شاپا چاپی: ۱۸۴۱-۲۷۸۳
شاپای الکترونیکی: ۱۹۲۲-۲۷۸۳

تمدن حقوقی

دوره ۷ - شماره ۲۰ - تابستان ۱۴۰۳

Legal Civilization
Vol.7, No.20, Summer 2024
Pages: 251-276
Article Type: Translation
https: //www.pzhfars.ir/article_199390.html
doi: 10.22034/LC.2024.464816.1508

تمدن حقوقی
دوره ۷، شماره ۲۰، تابستان ۱۴۰۳
صفحات: ۲۷۶-۲۵۱
نوع مقاله: ترجمه‌ای

Weapons of War Tools of Justice: Using Artificial Intelligence to Investigate International Crimes

Lindsay Freeman
University of California Law School, Berkeley, USA

Navid Zamaneh Ghadim
PhD in International Law, Lecturer, Rushdieh Institute of Higher Education, Tabriz, Iran (Corresponding Translator)

Aram Abbaspour Jalali
Senior expert in private law, lecturer at Rushdieh Institute of Higher Education, Tabriz, Iran

Abstract

Just as the internal combustion engine revolutionized warfare in the early twentieth century, artificial intelligence is shaping warfare in the Digital Age. Fuelled by data rather than gasoline, artificial intelligence (AI) derivative technologies are driven by innovation in both the military and civilian sectors. Today's defence scientists and engineers, like their predecessors, develop physical equipment and weapons, but instead of simply making them more powerful and lethal, they are also making them more intelligent and connected. As AI is increasingly integrated into military tools, the digital footprints of modern battlefields will grow exponentially, generating new sources and types of data that will fundamentally alter war crimes investigations. This article examines emerging military applications of AI in order to identify what opportunities and challenges these tools might offer international criminal investigators. Will more sensors and smart devices on the battlefield benefit or burden the investigation of war crimes? Moreover, will intelligent machines add to the fog of war or help us see through it?

Keywords: Artificial Intelligence, Criminal Justice, International Crime Investigation, Weapons of War, Internet of Things.

Received: 2024/04/22 -Review: 2024/07/04 -Accepted: 2024/08/14

سلاح‌های جنگ، ابزار عدالت: استفاده از هوش مصنوعی در مرحله تحقیقات جرایم بین‌المللی

لیندسی فریمن
دانشکده حقوق دانشگاه کالیفرنیا، برکلی، ایالات متحده امریکا
lfreeman@berkeley.edu

نوید زمانه قدیم
دکتری حقوق بین‌الملل، مدرس مؤسسه آموزش عالی رشدیه، تبریز، ایران (مترجم مسئول)
navid.zamani90@gmail.com
http://orcid.org/0000-0001-5069-1573

آرام عباسپور جلالی
کارشناس ارشد حقوق خصوصی، مدرس مؤسسه آموزش عالی رشدیه، تبریز، ایران
aram.abbaspour@gmail.com

چکیده

همان‌طور که موتور احتراق داخلی، جنگ را در اوایل قرن بیستم متحول کرد؛ هوش مصنوعی نیز جنگ را در عصر دیجیتال شکل می‌دهد. فناوری‌های مشتق شده از هوش مصنوعی که به جای بنزین از داده‌ها تغذیه می‌کنند، با نوآوری در بخش‌های نظامی و غیرنظامی هدایت می‌شوند. دانشمندان و مهندسان دفاعی امروزی، مانند پیشینیان خود، تجهیزات فیزیکی و تسلیحات را توسعه می‌دهند، اما به جای این که صرفاً آن‌ها را قوی‌تر و کشنده‌تر کنند، آن‌ها را باهوش‌تر و دقیق‌تر می‌کنند. همان‌طور که هوش مصنوعی به طور فزاینده‌ای در ابزارهای نظامی ادغام می‌شود، ردپای دیجیتالی میدان‌های نبرد مدرن به طور تصاعدی رشد می‌کند و منابع و انواع داده‌های جدیدی تولید می‌کند که اساساً مرحله تحقیقات جنایات جنگی را تغییر می‌دهد. این پژوهش کاربردهای نظامی نوظهور هوش مصنوعی را بررسی می‌کند تا مشخص کند این ابزارها چه فرصت‌ها و چالش‌هایی را می‌توانند به بازرسان جنایی بین‌المللی ارائه دهند. آیا حسگرها و دستگاه‌های هوشمند در میدان نبرد به جهت بار اثباتی به نفع رسیدگی به جنایات جنگی هستند؟ علاوه بر این، آیا ماشین‌های هوشمند به آتش جنگ می‌افزایند یا به ما کمک می‌کنند تا از آن عبور کنیم؟

واژگان کلیدی: هوش مصنوعی، عدالت کیفری، تحقیقات جرایم بین‌المللی، سلاح‌های جنگی، اینترنت اشیاء.

دریافت مقاله: ۱۴۰۳/۰۲/۰۳ – بازنگری مقاله: ۱۴۰۳/۰۴/۱۴ – پذیرش مقاله: ۱۴۰۳/۰۵/۲۴

مقاله حاضر در نشریه Journal of International Criminal Justice در سال ۲۰۲۱ میلادی منتشر شده است.

ارجاع:
فریمن، لیندسی؛ (۱۴۰۳)، سلاح‌های جنگ، ابزار عدالت: استفاده از هوش مصنوعی در مرحله تحقیقات جرایم بین‌المللی، ترجمه نوید زمانه قدیم و آرام عباسپور جلالی، تمدن حقوقی، شماره ۲۰.

پیشگفتار مترجم‌ها

توسعه سیستم‌های تسلیحاتی بر مبنای فناوری دیجیتال و به طور کلی‌تر، نقش هوش مصنوعی در جنگ، ممکن است چالش‌های بی‌سابقه‌ای را برای حقوق بین‌الملل کیفری ایجاد کند، از جمله با دشوار کردن ارتباط آسیب به افرادی که می‌توانند مسئول شناخته شوند. در این زمینه، مفهوم کنترل معنادار انسانی برای پرداختن به برخی از چالش‌های تضمین مسئولیت کیفری در قبال نقض جدی قوانین بین‌المللی بشردوستانه پیشنهاد شده است. یک امکان ممکن است پیوند (از نظر مفهومی یا حتی قانونی) کنترل معنادار انسانی با «نظریه کنترل» ارائه شده در دادگاه کیفری بین‌المللی برای تعیین مسئولیت کیفری باشد. بر اساس این نظریه، انتساب مسئولیت کیفری به یک فرد به‌عنوان مرتکب مستقیم مستلزم ارزیابی این است که آیا آن‌ها از توانایی مؤثر برای تصمیم‌گیری در مورد ارتکاب جرم برخوردار هستند یا خیر؟. این پژوهش برخی از مسائل ناشی از این رویکرد را توضیح می‌دهد؛ بدین توضیح که با روشن کردن تأثیر هوش مصنوعی در توسعه ابزار جنگی، به روی دیگر سکه یعنی استفاده از هوش مصنوعی توسط بازرسان و دادرسان در مرحله تحقیقات جرایم بین‌المللی می‌پردازد.

شایان ذکر است نویسنده این پژوهش «لیندسی فریمن»، مدیر حقوق و سیاست برنامه فناوری و حقوق بشر در مرکز حقوق بشر، دانشکده حقوق دانشگاه کالیفرنیا برکلی ایالات متحده امریکا است. او عضو

شورای سیاست بین‌الملل اقیانوس آرام، گروه مشاوره استانداردهای عدالت کیفری بین‌المللی[1] و هیئت مشاوره فناوری دفتر دادستان دادگاه کیفری بین‌المللی است.

مقدمه

جنگ بعدی ممکن است هرگز رخ ندهد. می‌توان تصور کرد که موافقت مقدماتی در مورد داوری و امنیت، که اکنون از طریق جامعه ملل در حال مذاکره است، ممکن است وسیله‌ای برای فرار از فاجعه نهایی درگیری فیزیکی باشد. اما اگر درگیری بین‌المللی دوباره تجدید شود، خشونت جنگ جهانی اخیر {اول} ممکن است برخلاف نیروهای عظیمی که انسان‌ها برای تحمیل اراده‌شان بر «دشمن» استفاده خواهند کرد، ناچیز به نظر برسد.

نیویورک تایمز این پیام پیشگویانه امید را با احتیاط در مورد «ابزارهای جدید جنگ» در سال ۱۹۲۴ میلادی منتشر کرد. این پژوهش توسط روزنامه نگار «ویلیام ال. چنری» نوشته شده است، این پژوهش پیشرفت‌های قابل توجهی را در تحقیقات نظامی نشان می‌دهد و فناوری‌های خاص آن دوران را برجسته می‌کند. از جمله تانک‌ها، هواپیماها، موشک‌های ضدهوایی، مسلسل‌های کالیبر پنجاه، بمب‌های تخریب و گازهای سمی تسلیحاتی. با هر فناوری نوظهور، چنری توسعه و کاربردهای بالقوه آن را در یک جنگ آینده، در صورت بروز درگیری مسلحانه جهانی دیگر، توضیح داد. جنگ جهانی دوم پانزده سال پس از نوشتن این کلمات آغاز شد و هشدار چنری را بسیار واقعی کرد. در سال ۱۹۲۴ میلادی، ابزارهای جنگ برای حرکت و قدرت هرچه بیشتر نیرو ساخته و اصلاح شد. به نقل از فرمانده ویلیامز، چنری توضیح داد که تقاضای آینده مستلزم ساخت تسلیحات متحرک‌تر، قدرتمندتر و مرگبارتر است.

چنری در تحقیق خود برای پژوهش، پارادوکس جالبی را در خطوط دوگانه پژوهش مشاهده کرد که در آن زمان توسط مخترعان مهمات دنبال می‌شد. دانشمندانی که برای ساختن مرگبارترین سلاح‌ها تلاش می‌کردند، ابزارهای محافظت در برابر آن‌ها را نیز بهبود می‌دادند. متخصصان توپخانه گلوله‌هایی را برای نفوذ به زره‌های موجود به موازات ساخت زره‌های قوی برای جلوگیری از نفوذ ساختند. مهندسان سلاح‌های ضدهوایی را برای سرنگون کردن هواپیماها می‌ساختند، درحالی‌که درعین‌حال سلاح‌های هواپیماهای قدرتمندی می‌ساختند تا آن هواپیماها را حتی کشنده‌تر کند. شیمیدان‌ها سموم و پادزهرهای آن‌ها را کِشت کردند.

