



کمیسیون حقوق بشر اسلامی ایران
Independent Iranian Islamic Human Rights Commission
لجنة حقوق الانسان الاسلاميه في ايران

گزارش مطالعه کمیته مشورتی شورای حقوق بشر سازمان ملل در مورد پیامدهای حقوق بشری فناوری‌های جدید و نوظهور در حوزه نظامی

(ارائه در نشست شصتم شورای حقوق بشر - ۸ سپتامبر تا ۱۳ اکتبر ۲۰۲۵)



امور پژوهشی، آموزشی و ترویجی کمیسیون حقوق بشر اسلامی ایران

تیرماه ۱۴۰۵

اشاره:

با توسعه فناوری های نوین، فرصت ها و چالش های متنوعی پیش روی جامعه بشری ظهور و بروز یافته است. یکی از عرصه های ذیربط مربوط به هوش مصنوعی است. کمتر جامعه ای را می توان یافت که در تلاش برای بهره مندی از هوش مصنوعی نباشد. سرمایه گذاری های عظیم در این زمینه از سوی دولتها و شرکت های خصوصی حکایت از اهمیت برجسته هوش مصنوعی در دنیای کنونی و جهان آینده دارد. یکی از زمینه هایی که ده ها مسئله جدید را برانگیخته و ابهامات و نگرانی های خاص خود را در پی داشته، کاربرد هوش مصنوعی در حوزه نظامی است. کشورهایی که از سطح علمی و فناوری بالاتری برخوردارند و از سال ها قبل برنامه های توسعه هوش مصنوعی و کاربرد آن در اهداف نظامی و امنیتی را مد نظر داشته اند، مدهاست از هوش مصنوعی به شکل هایی بهره می گیرند که آشکارا با موازین بین المللی حقوق بشر همخوانی ندارد و انواع نقض حقوق انسانی را در پی دارد. آمریکا و اسرائیل از جمله بهره برداران برجسته این حوزه هستند که نتایج عملکرد آنها را جامعه بشری در نسل کشی غزه و ده ها جنایت دیگر به عینه دیده اند. همین عملکردها و نگرانی های ذیربط موجب شده که مراکز تحقیقاتی گوناگون متمرکز بر حقوق انسانی یا پیشبرد اخلاق و فعال در سطح بین المللی یا ملی کشورهای مختلف به این موضوع توجه نشان دهند و با بررسی های علمی و میدانی مختلف تلاش نمایند تا ابعاد مسئله به خوبی تبیین و سپس حساسیت ها برای رفع مشکلات و چالش های موجود فراهم شود.

گزارش حاضر یکی از جدیدترین مطالعاتی است که در سطح بین المللی صورت گرفته است. روند تهیه گزارش حاضر بدین صورت بوده که ابتدا شورای حقوق بشر سازمان ملل با توجه به اهمیت موضوع هوش مصنوعی و حقوق بشر لازم دیده است که بررسی مطالعاتی را در خصوص این موضوع با تمرکز بر کاربرد آن در حوزه نظامی به نهاد تابعه خود یعنی کمیته مشورتی شورای حقوق بشر ارجاع دهد. کمیته یاد شده متشکل از ۱۸ کارشناس منتخب شورا که وظیفه ارائه مطالعات مشورتی به شورای حقوق بشر را بر عهده دارد پیرو ارجاع شورا، مشورت های مختلف را با مراکز علمی و مطالعاتی جهانی انجام داده و سپس نتیجه بررسی خود را در قالب گزارش حاضر تدوین و به نشست شصتم شورا در اواخر تابستان ۱۴۰۴ ارائه کرده است. گزارش حاضر از حیث محتوایی حاوی نکات فنی متعددی است که چه بسا هر بند آن باید مورد تامل جدی قرار گیرد.

نظر به اینکه موضوع پیامدهای حقوق بشری هوش مصنوعی در حوزه نظامی در کشورهای مختلف از جمله ایران در مراحل آغازین مطالعات و سیاست گذاری ها قرار دارد، شایسته است سیاست گذاران امور نظامی، امور فناوری و

هوش مصنوعی، مراجع قضایی، مراکز دانشگاهی، شرکت های بخش خصوصی فعال در زمینه هوش مصنوعی و سایر نهادها و افراد ذیربط این قبیل مطالعات را با جدیت مورد توجه قرار دهند تا در فعالیت های ملی در جوار تلاش ها برای پیشرفت توسعه علمی و فناوری های مختلف از جمله هوش مصنوعی، بیش از پیش رعایت حقوق انسانی و اخلاق را مد نظر قرار دهند و همچنین در مواردی که توسط دشمنان کشورمان همانند جنگ ۱۲ روزه یا جنگ رمضان از هوش مصنوعی بر خلاف موازین حقوقی بین المللی انواع سو استفاده ها به عمل آمد و جنایات متعددی شکل گرفت، ابعاد فنی نقض حقوق انسانی به دقت شناسایی و با هوشیاری و عالمانه دفاع موثر از حقوق ملت ایران و حقوق بشریت به عمل آید. یادآوری این نکته ضروری است که در برگردان انگلیسی به فارسی سعی شده هم ارجاعات متن گزارش عینا حفظ شود و هم معادل انگلیسی برخی واژگان مهم بکار رفته در گزارش در ذیل هر صفحه قید گردد تا امکان استفاده تخصصی بیشتر از مطالعه این اثر فراهم گردد. در برخی موارد کلماتی داخل براکت [] اضافه شد و چند مورد نیز توضیحاتی در زیرنویس درج گردید و فهرست مطالب گزارش هم در ابتدای متن افزوده شد.

امور پژوهشی، آموزشی و ترویجی کمیسیون حقوق بشر اسلامی ایران / تیرماه ۱۴۰۵

♦ نویسنده: کمیته مشورتی شورای حقوق بشر سازمان ملل

♦ متصدی روند برگردان انگلیسی به فارسی: خانم مریم صداقتی، مدرس رشته علوم کامپیوتر دانشگاه و همیار افتخاری کمیسیون حقوق بشر اسلامی ایران / ویرایش و نهایی سازی در امور پژوهشی کمیسیون حقوق بشر اسلامی ایران، تیرماه ۱۴۰۵

♦ ماخذ: سامانه اطلاع رسانی شورای حقوق بشر سازمان ملل، اسناد نشست شصتم شورا

♦ شناسه متن: ۰۵/۲/۲۰۱

هر گونه نقل مطالب گزارش حاضر یا باز نشر جزئی یا کلی آن با ذکر ماخذ و رعایت استناد به امور پژوهشی کمیسیون حقوق بشر اسلامی ایران، مجاز است.

امور پژوهشی کمیسیون از هر گونه نظر و پیشنهاد مخاطبان ارجمند به ویژه صاحب نظران و کارشناسان محترم در راستای ارتقای تلاش ها استقبال می کند. مشارکت در فعالیت های عام المنفعه نیز برای همه میسر است.

www.ihrc.ir

فهرست مطالب:

بخش اول) مقدمه

الف- حوزه مأموریت

ب- دامنه مطالعه

پ- چارچوب مفهومی و معیارهای هنجاری

۱. فناوری‌های جدید و نوظهور، حوزه نظامی و فناوری‌های دارای کاربرد دوگانه

۲. چارچوب‌های حقوقی بین‌المللی قابل اعمال در سراسر چرخه حیات فناوری‌های جدید و نوظهور در حوزه نظامی

بخش دوم) تأثیر [بر] حقوق بشر

الف) هوش مصنوعی به عنوان یک فناوری توانمندساز در حوزه نظامی

ب) سامانه‌های تسلیحاتی خودمختار و پیامدهای آنها برای عاملیت انسانی و پاسخگویی

ج) فناوری‌های ارتقای توانمندی‌های انسانی در حوزه نظامی

د) اجرای قانون و کنترل مرزها

ه) جنگ شناختی

و) همگرایی بالقوه هوش مصنوعی و فناوری‌های زیستی، از جمله سلاح‌های زیستی

ز) هوش مصنوعی و سامانه‌های فرماندهی، کنترل و هدایت [نیروهای] هسته‌ای

ح) سلاح‌های انرژی هدایت‌شده

بخش سوم) نقش دولت‌ها و بازیگران غیردولتی در طراحی، آموزش، استقرار، به کارگیری و اکتساب فناوری‌های

جدید و نوظهور در حوزه نظامی

الف) تعهدات دولت‌ها در پیشگیری از نقض حقوق بین‌الملل و تنظیم‌گری و نظارت بر فناوری‌های جدید و نوظهور

در حوزه نظامی

ب) ارائه‌دهندگان و بنگاه‌های فعال در حوزه فناوری‌های جدید و نوظهور در حوزه نظامی

بخش چهارم) حقوق بشر در چرخه عمر فناوری‌های جدید و نوظهور در حوزه نظامی

الف) رویکرد مبتنی بر چرخه عمر

۱. نهادینه‌سازی حقوق بشر در مراحل طراحی و توسعه

۲. مدیریت مخاطرات در مراحل استقرار و به‌کارگیری عملیاتی

۳. تدابیر حفاظتی در مراحل امحاء، خروج از خدمت و پیشگیری از اشاعه [فناوری‌ها]

ب) شفافیت و پاسخگویی

ج) خلأهای موجود در چارچوب کنونی حقوق بشر

توصیه‌ها

الف) دولت‌ها و جامعه بین‌المللی

ب) بنگاه‌های اقتصادی

ج) تمامی ذی‌نفعان

متن سند:

شورای حقوق بشر

شصتین جلسه

۸ سپتامبر تا ۳ اکتبر ۲۰۲۵

دستور کار ۳ و ۵

ترویج و حمایت از همه حقوق بشر، حقوق مدنی، سیاسی، اقتصادی، اجتماعی و فرهنگی، از جمله حق توسعه نهادها و سازوکارهای حقوق بشر

پیامدهای حقوق بشری فناوری‌های جدید و نوظهور در حوزه نظامی

گزارش کمیته مشورتی شورای حقوق بشر [سازمان ملل]

A/HRC/60/63

بخش اول) مقدمه

الف- حوزه ماموریت

۱. این گزارش بر اساس قطعنامه ۵۱/۲۲ شورای حقوق بشر تهیه شده است. در این قطعنامه، شورای حقوق بشر از کمیته مشورتی خود درخواست کرده است که مطالعه‌ای را برای بررسی پیامدهای حقوق بشری فناوری‌های جدید و نوظهور در حوزه نظامی تهیه و ارائه کند.

۱. قطعنامه ۵۱/۲۲ شورای حقوق بشر سازمان ملل متحد (سند A/HRC/RES/51/22) با عنوان «پیامدهای حقوق بشری فناوری‌های جدید و نوظهور در حوزه نظامی» در ۱۷ اکتبر ۲۰۲۲ و در پنجاه و یکمین نشست شورای حقوق بشر، با اجماع و بدون رأی گیری (by consensus) به تصویب رسید. مهم‌ترین نکات این قطعنامه عبارت‌اند از:

ابراز نگرانی درباره تأثیر فناوری‌های نوین نظامی بر حقوق بشر: شورای حقوق بشر تصریح می‌کند که استفاده از فناوری‌های جدید و نوظهور در حوزه نظامی، به‌ویژه سامانه‌های مبتنی بر هوش مصنوعی و تصمیم‌گیری خودکار، ممکن است در برخی شرایط موجب نقض یا تسهیل نقض حقوق بشر شود.

۲. کمیته مشورتی [شورای حقوق بشر] در بیست و نهمین جلسه خود یک گروه برای تهیه و تدوین [ماموریت محوله] متشکل از بوهم سوک باک^۲ (رئیس)، نادیا امل برنوسی^۳، میلنا کاستاس تراسکاساس^۴، الساندر داولسکی^۵، جواهر ماژور^۶، خاویر پالومو^۷ (گزارشگر)، واسیلکا سانسین^۸، واسیلیس تزولکوس^۹، کاترین وان دی هاینینگ^{۱۰}، فرانس ویلجون^{۱۱} و یو ژانگ^{۱۲} شکل داد.

ب- دامنه مطالعه

۳. کمیته مشورتی [شورای حقوق بشر] در این مطالعه، چرخه کامل حیات فناوری‌های جدید و نوظهور در حوزه نظامی را مورد بررسی قرار می‌دهد. این کمیته بررسی می‌کند که حقوق بین‌الملل بشر چگونه فرایند تصمیم‌گیری درباره گردآوری و مدیریت داده‌ها، شفافیت، پاسخگویی، منع تبعیض و حمایت از حقوق بشر را هدایت می‌کند. همچنین، چارچوب‌های حقوقی بین‌المللی قابل اجرا بر طراحی، توسعه، استقرار و نظارت بر به کارگیری این فناوری‌ها را تبیین و کاربرد دوگانه بالقوه آنها (نظامی و غیرنظامی) را تشریح می‌کند.

توجه به خطر تبعیض الگوریتمی: قطعنامه هشدار می‌دهد که اگر این فناوری‌ها بر داده‌های غیرنماینده [از سوی مردم] یا الگوریتم‌های دارای سوگیری متکی باشند، ممکن است تبعیض‌های موجود را تشدید کرده و نتایج غیرقابل پیش‌بینی ایجاد کنند. (توضیح افزوده بر متن)

^۲. Buhm-Suk Baek

^۳. Nadia Amal Bernoussi

^۴. Milena Costas Trascasas

^۵. Alessandra Devulsky

^۶. Jewel Major

^۷. Javier Palummo

^۸. Vasilka Sancin

^۹. Vassilis Tzevelekos

^{۱۰}. Catherine Van de Heyning

^{۱۱}. Frans Viljoen

^{۱۲}. Yue Zhang

۴. این مطالعه شامل تحلیلی از چگونگی نقش معاهدات بین‌المللی موجود، حقوق بین‌الملل عرفی^{۱۳} و اسناد حقوق نرم^{۱۴}، از جمله اصول راهنمای تجارت و حقوق بشر^{۱۵}، در تنظیم، توسعه و استفاده از این فناوری‌ها، و همچنین بررسی اهمیت و نقش‌های مکمل حقوق بین‌الملل بشردوستانه^{۱۶} و حقوق بین‌الملل بشر^{۱۷} در این زمینه می‌باشد.

۵. این مطالعه هم‌چنین به بررسی پیامدهای حقوق بشری فناوری‌های جدید و نوظهور در حوزه نظامی می‌پردازد. در این بررسی، مباحث مطرح‌شده در سازمان ملل متحد، دیدگاه‌ها و مشارکت‌های ذی‌نفعان^{۱۸}، از جمله ۲۲ پاسخ به پرسشنامه^{۱۹} و نیز پژوهش‌های ثانویه مورد استفاده قرار گرفته‌اند تا وضعیت کنونی و نگرانی‌های نوظهور حقوق بشری مرتبط با فناوری‌های جدید و نوظهور در حوزه نظامی تحلیل شوند. این تحلیل با رویکردی آینده‌نگر انجام شده و سناریوهای احتمالی ناشی از ظهور فناوری‌های جدید را نیز مدنظر قرار می‌دهد. بخش پایانی این مطالعه به ارائه توصیه‌هایی برای اقدامات آتی اختصاص یافته است.

پ-چارچوب مفهومی و معیارهای هنجاری

۱. فناوری‌های جدید و نوظهور، حوزه نظامی و فناوری‌های دارای کاربرد دوگانه

۶. از منظر این گزارش، حوزه نظامی به محیط عملیاتی نیروهای مسلح و فعالیت‌های مرتبط با دفاع، از جمله نیروهای امنیتی اطلاق می‌شود. فناوری‌های جدید و نوظهور به فناوری‌هایی گفته می‌شود که در حال توسعه هستند یا به‌تازگی معرفی شده‌اند و معمولاً به دلیل ظرفیت تحول‌آفرین^{۲۰} خود شناخته می‌شوند. از آنجا که این فناوری‌ها حاصل پیشرفت در حوزه‌های مختلف، به‌ویژه هوش مصنوعی، علوم اعصاب، زیست‌فناوری، فناوری نانو و رباتیک

^{۱۳}: Customary international law

^{۱۴}: Soft law instruments

^{۱۵}: Guiding Principles on Business and Human Rights

^{۱۶}: International humanitarian law

^{۱۷}: International human rights law

^{۱۸}: Stakeholder contributions

^{۱۹}. برای ملاحظه پرسشنامه و پاسخ‌ها به لینک زیر مراجعه کنید:

www.ohchr.org/en/hr-bodies/hrc/advisory-committee/human-rights-implications

^{۲۰}: Operational environment

^{۲۱}: Transformative potential

هستند، فناوری‌های جدید و نوظهور در حوزه نظامی همواره مترادف با تسلیحات نیستند. به این معنا که اگرچه برخی تسلیحات از فناوری‌های جدید و نوظهور بهره می‌برند، اما همه فناوری‌های جدید و نوظهور در حوزه نظامی را نمی‌توان تسلیحات دانست.^{۲۲} با توجه به ماهیت دوگانه این فناوری‌ها، یافتن فناوری‌های جدید و نوظهور در حوزه نظامی که از نوآوری‌های فناورانه تأثیر نپذیرفته باشند، دشوار است. همان‌گونه که نوآوری‌های فناورانه را نیز نمی‌توان صرفاً به حوزه نظامی محدود کرد. فناوری‌های دارای کاربرد دوگانه^{۲۳} به نوآوری‌هایی اطلاق می‌شود که هم کاربردهای غیرنظامی و هم کاربردهای نظامی دارند و قابلیت استفاده در بخش‌های تجاری، عمومی و نظامی را دارا هستند.^{۲۴} در نتیجه، چارچوب مفهومی این گزارش باید چارچوبی انعطاف‌پذیر و با مرزهای نفوذپذیر^{۲۵} تلقی شود زیرا تعیین حدود دقیق این دسته‌بندی‌ها دشوار است.

