانی و گزارش‌های نهادهای حقوق بشری و رسانه‌های معتبر تطبیق یافته است. در عین حال، این فناوری‌ها با افزایش دقت هدف‌گیری، سرعت واکنش و اثربخشی عملیات، قدرت بازدارندگی دولت‌ها را تقویت کرده و جنگ‌ها را از الگوهای سنتی به سوی جنگ‌های داده‌محور سوق داده‌اند (Johnson, 2019: 860; Rid, 2020: 33). سامانه‌هایی مانند لوندرا و گاسپل با پردازش حجم عظیم

^۱. Autonomous Weapon Systems

داده‌ها، اهداف را شناسایی و حملات را طراحی می‌کنند (Davies & McKernan, 2024)، تحولی که ضمن افزایش سرعت و مقیاس عملیات، خطرات اخلاقی و حقوقی تازه‌ای نیز ایجاد کرده است. (The New Arab, 2024) افزون بر این، هرچند فناوری‌های پیشرفته ظرفیت اطلاعاتی و سرعت تصمیم‌گیری را افزایش می‌دهند، فشار روانی و مسئولیت تصمیم‌گیرندگان را نیز تشدید می‌کنند. (Brumfiel, 2023: 2)

۲-۳. روش‌شناسی

روش پژوهش حاضر تحلیلی، انتقادی است و بر پایه مطالعه داده‌های ثانویه استوار است. داده‌های مورد استفاده شامل گزارش‌های رسمی سازمان‌های بین‌المللی (مانند سازمان ملل متحد و عفو بین‌الملل)، مستندات منتشرشده توسط رسانه‌های مستقل و معتبر نظیر مجله +۹۷۲ و تحلیل‌های مراکز پژوهشی معتبر مانند مؤسسه رند^۱ هستند. همچنین، تحلیل محتوای فنی و توصیفی سامانه‌های هوش مصنوعی معرفی شده توسط ارتش رژیم اسرائیل (نظیر لوندر و گاسپل) نیز بخشی از فرایند گردآوری داده را تشکیل می‌دهد.

فرآیند تحلیل در این پژوهش بر مبنای رهیافت انتقادی و با تمرکز بر شناسایی تناقض‌ها، چالش‌های حقوقی، و پیامدهای اخلاقی و راهبردی ناشی از به‌کارگیری هوش مصنوعی در عملیات‌های نظامی است. در این چارچوب، یافته‌ها با تکیه بر مفاهیم نظری امنیت سایبری، اتوماسیون نظامی، و موازنه قوا در نظام بین‌الملل تحلیل و تفسیر می‌شوند. هدف اصلی از این روش، ارائه تصویری چندلایه از کاربست سامانه‌های هوشمند در جنگ غزه و پیامدهای آن برای حقوق بین‌الملل بشردوستانه و ساختار ژئوپلیتیکی منطقه است.

۴. معرفی سامانه‌های هوشمند

۴-۱. سامانه‌های لوندر و گاسپل

یکی از بحث‌برانگیزترین سامانه‌های استفاده‌شده در جنگ اخیر غزه، سیستم لوندر است. بر اساس گزارش مشترک مجله +۹۷۲ و روزنامه گاردین در سال ۲۰۲۴، سامانه لوندر یک ابزار مبتنی بر یادگیری ماشینی است که توسط واحد ۸۲۰۰ ارتش رژیم اسرائیل توسعه یافته و هدف آن شناسایی افراد مشکوک به عضویت در گروه‌های نظامی فلسطینی است. این گزارش که به گواه

^۱. RAND Corporation

شش کارمند سابق واحد ۸۲۰۰ استناد می‌کند، نشان می‌دهد لوندرا با تحلیل داده‌های رفتاری، شبکه‌های اجتماعی همچون واتساپ، ارتباطات تلفنی و داده‌های مکانی، به‌طور خودکار فهرستی از اهداف بالقوه ایجاد می‌کند. الگوریتم‌های این سامانه داده‌هایی شامل اطلاعات مخابراتی^۱، ردیابی موقعیت مکانی^۲، فعالیت‌های آنلاین و اطلاعات منابع انسانی را پردازش می‌کنند؛ منابعی که به دلیل حساسیت موضوع خواستار عدم افشای هویت خود شده‌اند.

لوندرا دقتی ادعا شده در حدود ۹۰ درصد برای شناسایی مردان فلسطینی ۲۰ تا ۴۰ ساله دارد، هرچند این تخمین همراه با خطای ۱۰ درصدی گزارش شده است. تایید نهایی اهداف توسط نیروی انسانی نیز محدود به بررسی‌ای کوتاه و حدوداً ۲۰ تا ۳۰ ثانیه‌ای برای هر هدف بوده است. این گزارش توسط گاردین و دیگر رسانه‌های معتبر بین‌المللی بازنشر و تایید شده و ابعاد نگران‌کننده‌ای از نقش هوش مصنوعی در عملیات‌های نظامی رژیم اسرائیل را افشا می‌کند (Abraham, 2024).

بر اساس گزارش تخصصی نظامی منتشر شده توسط نیروهای دفاعی اسرائیل^۳ در سال ۲۰۲۳ با عنوان کاربرد عملیاتی سیستم‌های هدف‌یابی مبتنی بر هوش مصنوعی در جنگ شهری، که به صورت داخلی تهیه و توسط مجله ۹۷۲ + افشا شده است، سامانه گاسپل یکی از ابزارهای کلیدی هدف‌گیری در عملیات‌های شهری محسوب می‌شود. طبق گزارش برگمن و مازتی (۲۰۲۳)، کارکرد اصلی گاسپل شناسایی و هدف‌گیری زیرساخت‌ها و تأسیسات نظامی با دقتی بین ۸۵ تا ۹۰ درصد است. این سامانه داده‌های گوناگونی را برای تحلیل و تصمیم‌گیری ترکیب می‌کند که شامل تصاویر ماهواره‌ای با وضوح ۳۰ سانتی‌متر با فناوری‌های مکسار^۴، سیگنال‌های الکترونیکی^۵ و داده‌های موقعیت‌یاب بلادرنگ^۶ می‌شود.

مکانیسم عمل گاسپل به این صورت است که داده‌های پردازش شده توسط سامانه لوندرا با اطلاعات جغرافیایی تلفیق می‌شوند تا «نقشه حرارتی اهداف» ایجاد شود. (Israel Defense Forces, 2023) این نقشه حرارتی به شناسایی و اولویت‌بندی سریع زیرساخت‌ها و اهداف نظامی در محیط‌های پیچیده شهری کمک می‌کند. در نقل‌قولی کلیدی، برگمن و مازتی تأکید می‌کنند: «سامانه گاسپل روزانه بیش از ۱۰۰۰ هدف بالقوه را پردازش می‌کند و زمان بررسی اهداف را از ۷۲ ساعت به کمتر از ۱۵ دقیقه برای هر هدف کاهش می‌دهد» (Bergman & Mazzetti, 2023: para. 7).

1. Call Detail Records

2. GSM/CellID

3. Israel Defense Forces

4. Maxar Technologies

5. ELINT

6. RTK-GPS

بنابراین می‌توان گفت ورود سامانه‌های لوندرو و گاسپل نشان‌دهنده‌ی یک مرحله جدید در تحول مفهوم جنگ‌های هوشمند است. برخلاف جنگ‌های سنتی که تکیه اصلی بر تصمیم‌گیری انسانی و اطلاعات میدانی داشتند، این سامانه‌ها به سطحی از خودکارسازی تصمیمات رسیده‌اند که مستقیماً جان انسان‌ها را هدف قرار می‌دهد. نکته کلیدی این است که زمان تایید انسانی به حداقل رسیده (۲۰ تا ۳۰ ثانیه برای لوندرو و کاهش زمان از ۷۲ ساعت به ۱۵ دقیقه در گاسپل). این امر سولاتی جدی در مورد کاهش آستانه استفاده از زور مطرح می‌کند و به‌طور ضمنی خشونت اتوماسیونی^۱ را به جلو می‌راند.