1. ABA

چنری به‌ویژه به نوآوری تانک اشاره کرد، ابزاری که می‌تواند هم برای نابود کردن و هم برای دفاع از آن استفاده شود. این ابزاری شبیه شمشیر و سپر بود.[۲] درحالی‌که ابزارهای جنگ گزارش شده توسط چنری به نظر نمی‌رسد که با تحقیقات جنایات جنگی مدرن مرتبط باشد، پیش‌بینی دقیق چنری از جنگ آینده بر اساس بررسی پروژه‌های تحقیق و توسعه دفاعی معاصر، چهارچوب قانع‌کننده‌ای را برای بازرسان جنایی بین‌المللی برای پیش‌بینی و آمادگی برای بازرسان جنایی ارائه می‌دهد. چالش‌های پیش رو امروزه، نزدیک به یک قرن پس از نوشتن چنری، پروژه‌های تحقیق و توسعه دفاعی تمرکز خود را از دنیای جنبشی به دنیای دیجیتال تغییر داده‌اند.

دانشمندان و مهندسان نظامی امروزی به جای این که ابزارهای جنگی را قدرتمندتر و مرگبارتر کنند، آن‌ها را باهوش‌تر و دقیقتر می‌کنند. همان پارادوکس مشاهده شده توسط چنری امروز نیز ادامه دارد. رمزنگارانی که نسل بعدی رمزگذاری درجه نظامی را توسعه می‌دهند، همچنین در حال توسعه نرم افزارهای پیچیده برای شکستن رمزگذاری پیشرفته هستند. محققان اینترنتی به دنبال راه‌های جدیدی برای بی‌نام کردن داده‌ها هستند، درحالی‌که سعی می‌کنند ناشناس بودن خود را هنگام جست‌وجوی داده‌های آنلاین حفظ کنند. مهندسانی که بر روی ابزارهای احراز هویت تصویر دیجیتال برای شناسایی دستکاری دیجیتال کار می‌کنند، درعین‌حال، الگوریتم‌های مورد استفاده برای ایجاد تصاویر و ویدیوهای جعلی را بهبود می‌بخشند.

محققان نظامی به طور فزاینده‌ای از شبکه‌های متخاصم مولد[۳] استفاده می‌کنند، که شبکه‌های عصبی عمیقی هستند که «قادرند از مجموعه‌ای از داده‌های آموزشی یاد بگیرند و داده‌های جدیدی با ویژگی‌های مشابه داده‌های آموزشی تولید کنند». این فرایند، پارادوکس چنری را به زیبایی نشان می‌دهد، مانند زمانی که دو شبکه عصبی در مقابل یکدیگر قرار می‌گیرند تا به طور هم‌زمان الگوریتمی را ایجاد کنند که می‌تواند تصاویر مصنوعی را تشخیص دهد و الگوریتمی که می‌تواند تصاویر مصنوعی تولید کند که از تشخیص فرار می‌کنند. مانند تانک، هوش مصنوعی می‌تواند هم به‌عنوان شمشیر و هم به‌عنوان سپر عمل کند. کارشناسان پیش‌بینی می‌کنند که «درگیری در آینده در فضای نبردی رخ خواهد داد که توسط

---

۲. فرهنگ لغت آکسفورد «تانک» را به‌عنوان «خودروی جنگی زرهی سنگینی که اسلحه حمل می‌کند و روی یک مسیر فلزی مفصلی پیوسته حرکت می‌کند» تعریف می‌کند. بنابراین، تانک مسلح و زره پوش است.

3. GAN

هوش مصنوعی و سایر فناوری‌های جدید شکل می‌گیرد». همان‌طور که موتور احتراق داخلی منجر به فناوری‌های مشتق متعددی شد که شخصیت جنگ را در یک قرن پیش شکل دادند (از جمله هواپیماها. زیردریایی‌ها و تانک‌ها) فناوری‌های مشتق شده از هوش مصنوعی (از جمله یادگیری ماشینی، پردازش زبان طبیعی، تشخیص تصویر، بیومتریک، اتوماسیون فرایند روباتیک، ایجاد محتوا و دفاع سایبری) در حال شکل‌گیری شیوه جنگ در عصر دیجیتال هستند.

مشارکت بین ارتش‌های دولتی، پیمانکاران دفاعی و شرکت‌های فناوری نشان می‌دهد که میدان‌های نبرد آینده مملو از دستگاه‌ها و حسگرهای هوشمند خواهد بود و هزینه‌های دفاعی توسط قدرت‌های بزرگ نشان‌دهنده این است که مزیت رقابتی در جنگ‌های آینده به باهوش‌ترین‌ها و نه فقط قوی‌ترین‌ها خواهد رسید. بنابراین، درحالی‌که سلاح‌های به کار رفته در جنگ جهانی دوم به اندازه ابزارهای مفیدی برای بازرسان جنایات جنگی نبودند، فناوری نظامی مدرن در واقع ممکن است به همان اندازه که برای کسانی که برای عدالت می‌جنگند، مفید واقع شود.

این پژوهش، با الهام از بینش‌های چنری در حدود یک قرن پیش، نگاهی عمیق به تلاش‌های تحقیقاتی نظامی کنونی متمرکز بر کاربرد و ادغام هوش مصنوعی در ابزارهای جنگی دارد. این پژوهش، به بررسی نحوه ادغام هوش مصنوعی در سلاح‌های نظامی، تجهیزات، وسایل نقلیه، زیرساخت‌ها و سیستم‌ها می‌پردازد تا بهبود قابلیت‌های اطلاعات استراتژیک با جمع‌آوری و تجزیه‌وتحلیل داده‌های پیشرفته و قابلیت‌های فریب تاکتیکی را با دستکاری داده‌های پیشرفته توسط ماشین بهبود بخشد. علاوه بر این، این پژوهش به این موضوع می‌پردازد که چگونه افزایش استفاده از فناوری‌های مشتق از هوش مصنوعی در جنگ ممکن است بر کسانی که به دنبال عدالت و پاسخگویی در مورد نقض قوانین بین‌المللی بشردوستانه و قوانین کیفری بین‌المللی هستند، تأثیر بگذارد. بررسی می‌کند که آیا و چگونه بازرسان جنایات جنگی می‌توانند از داده‌های جمع‌آوری شده و پردازش شده توسط حسگرها و دستگاه‌های هوشمند در میدان نبرد استفاده کنند؟ و این که آیا استفاده از هوش مصنوعی برای ایجاد و انتشار اطلاعات نادرست در طول عملیات‌های نظامی، بازرسان را در جست‌وجوی حقیقت با مشکل مواجه می‌کند یا خیر؟.

در نهایت، این پژوهش به مثال‌هایی اشاره می‌کند که چگونه کاربردهای مشابه هوش مصنوعی، به‌ویژه تقویت تشخیص تصویر و اشیاء از طریق یادگیری ماشینی، در تحقیقات جنایات جنگی فعلی ادغام می‌شوند. هوش مصنوعی پتانسیل زیادی برای کمک به تحقیق و تعقیب جنایات جنگی و سایر موارد

نقض قوانین بین‌المللی دارد، اما به ناچار موانع جدیدی را برای کسانی که به دنبال عدالت و پاسخگویی هستند ایجاد خواهد کرد. بنابراین، نهادها و شاغلین بین‌المللی عدالت کیفری باید با پیش‌بینی و درک این که چگونه فناوری‌های هوش مصنوعی در حال تغییر ماهیت جنگ و ماهیت تحقیقات جنایات جنگی هستند، برای رسیدگی به این چالش‌های نوظهور آماده شوند.

۱- هوش کامپیوتری

«سون تزو»، استراتژیست نظامی چینی در کتاب خود «هنر جنگ» اشعار داشته: «فقط فرمانروای روشنفکر و ژنرال دانا است که از بالاترین هوش ارتش برای اهداف جاسوسی استفاده می‌کند و از این طریق به نتایج بزرگی دست می‌یابد». بینش وی بر اهمیت زیاد تجارت اطلاعاتی در دستیابی به پیروزی‌های نظامی تأکید می‌کند. ژنرال «سون تزو»، در نوشته‌ای مشابه چنین نگاشته است که: «تمام جنگ‌ها بر اساس فریب است. ازاین‌رو وقتی قادر به حمله هستیم، باید ناتوان به نظر برسیم. هنگام استفاده از نیروهای خود، باید غیرفعال ظاهر شویم. وقتی نزدیک هستیم، باید به دشمن چنین وانمود کنیم که دور هستیم. وقتی دور هستیم، باید کاری کنیم که او باور کند که نزدیک هستیم». راهنمایی‌های او کاربرد تاکتیکی فریب و اطلاعات نادرست در جنگ را برجسته می‌کند.

در این پژوهش، به بررسی استفاده از هوش مصنوعی برای پیشبرد هر دو هدف می‌پردازیم، در یک بخش بر روی استفاده از هوش مصنوعی برای اهداف اطلاعاتی و در بخش بعدی بر استفاده از هوش مصنوعی برای اهداف فریب تمرکز خواهیم کرد. این بخش به بررسی نوآوری‌های تکنولوژیکی می‌پردازد که نشان می‌دهد چگونه فناوری‌های مشتق شده هوش مصنوعی می‌توانند و در حال ادغام با اشیاء و تجهیزات نظامی برای بهبود آگاهی موقعیتی و هوش عملیاتی هستند. با استفاده از نمونه‌های عینی هوش مصنوعی در اطلاعات نظامی، این بخش به بررسی این موضوع می‌پردازد که چگونه این فناوری‌های جدید و نوظهور ممکن است بر تحقیقات جنایات جنگی تأثیر بگذارند؟ و علاوه بر این، آیا بازرسان جنایات جنگی ممکن است بتوانند از فناوری‌های مشابه به نفع خود استفاده کنند یا خیر؟.

۱-۱- داده‌ها به‌عنوان سلاح‌های جنگی

هدف به حداکثر رساندن هوش مصنوعی در جنگ چیز جدیدی نیست. وزارت دفاع ایالات متحده امریکا، اطلاعات نظامی را این گونه تعریف می‌کند: «رشته‌ای نظامی است که از روش‌های جمع‌آوری و

تحلیل اطلاعات برای ارائه دستورالعمل و راهنمایی برای کمک به فرماندهان در تصمیم‌گیری‌های شان استفاده می‌کند». انواع مختلفی از هوش وجود دارد. از جمله هوش انسانی، هوش سیگنال[۴]، هوش مکانی[۵] و هوش منبع باز[۶] که مدت‌ها بخش مهمی از استراتژی مبارزه مسلحانه و نوآوری‌های تکنولوژیکی بوده و مدت‌ها است که بخشی جدایی‌ناپذیر از کار اطلاعاتی بوده است.

با این حال، فناوری‌های دیجیتال در حال ظهور در سال‌های اخیر منجر به نوع جدیدی از اطلاعات نظامی شده است؛ که هوش ماشینی نام دارد. هوش ماشینی شامل جمع‌آوری خودکار، پردازش، تجزیه‌وتحلیل و تفسیر داده‌های چندمنبعی توسط الگوریتم‌های یادگیری ماشینی به جای تحلیلگران انسانی است. در گذشته، بزرگ‌ترین چالش برای اطلاعات نظامی توانایی به دست آوردن داده‌های کافی بود، بنابراین محققان بر روی یافتن راه‌های بهتر برای دسترسی به داده‌های بیشتر تمرکز کردند. امروزه در عصر اطلاعات که منابع اطلاعاتی فراوانی وجود دارد، چالش کلیدی از کمبود داده به بارگذاری بیش از حد داده تغییر یافته است. چالش جدید یافتن راهی برای سازمان‌دهی، تجزیه‌وتحلیل و تفسیر مؤثر همه آن داده‌ها است. درحالی‌که فناوران، به کار بر روی افزایش توانایی جمع‌آوری داده‌های بیشتر با فناوری‌های جدید ادامه می‌دهند، متخصصان دفاعی بیشتر بر فناوری‌هایی متمرکز هستند که می‌توانند داده‌ها را با سرعت و سطحی از دقت پردازش کنند که تصمیم‌گیری عملیاتی را در زمان واقعی امکان‌پذیر می‌سازد.