۷. اگرچه تسلیحات نظامی همواره از فناوری‌های نوین بهره برده‌اند، پیشرفت‌های دیجیتال امروز، به‌ویژه در حوزه هوش مصنوعی، جهشی چشمگیر در این روند ایجاد کرده است. این دگرگونی بنیادین^{۲۶} در بستر از شکاف فناورانه^{۲۷} و عدم تقارن قدرت^{۲۸} رخ می‌دهد؛ وضعیتی که در آن فناوری‌های نظامی توسعه‌یافته در برخی نقاط جهان ممکن است در کشورهایی به کار گرفته شوند که نفوذ یا نقش محدودی در فرایند توسعه آن فناوری‌ها داشته‌اند. برای نمونه، کشورهای جنوب جهانی^{۲۹} (مجموعه کشورهای در حال توسعه یا کمتر توسعه‌یافته) غالباً از فرایند توسعه و حکمرانی فناوری‌های جدید و نوظهور در حوزه نظامی کنار گذاشته می‌شوند، در حالی که جمعیت آن‌ها ممکن است به‌طور نامتناسب بیش از دیگران از به‌کارگیری این فناوری‌ها متأثر شوند.^{۳۰}

۸. فناوری‌های جدید و نوظهور در حوزه نظامی، چالش‌های قابل توجهی را برای دولت‌ها و سایر بازیگران در رعایت تعهدات ناشی از حقوق بین‌الملل بشر ایجاد می‌کنند. در بنیادی‌ترین سطح، استفاده از این فناوری‌ها در حوزه نظامی خطر انسان‌زدایی از به‌کارگیری زور^{۳۱} را در پی دارد؛ به‌گونه‌ای که روندهایی را تشدید می‌کند که در آن، از طریق

^{۲۲}. برای مطالعه بیشتر در این زمینه به لینک زیر مراجعه کنید

international-conference_military-technologies-vis-a-vis-human-rights-concerns_-summary-report.pdf

^{۲۳}. Dual-use technologies

^{۲۴}. Marcello Ienca and Effy Vayena, "Dual use in the 21st century", Swiss Medical Weekly, vol. 148, No. 4748 (2018); and Marcus Schulzke, "Drone proliferation and the challenge of regulating dual-use

^{۲۵}. Porous conceptual framework

^{۲۶}. Paradigm shift

^{۲۷}. Technological divide

^{۲۸}. Power asymmetry

^{۲۹}. Global South

^{۳۰}. Disproportionately affected

^{۳۱}. Dehumanizing the use of force

برچسب‌گذاری و هدف‌گیری الگوریتمی^{۳۲} جان انسان‌ها به صرف نقاط داده تقلیل می‌یابد، ملاحظات اخلاقی و ارزشی ذاتی قضاوت انسانی^{۳۳} گم‌رنگ یا حتی حذف می‌شود و خطر استفاده خودسرانه و نامتناسب از زور افزایش می‌یابد. چنین انسان‌زدایی با اصول حقوق بشر از جمله حق حیات، حق بر تمامیت جسمی و روانی^{۳۴}، اصل منع تبعیض و کرامت انسانی^{۳۵} (که از ارکان بنیادین حقوق بین‌الملل بشر و بسیاری از نظام‌های حقوقی داخلی به شمار می‌رود) ناسازگار است. افزون بر این، فناوری‌های جدید و نوظهور در حوزه نظامی ممکن است آثار و پیامدهای متفاوتی بر حقوق بشر گروه‌های مختلف جامعه بر جای گذارند^{۳۶}.

۹. یکی از نگرانی‌های اساسی درباره فناوری‌های جدید و نوظهور در حوزه نظامی، میزان حفظ کنترل معنادار انسان بر این فناوری‌ها، به‌ویژه فناوری‌های مرتبط با به‌کارگیری زور، از جمله سامانه‌های تسلیحاتی خودمختار^{۳۷} و سایر سامانه‌های مسلح بدون سرنشین^{۳۸} است. این فناوری‌ها بر خودکارسازی و تصمیم‌گیری خودمختار متکی هستند و از این‌رو، خطر کاهش نظارت انسانی^{۳۹}، تضعیف پاسخگویی^{۴۰} را به همراه دارند. فناوری‌های خودمختار جدید و نوظهور در حوزه نظامی ممکن است به نقض‌های جدی حقوق بشر منجر شود؛ از جمله تهدید حق حیات^{۴۱}، آزادی بیان^{۴۲}، حریم خصوصی و اصل منع تبعیض^{۴۳} و نیز نقض‌های ممنوعیت سو رفتار^{۴۴}. از این‌رو، تمامی مراحل چرخه حیات این فناوری‌ها باید تابع یک چارچوب مستحکم حمایت از حقوق بشر باشد تا اطمینان حاصل شود که پیشرفت‌های فناورانه به تضعیف حقوق بشر نمی‌انجامد و قربانیان نیز به سازوکارهای پاسخگویی و جبران خسارت دسترسی مؤثر داشته باشند.

^{۳۲}. Algorithmic labelling and targeting

^{۳۳}. Christof Heyns, "Autonomous weapons in armed conflict and the right to a dignified life", South African Journal on Human Rights, vol. 33, No. 1 (2017)

^{۳۴}. Personal integrity

^{۳۵}. Human dignity

^{۳۶}. در این زمینه می‌توانید مراجعه کنید به :

International Conference of the Red Cross and Red Crescent, resolution 34IC/24/R2.

^{۳۷}. Meaningful human control

^{۳۸}. Autonomous weapons systems

^{۳۹}. Armed uncrewed systems

^{۴۰}. Human oversight

^{۴۱}. Accountability

^{۴۲}. Threats to the rights to life

^{۴۳}. Freedom of expression

^{۴۴}. Privacy and non-discrimination

^{۴۵}. Violations of the prohibition of ill-treatment

۱۰. چالش دیگری که در این زمینه این است که فناوری‌های جدید و نوظهور در حوزه نظامی (از کالاهای و سخت‌افزارهای رایانه‌ای گرفته تا نرم‌افزارها) به عنوان «فناوری‌های دارای کاربرد دوگانه»^{۴۶} شناخته می‌شوند و قابلیت استفاده در حوزه‌های تجاری، عمومی و نظامی را دارند. با توجه به شکاف‌های احتمالی میان چارچوب‌های حقوقی و استفاده یا به کارگیری فناوری‌های جدید و نوظهور، ضروری است نگرانی‌های نوظهور حقوق بشری پیش از آنکه این فناوری‌ها وارد مرحله بهره‌برداری عملیاتی شوند^{۴۷}، به‌ویژه در شرایط مخاصمات مسلحانه^{۴۸}، مورد توجه و رسیدگی قرار گیرند. این مخاطرات با توجه به نقش محوری بخش خصوصی در توسعه فناوری‌های جدید و نوظهور، بیش از پیش تشدید می‌شوند. از این رو، بنگاه‌های اقتصادی^{۴۹} نقشی اساسی در پیشگیری از نقض‌ها و سوءاستفاده‌های حقوق بشری بر عهده دارند.

۲. چارچوب‌های حقوقی بین‌المللی قابل اعمال در سراسر چرخه حیات فناوری‌های جدید و نوظهور در حوزه نظامی

۱۱. حقوق بین‌الملل، اعم از حقوق مبتنی بر معاهدات^{۵۱} و حقوق بین‌الملل عرفی^{۵۲}، بر توسعه و استفاده از فناوری‌های جدید و نوظهور در حوزه نظامی حاکم است و دولت‌ها مکلف به رعایت آن هستند. افزون بر این، دولت‌ها تعهدی ایجابی^{۵۳} بر عهده دارند تا در مواردی که این فناوری‌ها توسط بازیگران غیردولتی تابع صلاحیت آن‌ها^{۵۴} به کار گرفته می‌شوند، رعایت این قواعد را تضمین کنند. تمامی مراحل چرخه حیات فناوری‌های جدید و نوظهور در

^{۴۶}. Dual-use technologies

^{۴۷}. Become operational

^{۴۸}. Conflict settings

^{۴۹}. Businesses

^{۵۰}. Human rights violations and abuses

^{۵۱}. Treaty-based law

^{۵۲}. Customary law

^{۵۳}. Positive duty

^{۵۴}. Non-State actors falling under their jurisdiction

حوزه نظامی تحت حاکمیت و شمول^{۵۵} مجموعه‌ای از چارچوب‌های حقوقی بین‌المللی قرار دارند^{۵۶} که [این قواعد حقوقی] به صورت مکمل و تقویت کننده یکدیگر^{۵۷} اعمال می‌شوند.^{۵۸}

۱۲. حقوق بین‌الملل بشر^{۵۹} نقش اساسی در تنظیم و حکمرانی بر فناوری‌های جدید و نوظهور در حوزه نظامی ایفا می‌کند و هم در زمان صلح و هم در جریان مخاصمات مسلحانه قابل اعمال است. برخی حقوق بشر، حتی در زمان مخاصمات مسلحانه نیز، غیرقابل تعلیق هستند؛ از جمله حق حیات^{۶۰}، ممنوعیت شکنجه و سایر رفتارها یا مجازات‌های ظالمانه، غیرانسانی یا تحقیرآمیز، ممنوعیت بردگی و بندگی^{۶۱}، و نیز اصول قانونی بودن^{۶۲}، عطف به ماسبق نشدن قوانین^{۶۳} و آزادی اندیشه، وجدان و مذهب.^{۶۴}

۱۳. از مهم ترین اسناد بین‌المللی مرتبط با فناوری‌های جدید و نوظهور در حوزه نظامی می‌توان به «منشور بین‌المللی حقوق بشر»^{۶۵} و سایر اسناد بنیادین حقوق بین‌الملل بشر اشاره کرد. با توجه به ظرفیت این فناوری‌ها برای استفاده در نظارت گسترده و اعمال تبعیض‌آمیز، رعایت اصول شفافیت و پاسخگویی در این زمینه از اهمیت اساسی برخوردار است. حقوقی همچون حق بر حریم خصوصی، آزادی بیان و اصل منع تبعیض، و نیز حقوق مرتبط با سلامت، فرهنگ و کار، باید در تمامی مراحل طراحی، توسعه و استقرار این فناوری‌ها مورد حمایت و صیانت قرار گیرند. همچنین، ممنوعیت شکنجه و سایر رفتارها یا مجازات‌های ظالمانه، غیرانسانی یا تحقیرآمیز بر نحوه استفاده از این فناوری‌ها نیز

°° Governed by

۵۶. این شامل سایر حوزه‌های حقوق بین‌الملل (مثلاً حقوق محیط زیست و کار) نیز می‌شود. گروه‌هایی از کشورها نیز بیانیه‌ها، تعهدات و ضوابط رفتاری مرتبطی را تصویب کرده‌اند.

۵۷. Complementary and mutually reinforcing manner

۵۸. International Legal Protection of Human Rights in Armed Conflict (United Nations publication, 2011). See also Human Rights Council resolution 51/22.

۵۹. International human rights law

۶۰. Non-derogable rights

۶۱. مراجعه کنید به:

Human Rights Committee, general comment No. 36 (2018).

۶۲. Servitude

۶۳. Principle of legality

۶۴. Non-retroactivity

۶۵. مراجعه کنید به:

Human Rights Committee, general comment No. 29 (2001).

۶۶. International Bill of Human Rights

منظور ترکیب سه سند بین‌المللی مبنایی نظام بین‌المللی حقوق بشر است شامل: اعلامیه جهانی حقوق بشر، میثاق بین‌المللی حقوق مدنی و سیاسی و میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی (توضیح افزوده بر متن)

حاکم است. اصل منع تبعیض در این حوزه از اهمیت ویژه‌ای برخوردار است، زیرا فناوری‌های جدید و نوظهور، در صورتی که الگوریتم‌های آن‌ها به‌درستی طراحی و نظارت نشوند، می‌توانند سوگیری‌ها و تبعیض‌های موجود علیه گروه‌های حاشیه‌نشین و آسیب‌پذیر را تقویت کنند. دولت‌ها باید اطمینان حاصل کنند که توسعه و استفاده از فناوری‌های جدید و نوظهور در حوزه نظامی با الزامات حقوق بین‌الملل بشر مطابقت دارد و برای موارد نقض حقوق بشر، راهکارهای جبرانی مؤثر فراهم می‌شود. بنگاه‌های اقتصادی و سایر اشخاص تجاری که در توسعه یا استقرار این فناوری‌ها مشارکت دارند نیز باید مطابق «اصول راهنمای کسب‌وکار و حقوق بشر» عمل کنند، از نقض حقوق بشر اجتناب ورزند و به‌صورت پیشگیرانه برای شناسایی و کاهش مخاطرات بالقوه حقوق بشری در فعالیت‌های خود اقدام نمایند.

۱۴. حقوق بین‌الملل بشردوستانه نیز نقش بنیادینی در تنظیم و حکمرانی بر فناوری‌های جدید و نوظهور در حوزه نظامی ایفا می‌کند. اگرچه برخی معاهدات به‌طور خاص به تنظیم یا ممنوعیت برخی انواع تسلیحات می‌پردازند، اما کنوانسیون‌های ژنو و پروتکل‌های الحاقی آن‌ها بر تمامی اشکال جنگ و همه انواع تسلیحات، از جمله تسلیحاتی که هنوز توسعه نیافته‌اند، حاکم هستند؛ امری که توسط دیوان بین‌المللی دادگستری^{۶۷} نیز مورد تأیید قرار گرفته است.^{۶۸} ماده ۳۶ پروتکل الحاقی به کنوانسیون‌های ژنو مورخ ۱۲ اوت ۱۹۴۹ درباره حمایت از قربانیان مخاصمات مسلحانه بین‌المللی (پروتکل اول)، دولت‌های عضو را ملزم می‌کند بررسی کنند که آیا سلاح‌ها، وسایل یا روش‌های جدید جنگی که در حال مطالعه، توسعه، تحصیل یا پذیرش آن‌ها هستند، بر اساس این پروتکل یا سایر قواعد حقوق بین‌الملل ممنوع محسوب می‌شوند یا خیر. اگرچه این مقرر از لحاظ حقوقی تنها برای دولت‌های عضو این پروتکل الزام‌آور است، برخی دولت‌های غیرعضو نیز فرایند بررسی حقوقی تسلیحات را انجام می‌دهند.

۱۵. کنوانسیون منع یا محدودیت کاربرد برخی سلاح‌های متعارف^{۶۹} با هدف ممنوع یا محدود کردن استفاده از برخی انواع سلاح‌هایی تدوین شده است که موجب رنج غیرضروری یا ناموجه رزمندگان یا اثرگذاری بی‌هدف بر غیرنظامیان می‌شوند. پروتکل‌های الحاقی این کنوانسیون، استفاده از سلاح‌های مشخص و نیز توسعه فناوری‌های تسلیحاتی را بر پایه سه اصل بنیادین حقوق بین‌الملل بشردوستانه تنظیم می‌کنند:

^{۶۷} International Court of Justice

^{۶۸} Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, para. 86

^{۶۹} Convention on Certain Conventional Weapons (CCW)

الف) حق طرف‌های مخاصمه مسلحانه در انتخاب روش‌ها یا ابزارهای جنگ نامحدود نیست.

ب) جمعیت غیرنظامی باید در برابر آثار ناشی از مخاصمات حمایت شوند.

ج) وارد کردن آسیب‌های زائد یا تحمیل رنج غیرضروری به رزمندگان ممنوع است.

علاوه بر این، گروه کارشناسان دولتی درباره فناوری‌های نوظهور در حوزه سامانه‌های تسلیحاتی خودمختار^{۷۲} بار دیگر تأکید کرده است که حقوق بین‌الملل بشردوستانه همچنان به‌طور کامل بر توسعه و استفاده احتمالی از سامانه‌های تسلیحاتی خودمختار^{۷۳} گشوده حاکم است.

۱۶. حقوق بین‌الملل بشردوستانه همچنان نقشی اساسی در حمایت از غیرنظامیان در برابر آثار مخاصمات مسلحانه، در مواجهه با پیشرفت شتابان فناوری، ایفا می‌کند. از این رو، دولت‌ها مکلف‌اند صرف‌نظر از تحولات علمی و فناوری، رعایت قواعد آن را تضمین کنند.^{۷۴} حتی اگر دولت‌ها عضو معاهدات پیش‌تر ذکر شده نباشند، همچنان به موجب حقوق بین‌الملل عرفی، که چندین هنجار از آن ماهیت آمرانه^{۷۵} دارند، متعهد هستند. دولت‌ها همچنین موظف به رعایت تعهدات ناشی از اصل نظارت و دقت لازم^{۷۶} [رعایت حقوق بشر]^{۷۶} هستند؛ بدین معنا که باید تمامی اقدامات مقتضی را برای پیشگیری از نقض تعهدات بین‌المللی، از جمله از طریق وضع قوانین و مقررات و اتخاذ تدابیر لازم، به عمل آورند. افزون بر این، آن‌ها مکلف به اجرای تکلیف مراقبت^{۷۷} نیز هستند که نسبت به فعالیت‌های بازیگران دولتی و خصوصی اعمال می‌شود.^{۷۸} شایان ذکر است که تعهد به نظارت و دقت لازم^{۷۹} [رعایت حقوق بشر]، «تعهد به وسیله»^{۷۹} است و نه «تعهد به نتیجه»^{۸۰}.

^{۷۰} Superfluous injury

^{۷۱} Unnecessary suffering upon combatants

^{۷۲} Lethal Autonomous Weapons Systems (LAWS)

^{۷۳} CCW/GGE.1/2023/2, para. 21 (a)

^{۷۴} . حقوق معاهدات نیز در این زمینه قابل اجرا است (به عنوان مثال پروتکل اول الحاقی به کنوانسیون‌های ژنو ۱۹۴۹)

^{۷۵} Jus cogens

^{۷۶} Due diligence

^{۷۷} Duty of vigilance

^{۷۸} International Court of Justice, Pulp Mills on the River Uruguay (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p.14, para. ۱۹۷.

^{۷۹} Obligation of means

^{۸۰} Obligation of result

۱۷. تعهد به تضمین اینکه توسعه فناوری‌های جدید و نوظهور در حوزه نظامی به نقض حقوق بین‌الملل منجر نشود، از جمله تعهدات اولیه^{۸۱} هر کشوری است.^{۸۲} از این رو، دولت‌ها باید ارزیابی‌های جامع و فراگیری^{۸۳} انجام دهند تا مشخص شود قواعد خاص حقوق بین‌الملل چگونه بر فناوری‌های جدید و نوظهور در حوزه نظامی اعمال می‌شوند. در این زمینه، نهادهای ملی حقوق بشر باید نقش مؤثر و شایسته‌ای ایفا کنند.^{۸۴} همچنین، بازنگری به موقع^{۸۵} قوانین داخلی هر دولت برای شناسایی و رفع هرگونه ناسازگاری با حقوق بین‌الملل از اهمیت اساسی برخوردار است.

۱۸. با وجود چارچوب‌های حقوقی موجود، پیشرفت شتابان فناوری‌های جدید و نوظهور در حوزه نظامی، اجرای مؤثر این چارچوب‌ها را با چالش مواجه ساخته است. این وضعیت، مباحث و گفت‌وگوهای گسترده‌ای را درباره نحوه اعمال حقوق بین‌الملل بر فناوری‌های جدید و نوظهور در حوزه نظامی برانگیخته است؛ از جمله در زمینه تصمیم‌گیری مبتنی بر هوش مصنوعی^{۸۶}؛ سامانه‌های تسلیحاتی خودمختار، سامانه‌های بدون سرنشین^{۸۷} و برنامه‌های نظامی با هدف ارتقای توانایی‌های جسمی و شناختی رزمندگان. اگرچه هوش مصنوعی و سایر فناوری‌های جدید و نوظهور مفاهیم و اصطلاحات جدیدی را وارد این حوزه کرده‌اند، ذی‌نفعان باید اطمینان حاصل کنند که این مفاهیم و اصطلاحات با زبان، مفاهیم و استانداردهای حقوق بین‌الملل همسو و منطبق باشند.^{۸۸}

بخش دوم) تأثیر [بر] حقوق بشر

الف) هوش مصنوعی به عنوان یک فناوری توانمندساز در حوزه نظامی

۱۹. در حوزه نظامی، هوش مصنوعی به عنوان یک فناوری توانمندساز^{۸۹} کلیدی عمل می‌کند و قابلیت‌های عملیاتی را در طیف گسترده‌ای از کارکردها ارتقا می‌بخشد. در این زمینه، تمایز میان فناوری‌های مبتنی بر هوش مصنوعی^{۹۰}

^{۸۱} Primary obligation

^{۸۲} International Committee of the Red Cross (ICRC), Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons (Geneva, 2016).