از منظر حقوق بین‌الملل، استفاده از این سامانه‌ها چالش‌هایی را در زمینه رعایت اصل تناسب و تمایز مطرح می‌کند. به‌ویژه لوندرو که بر اساس تحلیل داده‌ها، مردان فلسطینی ۲۰ تا ۴۰ ساله را هدف می‌گیرد، می‌تواند با اصل تمایز بین نظامیان و غیرنظامیان تعارض پیدا کند. همچنین، گزارش‌های مستند نشان می‌دهند که با وجود ادعای دقت ۹۰ درصدی، ۱۰ درصد خطا عملاً به معنای کشته‌شدن تعداد زیادی غیرنظامی است. این مسئله خطر ارتکاب جنایات جنگی را افزایش می‌دهد و زمینه‌های تقویت درخواست‌های بین‌المللی برای پاسخگویی حقوقی را فراهم می‌آورد.

این دو سامانه در مجموع نمایانگر گذار به یک نظم امنیتی نوین هستند که در آن فناوری هوش مصنوعی نه فقط به عنوان ابزار، بلکه به عنوان یک «کنشگر امنیتی مستقل» ظاهر می‌شود. اگرچه ارتش اسرائیل مدعی کارایی و دقت بالا است، اما حجم وسیع خطاهای بالقوه، زمان‌بندی بسیار کوتاه تایید انسانی، و تاکید بر خودکارسازی خشونت، همگی ضرورت بازنگری جدی در چارچوب‌های قانونی و اخلاقی موجود را نشان می‌دهند. این تحولات همچنین فشار بیشتری بر نهادهای بین‌المللی برای بازتعریف مفاهیمی همچون مسئولیت حفاظت، پاسخگویی دیجیتال و عدالت الگوریتمی وارد خواهند کرد.

۴-۲. تأثیرات عملیاتی سامانه‌های هوشمند

افزایش دقت هدف‌گیری: استفاده از این سامانه‌ها باعث افزایش چشمگیر در سرعت و دقت شناسایی اهداف نظامی شده است. به گزارش اندیشکده رند ۲۰۲۱، استفاده از هوش مصنوعی در عملیات‌های ارتش رژیم صهیونیستی موجب شد که زمان تشخیص و انهدام یک هدف از چندین ساعت به کمتر از ۲۰ دقیقه کاهش یابد. این پیشرفت، مزیت تاکتیکی قابل توجهی برای ارتش فراهم

^۱. Automated Violence

کرده و به کاهش نیاز به مداخله انسانی در تصمیم‌گیری‌های آنی منجر شده است. هوش مصنوعی صرفاً یک فناوری واحد نیست، بلکه طبقه‌ای از فناوری‌ها است که می‌توانند در طیف گسترده‌ای از کاربردهای نظامی ادغام شوند. این فناوری‌ها، علاوه بر افزایش سرعت تصمیم‌گیری، قابلیت خودکارسازی فرایند انتخاب اهداف و حتی اجرای هم‌زمان حملات را فراهم می‌کنند و از این طریق اشکال تازه‌ای از تحلیل نظامی و قدرت رزمی را ممکن می‌سازند. (RAND Corporation, 2021: 118) هدف‌گیری خودکار به کار گرفته می‌شود، می‌تواند مرز میان انسان و ماشین در تصمیم‌گیری‌های مرگ و زندگی را به‌طور بنیادین جابه‌جا کند.

در همین راستا، گزارش رند تأکید می‌کند که گسترش سریع هوش مصنوعی در حوزه‌هایی چون تشخیص اشیاء، پشتیبانی از تصمیم‌گیری و سامانه‌های تسلیحاتی خودکار، نشانه‌ای از تحولی اساسی در ماهیت جنگ است. با افزایش سرعت پردازش و واکنش این سامانه‌ها، نقش عاملیت انسانی در عملیات نظامی به‌تدریج کمرنگ می‌شود و سیستم‌های خودمختار به بازیگران اصلی میدان نبرد بدل می‌گردند. این تحول، که در جنگ غزه در قالب سامانه‌هایی مانند لوندرو و گاسپل به‌شکل عینی مشاهده شد، نشان می‌دهد که ادغام هوش مصنوعی در فرایندهای هدف‌گیری نه‌تنها مزیت عملیاتی ایجاد می‌کند، بلکه ریسک‌های اخلاقی، حقوقی و راهبردی جدیدی را نیز برمی‌انگیزد؛ ریسک‌هایی که نیازمند بازنگری جدی در چارچوب‌های نظارتی و اصول حقوق بین‌الملل بشردوستانه هستند. (RAND Corporation, 2021: 141)

کاهش زمان واکنش: سامانه لوندرو به گونه‌ای طراحی شده که روزانه بیش از ۳۷ هزار هدف احتمالی را در بانک اطلاعاتی خود ثبت و رتبه‌بندی می‌کند. فرماندهان می‌توانند بر اساس این فهرست، در عرض چند دقیقه تصمیم به حمله بگیرند، بی‌آنکه فرایند شناسایی انسانی طی شود. سیستم لوندرو با خطای بالا (حدود ۱۰٪) کار می‌کند و به دلیل حجم بالای اهداف، منجر به تلفات غیرنظامی شده است. این امر اگرچه موجب افزایش سرعت عملیات شده، اما سطح اتکای اخلاقی و مسئولیت‌پذیری تصمیم‌گیرندگان را تضعیف کرده است. (+972 Magazine, 2024, April 3)

پیوند با شبکه‌های اطلاعاتی و داده‌های کلان: یکی دیگر از وجوه متمایز این سامانه‌ها، ادغام آن‌ها با شبکه‌های گسترده اطلاعاتی شامل نظارت‌های الکترونیکی، داده‌های سوشال مدیا، سامانه‌های مکان‌یابی و تحلیل متن است. برای مثال، گاسپل از داده‌های ویدئویی و سیگنالی بلادرنگ برای تعیین دقیق محل اختفای افراد و تجهیزات استفاده می‌کند. این ادغام، قدرت

پیش‌بینی و اقدام فوری را به‌شدت افزایش داده، ولی هم‌زمان نظارت بیش‌ازحد بر غیرنظامیان را نیز ممکن کرده است. سامانه گاسپل یکی از پیشرفته‌ترین ابزارهای هوش مصنوعی است که ارتش رژیم اسرائیل از آن برای شناسایی اهداف نظامی در جریان درگیری با حماس در غزه استفاده می‌کند. این سامانه با بهره‌گیری از حجم عظیمی از داده‌های نظارتی، شامل اطلاعات مکانی تلفن‌های همراه، مکالمات شنود شده، تصاویر پهپادی و ماهواره‌ای، و همچنین اطلاعات میدانی از منابع انسانی، فرآیند پردازش و تحلیل را به گونه‌ای انجام می‌دهد که به ارتش امکان می‌دهد در مدت زمانی بسیار کوتاه، صدها هدف بالقوه را شناسایی کند.

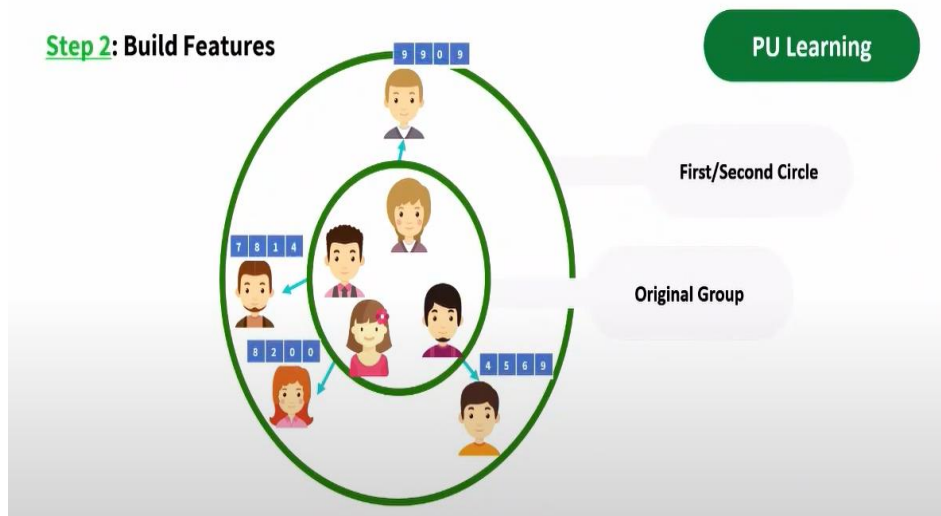
گاسپل عملاً نقش یک تیم اطلاعاتی انسانی را ایفا می‌کند؛ کاری که پیش‌تر توسط گروهی از افسران اطلاعاتی انجام می‌شد، اکنون با سرعت و حجم بالاتری توسط این سامانه انجام می‌گیرد. به عنوان نمونه، در جنگ سال ۲۰۲۱ با حماس، گاسپل توانست ۲۰۰ هدف را ظرف مدت کوتاهی شناسایی کند؛ کاری که تحلیل‌گران انسانی به‌تنهایی قادر به انجام آن در آن بازه زمانی نبودند. در واقع لوندِر پایگاه داده‌ای از ده‌ها هزار فرد ایجاد کرد که عمدتاً به‌عنوان اعضای رده پایین شاخه نظامی حماس علامت‌گذاری شده بودند. این سامانه همراه با سیستم پشتیبانی تصمیم‌گیری گاسپل استفاده می‌شد که ساختمان‌ها و سازه‌ها را به‌عنوان اهداف معرفی می‌کرد، نه افراد را (Brumfiel, 2024).