یکی از حوزه‌های نوظهور تحقیق و توسعه نظامی، اینترنت اشیاء نظامی است.[۷] اینترنت اشیاء سیستمی

---

۴. جاسوسی سیگنال به عملیات شنود اطلاعاتی گفته می‌شود که توسط سیگنال‌های الکترونیکی جابه‌جا می‌شود.

۵. اطلاعاتی درباره فعالیت‌های انسان روی زمین است که از بهره‌برداری و تجزیه‌وتحلیل تصاویر، سیگنال‌ها یا امضاءها با اطلاعات مکانی به دست می‌آید.

۶. منابع آشکار یا اطلاعات منبع آشکار داده‌هایی هستند که از منابع در دسترس همگانی گردآوری شده‌اند و در یک ارزیابی اطلاعاتی استفاده می‌شوند. گزاره «باز» در میان سازمان‌های اطلاعاتی به معنی آشکار و منابع در دسترس همگان است که در برابر منابع پنهان یا مخفیانه است. اطلاعات منبع آشکار ربطی به اطلاعات اشتراکی یا نرم‌افزار منبع آشکار ندارد.

۷. این پژوهش عمداً از بحث درباره اتوماسیون و هوش مصنوعی در توسعه سلاح‌ها و اسلحه‌ها دوری می‌کند. با وجود کمترین تعداد سلاح‌های رباتیکی خودکار در حال استفاده در جنگ امروز، بسیاری از کشورها در حال توسعه و آزمایش این قابلیت هستند و بسیاری از محققان به آن تمرکز دارند. در مقابل، تعداد نسبتاً کمی از تحقیقات علمی به مسئله تنظیم سلاح‌های خودکار کشنده معطوف شده است درحالی‌که در حوزه حقوق بین‌الملل بشردوستانه بسیار کمی درباره تأثیر سایر

از دستگاه‌های محاسباتی، الگوریتم‌ها و اشیاء فیزیکی به هم پیوسته با شناسه‌های منحصربه‌فرد است که می‌تواند داده‌ها را بدون دخالت انسان از طریق شبکه منتقل کند، بنابراین پردازش مستقل داده‌ها را ممکن می‌سازد. گارتنر، یک شرکت تحقیقاتی فناوری اطلاعات جهانی که گزارش‌های پیش‌بینی فناوری سالانه را منتشر می‌کند، اینترنت اشیاء را به‌عنوان «شبکه‌ای از اشیاء فیزیکی که حاوی فناوری‌های تعبیه شده برای برقراری ارتباط و حس یا تعامل با حالت‌های داخلی یا محیط خارجی هستند» توصیف می‌کند. اینترنت اشیاء طیف وسیعی از محصولات را در بر می‌گیرد. نه تنها گوشی‌های هوشمند و رایانه، بلکه اتومبیل، تلویزیون، لباس و لوازم جانبی، گرمایش خانه، سیستم‌های صوتی و امنیتی، یخچال، ضربان ساز، کنسول‌های بازی و حتی اسباب بازی‌های کودکان.

«دیوید ایوانز»، محقق سابق سیسکو توضیح می‌دهد که این شبکه همچنین شروع به شامل موارد بیولوژیکی مانند حیوانات خانگی، محصولات کشاورزی، دام و انسان کرده است. هوش مصنوعی به طور فزاینده‌ای در دستگاه‌های اینترنت اشیاء ادغام می‌شود تا بینش‌هایی از داده‌ها ارائه کند و از تصمیم‌گیری بدون دخالت انسان پشتیبانی کند. کارشناسان تخمین می‌زنند که تا سال ۲۰۲۰ میلادی تقریباً سی و یک میلیارد دستگاه به اینترنت متصل بوده است و حداقل ده میلیارد دستگاه دیگر تا سال ۲۰۲۷ میلادی به اینترنت اشیاء متصل خواهند شد. گارتنر پیش‌بینی می‌کند که تا سال ۲۰۲۲ میلادی، بیش از هشتاد درصد از پروژه‌های اینترنت اشیاء سازمانی شامل مؤلفه‌های هوش مصنوعی خواهند بود که این رقم در سال ۲۰۲۰ میلادی تنها ده درصد بود.

اینترنت اشیاء نظامی کاربرد فناوری‌ها و مفاهیم اینترنت اشیاء در حوزه نظامی است. مزایای آشکاری برای نیروهای مسلح در استفاده از دستگاه‌های اینترنت اشیاء برای فعالیت‌های رزمی و غیرجنگی از جمله تعمیر و نگهداری خودرو، نظارت بر پرسنل و کنترل انبار وجود دارد. اینترنت اشیاء نظامی کشتی‌ها، هواپیماها، تانک‌ها، پهپادها و پایگاه‌های عملیاتی را در یک شبکه منسجم به هم متصل می‌کند که آگاهی موقعیتی را افزایش می‌دهد، به ارزیابی ریسک کمک می‌کند و زمان پاسخ را بهبود می‌بخشد. ارتش ایالات متحده امریکا این مفهوم را حتی با ایده «میدان نبرد اشیاء» که به‌عنوان «هزاران دستگاه متشکل پویا با حسگرها در سراسر میدان نبرد، بهره‌برداری از خودمختاری و هوش مصنوعی برای ارائه آگاهی موقعیتی

کاربردهای اتوماسیون و هوش مصنوعی خارج از میدان جنگ نوشته شده است. بنابراین، این پژوهش به بررسی استفاده از این فناوری در سلاح‌ها پرداخته نمی‌شود، بلکه تمرکز خود را بر روی استفاده آن در سایر ابزارهای نظامی می‌گذارد.

و برآورده کردن اهداف مأموریت» در نظر گرفته شده است، پیش می‌برد.

دستگاه‌های اینترنت اشیاء نظامی با استفاده از ترکیبی از سنسورهای استراتژیک و اتوماسیون فوق‌العاده[۸] می‌توانند اطلاعات را «کشف، تجزیه‌وتحلیل، طراحی، اندازه‌گیری، نظارت و ارزیابی مجدد» کنند و به‌طور مستقل وظایف پیچیده‌ای را که به‌طور سنتی توسط سربازان انسانی انجام می‌شود، انجام دهند.[۹] جایگزینی جمع‌آوری‌کننده‌های داده‌های انسانی با ماشین‌های مستقل، به‌ویژه از نظر امنیت و منابع، ارزش زیادی دارد. به جای استفاده از نگهبانان یا پیشاهنگان، حسگرها می‌توانند داده‌های مهمی را از فاصله دور در اختیار خط مقدم قرار دهند. در این زمینه، هوش مصنوعی می‌تواند برای جمع‌آوری، تجزیه‌وتحلیل و تجسم سریع صدها هزار نقطه داده و حتی ارائه توصیه‌هایی برای تصمیم‌گیری در طول عملیات‌های جنگی مورد استفاده قرار گیرد. برای مثال، هوش مصنوعی می‌تواند از داده‌های حسگرهای جمع‌آوری اطلاعات در مورد شرایط آب و هوایی، تحرکات نیروها، حضور غیرنظامی، شرایط زمینی و سایر عوامل، همراه با داده‌های تاریخی مشابه، برای پیش‌بینی و جلوگیری از حرکت بعدی دشمن استفاده کند.

مفهوم سرباز شبکه‌ای کاملاً با اینترنت اشیاء نظامی پیوند خورده است (یک سرباز انسانی با قابلیت‌های پیشرفته ماشینی متصل به اینترنت اشیاء نظامی). این مفهوم استفاده از پوشیدنی‌ها و دستگاه‌های بیومتریک را به‌عنوان بخشی از اینترنت اشیاء نظامی گسترش می‌دهد و این مؤلفه را اضافه می‌کند که داده‌های جمع‌آوری‌شده در زمان واقعی با استفاده از هوش مصنوعی پردازش و تفسیر می‌شوند و به‌عنوان اطلاعات عملی به سربازان بازخورد داده می‌شوند. علاوه بر این، این مفهوم همچنین شامل فناوری‌های تقویت انسان می‌شود، که فناوری‌هایی هستند که تجارب شناختی و فیزیکی انسان را افزایش می‌دهند.

علاوه بر انواع مختلف تقویت شناختی، چهار دسته اصلی تقویت فیزیکی وجود دارد حسی، بیولوژیکی، مغزی و ژنتیکی.[۱۰] نیروهای مسلح سنتی تجهیزات ارتباطی و مهمات حمل می‌کنند،

---

۸ «هایپر اتوماسیون» گارتنر، که کاربرد پیچیده یادگیری ماشین (ML) در طیف وسیعی از ابزارها به منظور خودکارسازی وظایف انسانی است.

۹. از شناسایی گرفته تا تجزیه‌وتحلیل اطلاعاتی تا تصمیم‌گیری عملیاتی، اینترنت اشیاء نظامی می‌تواند تعداد سربازان انسانی مورد نیاز در میدان نبرد را تا حد زیادی به حداقل برساند.

۱۰. تقویت فیزیکی به چهار دسته اصلی تقسیم می‌شود: تقویت حسی (شنوایی، بینایی و ادراک)، تقویت زائده و عملکرد بیولوژیکی (اسکلت بیرونی و پروتز)، تقویت مغز (ایمپلنت برای درمان تشنج) و تقویت ژنتیکی (ژن سوماتیک و سلول درمانی). تقویت شناختی از طریق فناوری‌های عصبی در بخش غیرنظامی و همچنین ارتش در حال پیشرفت. به‌عنوان مثال،

درحالی‌که نیروهای مسلح آینده، همان‌طور که پیش‌بینی می‌شود، با دستگاه‌های تلفن همراه متصل به اینترنت، منابع برق پوشیدنی، حسگرهایی برای نظارت بر سلامت و ایمنی و فناوری‌هایی برای افزایش موقعیت، [۱۱] نوری و محیطی آگاه بسته خواهند شد.[۱۲] به منظور عملیاتی کردن هریک از این داده‌ها در زمان واقعی، هوش مصنوعی برای پردازش، انتقال، تجزیه‌وتحلیل و دریافت مقادیر عظیمی از داده‌هایی که توسط این سیستم‌ها تولید می‌شود، ضروری است.