^{۸۳} Conduct comprehensive evaluations

^{۸۴} Digital Rights Alliance submission

^{۸۵} Timely review

^{۸۶} AI-driven decision-making

^{۸۷} Uncrewed systems

^{۸۸} . مراجعه کنید به:

committees.parliament.uk/writtenevidence/120290/pdf

^{۸۹} Enabling technology

^{۹۰} AI-enabled technologies

(یعنی ابزارها و سامانه‌هایی که با بهره‌گیری از هوش مصنوعی از تصمیم‌گیری انسان پشتیبانی می‌کنند) و سامانه‌های خودمختار^{۹۱} از جمله سامانه‌های تسلیحاتی خودمختار که می‌توانند با مداخله محدود یا بدون مداخله انسان عمل کنند، اهمیت اساسی دارد. اگرچه هوش مصنوعی می‌تواند در فرایند تصمیم‌گیری به انسان کمک کند، اما همه سامانه‌های مبتنی بر هوش مصنوعی خودمختار نیستند و متقابلاً، خودمختاری نیز لزوماً مستلزم استفاده از هوش مصنوعی نیست. این بخش بر نقش هوش مصنوعی به‌عنوان ابزاری برای ارتقای توانمندی‌ها^{۹۲}، در چارچوب نظارت انسانی^{۹۳} تمرکز دارد.

۲۰. اگرچه هوش مصنوعی چندین دهه است که در حال توسعه بوده و می‌توان آن را فناوری نوظهوری با سابقه‌ای طولانی^{۹۴} دانست، نقش آن در افزایش خودمختاری سامانه‌های تسلیحاتی، پشتیبانی از فرایند تصمیم‌گیری نظامی^{۹۵} و ادغام در زنجیره‌های تأمین نظامی^{۹۶} در سال‌های اخیر به‌طور چشمگیری برجسته شده است. پیشرفت‌های اخیر در حوزه توان محاسباتی^{۹۷} نیز نقش هوش مصنوعی را در این زمینه‌ها بیش از پیش تقویت کرده است.^{۹۸}

۲۱. هوش مصنوعی به‌طور فزاینده‌ای در عملیات نظامی ادغام شده و برای ارتقای تحلیل اطلاعات^{۹۹}، برنامه‌ریزی سناریوها^{۱۰۰}، پشتیبانی لجستیکی و تصمیم‌گیری در میدان نبرد به‌کار گرفته می‌شود. سامانه‌های هوش مصنوعی می‌توانند با درجات متفاوتی از خودمختاری عمل کنند. باین‌حال، روند کلی آن است که هرچه میزان خودمختاری این سامانه‌ها افزایش یابد، نظارت و کنترل انسانی کاهش می‌یابد. برای مثال هوش مصنوعی می‌تواند از طریق پردازش سریع حجم عظیمی از داده‌ها، به فرایند تصمیم‌گیری کمک کند و حتی در برخی سناریوهای از پیش تعیین‌شده، مانند شرایط پرفشار، این ظرفیت را داشته باشد که قضاوت انسانی را نادیده بگیرد. با وجود این، استفاده از هوش مصنوعی نگرانی‌های جدی حقوق بشری را نیز به همراه دارد؛ از جمله در ارتباط با آزادی بیان، حق بر حریم خصوصی و اصل منع تبعیض. برای مثال، ممکن است یک سامانه هوش مصنوعی یک وسیله کمکی مورد استفاده افراد دارای

^{۹۱} Autonomous systems

^{۹۲} Enhancement tool

^{۹۳} Human oversight

^{۹۴} Long-standing emerging technology

^{۹۵} Military decision-making

^{۹۶} Military supply chains

^{۹۷} Computing advances

^{۹۸} Stefka Schmid, Thea Riebe and Christian Reuter, "Dual-use and trustworthy?", Science and Engineering Ethics, vol. 28, No. 2 (March 2022).

^{۹۹} Intelligence analysis

^{۱۰۰} Scenario planning

معلولیت^{۱۱} را به اشتباه به عنوان سلاح شناسایی کند و بدین ترتیب اصل منع تبعیض را نقض کند.^{۱۲} افزون بر این، سوگیری‌های الگوریتمی می‌توانند به تبعیض نژادی یا جنسیتی منجر شوند. از این رو، رعایت کرامت انسانی، آن گونه که موازین بین‌المللی حقوق بشر اقتضا می‌کند، باید در تمامی مراحل چرخه حیات هوش مصنوعی تضمین شود تا ارزش و منزلت برابر همه افراد^{۱۳} حفظ گردد.^{۱۴}

۲۲. هوش مصنوعی ممکن است نظارت انسانی و نیز توانایی انسان در اعمال قضاوت اخلاقی یا حقوقی^{۱۵} نسبت به نتایج و خروجی‌های آن را محدود کند. چالش اساسی در این زمینه آن است که مشخص شود حقوق بین‌الملل، تا چه میزان و در چه مواردی، وجود کنترل انسانی را در فرایندهایی مانند هدف‌گیری، بازداشت، استفاده از تسلیحات و صیانت از کرامت انسانی^{۱۶} الزامی می‌داند. این امر مستلزم رعایت چارچوب‌های حقوقی بین‌المللی، از جمله اعلامیه جهانی حقوق بشر است که تصریح می‌کند همه انسان‌ها «از خرد و وجدان برخوردارند و باید با یکدیگر با روحیه برادری [و همبستگی] رفتار کنند».

۲۳. یکی دیگر از مسائل اساسی، فقدان شفافیت در فرایند تصمیم‌گیری هوش مصنوعی است؛ به گونه‌ای که بسیاری از سامانه‌های هوش مصنوعی به صورت «جعبه سیاه»^{۱۷} عمل می‌کنند و از این رهگذر، اصول حقوق بشری شفافیت و دسترسی به جبران مؤثر^{۱۸} را با چالش مواجه می‌سازند. چارچوب‌های موجود مسئولیت^{۱۹} که بر مبنای کنش و تصمیم انسان شکل گرفته‌اند، ممکن است در نتیجه ادغام با هوش مصنوعی، به‌ویژه در سامانه‌های مبتنی بر یادگیری ماشین^{۲۰} دستخوش اختلال شوند. تضمین وجود خطوط روشن و مشخص مسئولیت^{۲۱} امری ضروری است اما هنگامی که هوش مصنوعی با درجه بالایی از خودمختاری عمل می‌کند یا فرایند استدلال و تصمیم‌گیری آن غیرشفاف است، تحقق این امر با دشواری همراه می‌شود. پاسخگویی نه تنها شامل اقدامات پیشگیرانه، بلکه مستلزم ارزیابی‌های

^{۱۱} Disability assistive device

^{۱۲} A/HRC/49/52, para. 54

^{۱۳} Equal worth for all individuals

^{۱۴} United Nations Educational, Scientific and Cultural Organization, Recommendation on the Ethics of Artificial Intelligence.

^{۱۵} Exercise moral or legal judgment

^{۱۶} Safeguarding human dignity

^{۱۷} Black boxes

^{۱۸} Effective remedy

^{۱۹} Responsibility frameworks

^{۲۰} Machine learning

^{۲۱} Clear lines of responsibility

پسینی^{۱۲} درباره نقض‌های احتمالی حقوق بین‌الملل نیز هست. در این زمینه، سازوکارهای اصلی پاسخگویی بین‌المللی هم در خصوص مسئولیت کیفری افراد و هم در خصوص مسئولیت بین‌المللی دولت‌ها^{۱۳} قابل اعمال هستند.

۲۴. از منظر حقوق بشر، یکی دیگر از نگرانی‌های مهم آن است که فناوری‌های جدید و نوظهور در حوزه نظامی، به‌ویژه فناوری‌های مبتنی بر هوش مصنوعی، مقادیر قابل توجهی انرژی مصرف می‌کنند، انتشار گسترده گازهای گلخانه‌ای و کربن^{۱۴} به همراه دارند و وابستگی زیادی به مواد خامی همچون نیکل، کبالت و گرافیت دارند. این امر مخاطرات بلندمدتی، از جمله برای حق برخورداری از محیط‌زیستی پاک، سالم و پایدار، ایجاد می‌کند. از این رو، همگام با تکامل و گسترش این فناوری‌ها، توجه به پیامدهای زیست‌محیطی و حقوق بشری آن‌ها و اتخاذ تدابیر لازم برای مواجهه با این آثار، امری ضروری است.

ب) سامانه‌های تسلیحاتی خودمختار و پیامدهای آن‌ها برای عاملیت انسانی و پاسخگویی

۲۵. سامانه‌های تسلیحاتی خودمختار می‌توانند با مداخله محدود یا بدون مداخله انسان، تصمیم‌هایی را به‌طور مستقل اتخاذ کنند. سامانه‌های تسلیحاتی خودمختار^{۱۵} گشوده، که زیرمجموعه‌ای از سامانه‌های تسلیحاتی خودمختار به شمار می‌روند، به دلیل توانایی خود در اجرای مستقل تصمیم‌هایی که ممکن است متضمن استفاده از نیروی مرگبار^{۱۶} باشند، از اهمیت ویژه‌ای برخوردارند. یکی از چالش‌های حقوقی در این زمینه، تعریف سامانه‌های تسلیحاتی خودمختار است؛ زیرا میزان مداخله و کنترل انسانی در این سامانه‌ها می‌تواند متفاوت باشد. افزون بر این، فقدان اجماع میان دولت‌ها درباره ارائه یک تعریف حقوقی از این سامانه‌ها، تنظیم‌گری و تدوین قواعد حاکم^{۱۷} بر آن‌ها را با دشواری بیشتری مواجه کرده است^{۱۸}.

^{۱۲} Ex-post evaluations

^{۱۳} State responsibility

^{۱۴} Carbon emissions

^{۱۵} Lethal force

^{۱۶} Regulation

^{۱۷} مراجعه کنید به:

[www.docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_\(2023\)/CCW_GGE1_2023_CRP.1_0.pdf](http://www.docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf).

۲۶. برخلاف سامانه‌های تصمیم‌گیری خودکار که بر اساس دستورات و معیارهای از پیش تعیین‌شده عمل می‌کنند، سامانه‌های تسلیحاتی خودمختار به گونه‌ای طراحی شده‌اند که با سطوح بالاتری از خودمختاری عمل کنند. از این رو، این سامانه‌ها پرسش‌های حقوقی پیچیده‌ای را درباره میزان انطباق آن‌ها با حقوق بین‌الملل مطرح می‌کنند. برای نمونه، این سامانه‌ها چالش‌های منحصربه‌فردی را در زمینه کرامت انسانی، کنترل انسانی و شفافیت ایجاد می‌کنند که بر حقوقی همچون حق حیات، حق برخورداری از جبران مؤثر^{۱۱۸} و حق بر حریم خصوصی تأثیر می‌گذارند.^{۱۱۹} در حوزه حقوق بین‌الملل بشردوستانه نیز، مهم‌ترین چالش‌ها به اصول تفکیک^{۱۲۰}، اصل تناسب^{۱۲۱}، احتیاط در حمله^{۱۲۲} و الزام به انجام بررسی حقوقی تسلیحات^{۱۲۳} مربوط می‌شود.

۲۷. طرفداران ممنوعیت سامانه‌های تسلیحاتی خودمختار استدلال می‌کنند که این سامانه‌ها ممکن است با شرط مارتنس^{۱۲۴} مقرر می‌دارد در مواردی که قاعده و قراردادی مشخصی وجود ندارد، اصول انسانیت و مقتضیات وجدان عمومی همچنان بر رفتار طرف‌های مخاصمه حاکم خواهند بود. مندرج در کنوانسیون حل و فصل مسالمت‌آمیز اختلافات بین‌المللی مغایرت داشته باشند؛ شرطی که بر اساس آن، سلاح‌ها باید با «اصول انسانیت و مقتضیات وجدان عمومی» مطابقت داشته باشند.^{۱۲۵} با این حال، آنان غالباً شرط مارتنس را بیش از آنکه مبنایی برای ممنوعیت کامل این سامانه‌ها بدانند، مبنایی برای تنظیم‌گری و وضع قواعد حاکم بر آن‌ها تلقی می‌کنند. در مقابل، مخالفان ممنوعیت حتی ممکن است ارزش حقوقی این شرط را نیز مورد تردید قرار دهند.^{۱۲۶}

۲۸. با وجود اجماع کلی درباره ضرورت حفظ کنترل معنادار انسان^{۱۲۷} بر سامانه‌های تسلیحاتی خودمختار، هنوز مقررات و استانداردهای بین‌المللی مشخصی برای تضمین چنین کنترلی بر استفاده از زور^{۱۲۸} وجود ندارد.^{۱۲۹}

^{۱۱۸} Adequate remedy

^{۱۱۹} Privacy International submission

^{۱۲۰} Principle of distinction

^{۱۲۱} Principle of proportionality

^{۱۲۲} Precaution in attack

^{۱۲۳} Weapons reviews

اشاره به بررسی موضوع ماده ۳۶ پروتکل اول الحاقی به کنوانسیون‌های ژنو

^{۱۲۴} Martens Clause

^{۱۲۵} Rupert Ticehurst, "The Martens clause and the laws of armed conflict", International Review of the Red Cross, No. 317, April 1997.

^{۱۲۶} . مراجعه کنید به:

www.blogs.icrc.org/law-and-policy/2017/11/14/ethics-source-law-martens-clause-autonomous-weapons

^{۱۲۷} Meaningful human control

^{۱۲۸} Use of force

^{۱۲۹} . مراجعه کنید به:

پیشنهادهای مختلف، عناصر عملی گوناگونی را برای تحقق کنترل انسانی شناسایی کرده‌اند؛ از جمله اعمال محدودیت بر پارامترهای استفاده از این سامانه‌ها^{۱۳۰} و تعیین حدود و شرایط محیط عملیاتی آن‌ها. همچنین، تدابیری نظیر محدودیت در انتخاب اهداف، الزام به نظارت انسانی و ایجاد سازوکارهای پاسخگویی، به منظور مقابله با مخاطرات و غیرقابل‌پیش‌بینی بودن ذاتی^{۱۳۱} توسعه، استقرار و استفاده از این سامانه‌ها پیشنهاد شده‌اند^{۱۳۲}. در چارچوب «گروه کارشناسان دولتی»^{۱۳۳} که حوزه فعالیت آن هم فناوری‌های خودمختار و هم فناوری‌های مبتنی بر هوش مصنوعی را دربر می‌گیرد، بحث‌های مستمری درباره مفهوم «کنترل معنادار انسان» در جریان بوده است؛ با این حال، تاکنون اجماعی درباره تعریف دقیق این مفهوم حاصل نشده است. با وجود این، توافق گسترده‌ای درباره ضرورت حفظ نوعی از مداخله و مشارکت انسانی^{۱۳۴} وجود دارد. افزون بر این، ملاحظات حقوق بشری همچنان تا حد زیادی در مباحث این گروه کارشناسان دولتی جایگاه شایسته‌ای نیافته است.

۲۹. ادغام هوش مصنوعی و فناوری‌های خودمختار در این سامانه‌های جدید، چالش‌های منحصربه‌فردی را از منظر حقوق بین‌الملل ایجاد می‌کند. بر اساس نظام حقوقی کنونی، به کارگیری هوش مصنوعی ممکن است تعیین مسئولیت و پاسخگویی در قبال نقض‌های حقوق بین‌الملل را با پیچیدگی مواجه سازد. کاهش شفافیت در فرایند هدف‌گیری مبتنی بر هوش مصنوعی می‌تواند به ایجاد خلأهایی بینجامد که انتساب مسئولیت کیفری فردی برای جنایات جنگی یا مسئولیت بین‌المللی دولت‌ها در قبال نقض‌های حقوق بین‌الملل را دشوارتر می‌سازد. اگرچه مسئولیت کیفری فردی در آثار حقوقی^{۱۳۵} و مباحث سازمان ملل متحد به‌طور گسترده مورد بحث قرار گرفته است، گفت‌وگوها درباره چالش‌هایی که سامانه‌های تسلیحاتی خودمختار برای مسئولیت بین‌المللی دولت‌ها ایجاد می‌کنند، همچنان در مراحل ابتدایی قرار دارد.^{۱۳۶} برای تحقق پاسخگویی، لازم است مسئولیت‌های مشخص توسعه‌دهندگان فناوری، بهره‌برداران،

www.ejiltalk.org/what-level-of-human-control-over-autonomous-weapon-systems-is-required-by-international-law

^{۱۳۰} Parameters of their use

^{۱۳۱} Inherent unpredictability

^{۱۳۲} Ibid.; Vincent Boulanin and others, Limits on Autonomy in Weapon Systems (Stockholm, Stockholm International Peace Research Institute and ICRC, 2020); and CCW/GGE.1/2023/WP.6

^{۱۳۳} Group of Governmental Experts

^{۱۳۴} Human involvement

^{۱۳۵} Legal doctrine

^{۱۳۶} Robin Geiß, “State control over the use of autonomous weapon systems”, in Military Operations and the Notion of Control Under International Law, Rogier Bartels and others., eds. (The Hague, Asser Press, ۲۰۲۱); and Lutiana Valadares Fernandes Barbosa, Autonomous Weapons Systems and the Responsibility of States: Challenges and Possibilities (Boca Raton, Florida, United States of America, and Abingdon, United Kingdom of Great Britain and Northern Ireland, CRC Press, 2024).

فرماندهان نظامی و نیز تعهدات دولت‌ها بر اساس حقوق بین‌الملل، از جمله «اصول راهنمای کسب‌وکار و حقوق بشر»، به‌روشنی تبیین شود. افزون بر این، ایجاد شفافیت بیشتر در قواعد حقوقی^{۱۳۷} حاکم بر این موضوع همچنان ضروری است، زیرا هر فناوری جدید و نوظهور، چالش‌های خاص خود را در سطوح مختلف مسئولیت ایجاد می‌کند.