به گزارش روزنامه گاردین، طی مصاحبه‌ای با چند تن از افسران اطلاعاتی ارتش رژیم اسرائیل، اعلام شده است که مردان فلسطینی دارای ارتباط با شاخه نظامی جنبش حماس، بدون توجه به درجه یا اهمیت عملیاتی، به‌عنوان اهداف بالقوه شناسایی و در فهرست هدف‌گیری قرار می‌گیرند. همچنین تأکید شده است که اعضای رده پایین حماس به‌طور ترجیحی هدف حملات قرار می‌گیرند. بنا بر اظهارات دو منبع مطلع، حملات علیه این دسته از نیروهای رده پایین غالباً با استفاده از بمب‌های غیرهوشمند^۱ صورت می‌گیرد که منجر به تخریب کامل ساختمان‌ها و کشته شدن تمامی افراد حاضر در محل می‌شود. یکی از این منابع تصریح کرده است که رژیم اسرائیل از به‌کارگیری بمب‌های گران‌قیمت برای هدف قرار دادن افراد کم‌اهمیت اجتناب می‌کند (The Guardian, 2024, April 3).

^۱. dumb bombs

تصویر ۱: گام دوم: فرآیند ایجاد ویژگی‌ها

How Does it Work?



منبع: (+972 Magazine, 2024, April 3)

این تصویر مربوط به یکی از اسلایدهای ارائه نیروهای اطلاعاتی ارتش اسرائیل^۱ درباره نحوه عملکرد سامانه شناسایی هدف خودکار با کمک یادگیری ماشین است. تصویر مرحله دوم این فرایند را تحت عنوان مرحله ۲؛ ایجاد ویژگی‌ها^۲ نشان می‌دهد که در ادامه به تحلیل اجزای کلیدی تصویر می‌پردازیم:

۴-۲-۱. ساختار دو دایره‌ای؛ (گروه اصلی و دایره اول / دوم):

دایره داخلی: گروه اصلی^۳، افراد شناخته‌شده‌ای هستند که به صورت قطعی به عنوان اعضای گروه‌های مسلح (مثلاً حماس یا جهاد اسلامی) شناسایی شده‌اند. این داده‌ها به عنوان نمونه‌های آموزش مورد استفاده قرار می‌گیرند.

^۱. IDF Intelligence Directorate

^۲. Step 2: Build Features

^۳. Original Group

دایره بیرونی^۱: دایره اول/ دوم افرادی هستند که شباهتهایی با گروه اولیه دارند. آن‌ها بر اساس ویژگی‌های مشترک با گروه اول رتبه‌بندی شده‌اند و هدف تحلیل الگوریتمی برای شناسایی تهدیدات بالقوه هستند. (The Guardian, 2024, April 3)

۴-۲-۲. یادگیری مثبت و نامشخص^۲

این نوع یادگیری ماشینی زمانی استفاده می‌شود که تنها داده‌های مثبت (در اینجا افراد تأییدشده به عنوان اعضای گروه‌های نظامی) در دسترس است و داده‌های منفی (غیرنظامیان تأییدشده) وجود ندارد. الگوریتم تلاش می‌کند با استفاده از این داده‌های ناقص، شباهتهای پنهان را شناسایی کرده و افراد مشکوک را رتبه‌بندی کند (Charte et al., 2015: 14)

۴-۲-۳. امتیازهای دیجیتال کنار هر فرد

این اعداد نمایانگر «ویژگی‌های کمی»^۳ هستند که به صورت خودکار توسط الگوریتم بر اساس داده‌های رفتاری، ارتباطی، یا مکانی فرد تولید شده‌اند. هرچه این اعداد به افراد دایره داخلی شباهت بیشتری داشته باشند، فرد هدف دارای اولویت بیشتری برای حمله خواهد بود. در سامانه‌هایی مانند لوند، به هر فرد موجود در پایگاه داده، امتیاز دیجیتالی اختصاص می‌یابد که بازتابی از میزان شباهت آن فرد به اعضای شناخته‌شده گروه‌های مسلح (نظیر حماس یا جهاد اسلامی) است. این امتیازها، در واقع ویژگی‌های کمی هستند که به‌طور خودکار از طریق الگوریتم‌های یادگیری ماشین و بر پایه داده‌های رفتاری، مکانی، و ارتباطی افراد تولید می‌شوند. هرچه این ویژگی‌ها با ویژگی‌های افراد گروه اصلی (دایره داخلی) هم‌پوشانی بیشتری داشته باشد، احتمال هدف قرار گرفتن فرد نیز بیشتر خواهد بود.

برخی از مهم‌ترین ویژگی‌هایی که منجر به افزایش این امتیاز می‌شوند، شامل مواردی چون عضویت در یک گروه واتس‌آپی با عضو شناخته‌شده حماس، تعویض مکرر تلفن همراه، یا جابجایی‌های مکرر محل سکونت هستند. این اطلاعات می‌توانند از منابع مختلفی مانند داده‌های تصویری، اطلاعات مخابراتی، شبکه‌های اجتماعی، اطلاعات میدانی و فهرست تماس‌های تلفنی استخراج شوند. فرمانده فعلی یگان ۸۲۰۰ ارتش رژیم اسرائیل، در کتابی که به صورت غیرمستقیم به عملکرد چنین سامانه‌هایی پرداخته، تأکید

¹. First/Second Circle

². Positive-Unlabeled Learning, PU Learning

³. Quantitative Features

می‌کند: «هرچه اطلاعات بیشتر و متنوع‌تر باشد، بهتر است.» او توضیح می‌دهد که در مراحل اولیه، انسان‌ها وظیفه انتخاب ویژگی‌های معنادار را برعهده دارند، اما به مرور، ماشین قادر خواهد بود به‌طور مستقل ویژگی‌های جدید را شناسایی و در روند رتبه‌بندی به کار گیرد (+972 Magazine, 2024, April 3)

۴-۲-۴. عملکرد الگوریتم در زمینه نظامی

این سامانه بر پایه تشخیص الگو و دسته‌بندی آماری کار می‌کند، نه تحلیل انسانی مستقیم. افراد از روی شباهت رفتاری یا ارتباطی (مثلاً تماس با افراد حماس، استفاده از تلفن مشترک با یکی از اعضای گروه، یا شباهت اسمی) مورد هدف قرار می‌گیرند.

به گزارش مجله +۹۷۲، سامانه لوندرا با بهره‌گیری از تکنیک‌های داده‌کاوی و رتبه‌بندی آماری، به هر فرد در پایگاه اطلاعاتی خود «امتیاز دیجیتال» اختصاص می‌دهد که نشانگر میزان شباهت او با اعضای شناخته‌شده گروه‌های مسلح است؛ این امتیاز می‌تواند بر پایه داده‌های مکانی، رفتاری یا ارتباطی مانند تماس با یک فرد خاص یا استفاده از خطوط تلفن مشترک، تعیین شود این تصویر نشان می‌دهد که سامانه هوشمند (لوندرا یا مشابه آن) با استفاده از یادگیری مثبت و نامشخص، شبکه‌ای از افراد را تنها بر اساس شباهت احتمالی با افراد شناخته‌شده ایجاد می‌کند. هرچند این روش دقت آماری نسبتاً بالایی دارد، اما به دلیل نبود داده‌های منفی قطعی و فقدان ارزیابی انسانی مستقل، احتمال خطاهای کشنده علیه غیرنظامیان بسیار بالاست. به همین دلیل این سامانه در سطح بین‌المللی از منظر اخلاقی و حقوق بشری بسیار مورد نقد قرار گرفته است. (+972 Magazine, 2024, April 3)

تصویر ۲: گام سوم؛ فرآیند رتبه‌بندی

How Does it Work?