اگر این چشم‌انداز از جنگ آینده محقق شود، سربازان و میدان‌های نبرد آینده ردپای دیجیتالی بسیار بزرگ‌تری نسبت به قبل خواهند داشت. دستگاه‌های دیجیتال جاسازی شده که قادر به نظارت، جمع‌آوری و تجزیه‌وتحلیل داده‌ها هستند، می‌توانند توسط بازرسان جنایی بین‌المللی برای تعیین این که چه کسی؟، چه چیزی؟، چه زمانی؟، کجا؟ و چگونه؟ رویدادها باید رخ دهد، مورد بهره‌برداری قرار گیرند. این پیشرفت‌های مبتنی بر هوش مصنوعی در نوآوری‌های نظامی، داده‌های بزرگی را تولید می‌کند که از نظر تئوری، موقعیت جغرافیایی دقیق و حرکت هر رزمنده و غیرنظامی ردیابی و ثبت می‌شود. تصاویر ماهواره‌ها، هواپیماهای بدون سرنشین، دوربین‌های مداربسته و دوربین‌های بدنه برای ارائه نمای سیصد و شصت درجه از کل فضای درگیری یکپارچه خواهند شد.

نمونه‌های اولیه‌ای از این مورد در زمینه جنگ سوریه دیده می‌شود، جایی که نرم‌افزار تجسم برای بازسازی حملات نظامی با استفاده از فیلم‌های دوربین مداربسته، تلفن‌های قربانیان، دوربین‌هایی[۱۳] که توسط اولین واکنش‌دهنده‌ها مانند کلاه‌های سفید پوشیده می‌شوند و خبرنگارانی که عواقب پس از آن را ثبت می‌کنند، استفاده شده است. داده‌های دقیق محیطی، مانند تغییرات در شرایط باد و داده‌های شخصی، مانند ضربان قلب و فشار خون سربازان انسانی، جمع‌آوری، پردازش و ذخیره خواهند شد. شاید مهم‌تر از همه، به دلیل افزایش فضای ذخیره‌سازی و افزایش ظرفیت جمع‌آوری داده‌ها، ارتباطات دیجیتالی دارای مهر زمان (چه شفاهی و چه مبتنی بر متن) تولید و حتی حفظ خواهد شد. این مورد شامل دستورات و

پروژه Neuralink ایلان ماسک را ملاحظه نمایید که در حال توسعه رابط‌های مغز و ماشین با پهنای باند فوق‌العاده بالا برای اتصال انسان و رایانه است.

۱۱. توانایی بهبود یافته در شناخت بصری با استفاده از دوربین‌های محاسباتی (SCENICC) برای سربازان.

۱۲. مزیت آن، افزایش آگاهی موقعیتی، محیطی و بهداشتی است.

13. Go Pro

پاسخ‌های بالا و پایین در زنجیره فرماندهی است که می‌تواند به‌عنوان مدرک مستقیم جنایات جنگی باشد. این شواهد ارتباط دیجیتالی به‌ویژه برای بازرسانی که اغلب با ایجاد ارتباط بین مجرمان سطح بالا و جنایات مرتکب شده توسط نیروهای سطح پایین در زمین مبارزه می‌کنند، ارزشمند است.

با این حال، تمام داده‌های پردازش شده توسط اینترنت اشیاء نظامی تنها در صورتی برای بازرسان جنایات جنگی مفید خواهد بود که توانایی جمع‌آوری، سازمان‌دهی، تجزیه‌وتحلیل و تفسیر آن را داشته باشند. بنابراین، داده‌ها باید برای بازرسان، وکلا و قضات قابل دسترس، خواندنی، قابل فهم و قابل توضیح باشند. فلذا این امر این سؤال اساسی را مطرح می‌کند: با زیرساخت فنی و منابع مختلف دادگاه‌ها و دیوان‌های بین‌المللی، نهادهای اجرایی قوانین ملی، کمیسیون‌های تحقیق و حتی سازمان‌های غیردولتی، آیا انجام این کارها امکان‌پذیر خواهد بود؟

۱-۲- ابزارهایی برای تجزیه‌وتحلیل، تفسیر و تجسم

حجم انبوهی از داده‌های تولید شده توسط اینترنت اشیاء نظامی و سربازان شبکه‌ای، علاوه بر داده‌های تولید شده توسط دستگاه‌های دیجیتال سنتی مانند رایانه‌ها و دستگاه‌های تلفن همراه غیرنظامی نزدیک، برای انسان چالش بزرگی است، چه رسد به بررسی و تجزیه‌وتحلیل این داده‌ها. اطلاعات بازار پیش‌بینی می‌کند که مجموع داده‌های جمعی جهان تا سال ۲۰۲۵ میلادی به یکصد و هفتاد و پنج زتابایت خواهد رسید. همان‌طور که اینترنت اشیاء نظامی رشد می‌کند، حجم و پیچیدگی داده‌های موجود برای تصمیم‌گیری نظامی نیز افزایش می‌یابد. تجزیه‌وتحلیل کلان داده‌ها به یک ماشین کمکی نیاز دارد، زیرا چهار ویژگی تعیین‌کننده آن (حجم، سرعت، تنوع و صحت) بررسی و تحلیل انسانی را غیرممکن می‌کند. رایانه‌هایی برای بررسی داده‌های در مقیاس بزرگ، جمع‌آوری و تجزیه‌وتحلیل داده‌های در حال حرکت، ارزیابی فرمت‌های مختلف داده‌ها و رسیدگی به عدم قطعیت داده‌ها مورد نیاز هستند. نرم افزار تجزیه‌وتحلیل نیز برای درک داده‌ها و آشکار کردن ارزش آن مورد نیاز است.

به منظور استفاده از داده‌های تولید شده توسط فناوری‌های نظامی مورد بحث در فوق، بازرسان جنایات جنگی و دادستان‌ها به زیرساخت‌های فنی خود، از جمله نرم افزار و سخت افزار، برای پردازش، تجمیع یا تفکیک، تجزیه‌وتحلیل و نتیجه‌گیری از اطلاعات موجود که در مالکیت خود باشند، نیاز دارند. آن‌ها احتمالا به نرم افزار تخصصی نیز برای دریافت داده‌ها نیاز خواهند داشت. علاوه بر این، هر سازمانی که در مورد

جنایات جنگی تحقیق می‌کند، برای استفاده از فناوری و نظارت بر عملکرد آن، به پرسنل آگاه و آموزش دیده مناسب نیاز دارد. سیستم‌های ادغام شده با هوش مصنوعی اینترنت اشیاء (چه غیرنظامی و چه نظامی) سؤالات متعددی را مطرح می‌کنند. به طور خاص، بازرسان جنایات جنگی برای استفاده از داده‌های تولید شده توسط اینترنت اشیاء نظامی به چه زیرساخت‌هایی نیاز دارند؟ [۱۴] علاوه بر این، آیا بازرسان جنایات جنگی می‌توانند از دستگاه‌های اینترنت اشیاء خود برای جمع‌آوری داده‌های مرتبط استفاده کنند؟

فناوری‌های مشتق از هوش مصنوعی که قبلاً توسط محققین مورد استفاده قرار گرفته‌اند شامل پردازش زبان طبیعی و تشخیص تصویر است که توسط نرم‌افزار یادگیری ماشین توسعه یافته است. پردازش زبان طبیعی جست‌وجوی کلیدواژه اسناد دیجیتالی مبتنی بر متن را فعال و افزایش می‌دهد، درحالی‌که تشخیص تصویر عملکرد مشابهی را برای علائم و نمادها فعال می‌کند. برای مثال، مکانیسم بی‌طرف، مستقل و تحقیقی در سوریه[15] از نرم‌افزاری برای اسکن اسناد عربی زبان برای شناسایی علائم و همچنین کلمات کلیدی استفاده می‌کند. با این حال، توانایی اجرای جست‌وجوهای مبتنی بر متن در همه زبان‌ها به یک اندازه مؤثر نیست. به طور خاص، اسنادی که به زبان‌هایی نوشته شده‌اند که از الفبای متفاوتی نسبت به الفبای رومی استفاده می‌کنند، اسنادی که به زبان‌های کمتر رایج نوشته شده‌اند، و اسنادی که حاوی نماد آوایی زبان‌های فقط گفتاری هستند، چالش‌های مداومی را ایجاد می‌کنند. در بسیاری از موارد، ممکن است تقاضا به اندازه کافی زیاد نباشد که شرکت‌های خصوصی را تشویق کند تا این ویژگی‌های کمتر مورد استفاده را توسعه دهند که ارزش زیادی برای کل بخش عدالت کیفری بین‌المللی دارد. علاوه بر این، در حال حاضر نمی‌توان تصاویر دیجیتال و مطالب صوتی و تصویری را به راحتی جست‌وجو کرد، اگرچه در سال‌های اخیر تحولات قابل توجهی در این زمینه رخ داده است.

به‌عنوان مثال، یک سازمان غیردولتی[16] که نرم افزاری را برای خیر اجتماعی ایجاد می‌کند، دقیقاً روی این موضوع کار می‌کند. پلتفرمی[17] قصد دارد با استفاده از هوش مصنوعی برای خودکارسازی و بهبود فرایند تجزیه، تحلیل و ایجاد حجم عظیمی از داده‌ها، با تمرکز خاص بر تطبیق و کپی‌برداری از تصاویر و

۱۴. این پژوهش، چالش‌های قانونی را برای بازرسان جنایات جنگی در به‌دست‌آوردن داده‌های نظامی تأیید می‌کند، اما به آن‌ها نمی‌پردازد، اگر چه این چالش‌ها قابل توجه هستند. تمرکز این پژوهش همچنان بر چالش‌های تکنولوژیک است.

15. IIIM
16. Benetech
17. JusticeAI Benetech

ویدیوهای دیجیتال، «داده‌های تضاد را به شواهد عملی تبدیل کند». به‌عنوان بخشی از پروژه هوش مصنوعی مایکروسافت برای اقدام بشردوستانه، این سازمان غیردولتی همچنین در حال توسعه سیستم‌هایی برای شناسایی مهمات خوشه‌ای و سایر انواع سلاح‌ها در صور دیجیتال است. به طور مشابه، بایگانی سوریه با یک شرکت فناوری مستقر در برلین[۱۸]، همکاری کرده تا ماشین‌ها را قادر سازد تصاویر یا صداهای سلاح‌های خاص را تشخیص دهند. مرکز علوم حقوق بشر دانشگاه کارنگی ملون از هوش مصنوعی با هدف بررسی نقض حقوق بشر بین‌المللی با سیستم بازسازی و تحلیل رویدادهای ویدئویی[۱۹] و برچسب‌گذاری رویداد از طریق پردازش رسانه‌های تحلیلی[۲۰] بهره‌برداری می‌کند. با اتخاذ رویکردی مشابه، برنامه عفو بین‌الملل[۲۱] در حال آزمایش با استفاده از هوش مصنوعی برای تشخیص الگو، در میان سایر کاربردهای بالقوه برای فعالیت‌های خود است. این نوع تشخیص خودکار الگو، می‌تواند ابزار مفیدی برای بازرسان جنایی و دادستان‌های بین‌المللی باشد که ممکن است مجبور باشند ماهیت سیستماتیک یا گسترده جرایم خاص یا شیوه‌های عمل یک مرتکب خاص را اثبات کنند.