۳۰. افزون بر این، انتساب رفتار^{۱۳۸} به دولت، به‌منظور احراز مسئولیت بین‌المللی دولت‌ها در چارچوب حقوق بین‌الملل و در ارتباط با سامانه‌های تسلیحاتی خودمختار، پرسش‌های حقوقی مهمی را مطرح می‌کند که نیازمند بررسی دقیق و عمیق هستند. اگرچه دولت‌های عضو «گروه کارشناسان دولتی» با اجماع توافق کرده‌اند که هر فعل متخلفانه بین‌المللی^{۱۳۹} منتسب به یک دولت، از جمله افعالی که ممکن است با سامانه‌های تسلیحاتی خودمختار^{۱۴۰} گشوده مرتبط باشند، موجب مسئولیت بین‌المللی آن دولت می‌شود، اما درباره نحوه انتساب مسئولیت بین‌المللی دولت در قبال نقض‌های حقوق بین‌الملل، توضیح یا شفاف‌سازی بیشتری ارائه نکرده‌اند.^{۱۴۱} در نخستین پیش‌نویس پیشنهاد رئیس گروه، تصریح شده بود که رفتار ارکان یک دولت (از جمله مأموران آن و تمامی افرادی که بخشی از نیروهای مسلح آن را تشکیل می‌دهند) به آن دولت قابل انتساب است و این امر، اعمال و ترک فعل‌های^{۱۴۲} مرتبط با استفاده از چنین سامانه‌هایی را نیز دربر می‌گیرد.^{۱۴۳}

۳۱. یکی از ملاحظات اساسی آن است که آیا و تحت چه شرایطی، رفتار سامانه‌های تسلیحاتی خودمختار را می‌توان، یا باید به دولت منتسب کرد، و نیز اینکه آیا نظام کنونی مسئولیت بین‌المللی دولت‌ها، که بر مبنای الگوی کنش انسانی^{۱۴۴} شکل گرفته است، برای انتساب مسئولیت در زمینه استفاده از این سامانه‌ها کفایت می‌کند یا خیر. اگرچه دولت‌ها بر اساس حقوق بین‌الملل بشر دارای تعهدات ایجابی هستند تا اطمینان حاصل کنند که این فناوری‌ها با حقوق بین‌الملل مطابقت دارند و تدابیر پیشگیرانه لازم را برای به حداقل رساندن مخاطرات اتخاذ کنند، صرف چارچوب تعهدات ایجابی ممکن است برای احراز مسئولیت بین‌المللی دولت در مواردی که سامانه‌های تسلیحاتی خودمختار با

^{۱۳۷} Further legal clarity

^{۱۳۸} Attributing conduct

^{۱۳۹} Internationally wrongful act

^{۱۴۰} CCW/GGE.1/2022/2, para. 19.

^{۱۴۱} Acts and omissions

^{۱۴۲} . مراجعه کنید به

www.documents.unoda.org/wp-content/uploads/2022/07/CCW-GGE.1-2022-CRP.1.docx. See also CCW/GGE.1/2022/WP.2; and Alisha Anand Ioana Puscas, “Proposals related to emerging technologies in lethal autonomous weapons systems” (United Nations Institute for Disarmament Research, 2022).

^{۱۴۳} Human action paradigm

درجه بالایی از خودمختاری و فراتر از حدود پیش‌بینی‌پذیری^{۴۴} شخص مسئول عمل می‌کنند، کافی نباشد. چالش اصلی در تعیین این موضوع نهفته است که در چه شرایطی باید اقدامات انجام شده در چارچوب عملکرد این سامانه‌ها به منزله رفتار دولت به کارگیرنده آن‌ها تلقی شود و در نتیجه، مسئولیت بین‌المللی آن دولت را برای آن اقدامات به دنبال داشته باشد. پرداختن به این پرسش‌ها برای تضمین پاسخگویی و رعایت حقوق بین‌الملل امری ضروری است.

۳۲. ادغام قابلیت‌های خودمختار در سامانه‌های تسلیحاتی مبتنی بر فناوری هوش مصنوعی، چالش‌های ویژه‌ای را در فرایند بررسی‌های حقوقی ایجاد می‌کند. سامانه‌های تسلیحاتی خودمختار با محیط پیرامون خود تعامل دارند و از این رو، باید در طیف گسترده‌ای از سناریوهای مختلف مورد آزمایش قرار گیرند. با افزایش اتکای انسان به هوش مصنوعی، لازم است توجه بیشتری به میزان انطباق این سامانه‌ها با استانداردهای حقوقی معطوف شود. اگرچه انتخاب و بازنگری داده‌های الگوریتمی از مؤلفه‌های اساسی این فرایند به شمار می‌رود، بررسی جامع حقوقی سامانه‌های تسلیحاتی خودمختاری که از سامانه‌های هوش مصنوعی بهره می‌برند، باید تعهدات دولت‌ها بر اساس حقوق بین‌الملل بشر را نیز در نظر بگیرد؛ از جمله حق حیات، حق بر تمامیت جسمی و روانی، اصل منع تبعیض و حق بر حریم خصوصی، و همچنین اصول شفافیت و پاسخگویی و مخاطرات احتمالی ناشی از پیامدهای ناخواسته. تعهدات ناشی از اصل نظارت و دقت لازم [رعایت حقوق بشر] نیز باید به گونه‌ای مشخص و تبیین شوند که هرگونه سوگیری و تبعیض ناخواسته، به‌ویژه در مواردی که ممکن است به نقض حقوق مورد حمایت حقوق بین‌الملل بینجامد، برطرف شود. افزون بر این، کارشناسان حقوقی باید از مراحل اولیه طراحی این سامانه‌ها در فرایند توسعه مشارکت داشته باشند تا این مسائل به‌صورت پیشگیرانه مورد رسیدگی قرار گیرد و تضمین‌های لازم برای جلوگیری از نقض‌های احتمالی حقوق بشر پیش‌بینی و اجرا شود. با وجود این، همچنان پرسش‌هایی درباره سازگاری تصمیم‌گیری مبتنی بر ماشین^{۴۵} با اصول حقوق بشر باقی است^{۴۶}. همچنین، باید توجه داشت که درباره امکان طراحی، تولید و به کارگیری سامانه‌های تسلیحاتی خودمختار به گونه‌ای که به‌طور کامل با تمامی الزامات حقوق بین‌الملل مطابقت داشته باشند، همچنان بحث‌ها و اختلاف‌نظرهای قابل توجهی وجود دارد.

۳۳. ظهور فناوری‌های جدید و نوظهور در حوزه نظامی، از جمله فناوری‌های به کاررفته در سامانه‌های تسلیحاتی خودمختار، چالش‌هایی را برای قواعد موجود حقوق بین‌الملل ایجاد کرده و ضرورت تدوین قواعد جدید را برای تنظیم این فناوری‌ها و در موارد مقتضی، حتی ممنوعیت آن‌ها در صورتی که نتوانند با استانداردهای حقوق بین‌الملل

^{۴۴} Foreseeability

^{۴۵} Machine-based decision-making

^{۴۶} A/HRC/23/47.

مطابقت داشته باشند، برجسته ساخته است. «گروه کارشناسان دولتی» در حال بررسی یک رویکرد دوجبهی است که بر اساس آن، از یک سو سلاح‌هایی که با حقوق بین‌الملل بشردوستانه ناسازگار هستند ممنوع شوند و از سوی دیگر، سایر سلاح‌ها تحت مقررات و ضوابط مشخص قرار گیرند. این رویکرد با درخواست‌های دبیرکل سازمان ملل متحد و رئیس کمیته بین‌المللی صلیب سرخ برای تدوین قواعد جدید بین‌المللی به منظور صیانت از انسانیت^{۴۷} همسو است. دبیرکل سازمان ملل متحد نیز در گزارش خود که به موجب قطعنامه ۲۴۱/۷۸ مجمع عمومی (نخستین قطعنامه این نهاد درباره سامانه‌های تسلیحاتی خودمختار گشوده) تهیه شده است، از دولت‌ها خواست حداکثر تا سال ۲۰۲۶، یک سند حقوقی الزام‌آور^{۴۸} را به تصویب برسانند که سامانه‌های تسلیحاتی خودمختاری را که بدون کنترل یا نظارت انسانی عمل می‌کنند و امکان استفاده از آن‌ها مطابق با حقوق بین‌الملل بشردوستانه وجود ندارد، ممنوع کند و در عین حال، سایر انواع سامانه‌های تسلیحاتی خودمختار را تحت مقررات مشخص قرار دهد.^{۴۹} با وجود این، دولت‌ها همچنان درباره اینکه این مقررات باید ماهیتی الزام‌آور داشته باشند یا صرفاً داوطلبانه باشند، اختلاف نظر دارند.^{۵۰} افزون بر این، انجام بحث‌های بیشتر درباره ابعاد حقوق بین‌الملل بشر و سامانه‌های تسلیحاتی خودمختار نیز ضروری است.

ج) فناوری‌های ارتقای توانمندی‌های انسانی در حوزه نظامی

۳۴. با وجود آنکه فناوری‌های ارتقای توانمندی‌های جسمی و شناختی^{۵۱} انسان می‌توانند در به کارگیری راهبردهای غیرگشوده و کاهش فشارهای روانی ناشی از مخاصمات نقش داشته باشند، توسعه این فناوری‌ها چالش‌های مهمی از جنبه‌های اخلاقی، حقوقی، اجتماعی و عملیاتی به همراه دارد. از جمله نگرانی‌های مطرح در این زمینه می‌توان به تأثیر آن‌ها بر ارزش‌های نظامی، ایجاد معضلات عملیاتی، مسائل مربوط به اجرای حقوق و مقررات نظامی، و رعایت اصل رضایت آگاهانه^{۵۲} اشاره کرد. افزون بر این، انواع مختلف فناوری‌های ارتقای انسان اعم از ژنتیکی، زیستی یا سایبرنتیکی^{۵۳} فناوری‌هایی که از طریق رابط‌های انسان و ماشین یا سامانه‌های الکترونیکی، توانایی‌های انسان را افزایش می‌دهند) هر یک مخاطرات حقوق بشری و اخلاقی خاص خود را ایجاد می‌کنند. پیشرفت‌های مشابه در حوزه

^{۴۷} Safeguard humanity

^{۴۸} Legally binding instrument

^{۴۹} A/79/88, para. 90

^{۵۰} Ibid., paras. 63–86

^{۵۱} Physical and cognitive enhancement technologies

^{۵۲} Informed consent

^{۵۳} Cybernetic

غیرنظامی، از جمله در محیط‌های کاری، نیز نشان‌دهنده پیامدهای گسترده‌تر و ماهیت دوکاربردی این فناوری‌ها است.^{۱۵۴}

۳۵. پیشرفت‌های هوش مصنوعی ظرفیت فناوری‌های ارتقای توانمندی‌های انسانی را بیش از پیش گسترش داده و نقش مهمی در درمان‌های پزشکی و توان‌بخشی افراد دارای اختلالات جسمی و شناختی در محیط‌های غیرنظامی ایفا می‌کند.^{۱۵۵} با این حال، از منظر تاریخی، تلاش‌ها برای ارتقای عملکرد انسان عمدتاً بر موفقیت مأموریت‌های نظامی متمرکز بوده و گاه رفاه و سلامت فردی را تحت‌الشعاع قرار داده است. این تعارض ممکن است استقلال و اختیار^{۱۵۶} سربازان و نیز پزشکان نظامی را در تجویز و به‌کارگیری فناوری‌های عصبی^{۱۵۷} از جمله داروها، کاشتنی‌های عصبی^{۱۵۸} و پروتزهای عصبی^{۱۵۹} محدود کند. از این‌رو، تضمین شفافیت و رعایت کرامت انسانی و حق بر سلامت، از جمله احترام به استقلال فرد^{۱۶۰} در تصمیم‌گیری و توجه به وضعیت رزمندگان برخوردار از فناوری‌های ارتقا‌دهنده پس از پایان خدمت نظامی، امری ضروری است.^{۱۶۱}

۳۶. به‌کارگیری فناوری‌هایی مانند رابط‌های «مغز رایانه»^{۱۶۲} در حوزه نظامی، از جمله ابزارهایی تلقی می‌شود که می‌توانند از طریق ادغام هوش انسانی و هوش ماشینی، توانایی‌های شناختی انسان را ارتقا دهند. اگرچه توسعه رباتیک و فناوری‌های عصبی، از جمله رابط‌های «مغز رایانه»، ظرفیت‌های چشمگیری برای پیشرفت در حوزه مراقبت‌های سلامت و درمان فراهم کرده است، استفاده از این فناوری‌ها در بستر نظامی چالش‌های ویژه‌ای، به‌ویژه در زمینه اجرای قواعد حقوقی مربوط به پاسخگویی و حفظ کنترل انسانی بر عملیات نظامی و فرایندهای تصمیم‌گیری را به همراه دارد. علاوه بر این، رابط‌های «مغز رایانه» و سایر فناوری‌های عصبی پیشرفته ممکن است در بسترهای خصمانه، برای

^{۱۵۴} Timo Istace and Milena Costas Trascasas, "Between science-fact and science-fiction", Research Brief (Geneva, Geneva Academy of International Humanitarian Law and Human Rights, 2024).

^{۱۵۵} Yuval Shany and Tal Mimran, "Integrating privacy concerns in the development and introduction of new military or dual use technologies", in The Rights to Privacy and Data Protection in Times of Armed Conflict, Asaf Lubin and Russal Buchan, eds. (Talinn, NATO CCDCOE Publications, 2022); and Margaret Kosal and Joy Putney, "Neurotechnology and international security", Politics and the Life Sciences, vol. 42, No. 1 (spring 2023)

^{۱۵۶} Autonomy

^{۱۵۷} Neurotechnologies

^{۱۵۸} Neural implants

^{۱۵۹} Neuroprostheses

^{۱۶۰} Decision-making autonomy

^{۱۶۱} Sebastian Sattler and others, "Neuroenhancements in the military" Neuroethics, vol. 15, No. 1 (February 2022)

^{۱۶۲} Brain-computer interfaces (BCIs)

به کارگیری شیوه‌های قهرآمیز بازجویی^{۱۶۳} مورد سوءاستفاده قرار گیرند. استفاده از چنین روش‌هایی می‌تواند ناقض حقوق بشر باشد؛ زیرا حتی در نبود خشونت فیزیکی، ممکن است موجب آسیب‌های روانی شود یا مصداق شکنجه^{۱۶۴} یا سایر رفتارها و مجازات‌های ظالمانه، غیرانسانی یا تحقیرآمیز تلقی گردد.^{۱۶۵}

۳۷. به کارگیری فناوری‌های نوین ارتقای توانمندی‌های انسانی در فعالیت‌های نظامی، نگرانی‌های جدی درباره پیامدهای حقوقی و احتمال نقض حقوق بشر ایجاد می‌کند. این فناوری‌ها مخاطراتی به‌ویژه در ارتباط با حق بر حریم خصوصی، ضرورت اخذ رضایت آزادانه و آگاهانه، و احتمال نقض تمامیت جسمی و روانی^{۱۶۶} رزمندگان در بلندمدت را به همراه دارند. دولت‌ها و بنگاه‌های اقتصادی موظف‌اند این مخاطرات را مطابق با قواعد و مقررات قابل اعمال حقوق بین‌الملل شناسایی، مدیریت و برطرف کنند.^{۱۶۷}

۳۸. افزون بر این، نابرابری‌های قدرت ذاتی در حوزه نظامی، همراه با پیامدهای بلندمدت ناشی از گردآوری، پردازش و نگهداری داده‌های شخصی، ممکن است به نقض حریم خصوصی در مراحل بعدی منجر شود؛ نقض‌هایی که آثار آن‌ها، گاه تنها پس از گذشت زمان آشکار می‌شود. برای نمونه، استفاده قهرآمیز از این فناوری‌ها می‌تواند کرامت و خودمختاری سربازان را به شدت تضعیف کند. در حالی که حتی کاربردهای غیرقهرآمیز آن‌ها نیز پرسش‌های جدی اخلاقی درباره رضایت آزادانه و آگاهانه و نیز آثار بلندمدت آن‌ها بر سلامت افراد را مطرح می‌سازد. این ملاحظات ایجاب می‌کند که در موارد استفاده قهرآمیز از این فناوری‌ها، ممنوعیت‌های مشخص و صریح وضع شود و در خصوص کاربردهای غیرقهرآمیز نیز، به‌منظور جلوگیری از سوءاستفاده احتمالی از این فناوری‌ها، تعلیق موقت^{۱۶۸} یا محدودیت‌های مناسب پیش‌بینی و اعمال گردد.^{۱۶۹}

(د) اجرای قانون و کنترل مرزها

^{۱۶۳} Coercive interrogation techniques

^{۱۶۴} Constitute torture

^{۱۶۵} Charles N. Munyon, "Neuroethics of non-primary brain computer interface", *Frontiers in Neuroscience* (October 2018)

^{۱۶۶} Physical and mental integrity

^{۱۶۷} A/HRC/57/61

^{۱۶۸} Moratoriums

^{۱۶۹} Ibid., para. 80 (b)

۳۹. فناوری‌هایی مانند سامانه‌های نظارتی مبتنی بر هوش مصنوعی، مدل‌سازی پیش‌بینانه^{۱۷۰} و فناوری‌های زیست‌سنجی^{۱۷۱} به‌طور فزاینده‌ای از سوی مراجع مسئول مدیریت مرزها و نهادهای اجرای قانون مورد استفاده قرار می‌گیرند. اگرچه این ابزارها اغلب به دلیل ظرفیتشان در ارتقای امنیت عمومی (از طریق بهینه‌سازی واکنش به شرایط اضطراری، تسهیل عبور ایمن و روان از مرزها و کمک به پیشگیری از جرم) مورد حمایت قرار می‌گیرند، اما در عین حال، در حوزه اجرای قانون و مدیریت مرزها، مخاطرات جدی برای حقوق بشر نیز به همراه دارند.^{۱۷۲}

۴۰. کاربردهای فناوری‌های زیست‌سنجی در این حوزه شامل احراز هویت برای کنترل دسترسی و نیز شناسایی افراد هنگام دستگیری یا بازداشت است. اگرچه این سامانه‌ها ممکن است با خطا مواجه شوند، تاکنون توجه چندانی به پیامدهای احتمالی حقوق بشری استفاده از آن‌ها در حوزه نظامی، به‌ویژه نسبت به گروه‌های آسیب‌پذیر، از جمله افراد دارای معلولیت، سالمندان، کودکان، افراد با تبار آفریقایی، مهاجران و سایر گروه‌هایی که در معرض تبعیض تاریخی و ساختاری قرار داشته‌اند، نشده است. این نگرانی وجود دارد که به کارگیری این فناوری‌ها، از طریق سوگیری‌های الگوریتمی و ایجاد الگوهای تبعیض‌آمیز در شناسایی و دسته‌بندی افراد، نابرابری‌های موجود را تشدید کند. این سوگیری‌ها غالباً ریشه در پیش‌داوری‌های نهفته در شیوه‌های تاریخی گردآوری، پردازش و نگهداری داده‌ها دارند. در حوزه مدیریت مهاجرت نیز، تنوع موجود در داده‌های زیست‌سنجی که متأثر از تفاوت‌های فرهنگی است، می‌تواند این سوگیری‌ها را تشدید کند. برای مثال، فناوری‌های زیست‌سنجی مانند سامانه‌های تشخیص چهره ممکن است حق بر منع تبعیض را نقض کنند؛ زیرا احتمال خطای آن‌ها در شناسایی مردمان بومی و افراد با تبار آفریقایی، به‌ویژه زنان، بیشتر است. همچنین، در صورتی که دولت‌ها یا بنگاه‌های اقتصادی داده‌های زیست‌سنجی افراد را بدون رضایت آنان به اشتراک بگذارند، این امر می‌تواند ناقض حق بر حریم خصوصی باشد. با توجه به تأکید حقوق بین‌الملل بشر بر حق بر حریم خصوصی، برابری و منع تبعیض، انجام ارزیابی‌های تأثیر بر حقوق بشر^{۱۷۳} و بررسی چگونگی تأثیر این فناوری‌ها در تقویت نابرابری‌های موجود، امری ضروری است.^{۱۷۴}

۴۱. سامانه‌های نظارت تصویری^{۱۷۵} از جمله سامانه‌های نظارت هوایی^{۱۷۶} اکنون با بهره‌گیری از فناوری‌هایی مانند پهپادها و سامانه‌های تشخیص چهره، از قابلیت‌های بی‌سابقه‌ای برای نظارت، ثبت و ردیابی از راه دور افراد در اماکن عمومی، از جمله مناطق مرزی، برخوردار هستند. این پیشرفت‌های فناورانه از جمله برای حق آزادی رفت‌وآمد، آزادی

^{۱۷۰} Predictive modelling

^{۱۷۱} Biometrics

^{۱۷۲} Matias Leese and others, "Data matters", Geopolitics, vol. 27, No. 1 (2022).