Step 3: Ranking

PU Learning



منبع: (+972 Magazine, 2024, April 3)

این تصویر مربوط به مرحله سوم^۱ از فرایند تحلیل الگوریتمی در سامانه شناسایی خودکار اهداف توسط ارتش رژیم صهیونیستی است. این مرحله با بهره‌گیری از یادگیری با داده‌های مثبت و بدون برچسب منفی و نامشخص افراد را بر اساس میزان شباهت به تروریست‌های شناخته‌شده رتبه‌بندی می‌کند.

• افراد با برچسب واقعیت مبنا؛ GT^۲

چهار نفر اول از چپ دارای برچسب واقعیت مبنا هستند؛ یعنی این افراد قبلاً به‌صورت قطعی به‌عنوان اعضای گروه‌های نظامی (مثلاً حماس یا جهاد اسلامی) شناسایی شده‌اند. این‌ها داده‌های مثبت آموزشی برای الگوریتم هستند. (972 Magazine, 2024, April 3)

• افراد بدون برچسب^۳:

بقیه افراد بدون برچسب مشخص هستند، اما کنار آن‌ها عددی بین ۰ تا ۱ نوشته شده است. این عددها نشان‌دهنده‌ی امتیاز شباهت^۴ است که الگوریتم به آن‌ها اختصاص داده. هرچه عدد به ۱ نزدیک‌تر باشد، فرد از نظر الگوریتم شباهت بیشتری به تروریست‌های شناخته‌شده دارد. مثلاً: نفر پنجم (زن با پیراهن صورتی): ۰.۹۱ → احتمال بالای شباهت. نفر هشتم (زن با مو قرمز): ۱.۰۰ → حداکثر شباهت، یعنی با اطمینان بالا به‌عنوان هدف مشخص می‌شود.

این مدل صرفاً بر اساس شباهت آماری و بدون تأیید انسانی نهایی، افراد را هدف قرار می‌دهد. در این سیستم، ممکن است یک فرد بی‌گناه صرفاً به‌دلیل رفتار مشابه با فرد تروریست، یا تماس گرفتن با یک فرد عضو حماس (مثلاً برای یک کار شخصی)، در فهرست هدف قرار گیرد. این مسأله باعث نگرانی‌های جدی در حوزه حقوق بین‌الملل بشردوستانه شده است در این اسلاید، مرحله نهایی پیش از تصمیم‌گیری برای عملیات نظامی خودکار نمایش داده شده است. (Andersin, 2025: 10)

۳-۴. نمونه‌های کاربرد میدانی

بر اساس تحقیقات سازمان عفو بین‌الملل در جریان حمله به رفح در نوامبر ۲۰۲۳، سیستم لوندنر بیش از ۵۰ هدف را در بازه کمتر از ۴ ساعت شناسایی و برای انهدام به سامانه‌های پهنپادی معرفی کرد. با وجود هشدار نهادهای حقوق بشری درباره حضور غیرنظامیان در این منطقه، حملات

^۱. Step 3: Ranking

^۲. Ground Truth

^۳. Unlabeled

^۴. Similarity Score

هوایی به اجرا درآمد و منجر به کشته‌شدن بیش از ۷۰ غیرنظامی شد. در گزارش آمده است که بسیاری از این افراد بر اساس داده‌هایی که خطای الگوریتمی داشته‌اند، به‌عنوان «اهداف وابسته به حماس» دسته‌بندی شده بودند سازمان عفو بین الملل تأکید کرده است که در هیچ‌یک از این حملات نشانه‌ای از وجود اهداف نظامی مشروع در ساختمان‌های مسکونی هدف قرار گرفته‌شده وجود نداشته است، که این موضوع نگرانی‌هایی را درباره حملات مستقیم به غیرنظامیان و اشیاء غیرنظامی ایجاد کرده است (Amnesty International, 2024; Human Rights Watch, 2024).

۵. پیامدهای حقوقی، اخلاقی و انسانی

کاربست فناوری‌های نوین، به‌ویژه سامانه‌های مبتنی بر هوش مصنوعی، در جنگ غزه، مجموعه‌ای از پرسش‌های جدی و پیچیده را در حوزه حقوق بین‌الملل بشردوستانه، اخلاق جنگ، و مسئولیت‌پذیری حقوقی مطرح کرده است. استفاده از الگوریتم‌ها و سامانه‌های نیمه‌خودران برای شناسایی و هدف‌گیری، گرچه از منظر کارایی نظامی به‌عنوان نوآوری تلقی می‌شود، اما از منظر حقوقی و اخلاقی پیامدهای قابل‌توجهی به همراه داشته است. از جمله مهم‌ترین چالش‌ها می‌توان به خطاهای احتمالی در هدف‌گیری اشاره کرد که ممکن است منجر به تلفات گسترده غیرنظامیان شود؛ مسئله‌ای که اصل تمایز و تناسب در حقوق بین‌الملل بشردوستانه را به‌شدت تحت فشار قرار می‌دهد.

علاوه بر این، عدم شفافیت در روند تصمیم‌گیری این سامانه‌ها؛ که اغلب به‌دلیل ماهیت پیچیده الگوریتم‌ها و فرآیندهای مبتنی بر داده‌های کلان است، زمینه را برای بروز ابهام‌های جدی درباره امکان بررسی و پاسخگویی فراهم می‌کند. این وضعیت، مسئولیت حقوقی را نه‌تنها برای کاربران مستقیم این سامانه‌ها، بلکه برای توسعه‌دهندگان فناوری و حتی دولت‌های مرتبط، به موضوعی محل مناقشه بدل ساخته است. خلأهای موجود در نظام حقوقی بین‌المللی در زمینه مواجهه با سامانه‌های خودران و نیمه‌خودران، باعث شده چارچوب‌های سنتی حقوق جنگ کارایی محدودی در پاسخگویی به این تحولات داشته باشند.

به این ترتیب، تحولات اخیر نه‌تنها بازنگری در مقررات موجود را ضروری ساخته‌اند، بلکه اهمیت گفت‌وگویی میان‌رشته‌ای میان حوزه‌های حقوق، فناوری، و اخلاق را برای تبیین استانداردهای جدید و پاسخگویی مؤثر به چالش‌های نوظهور به‌خوبی برجسته کرده‌اند.

۵-۱. نقض اصول حقوق بشردوستانه: تمایز و تناسب

همانطور که پیشتر بدان اشاره شد پایه و اساس حقوق بین‌الملل بشردوستانه را کنوانسیون‌های ژنو ۱۹۴۹ و پروتکل‌های الحاقی آن تشکیل می‌دهند. به‌ویژه، پروتکل الحاقی (I) به کنوانسیون‌های ژنو ۱۹۴۹ که به حمایت از قربانیان مخاصمات مسلحانه بین‌المللی اختصاص دارد (مصوب ۸ ژوئن ۱۹۷۷)، اصول بنیادینی همچون تمایز و تناسب را به‌روشنی بیان می‌کند. ماده ۴۸ این پروتکل بر قاعده کلی تمایز میان جمعیت غیرنظامی و اهداف نظامی تأکید می‌ورزد و مقرر می‌دارد که طرفین مخاصمه باید همواره میان این دو گروه تفاوت قائل شوند تا از آسیب‌رساندن به غیرنظامیان جلوگیری شود. همچنین، ماده ۵۱ بند (۵)(ب) و ماده ۵۲ بند (۲) به اصل تناسب و تعریف دقیق اهداف نظامی پرداخته و تصریح می‌کنند که هرگونه حمله باید محدود به اهدافی باشد که به‌طور مؤثر به عملیات نظامی دشمن کمک می‌کنند و تخریب یا آسیب‌های جانبی نباید بیش از حد لازم باشد. این اصول هسته اصلی تعهدات حقوقی طرفین مخاصمه را تشکیل می‌دهند و تخطی از آن‌ها مصداق نقض جدی حقوق بین‌الملل بشردوستانه محسوب می‌شود. هرچند بر اساس اصول بنیادین حقوق بین‌الملل بشردوستانه، طرفین مخاصمه ملزم به تمایز میان اهداف نظامی و غیرنظامی هستند و هرگونه حمله باید با اصل تناسب همراه باشد (Protocol Additional to the Geneva Conventions, 1977). اما همانطور که بیان شد گزارش‌ها نشان می‌دهد سامانه‌های هوشمندی مانند لوندرا، که با درجه بالایی از خودکارسازی عمل می‌کنند، در شناسایی اهداف دچار خطاهای فاحش شده‌اند؛ برای مثال، تحلیل‌ها نشان می‌دهد تنها بر اساس الگوهای رفتاری دیجیتال و بدون تأیید انسانی، افراد غیرنظامی به‌عنوان اعضای حماس هدف قرار گرفته‌اند. به گفته سازمان عفو بین‌الملل، استفاده از الگوریتم‌هایی که معیارهای مبهم و فاقد نظارت انسانی دارند، به نقض سیستماتیک اصل تمایز و تناسب انجامیده و می‌تواند به‌عنوان «جنایت جنگی»^۱ طبقه‌بندی شود (Amnesty International, 2024).