علاوه بر تجزیه‌وتحلیل تصاویر دیجیتال، فیلم‌ها و اسناد، بازرسان جنایات جنگی به نرم افزاری نیاز دارند که بتواند داده‌های بزرگ و چندمنبعی را درک کند. تلاش‌های اولیه برای استفاده از این ابزارها و تکنیک‌ها در تحقیقات جنایات جنگی در حال انجام است. به‌عنوان مثال، سیستم هالا[۲۲] از پردازش زبان طبیعی و یادگیری ماشینی برای دریافت سریع داده‌های رسانه باز در مورد حملات هوایی گزارش شده استفاده می‌کند که به الگوریتم‌های ردیابی و پیش‌بینی آن وارد می‌شود. هالا با ترکیب داده‌های منابع خارجی با اطلاعات به دست آمده از ناظران انسانی و آژیرهای متصل به اینترنت، سیستمی را ایجاد کرده است که به غیرنظامیان در مورد حملات هوایی هشدار می‌دهد. به طور مشابه، Videre از دستگاه‌هایی برای جمع‌آوری داده‌ها استفاده می‌کند و به گروه‌های در معرض خطر در مناطق درگیری با هشدارهای اولیه حملات فیزیکی و دیجیتالی هشدار می‌دهد.

فناوری‌های هوش مصنوعی به پیشرفت‌های فوق‌العاده‌ای در توانایی تجسم مجموعه داده‌های متنوع کمک کرده‌اند. SITU Research و Forensic Architecture در حال آزمایش استفاده از هوش

18. VFRAME
19. VERA
20. E-LAMP
21. AI for good
22. Hala Systems

مصنوعی در کار خود برای تجسم و بازسازی رویدادهایی مانند اعتراضات[۲۳] در اوکراین هستند. درحالی‌که برخی از نرم افزارهای تجاری به همان اندازه برای تحلیلگران نظامی و تحقیقات جنایات جنگی قابل دسترسی هستند، مانند ابزارهای تجزیه‌وتحلیل پیوندهای گرافیکی.[۲۴] بسیاری از نرم افزارهای موجود در اختیار بازرسان جنایی و حقوق بشر بین‌المللی با آنچه مورد استفاده نظامیان حرفه‌ای قرار می‌گیرد بسیار متفاوت است. در درگیری‌های مسلحانه، از فناوری تشخیص تصویر برای شناسایی تهدیدها و خطرات احتمالی از قبیل بمب‌های دست‌ساز استفاده می‌شود. در تحقیقات جنایات جنگی، از همین فناوری برای شناسایی اشیاء پس از حمله، مانند ترکش یک دستگاه منفجر شده استفاده می‌شود. همان الگوریتم‌هایی که برای تشخیص غیرنظامیان از جنگجویان قبل از حمله استفاده می‌شوند، می‌توانند برای شناسایی آن تفاوت‌ها در تلفات بعد از آن استفاده شوند.[۲۵]

برای ایجاد هوش مصنوعی مؤثر، داده‌هایی برای آموزش آن مورد نیاز است: داده‌های خوب و متعدد. هنگامی که هوش مصنوعی آموزش داده شد، می‌توان از آن برای درک مجموعه داده‌های ناشناخته بر اساس آموخته‌هایش استفاده کرد. به‌عنوان مثال، اگر محققین نیاز به شناسایی نوع خاصی از مهمات در تصاویر داشته باشند، ابتدا باید با استفاده از داده‌های زیادی که به طور قابل اعتماد آن‌ها را به تصویر می‌کشند، به هوش مصنوعی آموزش دهند که این مهمات چگونه به نظر می‌رسند. منابع انسانی نیز در این فرایند آموزشی برای تأیید صحت هوش مصنوعی در حین آموزش ضروری هستند. تنها در این صورت است که می‌توان هوش مصنوعی را برای شناسایی صحیح در آینده مستقر کرد. در حال حاضر، محققان به کمک دانشگاه‌ها و سازمان‌های غیردولتی متکی هستند، اما ممکن است چرخ را دوباره اختراع کنند، زیرا ارتش قبلاً هوش مصنوعی خود را برای انجام این شناسایی‌ها آموزش داده است. به‌رغم شناخت واضح نیاز به بهبود ظرفیت فناوری، نهادهای تحقیق بین‌المللی با توانایی پذیرش چنین فناوری‌هایی دست

23. Euromaidan
24. Maltego, IBM's I2 Analyst Notebook
۲۵. درحالی‌که می‌توان از هوش مصنوعی برای متمایز کردن غیرنظامیان از نظامیان قبل از حمله ارتش استفاده کرد و پس از آن توسط محققان، به ناچار عوامل مؤثر در زمینه‌ای وجود خواهد داشت، مانند موقعیت‌هایی که شامل مبارزان غیریکنواخت شرکت در خصومت‌ها می‌شوند. به‌عنوان مثال، هوش مصنوعی نظامی احتمالاً به ترکیبی از شناخت تصویر و سایر منابع اطلاعاتی متکی است تا افراد را به‌عنوان مبارز یا اعضای یک گروه مسلح معرفی کند، اما همه اطلاعات موجود در اختیار ارتش در دسترس محققان جرایم جنگی قرار نخواهد گرفت.

و پنجه نرم کرده‌اند. بسیاری از کارشناسان به تنش ذاتی بین بوروکراسی سفت و سخت سازمان‌های بین‌المللی همراه با ماهیت محتاطانه حرفه حقوقی و انعطاف‌پذیری و کارایی مورد نیاز برای پذیرش فناوری‌های جدید اشاره کرده‌اند. چنین موانع بومی برای نوآوری باید مورد توجه قرار گیرد تا به درستی از امکانات فناورانه برای بررسی جنگ مدرن استفاده شود.

درک این موضوع که جنگ‌های آینده با حجم عظیمی از داده‌های تولید شده توسط حسگرها در محیط و پرسنل و تجهیزات نیروهای مسلح همراه خواهد بود، به این معنی است که بازرسان جنایات جنگی با انواع شواهد بسیار متفاوتی از آنچه امروز با آن مواجه می‌شوند، سروکار خواهند داشت. به منظور آمادگی کافی برای این امر، بازرسان و وکلا باید به چند سؤال اساسی بپردازند. اگر قرار باشد محققان از داده‌های تولید شده توسط ارتش به‌عنوان مدرک استفاده کنند، باید بدانند که چه نوع داده‌های مرتبط قانونی توسط این فناوری‌های جدید تولید می‌شود و همچنین کجا و چگونه ذخیره و نگهداری می‌شوند. آن‌ها همچنین به کانالی برای درخواست و دسترسی به داده‌ها نیاز دارند، که احتمالا با چالش‌های حقوقی و سیاسی اشتراک‌گذاری داده‌های فرامرزی، مانند قوانین حریم خصوصی و حفاظت از داده‌ها، علاوه بر چالش‌های فنی، همراه است. همه این سؤالات به دلیل منابع و زمان لازم برای ایجاد زیرساخت مناسب و گردش کار مربوطه باید از قبل بررسی شوند.

البته یک چالش کلیدی این است که چگونه بوروکرات‌ها را تشویق کنیم تا مشکلی را که هنوز با آن مواجه نشده‌اند حل کنند. تا به امروز، با افزایش زیاد شواهد مکانی و سمعی و بصری در سال‌های اخیر، اکثر تحقیقات و محاکمات جنایات جنگی به‌شدت بر شواهد و مدارک مستند تکیه کرده‌اند. اگر مجموعه داده‌های اضافی اینترنت اشیاء نظامی این انواع دیگر شواهد را تأیید کند، مطمئناً چنین مواردی را تقویت خواهد کرد. با این حال، اگر بین داده‌ها و گزارش‌های شاهد ناهماهنگی وجود داشته باشد، اثبات موارد دشوار فراتر از شک معقول، چالش‌برانگیزتر خواهد بود. سوابق دیجیتالی تولید شده توسط این فناوری‌های جدید و نوظهور می‌تواند امکان بازسازی دقیق رویداد و تجسم‌های قانع‌کننده را فراهم کند که می‌تواند در کمک به حقیقت‌یاب در بررسی‌ها بسیار مفید باشد. با این حال، این که آیا می‌توان از داده‌ها در این راه استفاده کرد یا خیر؟، هنوز یک سؤال باقی است. با کنار گذاشتن مسائل مربوط به دسترسی به این داده‌ها، که لاجرم چالشی برای نهادهای بین‌المللی است و به‌شدت به همکاری دولت‌ها برای جمع‌آوری شواهد متکی هستند، دادسراهای بین‌المللی به ظرفیت فنی، هم از نظر منابع انسانی و هم از

نظر زیرساخت، برای پردازش و ایجاد بستری برای این داده‌ها در جهت حفظ صحت، یکپارچگی و زنجیره نگهداری آن نیاز خواهند داشت.

۲- گمراهی ایجاد شده توسط رایانه

علاوه بر اصل مشهوری که گفته شد، همه جنگ‌ها بر اساس فریب است. «سان تزو» آموزش داده است «مردم را با آنچه آن‌ها انتظار دارند، جذب کنید». بدین‌ترتیب آن‌ها قادرند تشخیص دهند و پیش‌بینی‌های خود را تأیید کنند. این امر باعث ثبات آن‌ها می‌شود. الگوهای قابل پیش‌بینی واکنشی، ذهن آن‌ها را مشغول می‌کند درحالی‌که شما منتظر لحظه استثنایی هستید. با وجود سده‌های زیادی که از زمان نگارش این متن گذشته است، این متن به طور کامل پدیده مدرن تعیین نظرات اینترنت را توصیف می‌کند. واقعاً، دستورات داده شده در مزارع ترول روسیه برای شروع عملیات اطلاعاتی قبل از انتخابات ریاست جمهوری ایالات متحده امریکا در سال ۲۰۱۶ میلادی احتمالا حس مشابهی داشتند.

اطلاعات نادرست و جعل چیز جدیدی نیست، اما هوش مصنوعی کیفیت و حجم محتوای جعلی را به طور تصاعدی افزایش می‌دهد. فناوری‌های هوش مصنوعی به طور فزاینده‌ای برای ساخت و تقلید، تلاش برای تغییر و اطلاع‌رسانی نادرست، فریب و اطلاعات نادرست استفاده می‌شوند. در این بخش، برنامه‌های هوش مصنوعی در پروژه‌های تحقیق و توسعه نظامی برای بهبود قابلیت‌های فریب تاکتیکی مورد بررسی قرار می‌گیرد. هنگامی که هوش مصنوعی می‌تواند برای تولید داده‌های مصنوعی و پنهان کردن حقایق استفاده شود درباره یک تضاد مسلحانه، چندین اقدام کنترلی در حال توسعه است تا داده‌های مصنوعی را شناسایی کرده و تلاش کند تا دستکاری‌های دیجیتالی را شناسایی کند. اگر نیروهای نظامی آینده قصد دارند از فناوری برای تولید داده‌های مصنوعی به منظور بهره‌وری استراتژیک استفاده کنند، بازپردازان جنایات جنگ آینده نیاز به فناوری خواهند داشت تا تعیین کنند کدام داده‌ها قابل اعتماد هستند و کدام خیر؟.