^{۱۷۳} Human rights impact assessments

^{۱۷۴} A/HRC/51/17

^{۱۷۵} Optical surveillance systems

^{۱۷۶} Aerial surveillance

تشکل و انجمن، آزادی اجتماعات، حق بر حریم خصوصی و حق بر منع تبعیض مخاطرات جدی برای حقوق بشر به همراه دارند.

۴۲. در سال‌های اخیر، توجه فزاینده‌ای به سامانه‌های تسلیحاتی خودمختار معطوف شده است. اگرچه بخش عمده مباحث پیرامون این سامانه‌ها بر استفاده از آن‌ها در مخاصمات مسلحانه متمرکز بوده است، به تدریج آشکار شده که استفاده از آن‌ها برای مدیریت مرزها و اجرای قانون در داخل کشور نیز در دست بررسی قرار دارد. این تحول نگرانی‌های جدی حقوق بشری به‌ویژه در ارتباط با حق حیات، حق بر تمامیت جسمی و روانی^{۱۷۷} و کرامت انسانی را برمی‌انگیزد. برخلاف مخاصمات مسلحانه که در آن‌ها استفاده از زور عمدتاً تابع قواعد حقوق بین‌الملل بشردوستانه است، مأموران اجرای قانون تنها در صورتی مجاز به استفاده از زور هستند که این اقدام اجتناب‌ناپذیر^{۱۷۸} کاملاً ضروری^{۱۷۹} و متناسب با وظایف قانونی آنان باشد^{۱۸۰}.

ه (جنگ شناختی

۴۳. جنگ شناختی^{۱۸۱} با هدف کنترل افکار و ادراکات طرف مقابل، به‌منظور تأثیرگذاری بر تصمیم‌ها و اقدامات او صورت می‌گیرد. این نوع جنگ که ریشه در عملیات نظامی اطلاعات نادرست و گمراه‌کننده دارد، به‌دلیل آثار تحول‌آفرین هوش مصنوعی، به یکی از عرصه‌های نوین راهبردی تبدیل شده است. فناوری‌های پیشرفته امکان اعمال نفوذ روان‌شناختی^{۱۸۳} گسترده را فراهم می‌کنند؛ به‌گونه‌ای که می‌توانند بدون آگاهی افراد، فرایندهای شناختی آنان را هدف قرار دهند و دقت و اثربخشی این مداخلات را افزایش دهند. جنگ شناختی از طریق تغییر ادراکات و بهره‌برداری از آسیب‌پذیری‌های موجود در فرایند تصمیم‌گیری،^{۱۸۴} کسب برتری راهبردی^{۱۸۵} است.

۴۴. اگرچه جنگ شناختی به‌تنهایی ممکن است برای پیروزی در جنگ‌ها کافی نباشد، اما هنگامی که با عملیات فیزیکی و اطلاعاتی (از جمله عملیات انتشار اطلاعات نادرست و گمراه‌کننده مبتنی بر هوش مصنوعی^{۱۸۶}) همراه شود،

^{۱۷۷} Bodily integrity

^{۱۷۸} Unavoidable

^{۱۷۹} strictly necessary

^{۱۸۰} Code of Conduct for Law Enforcement Officials

^{۱۸۱} Cognitive warfare

^{۱۸۲} Jean-Marc Rickli, Federico Mantellassi and Gwyn Glasser, "Peace of mind", Policy Brief No. 9 (Geneva, Geneva Centre for Security Policy, 2023).

^{۱۸۳} Psychological influence

^{۱۸۴} Decision-making vulnerabilities

^{۱۸۵} Strategic advantages

^{۱۸۶} AI-driven disinformation

می‌تواند به برتری بر طرف مقابل منجر شود. غیررزمندگان، از جمله غیرنظامیان، بیش از پیش در معرض راهبردهای جنگ شناختی قرار می‌گیرند و این امر نگرانی‌های جدی درباره حمایت از حقوق بشر در این حوزه ایجاد کرده است. این تاکتیک‌ها می‌توانند مواردی از جمله حق بر حریم خصوصی از طریق گردآوری داده‌ها و ایجاد پروفایل از افراد^{۱۸۷}، حق آزادی عقیده و بیان در نتیجه دستکاری اطلاعات و انتشار اطلاعات نادرست و گمراه‌کننده، حق دسترسی به اطلاعات صحیح^{۱۸۸} و حق بر تمامیت روانی را به مخاطره اندازند. علاوه بر این، عملیات شناختی هدفمند ممکن است تبعیض مبتنی بر قومیت، دین، جنسیت یا گرایش سیاسی را تشدید کرده و در نتیجه، حق بر منع تبعیض را نقض کند.

۴۵. توسعه شتابان هوش مصنوعی، شیوه‌های انتشار اطلاعات^{۱۸۹} را به‌طور بنیادین دگرگون کرده و شناخت انسانی را به یکی از عرصه‌های اصلی تقابل نظامی تبدیل کرده است. افزون بر این، شبیه‌سازی‌های واقعیت مجازی مبتنی بر شرایط پرفشار^{۱۹۰} برای آموزش‌های رزمی مورد استفاده قرار می‌گیرند و داده‌های گردآوری‌شده از این فرایندها در ارتقای آمادگی‌های آینده به کار گرفته می‌شوند. این امر نشان‌دهنده اهمیت راهبردی و مخاطرات بالای رقابت در حوزه شناختی^{۱۹۱} است^{۱۹۲}.

و) همگرایی بالقوه هوش مصنوعی و فناوری‌های زیستی، از جمله سلاح‌های زیستی

۴۶. هوش مصنوعی به یکی از ارکان اساسی علوم زیستی^{۱۹۳} تبدیل شده و زمینه‌ساز پیشرفت‌های چشمگیری در زیست‌فناوری شده است که به مقابله با چالش‌های جهانی، از جمله امنیت غذایی^{۱۹۴} و دسترسی به آب سالم، کمک می‌کند. با این حال، همگرایی هوش مصنوعی و زیست‌فناوری، به‌ویژه از طریق توسعه یا به کارگیری سلاح‌های زیستی تقویت‌شده با هوش مصنوعی^{۱۹۵} می‌تواند مخاطرات جدی برای حقوق بشر به همراه داشته باشد. توسعه، تولید، تحصیل، انتقال، انباشت و استفاده از سلاح‌های زیستی بر اساس «کنوانسیون منع توسعه، تولید و انباشت سلاح‌های

^{۱۸۷} Profiling

^{۱۸۸} Truthful information

^{۱۸۹} Information dissemination

^{۱۹۰} High-stress virtual-reality simulations

^{۱۹۱} Cognitive domain competition

^{۱۹۲}. مراجعه کنید به:

www.act.nato.int/activities/cognitive-warfare/.

^{۱۹۳} Life sciences

^{۱۹۴} Food security

^{۱۹۵} AI-enhanced biological weapons

باکتریولوژیک (زیستی) و سمی و انهدام آن‌ها^{۹۶} ممنوع است. این ممنوعیت، صرف‌نظر از فناوری‌های مورد استفاده، ماهیتی جامع دارد. از این رو، سلاح‌های زیستی تقویت‌شده با هوش مصنوعی نیز مشمول این ممنوعیت هستند.

۴۷. ادغام هوش مصنوعی با زیست‌شناسی مصنوعی^{۹۷} (که به بازطراحی موجودات زنده^{۹۸} برای دستیابی به اهداف مشخص می‌پردازد) می‌تواند ایجاد موجودات زنده کاملاً جدید با ویژگی‌های متناسب با اهداف مشخص^{۹۹} را تسهیل کند. این امر خطر توسعه عوامل زیستی پیش‌بینی‌نشده و مخاطره‌آمیز را به همراه دارد و ممکن است به ظهور اشکال جدیدی از تهدیدات زیستی بینجامد.^{۱۰۰} علاوه بر این، اگرچه هوش مصنوعی می‌تواند دسترسی به اطلاعات و انتشار دانش را تسهیل کند. در عین حال ممکن است مخاطرات امنیت زیستی را نیز افزایش دهد؛ زیرا امکان اشتراک‌گذاری دانش حساس با افرادی که فاقد صلاحیت هستند یا دارای اهداف نادرست یا سوءنیت‌اند را فراهم می‌سازد.^{۱۰۱}

۴۸. سلاح‌های زیستی تقویت‌شده با هوش مصنوعی، چالش‌های جدی برای حق حیات، حق بر تمامیت جسمی و روانی، حق بر سلامت و حق بر خورداری از محیط زیستی پاک، سالم و پایدار ایجاد می‌کنند. افزون بر این، این سلاح‌ها می‌توانند از منظر امنیت زیستی و ایمنی زیستی نیز چالش‌هایی را در زمینه شناسایی و انتساب منشأ حملات^{۱۰۲} به وجود آورند؛ به‌ویژه زمانی که به‌گونه‌ای طراحی شوند که بتوانند از سامانه‌های موجود شناسایی عبور کنند و بدین ترتیب، تشخیص و واکنش به حمله از سوی یک طرف متخاصم را دشوار سازند. همچنین، ممکن است سلاح‌های زیستی به‌گونه‌ای طراحی شوند که شیوع‌های طبیعی بیماری‌ها را شبیه‌سازی کنند. چنین وضعیتی، انتساب حمله و تعیین منشأ آن را با دشواری بیشتری مواجه کرده، مانع از اتخاذ واکنش مناسب می‌شود و در نتیجه، ممکن است حق بر خورداری از جبران مؤثر را نیز با اختلال مواجه سازد.^{۱۰۳}

^{۹۶} Biological Weapons Convention

^{۹۷} Synthetic biology

^{۹۸} Redesigning organisms

^{۹۹} Tailored characteristics

^{۱۰۰} Anshula Sharma and others, "Next generation agents (synthetic agents)", in Handbook on Biological Warfare Preparedness, S.J.S Flora and Vidhu Pachaur, eds. (London, Elsevier, 2020)

^{۱۰۱} Zhaohui Su and others, "Addressing biodisaster X threats with artificial intelligence and 6G technologies", Journal of Medical Internet Research, vol. 23, No. 5 (May 2021); and Renan Chaves de Lima and others, "Artificial intelligence challenges in the face of biological threats", Frontiers in Artificial Intelligence (May 2024).

^{۱۰۲} Detection and attribution

^{۱۰۳} Connor O'Brien, Kathleen Varty and Anna Ignaszak, "The electrochemical detection of bioterrorism agents", Microsystems and Nanoengineering, vol. 7, No. 1 (2021)

۴۹. مقابله با این مخاطرات مستلزم اتخاذ رویکردی چندوجهی و مبتنی بر حقوق بشر است. این رویکرد باید شامل اجرای مؤثر حقوق بین الملل بشر، نهادینه سازی چارچوب های بین المللی از جمله کنوانسیون سلاح های زیستی، تقویت همکاری های چندجانبه، سرمایه گذاری در حوزه امنیت زیستی و حمایت از پژوهش در زمینه فناوری های دفاعی باشد.

ز) هوش مصنوعی و سامانه های فرماندهی، کنترل و هدایت [نیروهای] هسته ای

۵۰. اگرچه دولت های دارای توانمندی هسته ای^{۲۰۴} تا حدودی مخاطرات ناشی از ادغام هوش مصنوعی در سامانه های فرماندهی و کنترل هسته ای^{۲۰۵}، به ویژه برای ارتقای آگاهی موقعیتی و شناسایی تهدیدها، را پذیرفته اند، تلاش برای کسب برتری راهبردی در محیط متحول هسته ای (همراه با نگرانی از عقب ماندن در رقابت نوآوری های هوش مصنوعی) ممکن است به پذیرش شتاب زده و زود هنگام این فناوری ها بینجامد^{۲۰۶}. در این زمینه، باید میان استفاده از سامانه های هوش مصنوعی برای آگاهی موقعیتی^{۲۰۷} و شناسایی تهدیدها، و استفاده احتمالی از آنها در فرایندهای تصمیم گیری درباره سلاح های هسته ای تمایز قائل شد. در حال حاضر، به نظر می رسد کاربرد هوش مصنوعی در سامانه های فرماندهی، کنترل و ارتباطات هسته ای^{۲۰۸} عمدتاً به شناسایی زود هنگام تهدیدها، گردآوری اطلاعات و پشتیبانی از تصمیم گیری محدود باشد. اگرچه گزارش هایی درباره وجود یک سامانه خودکار که برای استفاده در صورت وقوع حمله سرکرده زدایی^{۲۰۹} (حمله ای که با هدف از میان برداشتن رهبری سیاسی یا فرماندهی نظامی طرف مقابل انجام می شود) طراحی شده است منتشر شده، این سامانه پیش از ظهور نسل کنونی فناوری های هوش مصنوعی توسعه یافته است. با این حال، قابلیت اعتماد و پیامدهای به کارگیری هوش مصنوعی در چنین سامانه هایی همچنان موجب نگرانی است، به ویژه اگر پیشرفت های آینده به اتکای هر چه بیشتر به تصمیم گیری های مبتنی بر هوش مصنوعی منجر شود^{۲۱۰}.

^{۲۰۴} Nuclear-capable States

^{۲۰۵} Nuclear command and control systems

^{۲۰۶}. مراجعه کنید به :

www.warontherocks.com/2024/12/beyond-human-in-the-loop-managing-ai-risks-in-nuclear-command-and-control

^{۲۰۷} Situational awareness

^{۲۰۸} Nuclear command, control and communications (NC3)

^{۲۰۹} Decapitating strike

^{۲۱۰} Alice Saltini, "AI and nuclear command, control and communications" (London, European Leadership Network, 2023)

۵۱. ادغام سامانه‌های پیشرفته هوش مصنوعی مبتنی بر یادگیری عمیق^{۲۱۱}، چالش‌هایی فراتر از چالش‌های مدل‌های مبتنی بر قواعد^{۲۱۲} موجود ایجاد می‌کند. مهم‌ترین نگرانی‌ها در این زمینه شامل قابلیت اعتماد، شفافیت، آسیب‌پذیری در برابر حملات خصمانه و عدم همسویی^{۲۱۳} مدل‌های بزرگ‌مقیاس^{۲۱۴} با الزامات و اهداف مورد انتظار در کارکردهای حساس، از جمله تصمیم‌گیری درباره سلاح‌های هسته‌ای است.^{۲۱۵} مدل‌های یادگیری عمیق ذاتاً فاقد شفافیت^{۲۱۶} هستند و همین امر موجب می‌شود که فرایند تصمیم‌گیری آن‌ها به‌سختی قابل تفسیر باشد. این وضعیت می‌تواند به نتایج غیرقابل پیش‌بینی بینجامد و نظارت مؤثر انسان را تضعیف کند. افزون بر این، چرخه‌های بسیار سریع تصمیم‌گیری^{۲۱۷} این امکان را فراهم می‌کنند که هوش مصنوعی با سرعتی فراتر از توانایی انسان عمل کند. امری که ممکن است زمان در دسترس برای اتخاذ تصمیم درباره واکنش هسته‌ای را تا حدی کاهش دهد که اعمال کنترل مؤثر انسانی بر این فرایند دشوار شود. این وضعیت نگرانی‌های جدی درباره کرامت انسانی و حقوق بشر؛ از جمله در ارتباط با حق حیات، حق بر تمامیت جسمی و روانی، حق بر منع تبعیض، حق بر سلامت و حق برخورداری از محیط‌زیستی سالم ایجاد می‌کند.

۵۲. افزون بر این، این خطر وجود دارد که سامانه‌های هوش مصنوعی فعالیت‌های عادی یا هشدارهای کاذب را به‌اشتباه به‌عنوان تهدید تفسیر کنند و در نتیجه، موجب تشدید ناخواسته تنش‌ها^{۲۱۸} شوند. نگرانی مهم دیگر، پدیده «سوگیری ناشی از اتوماسیون»^{۲۱۹} است؛ وضعیتی که در آن، کاربران انسانی بیش از اندازه به تصمیم‌های اتخاذشده توسط سامانه‌های هوش مصنوعی اعتماد می‌کنند، حتی در مواردی که شهود انسانی^{۲۲۰}، آگاهی حاصل از آموزش یا سایر اطلاعات و ارزیابی‌های موجود، اتخاذ مسیر متفاوتی را ایجاب می‌کند. چنین وضعیتی می‌تواند به قضاوت‌های نادرست با پیامدهای بسیار پرخطر منجر شود. همچنین، فعالیت‌های مخرب در حوزه فناوری اطلاعات و ارتباطات^{۲۲۱} که سامانه‌های مبتنی بر هوش مصنوعی را هدف قرار می‌دهند، ممکن است این امکان را برای طرف‌های متخاصم

^{۲۱۱} Deep learning-based AI

^{۲۱۲} Rule-based models

^{۲۱۳} Misalignment

^{۲۱۴} Large-scale models

^{۲۱۵} Ibid

^{۲۱۶} Opaque

^{۲۱۷} Rapid decision cycles

^{۲۱۸} Unintended escalation

^{۲۱۹} Automation bias

^{۲۲۰} Human intuition

^{۲۲۱} Information and communications technology (ICT)

فراهم کنند که در این سامانه‌ها نفوذ کنند، آن‌ها را از کار بپندازند، دستکاری کنند یا پاسخ‌های جعلی^{۲۲} ایجاد کنند. این امر می‌تواند موجب ایجاد عدم اطمینان، محاسبات نادرست یا اقدامات ناخواسته شود.^{۲۳} افزون بر این، سامانه‌های هوش مصنوعی ذاتاً برای آموزش به مجموعه داده‌های گسترده^{۲۴} متکی هستند. طرف‌های متخاصم ممکن است این داده‌ها را آلوده یا دستکاری^{۲۵} کنند که در نتیجه، فرایندهای تصمیم‌گیری دچار نقص شده و حتی ممکن است به نقض حق بر منع تبعیض منجر شود.

۵۳. ادغام هوش مصنوعی در سامانه‌های فرماندهی و کنترل هسته‌ای، مخاطرات قابل توجهی را به همراه دارد که باید از طریق ترکیبی از ارزیابی‌های مخاطره^{۲۶}، تدابیر حفاظتی فنی^{۲۷}، ملاحظات اخلاقی^{۲۸} و چارچوب‌های حقوقی مستحکم، با نهایت احتیاط مدیریت شوند. شتاب روزافزون توسعه هوش مصنوعی مستلزم اتخاذ رویکردی پیش‌دستانه^{۲۹} و ابتکار عمل برای تسریع در ایجاد سازوکارهایی است که تضمین کنند این قابلیت‌ها به گونه‌ای مسئولانه، ایمن و منطبق با حقوق بین‌الملل بشر توسعه یافته و به کار گرفته شوند.