۵-۲. بحران در مسئولیت‌پذیری حقوقی و اخلاقی

مایکل هوروویتز (Horowitz, 2016: 26) اشاره می‌کند که ویژگی منحصربه‌فرد سلاح‌های خودمختار آن است که این سامانه تسلیحاتی، و نه یک شخص، اهداف را انتخاب و مورد حمله قرار می‌دهد. این موضوع مشکلی را در تعیین مسئولیت هنگامی که این سامانه‌ها موجب آسیب‌های

^۱. war crime

^۲. LAWS

غیرقابل توجیه اخلاقی می‌شوند، ایجاد می‌کند. هورویتز این چالش را اینگونه توصیف می‌کند: «مسئول می‌تواند برنامه‌نویس باشد، اما اگر برنامه‌نویس آن موقعیت خاص را تصور نکرده باشد چه؟ مسئول می‌تواند فرماندهی باشد که دستور فعال‌سازی سلاح را داده است، اما اگر سلاح به گونه‌ای رفتار کند که فرمانده به شکل معقولی قادر به پیش‌بینی آن نباشد چه؟» (Horowitz, 2016: 26-30). همان‌طور که هلن نیسنباوم (Nissenbaum, 1994: 76) تأکید دارد اگر بخواهیم استاندارد پاسخگویی برای شناسایی فرد مسئول استفاده کنیم، با شبکه‌ای پیچیده از علل و تصمیمات مواجه می‌شویم، بدون آنکه نقطه روشنی برای انتساب مسئولیت وجود داشته باشد. برخی پژوهشگران مانند سانتورو، مارینو و تامبورینی (Santoro et al., 2008) پیشنهاد می‌کنند از مسئولیت مطلق^۱ به عنوان راه‌حل حقوقی استفاده شود، اما این رویکرد صرفاً به مسئولیت حقوقی می‌پردازد و شکاف مسئولیت اخلاقی را حل نمی‌کند (Goetze, 2022: 5).

در نهایت، این پرسش مطرح می‌شود که آیا خود سامانه‌های خودران را می‌توان مسئول دانست؟ پاسخ این است که مگر این سامانه‌ها دارای هوش و درک اخلاقی معادل انسان باشند، انتساب مسئولیت به آنها نمایشی بی‌معناست، مانند تازیانه زدن خشایارشا به دریا (Goetze, 2022: 6, as cited in Herodotus, 1920, Book 7, Chs. 34-35).

در حالی که تلاش‌هایی در سطح بین‌المللی برای تنظیم مقررات مربوط به سلاح‌های خودمختار انجام شده است و کمیته بین‌المللی صلیب سرخ^۲ در آوریل ۲۰۲۵ توصیه‌هایی در حوزه ی هوش مصنوعی از جمله تضمین کنترل و قضاوت انسانی، الزامات طراحی سامانه؛ آزمون، ارزیابی، تأیید و اعتبارسنجی؛ بازبینی‌های حقوقی؛ محدودیت‌های عملیاتی بر استفاده، آموزش کاربران، بازبینی‌های پس از عملیات و پاسخگویی در حوزه نظامی به دبیرکل سازمان ملل ارائه می‌دهد. (International Committee of the Red Cross, 2025: 7) توصیه‌هایی به سازمان ملل داشته یا مذاکرات در چارچوب کنوانسیون سلاح‌های متعارف سازمان ملل؛ هنوز هیچ سند الزام‌آوری تصویب نشده است.

۶. پیامدهای راهبردی و ژئوپلیتیکی

به کارگیری هوش مصنوعی در جنگ غزه، صرفاً محدود به پیامدهای انسانی و حقوقی نیست، بلکه نشان‌دهنده آغاز مرحله‌ای جدید در تغییر موازنه قوا، رقابت تسلیحاتی فناورانه، و بازتعریف مشروعیت در استفاده از زور در سطح منطقه‌ای و بین‌المللی است. به‌ویژه، کاربست سامانه‌هایی

^۱. strict liability

^۲. ICRC

مانند لوندرو و گاسپل توسط ارتش رژیم اسرائیل، از منظر راهبردی، حامل پیام‌هایی فراتر از میدان نبرد غزه بوده است.

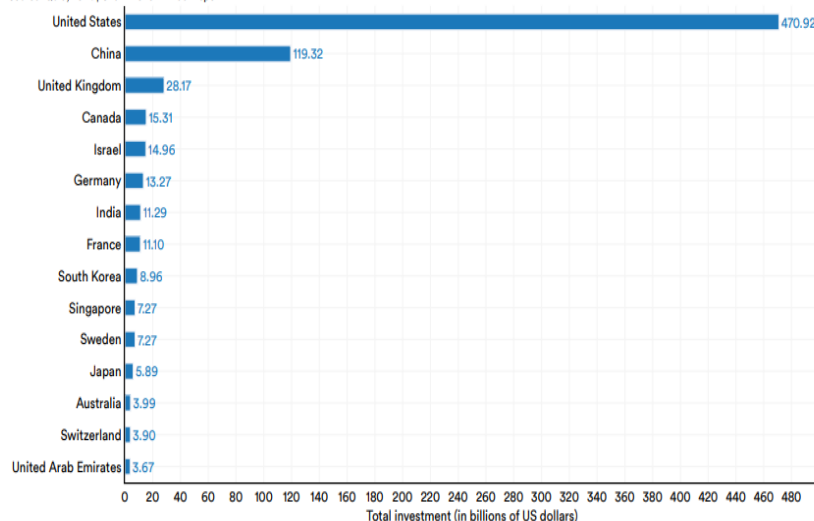
۱-۶. برتری تکنولوژیک و تغییر موازنه قوا

کشورهای کوچک با این خطر مواجه‌اند که از سوی بازیگران بزرگ‌تر کنار زده شوند، اما اگر در پذیرش هوش مصنوعی نظامی چابک‌تر عمل کنند، می‌توانند در سطح راهبردی تأثیری فراتر از اندازه خود داشته باشند (RAND Corporation, 2024: 81). کنشگران غیرسرزمینی داده‌گرا، همانند آمازون، مایکروسافت، اوپر، اینتل، وینتل، گوگل، اپل، فیسبوک، توییتر و سایر شرکت‌های بزرگی که از طریق هوش مصنوعی در حال استیلاء نوین بر نظم جهانی هستند؛ با استفاده از ژئوپولیتیک «سیلیکون ولی» نه تنها موضوعیت دولت-ملت و ستفالیایی را کمرنگ کرده‌اند بلکه موجبات تغییر نظریه هارتلند شده‌اند. به گونه‌ای که اگر پروفیسور سر هافورد جان مکیندر در این زمانه حضور داشت می‌توانست در نظریه هارتلند خود با رهیافتی تجدیدنظرطلبانه بنگرد؛ چون در حال حاضر، موقعیت هارتلندبودن یک کشور بسته به میزان تسلط آن بازیگر بر میکروفیزیک کلان-داده‌ها دارد. همچنین، می‌توان گفت هوش مصنوعی فضای کنش‌گری جهانی را پیچیده و با دگردیسی عمیق و ژرفی مواجه کرده است و در نتیجه، هم بر ویژگی‌های خود کنشگران و هم بر صورت‌بندی (شمار، گونه‌ها و جوهره تعاملات) کنشگران در عرصه امنیت جهانی تأثیر گذاشته است و از این طریق، پدیده امنیت و ماهیت تهدیدها را دستخوش دگرگونی نموده است (دهقانی فیروزآبادی و چهارآزاد، ۱۴۰۳، ص. ۳۰۸). قابلیت ارتش صهیونیستی در بهره‌برداری از سامانه‌های مبتنی بر هوش مصنوعی، آن را در میان بازیگران منطقه‌ای، در جایگاه برتر قرار داده است. این برتری فناورانه می‌تواند «هژمونی اطلاعاتی» رژیم اسرائیل را تثبیت کند.