۲-۱- دروغ‌ها به‌عنوان ابزارهای جنگ

هرچند علم نظامی و توسعه فناوری به طور قابل توجهی بر روی استفاده از هوش مصنوعی برای افزایش قابلیت‌های اطلاعاتی تمرکز دارد، تلاش‌های تحقیقاتی مشابه به همان اندازه به بهره‌گیری از هوش مصنوعی برای تلاش در جهت تحریک، فریب و گیج کردن نیروهای دشمن اختصاص داده شده است. در واقع، فناوری‌های مشتق شده از هوش مصنوعی به طور فزاینده برای تولید دیپ‌فیک‌ها و رسانه‌های

مصنوعی استفاده می‌شوند که با سرعت و مقیاس گسترده‌ای، اطلاعات غلط را منتشر می‌کنند. این برنامه‌های کاربردی هوش مصنوعی به منظور پنهان کردن فعالیت‌ها و استراتژی‌های نیروهای مسلح و همچنین تقویت جنگ اطلاعاتی به کار گرفته می‌شوند. سرهنگ دوم بازنشسته «اسکات پادجت» توضیح می‌دهد که عوامل دولتی از ابزارهای پیشرفته توسعه نرم افزار و هوش مصنوعی برای اختراع و بهبود قابلیت‌های تقلب جدید برای فریب هر دو انسان و ماشین در میدان نبرد مجازی استفاده می‌کنند.

پجت بازگو می‌کند که چگونه روسیه در سال ۲۰۱۴ میلادی یک «سلول بی‌ثبات‌کننده» را به داخل اوکراین برای انتشار اطلاعات نادرست و راه‌اندازی تظاهرات جعلی با استفاده از بازیگرانی که برای ترویج جنبش طرفداری از روسیه، استخدام و آموزش دیده بودند فرستاد. به‌عنوان یک مثال، استفاده از این تاکتیک اطلاعات غلط، پادجت بررسی می‌کند که چگونه این کار با استفاده از هوش مصنوعی انجام شده است: «اگر روس‌ها در سال ۲۰۱۴ میلادی سیستم‌های هوش مصنوعی هوشمند برای تلاش و ترکیب محتوای صوتی و تصویری داشتند، آن‌ها احتمالا چگونه از آن‌ها استفاده می‌کردند و با چه منافعی؟ » این فرضیه سناریوی ترسناکی را ایجاد می‌کند که در آن رویدادهای جعلی و شخصیت‌های مصنوعی می‌توانند به‌صورت دیجیتالی برای این هدف با هزینه بسیار کمتر و با خطر بسیار کمتر تولید شوند: «ویدئوی خبری تظاهرات را می‌توان به‌صورت دیجیتالی تغییر داد تا هزاران معترض را در مقابل صدها نفر نشان دهد. سیاست‌مداران مخالف برجسته را می‌توان به‌عنوان معترضانی که به راحتی در اعتراضات شناسایی می‌شوند، قرار داد. اظهارنظرهای رهبر اپوزیسیون در مصاحبه‌های اخبار جعلی می‌تواند برای تغییر عقاید و حقایق ساخته شود. به جای استفاده از ماکت‌ها، آن‌ها می‌توانند به‌صورت دیجیتالی درگیری‌های نظامی مصنوعی ایجاد کنند که هرگز در میدان نبرد جنبشی اتفاق نیفتاده است».

در سال ۲۰۱۹ میلادی، کارخانه‌های ترول روسیه همان تاکتیک‌های مشابه را با کمک هوش مصنوعی برای اتوماسیون ایجاد و توزیع محتوا در ونزوئلا به کار گرفتند، داستان اسب تروا را پخش کردند که ادعا می‌کرد که کمک‌های انسانی از طرف ایالات متحده امریکا و سازمان‌های بین‌المللی به‌عنوان پوششی برای وارد کردن سلاح‌های غیرقانونی به گروه‌های مخالف استفاده می‌شود. این روایت نادرست نه تنها به طور گسترده در رسانه‌های اجتماعی منتشر شد، بلکه از منابع رسانه‌ای جعلی به منابع قانونی مانند بی‌بی‌سی

منتقل شد.[۲۶] محققان اینترنت سه هزار و ششصد مقاله اسپانیایی با استفاده از این اصطلاح را از ترکیب حساب‌های بات مشکوک و همچنین رسانه‌های خبری معتبر پیدا کردند. روسیه درحالی‌که شاید جسورترین بازیگر در این فضا باشد، به‌هیچ‌وجه تنها دولتی نیست که از این تاکتیک‌ها استفاده می‌کند. به‌علاوه، استفاده از هوش مصنوعی برای ایجاد محتوا به منظور فریب انسان‌ها، توسعه‌دهندگان دفاعی همچنین در حال کار بر روی تاکتیک‌های فریب دیجیتالی برای فریب ماشین‌ها هستند.

محیط عملیاتی دیجیتالی که در بالا توضیح داده شد با میدان‌های جنگ داده‌های بزرگ که توسط اینترنت اشیاء نظامی تغذیه می‌شود، درعین‌حال که برای تاکتیک‌های نظامی مؤثر است، آسیب‌پذیری‌های جدیدی را برای هک، مسمومیت داده‌ها و سایر حملات خصمانه ایجاد می‌کند. سرهنگ بازنشسته «استفان باناخ» مفهوم «ازدیادی سرباز مصنوعی» را توصیف می‌کند که «از سیستم ایمنی بیولوژیکی انسان‌ها مشتق شده و به ساختار جنگ مجازی به منظور حفاظت از سربازان تعمیم یافته است». این مفهوم، سه لایه حفاظت برای سربازان در میدان‌های جنگ آینده را پیش‌بینی می‌کند، یکی از آن‌ها «ایمنی فعال» است. این نوع از هوش مصنوعی، از طریق «مخفی کردن، تقلید، شبیه‌سازی، جنگ رباتیک، اطلاعات الکترونیکی و سیگنال، امضاءهای تغییر مسیردهی و آواتارهای مجازی با اثرات فیزیکی»، جلوگیری از شناسایی سرباز را فراهم می‌کند. چنین مکانیزم‌های پنهان‌سازی دیجیتال قبلاً در مقیاس کوچک‌تری مورد استفاده قرار گرفته‌اند. به‌عنوان مثال، وزارت بازرگانی ایالات متحده امریکا تأمین‌کنندگان تصاویر ماهواره‌ای تجاری را نظارت می‌کند و گاهی اوقات از تصاویر عمومی که منتشر می‌شوند، می‌خواهد تا بحرانی‌ترین مکان‌ها مانند پایگاه‌های نظامی، مات شوند.

توانایی دستکاری تصاویر ماهواره‌ای که به‌شدت برای نقشه‌برداری درگیری‌های مسلحانه به آن تکیه می‌شود، چالشی واقعی برای محققین ایجاد می‌کند. اگر این داده‌ها ذخیره شود و بعداً توسط بازرسان جنایات جنگی به دست بیاید، هرگونه اطلاعات دستکاری شده می‌تواند درک بازرسان از حقایق مرتبط را مخدوش کند. سایر تکنیک‌های دستکاری دیجیتال و پنهان‌سازی در حال توسعه نه تنها برای محافظت طراحی شده‌اند، بلکه به‌عنوان اقدامات متقابل تهاجمی مانند استفاده از نرم‌افزار جلوه‌های بصری با پشتیبانی

---

۲۶. در بیست و دوم فوریه، اوو مورالس، رئیس‌جمهور بولیوی، در بیانیه‌ای به نقل از RT از این اصطلاح استفاده کرد و کمک‌های بشردوستانه ایالات متحده امریکا را به‌عنوان اسب تروا محکوم کرد. در همان روز، بی‌بی‌سی مقاله‌ای با عنوان «کمک به ونزوئلا: کمک واقعی یا اسب تروا؟ » منتشر کرد.

از هوش مصنوعی برای تغییر تصاویر و ویدیوها در زمان واقعی طراحی شده‌اند. کار خسته‌کننده فتوشاپ کردن تصاویر افراد و اشیاء، با ابزارهای هوشمندی جایگزین می‌شود که به کاربران اجازه می‌دهد فیلترها را اعمال کنند، عناصر ناخواسته را در فیلم‌های متحرک حذف کنند و پس زمینه جدیدی را در چند هزارم ثانیه پر کنند. اگر حسگرهای تصویری در میدان نبرد به طور کافی محافظت نشوند، اطلاعات صوتی، تصویری پخش زنده ممکن است تخریب شود، به‌عنوان مثال برای حذف نیروهای پیشرو از تصویر متحرک. این نرم افزار مفروضات قبلی در مورد زمان دستکاری فیلم‌ها و تصاویر را باطل می‌کند.

بنابراین، درحالی‌که داده‌های جامع با وضوح زمانی و بصری افزایش یافته تولید شده، توسط حسگرهای میدان نبرد و دستگاه‌های هوشمند در اینترنت اشیاء نظامی ممکن است تصویر واضح‌تری از اتفاقات رخ داده در اختیار بازرسان جنایات جنگی قرار دهد، خطر دستکاری دیجیتال و تغییر داده‌ها نگرانی بزرگی را در مورد توانایی تکیه بر چنین اطلاعاتی به‌عنوان مدرک در محاکمات جنایی ایجاد می‌کند.

۲-۲- ابزارهای بررسی و اعتبارسنجی

درحالی‌که دولت‌ها تلاش می‌کنند تا تأثیرات کمپین‌های اطلاعات نادرست را که منشاء آن روسیه و سایر دشمنان برای مقاصد نظامی است، کاهش دهند، بازرسان جنایی بین‌المللی باید تلاش کنند تا به درستی کمپین‌های اطلاعات نادرست را به منظور ایجاد پرونده‌های حقوقی شناسایی و تجزیه‌وتحلیل کنند. در پاسخ به تهدیدات دیپ فیک و اطلاعات غلط مانند آنچه که از انتخابات ریاست جمهوری ایالات متحده امریکا سال ۲۰۱۶ میلادی تا برگزاری رفراندوم استقلال کاتالونیا در اسپانیا در سراسر جهان ظاهر شده است، پاجت توضیح می‌دهد که «یک ارائه از نرم افزارهای پیشرفته تجزیه‌وتحلیل و ابزارهای کارآمد هوش مصنوعی برای بررسی این که دقیقاً چه کسانی این کمپین‌های اطلاعات غلط روسیه را اداره و حمایت می‌کردند، استفاده شدند». استفاده از این ابزارها برای بررسی اقدامات فعال روسیه منجر به اعلام اتهامات جدی در ماه فوریه ۲۰۱۸ میلادی علیه سیزده شهروند روسی و سه شرکت روسی شد.