ح) سلاح‌های انرژی هدایت‌شده

۵۴. سلاح‌های انرژی هدایت‌شده^{۳۰}، سامانه‌هایی هستند که بدون استفاده از پرتابه^{۳۱}، انرژی متمرکز^{۳۲} را در جهتی مشخص منتشر می‌کنند. در کاربردهای نظامی، این سلاح‌ها به جای اتکا به نیروی جنبشی^{۳۳}، از فناوری‌های مبتنی بر امواج الکترومغناطیسی یا ذرات برای از کار انداختن^{۳۴} یا نابود کردن اهداف استفاده می‌کنند. این دسته از سلاح‌ها شامل لیزرها، امواج مایکروویو، امواج میلی‌متری^{۳۵} و پرتوهای ذرات^{۳۶} هستند. این سلاح‌ها می‌توانند برای مقاصد

^{۲۲} Spoof responses

^{۲۳} Muhammad Mudassar Yamin and others, "Weaponized AI for cyber-attacks", Journal of Information Security and Applications, No. 57 (March 2021)

^{۲۴} Large datasets

^{۲۵} Corrupt data

^{۲۶} Risk assessments

^{۲۷} Technical safeguards

^{۲۸} Ethical considerations

^{۲۹} Proactive approach

^{۳۰} Directed energy weapons (DEWs)

^{۳۱} Projectiles

^{۳۲} Concentrated energy

^{۳۳} Kinetic force

^{۳۴} Neutralize

^{۳۵} Millimetre waves

^{۳۶} Particle beams

غیرگشوده، از جمله ایجاد اختلال^{۲۳۷} یا مختل کردن موقت بینایی انسان‌ها^{۲۳۸} یا عملکرد تجهیزات و سامانه‌های الکترونیکی، نیز مورد استفاده قرار گیرند^{۲۳۹}. هنگامی که سلاح‌های انرژی هدایت‌شده برای اهداف نظامی به کار گرفته می‌شوند، قادرند اهداف فیزیکی را با دقت و صحت بسیار بالا و از فاصله چندین کیلومتری مورد اصابت قرار داده و به آن‌ها آسیب وارد کنند.

۵۵. با پیشرفت فناوری سلاح‌های انرژی هدایت‌شده، سامانه‌های تسلیحاتی مبتنی بر این فناوری به‌طور فزاینده‌ای قدرتمندتر، گسترده‌تر و در سکوها عملیاتی هوایی، زمینی، دریایی و فضایی ادغام و مستقر می‌شوند. عملکرد این سلاح‌ها با سرعت نور^{۲۴۰}، دقت بالا، قابلیت مقیاس‌پذیری^{۲۴۱}، کارایی لجستیکی^{۲۴۲} و هزینه پایین هر بار شلیک^{۲۴۳}، مزایای قابل توجهی را برای کاربردهای غیرنظامی و نظامی فراهم می‌کند^{۲۴۴}.

۵۶. در زمینه کاربردهای نظامی، سلاح‌های انرژی هدایت‌شده می‌توانند بر غیرنظامیان نیز تأثیر بگذارند. اگرچه هنوز ابهاماتی درباره استقرار و به‌کارگیری کامل این سلاح‌ها وجود دارد، نمونه‌های اولیه و کاربردهای اخیر آن‌ها نشان می‌دهد که این فناوری از مرحله صرفاً نظری فراتر رفته است^{۲۴۵}. این سلاح‌ها می‌توانند صدمات شدیدی، از جمله نابینایی و سوختگی، ایجاد کنند. برای مثال، لیزرهای پرانرژی^{۲۴۶} قادرند بافت‌های بدن را بسوزانند، در حالی که سلاح‌های مبتنی بر امواج میکروویو^{۲۴۷} از طریق گرم کردن مایعات بدن، درد شدید ایجاد کرده و ممکن است به آسیب‌های جدی و ماندگار^{۲۴۸} منجر شوند^{۲۴۹}. با توجه به این آثار، این سلاح‌ها و پیامدهای به‌کارگیری مستقیم آن‌ها

^{۲۳۷} Jamming

^{۲۳۸} Dazzling

^{۲۳۹} Bhaman Zohuri, Directed Energy Weapons (Switzerland, Springer, 2016)

^{۲۴۰} Speed-of-light action

^{۲۴۱} Scalability

^{۲۴۲} Logistical efficiency

^{۲۴۳} Low cost per shot

^{۲۴۴}. مراجعه کنید به :

www.nationaldefensemagazine.org/articles/2020/10/13/uptick-in-spending-seen-for-directed-energy-weapons.

^{۲۴۵}. مراجعه کنید به :

www.article36.org/wp-content/uploads/2019/06/directed-energy-weapons.pdf; and <https://nualslawjournal.com/2023/07/25/bringing-directed-energy-weapons-within-the-purview-of-the-arms-control-regime>.

^{۲۴۶} High-energy lasers

^{۲۴۷} Microwave weapons

^{۲۴۸} Lasting injuries

^{۲۴۹} Gary M. Vilke and Theodore C. Chan, "Less lethal technology", Policing: An International Journal, vol. 30, No. 3 (2007); and Erdem Eren Demir and others, "The role of non-lethal weapons in public security", Journal of Criminal Law and Criminology, vol. 60, No. 3 (July–December 2022).

نگرانی‌های جدی از منظر حقوق بشر، از جمله در ارتباط با حق بر سلامت، حق بر تمامیت جسمی و روانی، و حتی حق حیات و حق برخورداری از محیط‌زیستی سالم ایجاد می‌کنند. شایان ذکر است که پروتکل چهارم الحاقی به کنوانسیون منع یا محدودیت استفاده از برخی سلاح‌های متعارف که ممکن است بیش از حد آسیب‌زا یا دارای آثار غیرقابل تفکیک باشند (پروتکل چهارم، تحت عنوان پروتکل سلاح‌های لیزری کورکننده)^{۲۰} استفاده از سلاح‌های لیزری را که به‌طور خاص برای ایجاد نابینایی دائمی طراحی شده‌اند، ممنوع می‌کند.

بخش سوم) نقش دولت‌ها و بازیگران غیردولتی در طراحی، آموزش، استقرار، به‌کارگیری و اکتساب فناوری‌های جدید و نوظهور در حوزه نظامی

الف) تعهدات دولت‌ها در پیشگیری از نقض حقوق بین‌الملل و تنظیم‌گری و نظارت بر فناوری‌های جدید و نوظهور در حوزه نظامی

۵۷. تعهدات حقوقی بین‌المللی باید در تمامی مراحل طراحی، توسعه و به‌کارگیری فناوری‌های جدید و نوظهور در حوزه نظامی ادغام و رعایت^{۵۱} شوند. دولت‌ها مکلف‌اند اطمینان حاصل کنند که استفاده از این فناوری‌ها به‌طور کامل با حقوق بین‌الملل بشر، از جمله حق حیات، حق بر تمامیت جسمی و روانی، حق بر منع تبعیض، حق بر حریم خصوصی و حق برخورداری از محیط‌زیستی سالم، مطابقت دارد. تعهدات ناشی از حقوق بین‌الملل بشردوستانه نیز در این زمینه از اهمیت ویژه‌ای برخوردار است. دولت‌ها نه تنها موظف‌اند به قواعد این نظام حقوقی (که متضمن ممنوعیت‌ها و محدودیت‌هایی در خصوص سلاح‌ها، ابزارها و روش‌های جنگ است) «احترام بگذارند»^{۵۲} بلکه «به تضمین این احترام به»^{۵۳} حقوق بین‌الملل بشردوستانه مکلف‌اند (ماده ۱ مشترک کنوانسیون‌های چهارگانه ژنو). با این حال، دامنه و محتوای این تعهد اخیر هنوز به‌طور دقیق تبیین نشده و برخی از ابعاد آن همچنان محل تفسیر است. افزون بر این، دولت‌ها باید بررسی‌های حقوقی جامع و دقیق درباره سلاح‌ها را انجام دهند.

^{۲۰} Protocol on Blinding Laser Weapons (Protocol IV)

^{۵۱} Integrated into

^{۵۲} Respect

^{۵۳} Ensure respect

۵۸. تعهد به «تضمین احترام»^{۲۹۴} می‌کند که دولت‌ها اجرای حقوق بین‌الملل و اعمال آن را در سطح ملی تضمین کنند. در این چارچوب، تعهدات مربوط به دقت لازم تمامی اقداماتی را که برای پیشگیری از نقض حقوق بین‌الملل توسط بازیگران دولتی و غیردولتی، از جمله توسعه‌دهندگان فناوری‌های جدید و نوظهور ضروری است، در بر می‌گیرد. برای آنکه مسئولیت ناشی از نقض تعهد دقت لازم محقق شود، دو شرط باید احراز گردد:

(الف) دولت امکانات و توانایی لازم برای پیشگیری یا جلوگیری از نقض تعهد بین‌المللی را در اختیار داشته باشد

(ب) از خطر وقوع نقض آگاه بوده یا با توجه به اوضاع و احوال، می‌بایست از آن آگاه می‌بود.^{۲۹۵}

این مسئولیت، تمام چرخه عمر^{۲۹۶} فناوری‌های جدید و نوظهور را در بر می‌گیرد و مستلزم تضمین انطباق آن‌ها با حقوق بین‌الملل است. علاوه بر این، این ارزیابی باید به صورت مستمر و مداوم انجام شود.

۵۹. دولت‌ها مکلف‌اند تدابیر لازم را برای پیشگیری از نقض حقوق بشر در قلمرو صلاحیت خود^{۲۹۷} اتخاذ کنند.^{۲۹۸} عدم ایفای این تعهد ممکن است موجب تحقق مسئولیت بین‌المللی دولت^{۲۹۹} شود. به کارگیری فناوری‌های جدید و نوظهور در حوزه نظامی به احتمال زیاد تعهدات مضاعف و استانداردهای بالاتری از دقت لازم را بر دولت‌ها تحمیل می‌کند تا اطمینان حاصل شود که تمامی اقدامات احتیاطی عملی و امکان‌پذیر^{۳۰۰} برای پیشگیری از نقض حقوق بین‌الملل اتخاذ شده است.

۶۰. دولت همچنین ممکن است در قبال پیامدهای ناشی از رفتار بازیگران غیردولتی مسئول شناخته شود، چنانچه در اتخاذ تدابیر لازم برای پیشگیری، نظارت، تنظیم‌گری، تحقیق یا اعمال ضمانت‌اجرا^{۳۰۱} نسبت به آن پیامدها قصور ورزد.^{۳۰۲} بنابراین، دولت‌ها مکلف‌اند در ارتباط با توسعه، تحصیل و به کارگیری فناوری‌های جدید و نوظهور در حوزه نظامی توسط بازیگران غیردولتی، به تعهدات مربوط به دقت لازم عمل کنند.

^{۲۹۴} The duty to “ensure respect”

^{۲۹۵} Antal Berkes, “The standard of ‘due diligence’ as a result of interchange between the law of armed conflict and general international law”, Journal of Conflict and Security Law, vol. 23, No. 3 (winter 2018)

^{۲۹۶} Entire life cycle

^{۲۹۷} Under their jurisdiction

^{۲۹۸} A/HRC/30/20.

^{۲۹۹} International responsibility

^{۳۰۰} All feasible precautions

^{۳۰۱} Sanction

^{۳۰۲} Articles on responsibility of States for internationally wrongful acts.

۶۱. بخش خصوصی، به‌ویژه در حوزه هوش مصنوعی، ممکن است فناوری‌هایی را توسعه دهد که قابلیت انطباق و استفاده در مقاصد نظامی را داشته باشند. شتاب در تجاری‌سازی^{۲۶۳} این فناوری‌ها، غالباً به دست کم گرفتن مخاطرات آن‌ها منجر می‌شود؛ از جمله خطر سوءاستفاده از هوش مصنوعی مولد^{۲۶۴} در عملیات مخرب فناوری اطلاعات و ارتباطات یا کارزارهای انتشار اطلاعات نادرست و گمراه‌کننده^{۲۶۵}. نگرانی دیگر، گسترش کنترل‌نشده^{۲۶۶} این فناوری‌ها است که دسترسی بازیگران غیردولتی به آن‌ها را تسهیل می‌کند. این بازیگران غالباً فناوری‌های جدید و نوظهور در حوزه نظامی را با تدابیر حفاظتی کمتر و با استانداردهای پایین‌تری از دقت و قابلیت اعتماد، در مقایسه با دولت‌ها، به کار می‌گیرند. بازیگران غیردولتی همچنین ممکن است از فناوری‌های جدید و نوظهور برای ایجاد اختلال در سامانه‌های ارتباطی یا تحریف عملکرد آن‌ها استفاده کنند؛ امری که می‌تواند دقت و قابلیت اعتماد این سامانه‌ها را به مخاطره اندازد.

۶۲. گسترش شتابان هوش مصنوعی و دستگاه‌های متصل به اینترنت اشیا^{۲۶۷} نقش تعیین‌کننده‌ای در عملیات سایبری نظامی^{۲۶۸} آینده خواهد داشت. بهره‌برداری از این فناوری‌ها می‌تواند آسیب‌پذیری‌های موجود را ایجاد یا تشدید کند و این امکان را برای بازیگران غیردولتی فراهم آورد که سامانه‌های هوش مصنوعی را دستکاری کنند، سامانه‌های اینترنت اشیا را به خطر اندازند، خدمات حیاتی مانند خدمات بهداشتی و درمانی^{۲۶۹} را مختل سازند یا به ارتکاب جرایم سایبری بپردازند. چنین حملاتی ممکن است به نقض امنیت داده‌ها، اختلال در عملکرد سامانه‌ها، وارد آمدن خسارات فیزیکی و تهدید حق حیات و حق بر تمامیت جسمی و روانی منجر شوند.^{۲۷۰}

^{۲۶۳} Commercialize

^{۲۶۴} Generative AI

نوعی از هوش مصنوعی که قادر به تولید محتوای جدید، از جمله متن، تصویر، صدا، ویدئو یا کد، بر اساس داده‌هایی است که پیش‌تر بر روی آن‌ها آموزش دیده است. (توضیح افزوده بر متن)

^{۲۶۵} Disinformation campaigns

^{۲۶۶} Uncontrolled proliferation

^{۲۶۷} Internet of Things (IoT)

اینترنت اشیا شبکه‌ای از دستگاه‌های به هم پیوسته است که داده‌های بلادرنگ را به اشتراک می‌گذارند. در نیروهای مسلح، این فناوری حسگرها، وسایل نقلیه و تجهیزات را به هم متصل می‌کند تا نظارت، لجستیک و تصمیم‌گیری را بهبود بخشد.

^{۲۶۸} Military cyber operations

^{۲۶۹} Healthcare

^{۲۷۰} Nicholas Tsagourias, "Cyber attacks, self-defense and the problem of attribution", Journal of Conflict and Security Law, vol. 17, No. 2 (2012).

۶۳. با توجه به مخاطرات چندوجهی ناشی از کسب یا توسعه فناوری‌های جدید و نوظهور در حوزه نظامی توسط بازیگران غیردولتی، دولت‌ها بر اساس حقوق بین‌الملل دارای تعهدی اساسی در زمینه دقت لازم هستند تا به‌طور مؤثر درباره نقض‌های حقوق بشر تحقیق کنند، جبران خسارت و سایر راهکارهای مؤثر برای قربانیان این نقض‌ها را فراهم سازند و اشخاص یا نهادهای مسئول این نقض‌ها را مورد پیگرد و اعمال ضمانت‌اجرا^{۲۷۱} قرار دهند. اجرای این تعهد مستلزم اتخاذ اقداماتی از قبیل ایجاد یک چارچوب تنظیم‌گری مستحکم^{۲۷۲} برای حمایت از حق حیات، حق بر تمامیت جسمی و روانی، حق بر منع تبعیض، حق بر سلامت، حق بر خورداری از محیط‌زیستی سالم و حق بر حریم خصوصی، تقویت سازوکارهای نظارتی^{۲۷۳}؛ از جمله ارتقای امنیت سایبری^{۲۷۴}؛ گسترش همکاری‌های بین‌المللی و ارائه آموزش‌های جامع به ذی‌نفعان درباره مخاطرات بالقوه و سوءاستفاده^{۲۷۵} از فناوری‌های جدید و نوظهور در حوزه نظامی است. عدم رسیدگی مؤثر به این مخاطرات می‌تواند به نقض حق حیات، حق بر تمامیت جسمی و روانی، حق بر حریم خصوصی و حق بر منع تبعیض منجر شود.

ب) ارائه‌دهندگان و بنگاه‌های فعال در حوزه فناوری‌های جدید و نوظهور در حوزه نظامی

۶۴. دولت‌ها اصلی‌ترین استفاده‌کنندگان از فناوری‌های جدید و نوظهور در حوزه دفاع ملی و امنیت عمومی هستند. همچنین، آنان از طریق تأمین مالی پژوهش‌ها و تقویت مشارکت‌های میان بخش عمومی و بخش خصوصی^{۲۷۶}، توسعه این فناوری‌ها را تسهیل و حمایت می‌کنند. در مقابل، نهادهای بخش خصوصی، از جمله پیمانکاران صنایع دفاعی^{۲۷۷} و بنگاه‌های فعال در حوزه فناوری اطلاعات و ارتباطات، به‌عنوان نوآوران و توسعه‌دهندگان این فناوری‌ها ایفای نقش می‌کنند و خدماتی از قبیل طراحی، توسعه، استقرار، نگهداری و آموزش را ارائه می‌دهند.