تصویر ۳: نمودار سرمایه‌گذاری خصوصی جهانی در هوش مصنوعی بر اساس منطقه جغرافیایی
(۲۰۲۴-۲۰۱۳)

Global private investment in AI by geographic area, 2013-24 (sum)

Source: Guid, 2024 | Chart: 2025 AI Index report



منبع: (AI Index Report 2025, 2025: 253-254)

بر اساس این نمودار، ایالات متحده با سرمایه‌گذاری ۴۷۰.۹۲ میلیارد دلاری در حوزه هوش مصنوعی، در جایگاه نخست قرار دارد. این رقم، تسلط قاطع آمریکا را در جذب سرمایه‌گذاری خصوصی در این حوزه نشان می‌دهد؛ جایگاهی که تا حد زیادی به دلیل حضور شرکت‌های بزرگ فناوری مانند گوگل^۱، مایکروسافت^۲ و آپن.ای.آی^۳ و همچنین اکوسیستم پویای استارت‌آپی این کشور حاصل شده است.

چین با ۱۱۹.۳۲ میلیارد دلار در رتبه دوم قرار دارد. با وجود فاصله زیاد با ایالات متحده، این رقم بازتابی از راهبرد صنعتی گسترده پکن برای تبدیل شدن به یک قدرت هوش مصنوعی است. در ادامه، بریتانیا (۲۸.۱۷ میلیارد دلار) و کانادا (۱۵.۳۱ میلیارد دلار) در جایگاه‌های سوم و چهارم قرار دارند که نشان‌دهنده تأثیر سیاست‌های حمایتی، دانشگاه‌های پیشرو و زیرساخت‌های تحقیقاتی آنهاست. (AI Index Report 2025, 2025: 253-254) اما آنچه توجه را جلب می‌کند، جایگاه رژیم

^۱. Google

^۲. Microsoft

^۳. OpenAI

اسرائیل در میان این قدرت‌های بزرگ است و با وجود جمعیت و وسعت جغرافیایی محدود، با سرمایه‌گذاری خصوصی ۱۴.۹۶ میلیارد دلاری در رتبه پنجم جهانی قرار دارد. این میزان سرمایه‌گذاری، که حتی از آلمان (۱۳.۲۷ میلیارد دلار) نیز فراتر رفته، بیانگر اولویت این رژیم برای توسعه هوش مصنوعی به‌ویژه در حوزه‌های امنیتی و دفاعی است.

رژیم اسرائیل با وجود وسعت جغرافیایی و جمعیت محدود، جایگاهی راهبردی و اثرگذار در معادلات نظامی و اطلاعاتی خاورمیانه به دست آورده است. این موقعیت منحصربه‌فرد تا حد زیادی ناشی از تلفیق توانمندی‌های فناوریانه پیشرفته با اهداف امنیتی رژیم است. سرمایه‌گذاری چشمگیر ۱۴.۹۶ میلیارد دلاری در حوزه هوش مصنوعی، که اسرائیل را در رتبه پنجم جهان قرار داده، بیانگر نگاهی راهبردی به این فناوری است؛ نگاهی که هوش مصنوعی را نه صرفاً یک ابزار اقتصادی، بلکه عاملی کلیدی در تضمین برتری اطلاعاتی، تقویت قدرت بازدارندگی و حفظ امنیت ملی قلمداد می‌کند.

۲-۶. تسریع در رقابت تسلیحاتی منطقه‌ای

استفاده افراطی رژیم اسرائیل از هوش مصنوعی (AI) در جنگ غزه، احتمالاً موجی از رقابت فناوریانه میان بازیگران منطقه‌ای ایجاد خواهد کرد و اکنون که تمرکز به‌سوی «نظامی‌سازی هوش مصنوعی» و «جنگ الگوریتمی» در حال تغییر است این روند می‌تواند خطر اشاعه فناوری‌های غیرمسئولانه، استفاده از سامانه‌های نیمه‌خودران بدون چارچوب اخلاقی مشخص، و کاهش آستانه استفاده از زور را افزایش دهد.

تصویر ۴: شاخص جهانی هوش مصنوعی و ظرفیت نسبی کشورها در توسعه و به‌کارگیری فناوری‌های

هوش مصنوعی									
Country	Overall	Talent	Infrastructure	Operating environment	Research	Development	Government strategy	Commercial	Intensity
 United States	1	1	1	28	1	1	8	1	5
 China	2	20	2	3	2	2	3	2	21
 Singapore	3	4	3	22	3	5	16	4	1
 United Kingdom	4	5	24	40	5	8	10	5	10
 Canada	5	6	23	8	7	11	5	7	7
 South Korea	6	12	7	11	12	3	6	18	6
 Israel	7	7	28	23	11	7	47	3	2
 Germany	8	3	12	13	8	9	2	11	15
 Switzerland	9	9	13	30	4	4	56	9	3
 Finland	10	13	8	4	9	14	15	12	4
 Netherlands	11	8	16	15	10	13	28	20	8
 Japan	12	11	5	10	20	6	18	23	25
 France	13	10	11	25	15	18	13	10	20
 India	14	2	59	12	30	21	38	13	51
 Australia	15	14	44	62	6	16	14	22	14

- توضیح: منظور از «شدت»^۱، ظرفیت هوش مصنوعی یک کشور نسبت به اندازه آن کشور از نظر جمعیت یا تولید ناخالص داخلی^۲ است.

منبع: (Black et al., 2024: 59–60)

نمودار بالا نشانگر آنست که هوش مصنوعی نظامی همچنین چالش‌ها و فرصت‌های منحصربه‌فردی را برای دولت‌های کوچک ایجاد می‌کند. اگرچه این کشورها از نظر منابع به پای قدرت‌های بزرگ نمی‌رسند، اما ماهیت نرم‌افزاری هوش مصنوعی و نقش آن به عنوان یک «ضریب

^۱. Intensity

^۲. GDP

قدرت‌افزا^۱ این امکان را فراهم می‌کند که توانمندی نظامی یا نفوذ جهانی یک کشور، بیش از اندازه جمعیت یا اقتصاد آن باشد.

همان‌طور که در نمودار بالا نشان داده شده، بسیاری از کشورهایی که در «شاخص جهانی هوش مصنوعی» رتبه بالایی دارند، کشورهایی کوچک هستند که با بهره‌گیری از نوآوری، توسعه ظرفیت‌های خاص در زنجیره ارزش هوش مصنوعی، ایجاد پیوندهای نزدیک میان دولت، صنعت و دانشگاه مانند مدل «مارپیچ سه‌گانه»^۲ و استفاده از چابکی نسبی خود، تأثیری فراتر از وزن واقعی‌شان در عرصه جهانی بر جای گذاشته‌اند؛ سنگاپور، رژیم اسرائیل، سوئیس، فنلاند یا هلند از جمله این نمونه‌ها هستند (Black et al., 2024: 59–60).

کشورهای کوچک می‌توانند با توسعه توانمندی‌های نامتقارن در برخی حوزه‌های خاص از هوش مصنوعی نظامی، به مزایای قابل توجهی در زمینه قدرت نظامی، صنعتی و نرم‌افزار دست یابند و در عین حال، در شکل‌دهی به ترتیبات حکمرانی جهانی نیز نقش‌آفرینی کنند (برای مثال، با تأثیرگذاری بر ائتلاف‌هایی که عضو آن هستند یا ایفای نقش میانجی بین قدرت‌های رقیب بزرگ‌تر). فناوری‌های نوین به کشورها امکان می‌دهد با هزینه کمتر و اثرگذاری بیشتر، قدرت بازدارندگی خود را افزایش دهند. این تحول، رقابت تسلیحاتی جدیدی را در حوزه‌هایی مانند هوش مصنوعی، پهپادها، و جنگ سایبری برانگیخته است (Johnson, 2019: 854). قدرت‌های بزرگ به دنبال پیشی گرفتن از رقبا در این زمینه‌ها هستند که به تغییر در توازن قوا و ساختار نظام بین‌المللی منجر می‌شود (Wirtz & Sloan, 2020: 6).