مؤسسات تحصیلی، مراکز تحقیقات نظامی و شرکت‌های خصوصی (گاهی اوقات به‌صورت مشارکتی کار می‌کنند) در جبهه توسعه فناوری احراز هویت دیجیتال قرار دارند. به‌عنوان مثال، دو پروژه دارپا از ابزارهای خودکار برای ارزیابی این که آیا یک تصویر یا ویدیو تغییر داده شده است استفاده می‌کنند: پروژه متافور، که از هوش مصنوعی در پزشکی رسانه استفاده می‌کند و پروژه سمافور، که از

هوش مصنوعی در پزشکی قانونی استفاده می‌کند. ابزارهای پیچیده پزشکی قانونی دیجیتالی که می‌توانند دستکاری‌های دستی را در تصاویر و ویدیوهای دیجیتال انجام دهند، مانند مواردی که با فتوشاپ انجام می‌شود، هنگام تشخیص تقلب‌های تولید شده توسط هوش مصنوعی، به اندازه کافی قابل اعتماد نیستند.

در طی پنج سال گذشته، در هر دو بخش خصوصی و غیرانتفاعی، فناوری‌های یادگیری عمیق برای اتوماسیون تشخیص دیپ فیک به وجود آمده است. یکی از این شرکت‌ها دیپ تریس است که «در حال توسعه فناوری‌های یادگیری عمیق برای شناسایی دیپ فیک‌های پنهان شده در دید عمومی و احراز هویت رسانه‌های سمعی و بصری دستکاری شده است». علاوه بر این، محصولات فناوری وجود دارند که با استفاده از ترکیبی از سخت‌افزار در تلفن‌های همراه و نرم‌افزارهایی مانند بلاک چین، روی ایجاد اصالت در نقطه عکس‌برداری تمرکز می‌کنند تا اطمینان حاصل شود که تصاویر و ویدیوها قابل دستکاری نیستند. به‌عنوان مثال، eyeWitness to Atrocities یک برنامه موبایل امن ارائه می‌دهد که کاربران می‌توانند تصاویر و ویدیوهای قابل اثبات را با استفاده از تلفن همراه خود ضبط کنند، که مستقیماً به یک انبار داده دیجیتال توسط LexisNexis ارسال می‌شوند تا از زنجیره حفظ آن‌ها اطمینان حاصل شود. هرچند نسخه‌های تصویر هنوز قابل تغییر هستند، همیشه یک اصل اساسی بدون تغییر برای مقایسه وجود خواهد داشت. به همین ترتیب، ProofMode و TruePic اپلیکیشن‌های موبایلی را با فناوری احراز هویت مشابهی از ابتدا تجهیز کرده‌اند.

علاوه بر راه‌حل‌های فنی، همیشه نیاز به استقرار تکنیک‌های تأیید انسانی وجود خواهد داشت. اعتماد کامل به ماشین‌ها مشکلات جدیدی را به وجود می‌آورد به دلیل «حماقت مصنوعی» که به روشی اشاره دارد که الگوریتم‌ها می‌توانند دنیا را به شکلی تفسیر کنند که هیچ انسانی تا به حال نمی‌توانسته باشد، زیرا آن‌ها داده‌ها را بر اساس ریاضیات و منطق تفسیر می‌کنند بدون این که از غرایز، بینش یا عقلانیت استفاده کنند. اینترنت وبسایت‌های بسیاری را با راهنماها و ترفندهایی برای فریب تکنولوژی تشخیص چهره ارائه می‌دهد، از کلاه‌هایی که با چراغ‌های ال‌ای دی[۲۷] مجهز شده‌اند تا آرایشی که برای تحت تأثیر قرار دادن دید کامپیوتری طراحی شده است. با این حال، درحالی‌که این حیله‌ها ممکن است برخی از الگوریتم‌ها را فریب دهند، اما به‌سرعت توسط هر انسانی قابل شناسایی است. یک مثال دیگر از مدیر پروژه دارپا، مت

27. LED

تورک، یک لیست آپارتمان مصنوعی[۲۸] است که «فرش ۷/۲۴» را تبلیغ کرد، یک خطای معنایی که از دست ماشین‌ها فرار کرد اما اکثر انسان‌ها آن را متوجه می‌شوند. تکنیک‌های راستی‌آزمایی مانند آنچه در روش پروتکل برکلی در مورد تحقیقات دیجیتال منبع باز ارائه شده است، باید به همراه ابزارهای هوش مصنوعی استفاده شوند که سلامت دیجیتالی، فیزیکی و معنایی مواد دیجیتال را ارزیابی می‌کنند.[۲۹]

به منظور تأیید اعتبار شواهد فیزیکی، دادگاه‌ها به زنجیره حفظ و نگهداری، از زمانی که بازرس مسئولیت مراقبت از اقلام را به عهده می‌گیرد تا زمانی که در دادگاه ارائه می‌شود، توجه می‌کنند. در مورد شواهد دیجیتال، به‌ویژه محتوای آنلاین، چالش اصالت با برقراری زنجیره حفاظت از زمان ایجاد تا زمان جمع‌آوری توسط بازپرس پیش می‌آید. اگر داده‌های نادرست به دلایل استراتژیک تولید و توزیع شود در طول یک درگیری مسلحانه، هرگونه داده در مورد آن درگیری می‌تواند زیرسؤال رود. بنابراین، تقریباً همیشه نیاز به شهادت انسانی وجود خواهد داشت که داده‌ها را معرفی کند تا پایه‌ای برای صحت و اعتبار آن‌ها ایجاد شود. هرچند برخی ممکن است فرض کنند که شواهد دیجیتال ممکن است روزی نیاز به شهادت شاهد را جایگزین کنند، اما واقعیت دقیقاً برعکس است زیرا اغلب باید شواهد دیجیتال از طریق شهادت انسانی در دادگاه معرفی شوند. دادگاه‌ها نه تنها به سؤال این که آیا شواهد ادعا شده تغییر یافته است؟ بلکه نیازمند اطلاع از نحوه استفاده از آن نیز خواهند بود.

مسائل کلیدی که نیازمند راه‌حل هستند عبارتند از: فقدان تفکیک نهادی بین عملکرد دادستانی و تحقیقات و عملکردهای عملیاتی دفاتر دادسراهای بین‌المللی، فقدان تضمینات رویه‌ای کافی و زیرساخت‌های جزئی با چالش‌های قابلیت همکاری. ارزش جلسات استماع شواهد در سیستم حقوقی کامن‌لا این است که طرفین مخالف را مجبور می‌کند تا در یک فراخوان عمومی، فرضیات یکدیگر را مورد چالش قرار دهند. این موضوع علاوه بر اطلاع‌رسانی به قضات برای تعیین قابلیت اعتماد و اهمیت مناسب اطلاعات، عموم را نیز آگاه می‌سازد. وکلای حقوقی نیاز به دانش و اعتماد به نفس با یادگیری روش‌های جست‌وجوی الگوریتم‌ها و همچنین نتیجه‌ها و صلاحیت‌های کارشناسان برای چالش جنبه‌های فنی شواهد دیجیتال دارند. سازمان‌های غیردولتی که در آینده حمایت از محاکمه جنایات جنگی می‌کنند،

28. Airbnb

۲۹. تأیید اطلاعات آنلاین به سه دسته اصلی تقسیم می‌شود: تجزیه‌وتحلیل محتوا، تجزیه‌وتحلیل منبع و تجزیه‌وتحلیل تکنیکی. شامل تکنیک‌هایی مانند جست‌وجوی عکس معکوس، موقعیت جغرافیایی و زمان‌بندی است.

باید اطلاعات بهتری در مورد جمع‌آوری و برخورد با شواهد دیجیتال داشته باشند و جمعیت قربانیان نیاز به درک بهتری از جزئیات فرایند دارند. در نهایت، استدلال و تفسیر دقیق قضایی درباره تصمیمات شواهد مربوط به داده‌های نظامی دیجیتال به‌عنوان یک ستون اساسی در این فرایند خدمت خواهد کرد.

نتیجه

سطح تحقیقات جنایات جنگی در حال ارتقاء است، زیرا محققان در دادگاه‌ها و دیوان‌های کیفری بین‌المللی، واحدهای جنایات جنگی‌ملی، کمیسیون‌های تحقیق و سازمان‌های غیردولتی از فناوری‌های نظامی در کار خود استفاده می‌کنند. اطلاعات منبع‌باز و تکنیک‌های تحقیق دیجیتال در حال حاضر توسط بسیاری از این نهادها استفاده می‌شوند و به طور فزاینده، تشخیص تصویر و چهره، الگوریتم‌های پیش‌بینی و بیومتریک رفتاری برای شناسایی و تجزیه‌وتحلیل شواهد در دست آزمایش قرار دارند.

تحقیق‌کنندگان بین‌المللی همچنین از برنامه‌های تلفن همراه ویژه استفاده می‌کنند تا تصاویر و ویدیوهای دیجیتال را ضبط و تأیید کنند، تصاویر ماهواره‌ای با وضوح بالا را برای تجزیه‌وتحلیل مکانیکی خریداری کنند و حتی از پهپادها استفاده کنند. در چند سال اخیر، در دادگاه‌های جنایی بین‌المللی از فتوگرامتری برای تکثیر صحنه‌های جرم و از واقعیت مجازی برای انتقال قضات به میدان جنگ استفاده شده است. تلاش برای دستیابی به مزیت نظامی یکی از بزرگ‌ترین محرک‌های نوآوری است. در سال ۱۹۲۴ میلادی، توسعه فناوری برای اهداف نظامی بر روی قدرت جنبشی تمرکز داشت، با این که بسیاری بمب‌های بزرگ‌تر و بهتر را به‌عنوان کلید پیروزی، می‌دانستند. ترندهای فعلی نشان می‌دهد که توسعه فناوری برای اهداف نظامی بر روی داده‌ها تمرکز خواهد کرد، با نیاز به مجموعه داده‌های بزرگ‌تر، داده‌های دقیق‌تر و تجزیه‌وتحلیل بهتر داده‌ها به‌عنوان کلید موفقیت عملیاتی.

تکنولوژی‌های مشابهی که برای افزایش کارآمدی نیروهای نظامی در جنگ استفاده می‌شود، می‌تواند به همان اندازه در پیشگیری از جنگ، پاسخ‌های انسانی به جنگ و تحقیقات درباره جرایم جنگی استفاده شود. کارشناسان جنایی بین‌المللی به طور قابل توجهی از یافتن کاربردهای این فناوری‌های جدید و نوظهور در کار خود بهره‌مند خواهند شد، اما آن‌ها نمی‌توانند این کار را به‌تنهایی انجام دهند. بازرسان جنایی بین‌المللی باید با شرکت‌های فناوری مشارکت‌های استراتژیک ایجاد کنند، کشورها را در مورد نیاز به سرمایه‌گذاری در نوآوری متقاعد کنند و همه افراد حاضر در این زمینه را به بهترین شیوه برای

آماده‌سازی برای چالش‌های قریب‌الوقوع به جای واکنش به آن‌ها وادار کنند.