۶۵. در سطح ملی، دولت‌ها با وضع چارچوب‌ها و استانداردهای حقوقی حاکم بر فعالیت بنگاه‌ها، نقش تنظیم‌گر^{۲۷۸} فناوری‌های جدید و نوظهور را ایفا می‌کنند. این چارچوب‌ها باید با تعهدات دولت‌ها ذیل حقوق بین‌الملل بشر سازگار باشند. حقوق بین‌الملل بشر، دولت‌ها را به رعایت، حمایت و تحقق حقوق بشر در ارتباط با فناوری‌های جدید و

^{۲۷۱} Sanction actors

^{۲۷۲} Robust regulatory framework

^{۲۷۳} Enhanced monitoring

^{۲۷۴} Strengthened cybersecurity

^{۲۷۵} Potential risks and misuse

^{۲۷۶} Public-private partnerships

^{۲۷۷} Defense contractors

^{۲۷۸} Regulators

نوظهور در حوزه نظامی ملزم می‌سازد. علاوه بر این، بنگاه‌های ذی‌ربط موظف‌اند تمامی قوانین و مقررات قابل اعمال را رعایت کرده و مطابق با آنچه در «اصول راهنما» آمده است، به حقوق بشر احترام بگذارند. این مسئولیت متوجه تمامی بنگاه‌های اقتصادی، از جمله شرکت‌های فناوری، صرف‌نظر از اندازه یا ساختار آن‌ها است.^{۲۷۹} بنگاه‌های اقتصادی باید از وقوع نقض حقوق بشر پیشگیری کرده و به هر گونه آثار و پیامدهای منفی ناشی از فعالیت‌های خود رسیدگی کنند. چنانچه نقض حقوق بشر رخ دهد، دولت‌ها موظف‌اند درباره آن تحقیق کنند و اطمینان حاصل نمایند که قربانیان به راهکارهای جبرانی مؤثر، از جمله از طریق سازوکارهای قضایی یا غیرقضایی مناسب، دسترسی دارند. «اصول راهنمای کسب و کار و حقوق بشر» و «گروه کاری موضوع حقوق بشر و شرکت‌های فراملی و سایر بنگاه‌های اقتصادی» [از سازوکارهای تابعه شورای حقوق بشر سازمان ملل] نقش اساسی در پیشگیری از نقض‌ها و کاهش آثار زیان‌بار آن‌ها ایفا می‌کنند. در همین راستا، گروه کاری یادشده خاطرنشان کرده است که شرکت‌های تولیدکننده تسلیحات غالباً در انجام دقت لازم در حوزه حقوق بشر، به‌ویژه در ارزیابی مخاطرات ناشی از استفاده از تجهیزات تولیدی آن‌ها در مخاصمات، کوتاهی می‌کنند.^{۲۸۰} افزون بر این، پروژه B-Tech دفتر کمیسر عالی حقوق بشر سازمان ملل متحد، رهنمودها و منابع معتبر و مرجع را برای اجرای «اصول راهنمای کسب و کار و حقوق بشر» در حوزه فناوری ارائه می‌کند و از بنگاه‌های اقتصادی و سیاست‌گذاران می‌خواهد که در مواجهه با چالش‌های ناشی از فناوری‌های جدید، رویکردی مبتنی بر حقوق بشر اتخاذ کنند.^{۲۸۱}

بخش چهارم) حقوق بشر در چرخه عمر فناوری‌های جدید و نوظهور در حوزه نظامی

الف) رویکرد مبتنی بر چرخه عمر

^{۲۷۹}. مراجعه کنید به:

www.ohchr.org/sites/default/files/2021-11/tech-2021-response-export-military-software.pdf

^{۲۸۰}. مراجعه کنید به:

www.ohchr.org/sites/default/files/2022-08/BHR-Arms-sector-info-note.pdf

^{۲۸۱}. مراجعه کنید به:

www.untoday.org/un-b-tech-project

۶۶. فناوری‌های جدید و نوظهور در حوزه نظامی، چالش‌های منحصربه‌فردی را برای حمایت و ارتقای حقوق بشر ایجاد می‌کنند. بسیاری از این فناوری‌ها ماهیتی دوکاربردی دارند که این امر، به‌ویژه در زمینه تعیین و توزیع مسئولیت‌ها^{۸۲} میان دولت‌ها و بازیگران بخش خصوصی، وضعیت را پیچیده‌تر می‌سازد. اتخاذ یک رویکرد مبتنی بر چرخه عمر برای مواجهه مؤثر با این چالش‌ها ضروری است تا از رعایت و حمایت از حقوق بشر در تمامی مراحل چرخه عمر این فناوری‌ها، از طراحی، توسعه و آموزش گرفته تا استقرار، بهره‌برداری عملیاتی و در نهایت امحا یا خروج از خدمت^{۸۳} آن‌ها، اطمینان حاصل شود.

۱. نهاده‌سازی حقوق بشر در مراحل طراحی و توسعه

۶۷. مرحله مفهوم‌پردازی^{۸۴} و طراحی فناوری‌های جدید و نوظهور در حوزه نظامی، نقشی اساسی در نهاده‌سازی ملاحظات حقوق بشری^{۸۵} از همان آغاز فرایند^{۸۶} ایفا می‌کند. این مرحله شامل شکل‌گیری ایده اولیه^{۸۷} و توسعه فناوری است؛ مرحله‌ای که در آن باید آثار و پیامدهای بالقوه فناوری بر حقوق بشر به‌صورت دقیق و جامع ارزیابی شود. فناوری‌ها ماهیتی خنثی ندارند^{۸۸} بلکه ذاتاً بر فرایندهای سیاست‌گذاری اثر می‌گذارند و ممکن است آزادی‌های فردی را محدود کنند^{۸۹}. از این رو، هم خود فناوری و هم طراحان و توسعه‌دهندگان آن می‌توانند بر حقوق بشر تأثیر بگذارند، زیرا فناوری‌ها و پدیدآورندگان آن‌ها غالباً بازتاب‌دهنده ارزش‌ها، پیش‌فرض‌ها و سوگیری‌های خاص هستند^{۹۰}.

۶۸. انجام ارزیابی‌های ناظر به تأثیر بر حقوق بشر^{۹۱} در این مراحل اولیه از اهمیت اساسی برخوردار است. این ارزیابی‌ها باید در فرایند توسعه فناوری ادغام شوند تا مخاطرات بالقوه برای حقوق بشر، از جمله حق بر حریم خصوصی، آزادی بیان، حق حیات، حق بر تمامیت جسمی و روانی، حق بر سلامت و حق بر برخورداری از محیط‌زیستی

^{۸۲} Allocation of responsibilities

^{۸۳} Disposal or decommissioning

^{۸۴} Conceptualization

^{۸۵} Embedding human rights considerations

^{۸۶} From the outset

^{۸۷} Ideation

^{۸۸} Technologies are not neutral

^{۸۹} A/HRC/47/52, para. 4

^{۹۰} Andrew Feenberg, *Transforming Technology* (Oxford, Oxford University Press, 2002); and Cathy O'Neil, *Weapons of Math Destruction* (New York, Crown, 2016)

^{۹۱} Human rights impact assessments

سالم، شناسایی و کاهش^{۲۹۲} یابند. هرچند نهاده‌سازی این ملاحظات^{۲۹۳} در مرحله طراحی می‌تواند به توسعه‌دهندگان در کاهش پیامدهای ناخواسته و سوءاستفاده‌های احتمالی کمک کند، اما ممکن است به‌تنهایی برای رفع کامل چالش‌ها و تعارض‌های ذاتی حقوقی^{۲۹۴} ناشی از برخی فناوری‌ها کافی نباشد. همچنان این پرسش مطرح است که آیا فناوری‌هایی مانند فناوری‌های به‌کاررفته در سامانه‌های تسلیحاتی خودمختار، اصولاً می‌توانند به‌طور کامل با استانداردهای حقوق بشر سازگار باشند، به‌ویژه هنگامی که استفاده از آن‌ها اصولی همچون حمایت از کرامت انسانی را با چالش مواجه می‌کند. از این رو، تضمین انطباق با استانداردهای بین‌المللی حقوق بشر، در برخی موارد، مستلزم تدوین چارچوب‌های تنظیم‌گری جامع‌تری است که به مسائل حقوقی خاص ناشی از این فناوری‌ها بپردازد.

۶۹. توسعه فناوری‌های جدید و نوظهور در حوزه نظامی غالباً مستلزم استفاده از مجموعه‌داده‌های بزرگ است. مجموعه‌داده‌هایی که ممکن است سوگیری‌های موجود را در خود بازتاب داده^{۲۹۵}، تثبیت و بازتولید کنند. برای پیشگیری از تبعیض، ضروری است که در مرحله طراحی، از الگوریتم‌های هوشیار نسبت به رعایت انصاف و مبتنی بر حقوق بشر^{۲۹۶} و تحلیل‌های مقاوم در مقابل فرضیات و استدلال‌های نادرست^{۲۹۷} استفاده شود. توسعه‌دهندگان همچنین باید تنوع در ترکیب تیم‌های توسعه را مدنظر قرار دهند و ارزیابی‌های [برگرفته از طیف‌های] متکثر^{۲۹۸} را انجام دهند تا احتمال استفاده از مجموعه‌داده‌های سوگیرانه و برنامه‌نویسی‌هایی که به تشدید پیش‌داوری‌ها و تبعیض^{۲۹۹} می‌انجامد، کاهش یابد.

۷۰. بنگاه‌های اقتصادی مشارکت‌کننده در توسعه فناوری‌های جدید و نوظهور موظف‌اند فعالیت‌ها و رویه‌های خود را با استانداردهای بین‌المللی حقوق بشر، به‌ویژه «اصول راهنمای کسب‌وکار و حقوق بشر»، همسو سازند. این امر مستلزم انجام دقت لازم در حوزه حقوق بشر است تا اطمینان حاصل شود که فناوری‌های توسعه‌یافته توسط این بنگاه‌ها، چه در بسترهای نظامی و چه در کاربردهای غیرنظامی، به نقض یا سوءاستفاده از حقوق بشر منجر نمی‌شوند یا در آن مشارکت ندارند. از آنجا که دولت‌ها نیز دارای تعهد به دقت لازم هستند، باید فعالیت بخش‌هایی را که بازیگران بخش

^{۲۹۲} Identify and mitigate

^{۲۹۳} Embedding these considerations

^{۲۹۴} Inherent legal tensions

^{۲۹۵} Embed and perpetuate biases

^{۲۹۶} Human rights-based fairness-aware algorithms

^{۲۹۷} Counterfactual analysis

^{۲۹۸} Diversity audits

^{۲۹۹} Exacerbate prejudices

خصوصی در آن‌ها فعالیت می‌کنند، به‌طور مؤثر تنظیم‌گری کنند و در چارچوب حقوق داخلی، تعهدات لازم را برای بنگاه‌های اقتصادی به‌منظور رعایت حقوق بشر مقرر سازند.

۲. مدیریت مخاطرات در مراحل استقرار و به‌کارگیری عملیاتی

۷۱. با ورود فناوری‌های جدید و نوظهور به مرحله بهره‌برداری عملیاتی، احتمال وقوع نقض حقوق بشر افزایش می‌یابد. از این‌رو، ضروری است استانداردهای حقوقی سخت‌گیرانه‌ای^{۳۰۰} وضع شود که در تمامی مراحل استقرار و به‌کارگیری این فناوری‌ها، رعایت کرامت انسانی، حفظ کنترل معنادار انسانی^{۳۰۱}، شفافیت^{۳۰۲} و پاسخگویی^{۳۰۳} را تضمین کند. به‌ویژه در شرایطی که اتوماسیون و هوش مصنوعی ممکن است به از دست رفتن کنترل معنادار انسانی، بروز سوگیری ناشی از اتوماسیون یا استفاده نادرست از فناوری به شیوه‌ای منجر شوند که ناقض حقوق بین‌الملل باشد.

۷۲. فرایندهای راستی‌آزمایی^{۳۰۴}، آزمون و ارزیابی باید با مشارکت گروه‌های متنوع انجام شوند تا سوگیری‌های احتمالی شناسایی و برطرف شوند و عواملی همچون سن، نژاد و جنسیت در این فرایندها مورد توجه قرار گیرند. این امر به تضمین آن کمک می‌کند که فناوری‌های جدید و نوظهور در حوزه نظامی آثار منفی خود بر حقوق بشر گروه‌های آسیب‌پذیر را تشدید نکنند و به تداوم یا بازتولید نابرابری‌های موجود دامن نزنند^{۳۰۵}. دولت‌ها باید یک چارچوب تنظیم‌گری مبتنی بر ارزیابی ریسک اتخاذ کنند و در مورد فناوری‌های پرخطری که تهدیدهای جدی علیه حق حیات، حق بر سلامت، امنیت شخصی و سایر حقوق بشر ایجاد می‌کنند، مقررات سخت‌گیرانه‌تر یا، حسب مورد، ممنوعیت‌هایی را اعمال کنند.

۷۳. شفافیت^{۳۰۶} در استقرار و به‌کارگیری فناوری‌های جدید و نوظهور، به‌ویژه در خصوص داده‌ها و الگوریتم‌های مورد استفاده، از اهمیت اساسی برخوردار است. برای شناسایی و رفع سوگیری‌های موجود در خروجی سامانه‌ها، باید از سازوکارهای دقت لازم، از جمله ابزارهای شناسایی سوگیری و ممیزی الگوریتم‌ها^{۳۰۷}، استفاده شود.

^{۳۰۰} Stringent legal standards

^{۳۰۱} Meaningful human control

^{۳۰۲} Accountability

^{۳۰۳} Transparency

^{۳۰۴} Verification

^{۳۰۵} Perpetuate existing inequalities

^{۳۰۶} Transparency

^{۳۰۷} Algorithm audits

۳. تدابیر حفاظتی در مراحل امحا، خروج از خدمت و پیشگیری از اشاعه [فناوری ها]

۷۴. مرحله نهایی چرخه عمر فناوری‌های جدید و نوظهور در حوزه نظامی (یعنی امحا یا خروج از خدمت) ملاحظات خاص خود را از منظر حقوق بشر و امنیت به همراه دارد. این مرحله شامل برچیدن فیزیکی^{۳۰۸} فناوری‌ها، دفع ایمن مواد خطرناک و حفاظت از داده‌های حساس گردآوری شده در طول مرحله بهره‌برداری عملیاتی است. اجرای تدابیر حفاظتی برای جلوگیری از خروج خارج از مسیر قانونی^{۳۰۹} مواد موجود در ذخایر و انبارها و نیز جلوگیری از فروش غیرمجاز تجهیزات مازاد، به‌منظور مقابله با مخاطرات اشاعه^{۳۱۰} امری ضروری است. همچنین، تضمین انجام این فرایندها با رعایت شفافیت و پاسخگویی و پیشگیری از تحمیل آثار نامتناسب^{۳۱۱} بر گروه‌هایی که به‌طور تاریخی در حاشیه قرار گرفته‌اند^{۳۱۲} از جمله مردمان بومی و زنان، برای حمایت از حقوق بشر اهمیت اساسی دارد^{۳۱۳}.

۷۵. با توجه به تحولات شتابان در عرصه فناوری‌های جدید و نوظهور در حوزه نظامی، اتخاذ تدابیر پیشگیرانه، جامع و مؤثر برای حمایت از حقوق بشر امری ضروری است. تحلیل‌های ارائه‌شده در این گزارش بر ضرورت تقویت چارچوب حقوقی بین‌المللی، افزایش پاسخگویی بنگاه‌های اقتصادی و تحکیم همکاری‌های چندجانبه^{۳۱۴} تأکید می‌کند. جامعه بین‌المللی می‌تواند از طریق ایجاد سازوکارهای نظارتی دقیق و مؤثر و ترویج شفافیت و مسئولیت‌پذیری حقوقی، اطمینان حاصل کند که توسعه، استقرار و خروج از خدمت فناوری‌های جدید و نوظهور در حوزه نظامی با اصول حقوق بشر سازگار بوده و در راستای رعایت آن‌ها انجام می‌شود.

(ب) شفافیت و پاسخگویی

۷۶. گسترش فناوری‌های جدید و نوظهور، چالش‌های حقوقی و تنظیم‌گری بی‌سابقه‌ای را به همراه آورده است. هوش مصنوعی این پرسش را مطرح می‌سازد که آیا چارچوب‌های حقوقی و تنظیم‌گری موجود برای مواجهه با این

^{۳۰۸}Physical dismantling

^{۳۰۹}Diversion

^{۳۱۰}Proliferation risks

^{۳۱۱}Differentiated impacts

^{۳۱۲}Historically marginalized populations

^{۳۱۳}A/75/290.

^{۳۱۴}Robust multilateral cooperation

تحولات کفایت می‌کنند.^{۳۱۵} در مواردی که خطرات جدی برای حقوق بشر وجود دارد، فشارها برای تسریع در بازنگری این چارچوب‌ها و ایجاد سازوکارهای جدید شفافیت و پاسخگویی به‌طور فزاینده‌ای افزایش یافته است.^{۳۱۶}

۷۷. فناوری‌های جدید و نوظهور می‌توانند عملکردها در انجام وظایف پیچیده را ارتقا دهند و به‌عنوان «تقویت‌کننده توان عملیاتی»^{۳۱۷}، سرعت، دقت و توانمندی‌های انسانی را افزایش دهند.^{۳۱۸} این فناوری‌ها به‌طور فزاینده‌ای در گردآوری اطلاعات، نظارت، شناسایی، تصمیم‌گیری نظامی و نیز در وظایفی مانند راستی‌آزمایی و انتخاب هدف به کار گرفته می‌شوند.^{۳۱۹} با این حال، بسیاری از این سامانه‌ها به‌صورت «جعبه سیاه» عمل می‌کنند؛ به این معنا که نحوه عملکرد و فرایند تصمیم‌گیری آن‌ها به دشواری قابل تفسیر و حتی دشوارتر از آن، قابل توضیح است. با توجه به اهمیت پیش‌بینی‌پذیری و قابلیت فهم در سامانه‌های هوش مصنوعی، اطمینان از اینکه این سامانه‌ها مطابق انتظار عمل می‌کنند و عملکرد آن‌ها برای انسان قابل درک است، از اهمیت اساسی برخوردار است. تلاش‌ها برای روشن ساختن سازوکارهای درونی این فناوری‌ها به‌طور فزاینده‌ای نوآورانه شده و نتایج قابل توجهی در ارتقای شفافیت به همراه داشته است. پژوهش‌های مربوط به توسعه «هوش مصنوعی توضیح‌پذیر»^{۳۲۰} نیز به‌طور چشمگیری گسترش یافته و در افزایش شفافیت سامانه‌های هوش مصنوعی موفقیت‌هایی به دست آورده است؛ امری که می‌تواند به کارگیری این فناوری‌ها را در حوزه‌های حساس و پرخطر تسهیل کند.^{۳۲۱} هدف بنیادین از توسعه هوش مصنوعی توضیح‌پذیر، رفع

^{۳۱۵} Stefan Larsson and Fredrik Heintz, “Transparency in artificial intelligence”, Internet Policy Review, vol. 9, No. 2 (2020); and Jordan Richard Schoenherr and others, “Designing AI using a human centered approach”, IEEE Transactions on Technology and Society, vol. 4, No. 1 (March 2023)

^{۳۱۶} A/HRC/48/31.

^{۳۱۷} Force multipliers

^{۳۱۸} Jonathan Han Chung Kwik and Tom van Engers, “Algorithmic fog of war”, Journal of Future Robot Life, vol. 2, No. 1 (2021).

^{۳۱۹} Hannah Bryce and Jacob Parakilas, “Conclusions and recommendations”, in Artificial Intelligence and International Affairs: Disruption Anticipated, M.L. Cummings and others, eds. (London, Chatham House, ۲۰۱۸); and ICRC, “Artificial intelligence and machine learning in armed conflict: a human-centred approach” (Geneva, 2019).

^{۳۲۰} Explainable AI (XAI)

رویکردی در طراحی سامانه‌های هوش مصنوعی که هدف آن قابل فهم و قابل توضیح کردن فرایند تصمیم‌گیری و خروجی‌های این سامانه‌ها برای انسان است. (توضیح افزوده بر متن)

^{۳۲۱} Arthur Holland Michel, “The black box, unlocked” (United Nations Institute for Disarmament Research, 2020); and Arun Das and Paul Rad, “Opportunities and challenges in explainable artificial intelligence (XAI)”, arXiv preprint (2020).