استفاده گسترده از فناوری‌های نوین، مسائل اخلاقی و حقوقی پیچیده‌ای ایجاد کرده است، از جمله آسیب‌های جانبی به غیرنظامیان، مسئولیت‌پذیری در تصمیمات خودکار، و چالش‌های رعایت حقوق بین‌الملل بشردوستانه (Casey-Maslen, 2018: 214). برای مثال، استفاده از بمب‌های هدایت‌ناپذیر برای هدف قرار دادن افراد کم‌اهمیت (Davies & McKernan, 2024). این پرسش را ایجاد می‌کند که آیا فناوری منجر به کاهش مسئولیت اخلاقی شده است یا خیر.

۳-۶. خلأ حقوقی و چشم‌انداز تدوین پروتکل‌های بین‌المللی

در حال حاضر، هیچ معاهده الزام‌آوری در سطح بین‌المللی برای تنظیم کاربست نظامی هوش مصنوعی وجود ندارد. گرچه تلاش‌هایی در سطح سازمان ملل، به‌ویژه در چارچوب گروه کارشناسان

¹. Force Multiplier

². Triple Helix

دولت‌ها^۱ ذیل کنوانسیون کنوانسیون ممنوعیت یا محدودیت استفاده از برخی سلاح‌های متعارف^۲ برای تنظیم سامانه‌های کشنده خودمختار در حال انجام است، اما تاکنون به اجماع مؤثری منجر نشده‌اند. (UN GGE, 2021: 5, paras. 16–18) در چنین فضایی، خطر نهادینه‌شدن استانداردهای متفاوت، و تقویت «استثناگرایی امنیتی» توسط قدرت‌های فناوری، بسیار جدی است.

۴-۶. مشروعیت بخشی به خشونت‌های یک‌جانبه تحت لوای داده‌محور بودن

یکی از مهم‌ترین نگرانی‌های راهبردی در سطح جهانی، مشروعیت بخشی به حملات مرگبار بر اساس داده‌های غیرشفاف یا تحلیل‌های آماری سامانه‌های هوشمند است. در جریان جنگ غزه، توجیه حمله به منازل مسکونی یا خودروهای غیرنظامی بر اساس احتمال عضویت در حماس، صرفاً با اتکا به داده‌های رفتاری دیجیتال، نمونه‌ای از این روند خطرناک است. سیستم‌های سلاح خودمختار می‌توانند تحت عنوان فناوری‌های "داده‌محور" و "پیشرفته" برای توجیه خشونت‌های یک‌جانبه مورد استفاده قرار گیرند، در حالی که چالش‌های حقوقی و اخلاقی متعددی را ایجاد می‌کنند. عدم قطعیت در عملکرد، مسئولیت ناپذیری، و نبود قوانین جامع بین‌المللی از جمله عواملی هستند که ممکن است به سوءاستفاده از این سیستم‌ها منجر شوند. همان‌طور که برخی تحلیلگران یادآور شده‌اند، قیاس سیستم‌های خودمختار با سلاح‌های متعارف یا جنگ‌جویان انسانی می‌تواند گمراه‌کننده باشد و به توجیه استفاده غیرقانونی از آنها منجر شود. این قیاس‌ها ممکن است برای مشروعیت بخشی به اقدامات یک‌جانبه مورد سوءاستفاده قرار گیرند نبود قوانین بین‌المللی مشخص برای تنظیم سیستم‌های سلاح خودمختار می‌تواند به دولتها اجازه دهد تا از این فناوری برای اهداف یک‌جانبه و بدون پاسخگویی استفاده کنند. تکنولوژی می‌تواند به سلاح مشروع ساز خشونت تبدیل شود؛ بدون آنکه پاسخگویی شفاف وجود داشته باشد. (Crootoof, 2021: 300–339)

نتیجه‌گیری

یافته‌های این پژوهش نشان می‌دهد که بهره‌گیری از هوش مصنوعی در منازعات مسلحانه، هرچند ظرفیت‌هایی چون افزایش سرعت تصمیم‌گیری نظامی، هدف‌گیری دقیق‌تر و کاهش تلفات در میدان نبرد را به همراه دارد، اما در عمل با چالش‌هایی جدی در حوزه‌های اخلاقی، حقوق بشری، و سیاسی مواجه است. مطالعه موردی جنگ غزه به روشنی نشان داد که استفاده ارتش رژیم اسرائیل

۱. GGE

۲. CCW

از سامانه‌هایی مانند لوندِر و گاسپِل، گرچه از منظر راهبردی موجب افزایش کارآمدی عملیات‌های نظامی شد، اما در مواردی نیز منجر به هدف‌گیری اشتباه، افزایش آسیب به غیرنظامیان، و نقض اصول بنیادین حقوق بین‌الملل بشردوستانه گردید.

از سوی دیگر، این فناوری‌ها در غیاب چارچوب‌های حقوقی الزام‌آور، می‌توانند به ابزار مشروعیت‌بخش خشونت‌های یک‌جانبه بدل شوند؛ خشونت‌هایی که تصمیم‌گیری درباره آن‌ها از مرزهای انسانی به حوزه تحلیل الگوریتمی منتقل شده و نظارت و پاسخ‌گویی را تضعیف می‌کنند. این واقعیت که تصمیم‌گیری درباره مرگ و زندگی در برخی موارد از حیطه اراده انسانی به الگوریتم‌های پیچیده و فاقد شفافیت منتقل شده، موجب تضعیف سازوکارهای نظارت و پاسخ‌گویی و نیز کاهش مشروعیت اخلاقی اقدامات نظامی می‌گردد. آنچه در این میان ضروری به نظر می‌رسد، پاسخ جمعی و هماهنگ جامعه بین‌المللی به این تحولات است.

در این میان، مسئولیت جامعه جهانی در هدایت توسعه و کاربست این فناوری‌ها بسیار خطیر و سرنوشت‌ساز است. بر این اساس، به‌منظور مواجهه با چالش‌های پیش‌رو باید دانست که استفاده نظامی از هوش مصنوعی نیازمند شفاف‌سازی و نظارت بین‌المللی است تا از سوءاستفاده‌های احتمالی جلوگیری شود. توصیه می‌شود و لازم است سازوکارهایی برای شفاف‌سازی اطلاعات درباره نحوه توسعه، آموزش و به‌کارگیری سامانه‌های هوشمند نظامی توسط کشورها ایجاد شود. این امر می‌تواند تحت نظارت نهادهایی چون سازمان ملل متحد یا نهادهای تخصصی مانند دفتر امور خلع سلاح سازمان ملل^۱ انجام گیرد. در این میان، شورای امنیت، به‌عنوان اصلی‌ترین نهاد مسئول حفظ صلح و امنیت بین‌المللی، باید نسبت به استفاده بی‌ضابطه از هوش مصنوعی در عملیات نظامی واکنش نشان دهد. همچنین، دیوان بین‌المللی کیفری^۲ باید در صورت اثبات هدف‌گیری نادرست غیرنظامیان توسط سامانه‌های هوشمند، صلاحیت بررسی کیفری فرماندهان یا توسعه‌دهندگان این سامانه‌ها را مورد ارزیابی حقوقی قرار دهد.

در این راستا، دکترین مشارکت در جنایات مشترک^۳ یک سازوکار قابل‌قبول برای پاسخ‌گویی به توسعه‌دهندگان نرم‌افزار به دلیل عملیات سلاح‌های خودمختار ارائه می‌دهد. این نظریه تثبیت‌شده، رویکردی متعادل و دقیق به یک مشکل دشوار ارائه می‌کند و توسعه‌دهندگانی را که از خطر جنایات فرعی حقوق بین‌الملل آگاه بودند و با این حال به مشارکت در این هدف مشترک ادامه دادند، شامل

۱. UNODA

۲. ICC

۳. JCE III

می‌شود. در مقابل، توسعه‌دهندگانی که نمی‌توانستند یا از خطر وقوع نقض آگاه نبودند، یا مشارکت آن‌ها آن قدر جزئی بود که مشمول معیار بسیار جزئی یا ناچیز^۱ می‌شود، از این دایره خارج خواهند شد. بنابراین، پذیرش دکترین مشارکت در جنایات مشترک اطمینان حاصل می‌کند که عدالت، حتی در صورت جایگزینی انسان‌ها با ماشین‌ها در میدان جنگ، از دست نمی‌رود. (Winter, 2021: 37)

با توجه به آنچه گذشت، کاربست هوش مصنوعی در جنگ‌ها باید در چارچوب قواعد بین‌المللی محدود و قانون‌مند شود و نباید اجازه داد که قدرت فناورانه جایگزین اصول انسانی گردد. در این راستا، کنوانسیون‌های جدید یا پروتکل‌های الحاقی به کنوانسیون‌های ژنو می‌توانند نقش مؤثری در تنظیم ابعاد حقوقی و اخلاقی این فناوری‌ها ایفا کنند. ایجاد یک اجماع جهانی برای تدوین چارچوب حقوقی الزام‌آور ضروری است تا بتوان از پیامدهای ناگوار استفاده غیرمسئولانه از هوش مصنوعی در میدان‌های نبرد جلوگیری کرد.