استفاده از هوش مصنوعی می‌تواند برای بازرسان جنایی بین‌المللی که به دنبال مسئول نگه داشتن مجرمان سطح بالا در قبال جنایات جنگی هستند، منافع فوق‌العاده به همراه داشته باشد، اما درعین‌حال ناتوانی در درک این فناوری‌های جدید، شکاف معافیت از مجازات را افزایش می‌دهد. فناوری به طور ذاتی خوب، بد یا بی‌طرف نیست. بلکه اجرای فناوری است که تعیین می‌کند آیا آن به پیشبرد اهداف جنگ یا صلح و در نهایت عدالت کمک می‌کند یا خیر؟. هیچ مثال واضح‌تری از این حقیقت وجود ندارد تا استفاده از هوش مصنوعی که هم‌زمان در منازعات مسلح مدرن برای روشن کردن و پنهان کردن حقایق استفاده می‌شود. برای استفاده از این فناوری‌ها به منظور پیشبرد اهداف دادگاه‌های بین‌المللی جنایی، دادگاه‌ها و دیوان‌های بین‌المللی باید اطمینان حاصل کنند که جریان‌کار، زیرساخت‌ها و مهارت‌های فنی کارکنان برای تحقیق درباره جنگ‌هایی که توسط هوش مصنوعی شکل گرفته‌اند، آماده هستند. این به معنای ایجاد فضایی برای آزمایش و نوآوری به‌صورت پیشگامانه است، سرمایه‌گذاری در راهکارهایی که به آینده‌نگری می‌پردازند، ایجاد شبکه‌ها و روابط برای تقویت احتمال به اشتراک‌گذاری داده‌ها و مقابله با راهکارهای مسائل قبل از بروز آن‌ها است.

همان‌طور که تأثیر منفی اجتماعی دیپ فیک و سایر اشکال از اطلاعات غلط افزایش می‌یابد، محققان باید به روش‌های تند و تیزی برای برقراری حقیقت و اطمینان از اعتماد عمومی به آن حقیقت روی آورند. ما در دورانی زندگی می‌کنیم که مدافعان حقوق بشر، بازپرسان و دادستانان جنایی بین‌المللی به طور مداوم مورد حمله قرار می‌گیرند. آن‌ها برای مقابله با این حملات نیاز به هر ابزاری در اختیار خود دارند.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

منابع

- Amnesty International, 2021, Amnesty Decoders, available online at https: //decoders.amnesty.org.
- Artificial Intelligence and National Security, 2021, Congressional Research Service, 26 August 2020, available online at https: //fas.org/sgp/crs/natsec/R45178.pdf.

- Benetech JusticeAI platform, 2021, available online at https: //benetech.org/lab/ethical-ai-to-promotejustice.
- Pellerin, 2021, Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence, US Department of Defense, 31 October 2016, available online at https: //www.defense.gov/Explore/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters americas-military-deterrence.
- Connected Soldier, 2021, Ansys, available online at https: //www.ansys.com/campaigns/internet-of-things/connected-soldier.
- Goldstein and G. Gordon, 2017, Documents could Link Russian Cybersecurity Firm Kaspersky to FSB Spy Agency, Chicago Tribune, and 3 July 2017, available online at https: //www.chicagotribune.com/nation-world/ct-kaspersky-cyber-russia-spy-agency-20170703-story.html.
- Schatsky, 2018, bringing the Power of AI to the Internet of Things, Wired, available online at https: //www.wired.com/brandlab/2018/05/bringing-power-ai-internet-things.
- DOD Dictionary of Military and Associated Terms, 2021, available online at https: //www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.
- Pirace´s and J. Aronson, 2020, The OTP and ICC Can Take Advantage of Open Source Evidence and Digital Evidence Repositories, Core Elements of Almost All Grave Crimes Investigations, if They Undertake Cultural, Procedural, and Bureaucratic Changes to Create a More Agile and Open Institutional Environment, ICC Forum, June 2020, available online at https: //iccforum.com/cyber-evidence#Aronson.
- Thomas, 2019, how to hack you're Face to Dodge the Rise of Facial Recognition Tech, Wired, available online at https: //www.wired.co.uk/article/avoid-facial-recognition-software.
- EyeWitness to Atrocities at https: //www.eyewitness.global/welcome, visited 17 February 2021.
- Forensic Architecture for several examples of visualizations and digital reconstructions of airstrikes, chemical weapons and attacks on hospitals in Syria: Syria, Forensic Architecture, available online at https: //forensic-architecture.org/location/syria, visited 17 February 2021.
- Press, 2014, 12 Big Data Definitions: What's Yours?, Forbes, available online at https: //www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitionswhats-yours/?sh¼28b0bd4113ae.
- Hala Systems website available online at https: //halasystems.com/, visited 17 February 2021.
- J. Keegan, 2004, Intelligence in War: The Value-and Limitations-of What the Military can learn about the Enemy.
- J.Y. Khan and M.R. Yuce, 2019, Internet of Things (IoT): Systems and Applications.
- K. Gyarmathy, 2020, Comprehensive Guide to IoT Statistics You Need to Know in 2020, Blog for vxchnge, 26 March 2020, available online at https: //www.vxchnge.com/blog/iot-statistics.
- K. Panetta, 2019, Gartner Top 10 Strategic Technology Trends for 2020, Gartner, 21 October 2019 available online at https: //www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020.
- L. Cameron, Context Aware Ubiquitous Biometrics in Edge of Military Things, IEEE Cloud Computing, available online at https: //www.computer.org/publications/tech-

news/research/internet-of-military-battlefield-things-iomt-iobt, visited 17 February 2021.
- L. Freeman, 2018, Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials', 41 Fordham International Law Journal.
- Licensing of Private Remote Sensing Space Systems (US Federal Register) , 20 May 2020, available online at https: //www.federalregister.gov/documents/ 2020/05/20/2020-10703/licensing-of-private-remote-sensing-space-systems.
- M. Cieslak, 2016, Virtual reality to Aid Auschwitz War Trials of Concentration Camp Guards, BBC News, 20 November 2016, available online at https: //www.bbc.com/news/technology-38026007.
- M. Farfour, 2019, Remote Sensing for Documenting Human Rights Abuses, Citizen Evidence Lab, 11 December 2019, available online at https: //citizenevidence.org/2019/ 12/11/remote-sensingfor-documenting-human-rights-abuses.
- M. Korda, 2018, Widespread Blurring of Satellite Imagery Reveals Secret Facilities, Federation of American Scientists.
- M. Trazzi and R.V. Yampolskiy, 2020, Artificial Stupidity: Data We Need to Make Machines Our Equals.
- N. Lopez and K. Atwell, 2021, Artificial Intelligence in Counterterrorism and Counterinsurgency, with Retired Gen. Stan McChyrstal and Dr. Anshu Roy, Modern War Institute at West Point.
- O. Haj Kadour with J.M. Mojon, 2018, Air Raid Warning Tech Gives Syrians Life-saving Minutes.
- Office of the Prosecutor, International Criminal Court, Strategic Plan 2019-2021, 17 July 2019, available online at https: //www.icc-cpi.int/itemsDocuments/20190726-strategic-planeng.pdf.
- P. Fraga-Lamas et al., 2016, a Review on Internet of Things for Defense and Public Safety, 16 Sensors.
- P.L. Hickman, 2020, The Future of Warfare Will Continue to be Human, War on the Rocks.
- Padgett, supra note 61; M. Alexander Kunz, 2017, Cloak: Remove Unwanted Objects in Video.
- ProofMode at https: //guardianproject.info/apps/org.witness.proofmode/ and Truepic at https: //truepic.com/, websites visited 17 February 2021.
- Poulter, 2021, The Internet of Military Things, available online at https: //www.c-iot.ecs.soton.ac.uk/sites/www.c-iot.ecs.soton.ac.uk/files/AndrewPoulter.pdf.
- Roland and P. Shiman, 2002, Strategic Computing: DARPA and the Quest for Machine Intelligence.
- R. Abdulrahim, 2021, AI Emerges as Crucial Tool for Groups Seeking Justice for Syria War Crimes, Wall Street Journal.
- R. Sammon, 2016, 8 Amazing New Military Technologies, Kiplinger.
- R. Whaley, 2019, the Big Data Battlefield, Military Embedded Systems, Military Embedded Systems.
- S. Padgett, 2019, The Art of Digital Deception Getting Left of Bang on Deep Fakes, Small Wars Journal.

- S. Shetty, 2017, Artificial Intelligence for Google, Amnesty International.
- S. Tzu and S. Griffith, 1964, the Art of War, Clarendon Press.
- S.J. Freedberg Jr., 2019, Attacking Artificial Intelligence: How to Trick the Enemy, Breaking Defense, Breaking Defense.
- SITU Research website, available online at https: //situ.nyc/research/projects/ euromaidan-eventreconstruction, 17 February 2021.
- Synthetic media describes media including videos and images that is either algorithmically created or modified. See also Pathmind, A Beginner's Guide to Generative Adversarial Networks (GANS) , A.I. Wiki.
- T. Thi Nguyen et al., 2020, Deep Learning for Deepfake Creation and Detection: A Survey.
- T. Wood, 2021, what is a Generative Adversarial Network, DeepAI, Deep AI.
- Rights Science, 2021, Carnegie Mellon University.
- war/#:text¼It%20is%20hard%20to%20know, during% 20the% 20Warring% 20States% 20period, visited 17 February 2021.
- The Four V's of Big Data, 2021, IBM Big Data & Analytics Hub, available online at https: //www.ibmbigdatahub.com/infographic/four-vs-big-data.
- Through both wearables and implants. D. Evans, 2015, The Agenda: Introducing the wireless cow, Politico.
- Top 15 Hot Artificial Intelligence Technologies, 2020, Blog of Edureka.
- Top 15 Hot Artificial Intelligence Technologies, 2020, Blog of Edureka.
- UC Berkeley Human Rights Center and Office of the High Commissioner of Human Rights, 2020, Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law.
- Unicef Innovation and Human Rights Center, 2019, UC Berkeley School of Law, Executive Summary: Artificial Intelligence and Children's Rights, UNICEF.
- Videre website, available online at https: //www.videreonline.org/, visited 17 February 2021.
- Voices from DARPA Podcast, 2021, Episode 33: The Verification Virtuoso.
- W.L. Chenery, 1924, New Tools of War Outstrip Those of 1918, the New York Times.
- WITNESS, 2021, Video as Evidence Field Guide.
- Y. Ng, 2020, How to Preserve Open Source Information Effectively, in S. Dubberley, A. Koenig, and D. Murray (eds) , Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability.
- Z. Yang et al., 2019, Deep Transfer Learning for Military Object Recognition under Small Training Set Condition.

Legal Civilization

ISSN: 2873-1841
ISSN: 2873-1922

No.20- Summer 2024