نگرانی‌های ناشی از فقدان شفافیت و پاسخگویی کافی است. با این حال، مخاطرات ناشی از پیاده‌سازی این رویکرد، از جمله نقض حریم خصوصی و افزایش آسیب‌پذیری سامانه‌ها در نتیجه شفافیت بیشتر، نباید نادیده گرفته شود.^{۳۲۲}

۷۸. حقوق بین‌الملل بشر مستلزم شفافیت است. در زمینه فناوری‌های جدید و نوظهور در حوزه نظامی، این امر به معنای تضمین دسترسی به اطلاعات مرتبط با توسعه، استقرار و آثار این فناوری‌ها است. شفافیت همچنین برای تضمین انطباق استفاده از این فناوری‌ها با حقوق بین‌الملل و حمایت از حقوقی همچون آزادی عقیده و بیان، حق بر حریم خصوصی، حق بر عدم تبعیض و حق بر برابری، از اهمیت اساسی برخوردار است.

۷۹. علاوه بر این، یکی از مسائل مهم در مواجهه با مخاطرات ناشی از فناوری‌های جدید و نوظهور در حوزه نظامی، آن است که قابلیت‌های تصمیم‌گیری ادغام‌شده در این سامانه‌ها ممکن است سوگیری‌ها و الگوهای تبعیض موجود در جامعه را بازتاب داده یا بازتولید کنند. یکی از چالش‌های اصلی، اطمینان از آن است که شکاف‌های موجود در فرایندهای گردآوری، پردازش و نگهداری داده‌ها، به تداوم یا تشدید نقض حقوق بشر منجر نشوند. رسیدگی به این چالش‌ها مستلزم شفافیت و اتخاذ سازوکارهای مؤثر پاسخگویی است؛ به گونه‌ای که تمامی بازیگران ذی‌ربط در قبال استفاده اخلاقی و قانونی از فناوری‌های جدید و نوظهور مسئول و پاسخگو باشند.

ج) خلأهای موجود در چارچوب کنونی حقوق بشر

۸۰. فناوری‌های جدید و نوظهور در حوزه نظامی، اجرای چارچوب‌های موجود حقوق بین‌الملل بشر را با چالش‌هایی مواجه می‌سازند. هرچند رعایت حقوق بین‌الملل امری ضروری است، برای تضمین حمایت مؤثر از حقوق بشر در این حوزه، باید به خلأهای اساسی موجود رسیدگی شود. با وجود اهمیت «اصول راهنمای کسب و کار و حقوق بشر» و فعالیت‌های پروژه B-Tech دفتر کمیساریای عالی حقوق بشر سازمان ملل متحد، هنوز استانداردهای بین‌المللی حقوق بشر که به‌طور مشخص الزامات حقوق بین‌الملل بشر را در زمینه فناوری‌های جدید و نوظهور در حوزه نظامی برای دولت‌ها و بازیگران غیردولتی تبیین کنند، وجود ندارند. افزون بر این، در سطح ملی نیز فناوری‌های جدید و نوظهور در حوزه نظامی تا حد زیادی فاقد مقررات هستند و چارچوب‌های قانونی یا سیاستی لازم برای هدایت صنعت و

^{۳۲۲}. مراجعه کنید به:

www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-11-16_techdispatch-22023-explainable-artificial-intelligence_en.

توسعه‌دهندگان در زمینه طراحی، توسعه و آزمون این فناوری‌ها وجود ندارد؛ چارچوب‌هایی که باید تضمین کنند تدابیر و سازوکارهای حفاظتی^{۳۳} روشن و منطبق با تعهدات حقوقی بین‌المللی ایجاد و اجرا شوند.

۸۱. برای مثال، راهبردهای شفاف تدارکات که کل زنجیره تأمین فناوری‌های جدید و نوظهور در حوزه نظامی را در برمی‌گیرند و تدابیر حفاظتی مبتنی بر حقوق بین‌الملل بشر را پیش‌بینی کنند، وجود ندارند و این امر خطر استفاده‌های تبعیض‌آمیز از برخی فناوری‌ها را افزایش می‌دهد. افزون بر این، فقدان سازوکارهای نظارتی بین‌المللی بر توسعه، تأمین و استفاده از این فناوری‌ها در حوزه نظامی، اجرای مؤثر تعهدات حقوقی بین‌المللی را، به‌ویژه در مواردی که مقررات ملی کافی نیستند، با مانع مواجه می‌سازد. اگرچه برخی کشورها چارچوب‌های تنظیم‌گری را به اجرا گذاشته‌اند، همچنان کاستی‌های قابل توجهی در سازوکارهای ملی نظارت و راستی‌آزمایی، به‌ویژه در ارتباط با بنگاه‌های اقتصادی و ارائه‌دهندگان فناوری‌های جدید و نوظهور در بخش خصوصی و بر مبنای «اصول راهنمای کسب‌وکار و حقوق بشر»، وجود دارد. این کاستی‌ها توانایی دولت‌ها را برای تضمین انطباق با استانداردهای ملی و بین‌المللی حقوق بشر محدود می‌کند. از این رو، رفع این خلأهای تنظیم‌گری برای پیشگیری از نقض و سوءاستفاده از حقوق بشر ناشی از توسعه و استفاده از فناوری‌های جدید و نوظهور در حوزه نظامی، امری ضروری است.

۸۲. یکی دیگر از خلأهای اساسی در چارچوب کنونی حقوق بین‌الملل بشر، به پیامدهای زیست‌محیطی فناوری‌های جدید و نوظهور مربوط می‌شود. توسعه، آموزش و استقرار این فناوری‌ها مستلزم مصرف بالای انرژی، تولید حجم قابل توجهی از انتشار کربن^{۳۴} و استفاده گسترده از مواد خامی همچون نیکل، کبالت و گرافیت است که پیامدهای بلندمدتی برای محیط زیست به همراه دارد.^{۳۵} این پیامدها، از جمله، شامل استفاده گسترده از آب برای خنک‌سازی مراکز داده و دفع پسماندهای خطرناک^{۳۶} در مرحله خروج از خدمت این فناوری‌ها می‌شود. حمایت از حقوق زیست‌محیطی همچنان به دلیل فقدان چارچوب‌های حقوقی جهانی و سازوکارهای اجرایی مؤثر با چالش مواجه است. در این زمینه، افشای شفاف اطلاعات، پایش مستحکم و مستمر زیست‌محیطی و ایجاد یک چارچوب پاسخگویی مبتنی بر همکاری، برای حمایت از حق بر محیط زیست پاک، سالم و پایدار ضروری است.

^{۳۳} Protective barriers

^{۳۴} Carbon footprint

^{۳۵} Wichuta Teeratanabodee, "The environmental impact of military AI", IDSS Paper No. 039 (S. Rajaratnam School of International Studies, 2022).

^{۳۶} Disposal of hazardous waste

توصیه‌ها

الف) دولت‌ها و جامعه بین‌المللی

۸۳. دولت‌ها باید فوراً راهبردها و سیاست‌های ملی را تدوین کرده و طراحی، توسعه و استفاده مسئولانه از فناوری‌های جدید و نوظهور در حوزه نظامی را، مطابق با تعهدات خود ذیل حقوق بین‌الملل، تنظیم‌گری^{۳۲۷} کنند. این امر مستلزم ایجاد چارچوب‌های جامع و مستحکم برای بازبینی تسلیحات^{۳۲۸} است که چالش‌های خاص ناشی از تسلیحات مبتنی بر فناوری‌های جدید و نوظهور را مورد توجه قرار دهد و نیز استقرار سازوکارهای مؤثر پیشگیرانه و پاسخگویی برای توسعه و استقرار این تسلیحات را تضمین کند. علاوه بر این، سازوکارهای نهادی باید به‌منظور پیش‌بینی و رسیدگی به موارد بالقوه نقض حقوق بشر تقویت شوند و در این راستا، توجه ویژه‌ای به ارتقای ظرفیت‌های نظارتی^{۳۲۹} نهادهای داخلی، از جمله نهادهای ملی حقوق بشر، معطوف شود.

۸۴. دولت‌ها و سازمان‌های بین‌المللی باید ملاحظات ناشی از حقوق بین‌الملل بشر را در تمامی مذاکرات چندجانبه مربوط به فناوری‌های جدید و نوظهور در حوزه نظامی وارد و ادغام کنند؛ به‌ویژه در چارچوب کارگروه دوم کمیسیون خلع سلاح، در ارتباط با تدوین توصیه‌های آن درباره تفاهم‌های مشترک پیرامون فناوری‌های نوظهور در امنیت بین‌المللی. هرگونه چارچوبی که در این زمینه تدوین می‌شود، باید علاوه بر ملاحظات امنیتی، مخاطرات حقوق بشری، از جمله رویه‌های تبعیض‌آمیز، را نیز مورد توجه قرار دهد. افزون بر این، چارچوب حقوق بین‌الملل بشر باید در مباحث مربوط به سامانه‌های تسلیحاتی خودمختار، از جمله در چارچوب گروه کارشناسان دولتی، نیز مورد توجه و بررسی قرار گیرد.

۸۵. دولت‌ها باید برای مقابله با چالش‌های امنیتی مرتبط، مشارکت‌های راهبردی را دنبال کنند. استمرار گفت‌وگوها، تبادل بهترین رویه‌ها^{۳۳۰} و ایجاد چارچوب‌های فراگیر با مشارکت دولت‌ها، بخش خصوصی، محافل دانشگاهی و سایر ذی‌نفعان، به حفظ ثبات و کاهش مخاطرات کمک خواهد کرد. همچنین، باید به اشتراک‌گذاری بررسی‌های حقوقی مربوط به فناوری‌های جدید و نوظهور در حوزه نظامی در اولویت قرار گیرد. افزون بر این، تقویت همکاری

^{۳۲۷}Regulate

^{۳۲۸}Weapon review

^{۳۲۹}Oversight capacities

^{۳۳۰}Best practice exchanges

میان جوامع علمی و فنی، جامعه مدنی و مدافعان و دست‌اندرکاران حقوق بشر، استفاده مسئولانه از فناوری‌های جدید و نوظهور در حوزه نظامی را ترویج خواهد کرد.

۸۶. دولت‌ها و سازمان‌های بین‌المللی باید اتخاذ اقدامات الزام‌آور یا سایر تدابیر مؤثر را برای تضمین این امر مدنظر قرار دهند که فناوری‌های جدید و نوظهور در حوزه نظامی که طراحی، توسعه یا استفاده از آن‌ها خطرات جدی سوءاستفاده، استفاده نادرست یا ورود آسیب‌های جبران‌ناپذیر^{۳۳۱} را به همراه دارد (به‌ویژه در مواردی که این خطرات ممکن است به نقض حقوق بشر منجر شوند) توسعه نیابند، مستقر نشوند و مورد استفاده قرار نگیرند. این امر، از جمله، فناوری‌های نظارت انبوه را که ناقض حق بر حریم خصوصی هستند^{۳۳۲} و نیز زیست‌فناوری‌ها و فناوری‌های عصبی را که، به‌ویژه در بسترهای قهرآمیز^{۳۳۳}، تمامیت جسمی و روانی افراد را تهدید می‌کنند، در بر می‌گیرد.

۸۷. دولت‌ها باید به‌طور قاطع تضمین کنند^{۳۳۴} که سامانه‌های تسلیحاتی خودمختار، مگر آنکه تحت کنترل معنادار انسانی عمل کنند، توسعه نیابند یا مستقر نشوند. همچنین، باید مقررات روشن و الزام‌آوری به‌منظور تضمین انطباق کامل این سامانه‌ها با استانداردهای حقوق بین‌الملل^{۳۳۵} به تصویب برسد.

۸۸. دولت‌ها باید با انجام ارزیابی‌های ریسک و ارزیابی‌های تأثیر بر حقوق بشر در مورد تمامی انواع فناوری‌های جدید و نوظهور در حوزه نظامی، اصل دقت لازم و اصل احتیاط را اعمال کنند. نهادهای مستقل، از جمله نهادهای ملی حقوق بشر، باید هدایت این ارزیابی‌ها را بر عهده داشته باشند^{۳۳۶} تا مشارکت عمومی و نظارت دموکراتیک تضمین شود. نتایج این ارزیابی‌ها باید مبنای تصمیم‌گیری دولت‌ها برای اتخاذ تدابیر لازم به‌منظور پیشگیری از ورود آسیب، تعلیق استفاده از فناوری‌های پرخطر و اجرای هنجارهای حاکم بر استفاده مسئولانه از فناوری‌های جدید و نوظهور در حوزه نظامی قرار گیرد. همکاری با چارچوب‌های بین‌المللی موجود (از جمله چارچوب‌های ایجادشده ذیل «کنوانسیون منع توسعه، تولید، انباشت و به‌کارگیری سلاح‌های شیمیایی و انهدام آن‌ها»^{۳۳۷} و «کنوانسیون سلاح‌های بیولوژیک»^{۳۳۸} که توسعه، تولید، تحصیل، انباشت، انتقال یا استفاده از سلاح‌های بیولوژیک، سمی و

^{۳۳۱} Irreversible harm

^{۳۳۲} Infringe on privacy

^{۳۳۳} Coercive contexts

^{۳۳۴} Categorically ensure

^{۳۳۵} Full compliance with international legal standards

^{۳۳۶} Lead these assessments

^{۳۳۷} Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons

^{۳۳۸} Biological Weapons Convention

شیمیایی را ممنوع می‌کنند) برای تقویت حکمرانی و ارتقای پاسخ جهانی به چالش‌های ناشی از فناوری‌های جدید و نوظهور، امری ضروری است.

۸۹. دولت‌ها و سازمان‌های بین‌المللی باید در حکمرانی فناوری‌های جدید و نوظهور در حوزه نظامی، رویکردی مبتنی بر همکاری اتخاذ کنند و ضمن تضمین رعایت حقوق بین‌الملل، به آثار نامتناسب این فناوری‌ها بر کشورهای کم‌برخوردار از منابع^{۳۳۹} نیز رسیدگی کنند؛ زیرا نابرابری‌ها در زمینه هوش مصنوعی و فناوری‌های نظامی نه تنها شکاف‌های موجود^{۳۴۰} را تشدید می‌کنند، بلکه ظرفیت ایجاد بی‌ثباتی بلندمدت را نیز دارند. دولت‌هایی که از توانایی لازم برخوردارند (از جمله دولت‌های توسعه‌دهنده این فناوری‌ها) باید از طریق به‌اشتراک‌گذاری دانش، ارائه کمک‌های فنی و اتخاذ تدابیری برای کاهش آثار بی‌ثبات‌کننده^{۳۴۱} این فناوری‌ها، در کاهش آسیب‌های ناشی از آن‌ها نقش ایفا کنند.

ب) بنگاه‌های اقتصادی

۹۰. بنگاه‌های اقتصادی، به‌ویژه در بخش‌های دفاعی و امنیتی، باید مطابق با «اصول راهنمای کسب‌وکار و حقوق بشر» به حقوق بشر احترام بگذارند و از طریق استقرار تدابیر حفاظتی قابل‌سنجش^{۳۴۲} و متناسب با شرایط خاص هر حوزه، و نیز حذف سوگیری‌ها و تبعیض از طریق انجام ارزیابی‌های تأثیر بر حقوق بشر، به این تعهد عمل کنند. این تدابیر باید، تا حد امکان، با در نظر گرفتن ملاحظات مربوط به محرمانگی صنعتی^{۳۴۳} از جمله گزارش‌دهی بنگاه‌های اقتصادی و راستی‌آزمایی مستقل، به گونه‌ای طراحی شوند که مشارکت فراگیر و متنوع جامعه مدنی را تضمین کنند. افزون بر این، شرکت‌ها باید مقررات وضع شده از سوی دولت‌ها را رعایت کنند و در عین حال، استانداردهای مبتنی بر ارزیابی مخاطرات حقوق بشری، از جمله الزامات مربوط به شفافیت، را بیش از پیش توسعه داده و در فعالیت‌های خود به کار گیرند. همچنین، سازوکارهای مرتبط با این استانداردها باید به‌طور منظم مورد بازنگری قرار گیرند تا اثربخشی آن‌ها و انطباقشان با حقوق بین‌الملل بشر تضمین شود.

۹۱. بنگاه‌های اقتصادی باید، مطابق با «اصول راهنمای کسب‌وکار و حقوق بشر»، فرایند دقت لازم در زمینه حقوق بشر را ایجاد و اجرا کنند تا بتوانند نحوه تأثیر فناوری‌های جدید و نوظهور در حوزه نظامی بر حقوق بشر را شناسایی،

^{۳۳۹} Less-resourced nations

^{۳۴۰} Existing disparities

^{۳۴۱} Destabilizing effects

^{۳۴۲} Measurable safeguards

^{۳۴۳} Industry secrecy

از آن پیشگیری، آثار آن را کاهش داده و در قبال آن پاسخگو باشند. این بنگاه‌ها همچنین باید به صورت پیشگیرانه، این فناوری‌ها و مدل‌های هوش مصنوعی را از منظر مخاطرات احتمالی، از جمله آثار آن‌ها بر حقوق بشر و امنیت بین‌المللی، ارزیابی کنند. چنانچه انجام آزمون‌های مربوط به مخاطرات شدید به دلیل طبقه‌بندی‌های دفاعی^{۳۴۴} با محدودیت مواجه باشد، هماهنگی با مراجع ملی ذی‌صلاح پیش از انتشار یا عرضه این فناوری‌ها، برای تضمین انطباق با حقوق بین‌الملل ضروری است.

ج) تمامی ذی‌نفعان

۹۲. همه ذی‌نفعان، از جمله محافل دانشگاهی، بنگاه‌های اقتصادی، جامعه مدنی، سازمان‌های بین‌المللی و دولت‌ها، باید پژوهش درباره پیامدهای حقوق بشری فناوری‌های جدید و نوظهور در حوزه نظامی را در اولویت قرار دهند و از سیاست‌هایی حمایت کنند که آثار فناوری‌های تحول‌آفرین^{۳۴۵} را ارزیابی می‌کنند و در عین حال، بر وابستگی متقابل، تفکیک‌ناپذیری و جهان‌شمولی تمامی حقوق بشر در تمامی مراحل توسعه این فناوری‌ها تأکید دارند.

۹۳. همه ذی‌نفعان باید برای تضمین توسعه و استقرار مسئولانه^{۳۴۶} فناوری‌های جدید و نوظهور در حوزه نظامی با یکدیگر همکاری کنند و اطمینان حاصل کنند که تنظیم‌گری این فناوری‌ها همگام با پیشرفت‌های فناوری به‌روز می‌شود. همچنین، آنان باید از گفت‌وگوی بین‌المللی به‌منظور تدوین و اجرای چارچوب‌های حقوقی تضمین‌کننده حمایت از حقوق بشر حمایت کنند.

^{۳۴۴} Defense classifications

^{۳۴۵} Disruptive technologies

^{۳۴۶} Responsible development and deployment