در نهایت، تحقق این اهداف مستلزم اراده سیاسی جمعی، هم‌افزایی نهادهای بین‌المللی، و توجه به صدای جوامعی است که بیشتر در معرض آسیب‌های این فناوری‌های پرخطر قرار دارند. فقدان نظارت مؤثر و چارچوب‌های الزام‌آور، می‌تواند جهان را به سمت نوعی «جنگ خودکار بدون پاسخگو» سوق دهد که پیامدهای آن نه تنها برای مناطق درگیر، بلکه برای کل نظم بین‌الملل مخاطره‌آمیز خواهد بود.

منابع و مآخذ

فارسی:

دهقانی فیروزآبادی، س. ج. و چهرآزاد، س (۱۴۰۳). ژئوپلیتیک هوش مصنوعی؛ رهنشان نظری رقابت‌های الگوریتمی بازیگران نظام جهانی. فصلنامه ژئوپلیتیک، سال بیستم (شماره سوم، پاییز)، ۲۷۰-۳۱۳.

انگلیسی:

1. Abraham, Y. (2024, January 4). Lavender: The AI machine directing Israel's bombing spree in Gaza. +972 Magazine. <https://www.972mag.com/lavender-ai-israel-gaza/>
2. Amnesty International. (2024). Israel/OPT: AI targeting of Palestinian civilians may amount to war crimes. <https://www.amnesty.org/en/latest/news/2024/04/israel-opt-ai-targeting-of-palestinian-civilians-may-amount-to-war-crimes/>

¹. De Minimis

3. Andersin, E. (2025). The use of the 'Lavender' in Gaza and the law of targeting: AI-decision support systems and facial recognition technology. *Journal of International Humanitarian Legal Studies*, 1–35. <https://doi.org/10.1163/18781527-15020002>
4. Bergman, R., & Mazzetti, M. (2023, December 1). Israel's AI-based 'Gospel' system guides airstrikes in Gaza. *Haaretz*. <https://www.haaretz.com/israel-news/2023-12-01/ty-article/.premium/israels-ai-based-gospel-system-guides-airstrikes-in-gaza/0000018c-2d9a-d3f4-a3cf-7dbfe3f30000>
5. Black, J., Eken, M., Parakilas, J., Dee, S., Ellis, C., Suman-Chauhan, K., ... & Palicka, O. (2024). Strategic competition in the age of AI: Emerging risks and opportunities from military use of artificial intelligence (RAND Research Report RRA3295-1). *RAND Corporation*. <https://www.rand.org/t/RRA3295-1>
6. Brumfiel, G. (2024, April 26). Israel says AI helps it choose bombing targets in Gaza. But is it accurate? NPR. <https://www.npr.org/transcripts/1218643254>
7. Casey-Maslen, S. (2018). *The Treaty on the Prohibition of Nuclear Weapons: A Commentary*. Oxford University Press.
8. Charte, F., Rivera, A. J., del Jesus, M. J., & Herrera, F. (2015). Addressing imbalance in multilabel classification: Measures and random resampling algorithms. *Neurocomputing*, 163, 3–16. <https://doi.org/10.1016/j.neucom.2014.08.091>
9. Crotoft, R. (2018). Autonomous weapon systems and the limits of analogy. *Harvard National Security Journal*, 9, 51–83. https://harvardnsj.org/wp-content/uploads/2018/06/2_Crotoft_LimitsOfAnalogy_06.08.18.pdf
10. Crotoft, R. (2021). A genealogy of autonomous weapons. *The University of Pennsylvania Law Review*, 169(1), 1–54.
11. Davies, H., & McKernan, B. (2024). “The machine did it coldly”: Israel used AI to identify 37,000 Hamas targets. *The Guardian*. <https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes>
12. Goetze, T. S. (2022). *Mind the gap: Autonomous systems, the responsibility gap, and moral entanglement*. Harvard University Department of Philosophy.
13. Herodotus. (1920). *The Histories* (A. D. Godley, Trans.). Harvard University Press. (Original work published 5th century BCE)
14. Henckaerts, J.-M., & Doswald-Beck, L. (2005). *Customary international humanitarian law: Volume I – Rules*. Cambridge University Press. (Published by the International Committee of the Red Cross)
15. Horowitz, M. C. (2016). The ethics & morality of robotic warfare: Assessing the debate over autonomous weapons. *Daedalus*, 145(4), 25–36.
16. Human Rights Watch. (2024, September 10). Gaza: Israeli military's digital tools risk civilian harm. <https://www.hrw.org/news/2024/09/10/gaza-israeli-militarys-digital-tools-risk-civilian-harm>
17. International Committee of the Red Cross (ICRC). (1977). *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977. <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977>
18. International Committee of the Red Cross (ICRC). (2016, April 11). Views of the ICRC on autonomous weapon systems. <https://www.icrc.org/en/document/views-icrc-autonomous-weapon-systems>

19. International Committee of the Red Cross (ICRC). (2023). *Autonomous weapon systems: Implications for international humanitarian law*. Geneva: ICRC Publications.
20. International Committee of the Red Cross (ICRC). (2025, April 11). Artificial intelligence in the military domain: ICRC submits recommendations to UN Secretary-General. <https://www.icrc.org/en/article/artificial-intelligence-military-domain-icrc-submits-recommendations-un-secretary-general>
21. International Institute for Strategic Studies (IISS). (2022). *The Military Balance 2022*. London: Routledge.
22. Israel Defense Forces. (2023). *Operational use of AI targeting systems in urban warfare* (Internal Report leaked to +972 Magazine).
23. Johnson, J. (2019). Artificial intelligence and the future of warfare: The USA, China, and strategic stability. *Journal of Strategic Studies*, 42(6), 841–863.
24. McKernan, B. (2024, April 3). Israel used AI to identify 37,000 Hamas targets, report claims. *The Guardian*. <https://www.theguardian.com/world/2024/apr/03/israel-used-ai-to-identify-37000-hamas-targets-report>
25. Nissenbaum, H. (1994). Computing and accountability. *Communications of the ACM*, 37(1), 72–80.
26. RAND Corporation. (2021). The Department of Defense posture for artificial intelligence: Assessment and recommendations (Research Report No. RR-3139-1). https://www.rand.org/pubs/research_reports/RR3139-1.html
27. RAND Corporation. (2024). Artificial intelligence and the future of warfare in Israel and beyond (Research Report No. RRA3295-1). https://www.rand.org/pubs/research_reports/RRA3295-1.html
28. Rid, T. (2020). Active measures: *The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
29. Singer, P. W. (2009). *Wired for war: The robotics revolution and conflict in the 21st century*. New York: Penguin Press.
30. Stanford Institute for Human-Centered Artificial Intelligence. (2025). *Artificial Intelligence Index Report 2025* (pp. 253–254). Stanford University. <https://aiindex.stanford.edu/report/>
31. The Guardian. (2024, April 3). Revealed: Israel's AI targeting systems in Gaza war – 'Lavender' and 'Gospel'. <https://www.theguardian.com/world/2024/apr/03/israel-ai-targeting-gaza-lavender-gospel>
32. United Nations Group of Governmental Experts (UN GGE). (2021). Report on emerging technologies in the area of lethal autonomous weapons systems. Geneva: *UN Office for Disarmament Affairs*.
33. Winter, E. (2021). The accountability of software developers for war crimes involving autonomous weapons: The role of the joint criminal enterprise doctrine. *University of Pittsburgh Law Review*, 83(1). <https://doi.org/10.5195/lawreview.2021.822>
34. Wirtz, J. J., & Sloan, E. (2020). *Innovation and the modern military: Winning the next war*. Stanford University Press.

