Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

هوش مصنوعی و جنگ‌های سایبری: ابعاد حقوقی مسئولیت دولت‌ها در حقوق بین الملل

صفیه طلائی کارشناسی ارشد حقوق بین الملل، دانشگاه آزاد اسلامی، تبریز، ایران

دکتر محمدهادی جعفرپور مدرس دانشگاه آزاد اسلامی، گروه حقوق

فصلنامه علمی فقه و حقوق نوین

Print ISSN: 2717- 1469
Online ISSN: 2717 – 1477

ISC.SID.NOORMAGZ.MAGIRAN
GOOGLESCHOLAR.ENSANI
www.jaml .ir

سال ۱۴۰۴، سال ششم، شماره ۲۲،
صفحات ۱۳-۱

چکیده

با گسترش سریع فناوری‌های نوین به‌ویژه در حوزه هوش مصنوعی، ساختار و شیوه‌های سنتی مخاصمات مسلحانه دگرگون شده‌اند. بهره‌گیری از سامانه‌های هوشمند در حملات سایبری، مسئولیت دولت‌ها را در قبال اقدامات صورت‌گرفته در فضای مجازی با پرسش‌های جدیدی مواجه کرده است؛ به‌ویژه از حیث انتساب عمل، اثبات نقض قواعد آمره و لزوم رعایت اصول بنیادین حقوق بین‌الملل مانند حاکمیت، منع توسل به زور و اصل عدم مداخله.این مقاله با هدف تحلیل ابعاد حقوقی جنگ‌های سایبری متکی بر هوش مصنوعی، ضمن بررسی چارچوب‌های موجود در حقوق بین‌الملل عمومی و حقوق مخاصمات مسلحانه، به چالش‌های مرتبط با مسئولیت بین‌المللی دولت‌ها می‌پردازد. در این راستا، نقش سازمان‌های بین‌المللی، خلأهای حقوقی موجود، و ضرورت تدوین قواعد جدید مورد بررسی قرار می‌گیرد تا راهکاری برای ارتقاء پاسخ‌گویی حقوقی در مواجهه با تهدیدات نوین ارائه گردد.

واژگان کلیدی: هوش مصنوعی، جنگ سایبری، مسئولیت بین‌المللی، حقوق بین‌الملل، انتساب، مخاصمات مسلحانه، حاکمیت دولت‌ها

طبقه‌بندی JEL: فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Artificial Intelligence and Cyberwarfare: Legal Dimensions of State Responsibility in International Law

Scientific Journal of Modern Jurisprudence and Law

Print ISSN: 2717- 1469
Online ISSN: 2717 - 1477

Profile in ISC,SID, Noormags, Magiran, Ensani, GoogleScholar
www.jaml .ir

Year 2025، Sixth year ,Issue 22

Pages 1-13

Safiye talae — Master of International Law, Islamic Azad University, Tabriz, Iran

Dr.Mohammad Hadi Jafarpour — Lecturer at Islamic Azad University, Law Department

Abstract

The rapid advancement of emerging technologies, particularly in the field of artificial intelligence, has significantly transformed the traditional framework and methods of armed conflict. The deployment of intelligent systems in cyberattacks raises new legal questions regarding state responsibility for actions committed in cyberspace—especially in terms of attribution, the breach of peremptory norms, and adherence to core principles of international law such as sovereignty, the prohibition of the use of force, and non-intervention.This article aims to analyze the legal dimensions of AI-driven cyber warfare by examining existing frameworks under public international law and the law of armed conflict. It addresses the challenges of holding states internationally accountable and evaluates the role of international organizations, existing legal gaps, and the urgent need for new regulatory norms to ensure enhanced legal accountability in the face of emerging threats.

Keywords: Artificial Intelligence, Cyber Warfare, State Responsibility, International Law, Attribution, Armed Conflict, State Sovereignty

JEL Classification: Jurisprudence - Law - Criminal and Criminology - International Law - Private Law

مقدمه

در دهه‌های اخیر، فناوری‌های نوظهور به‌ویژه در حوزه هوش مصنوعی، مرزهای سنتی مخاصمات و تعاملات بین‌المللی را به‌طور چشمگیری جابه‌جا کرده‌اند. فضای سایبری به یکی از صحنه‌های اصلی رقابت و درگیری میان دولت‌ها بدل شده است؛ جایی که بدون شلیک حتی یک گلوله، زیرساخت‌های حیاتی، اطلاعات حساس و امنیت ملی کشورها می‌تواند هدف قرار گیرد. این تحولات نه‌تنها مفاهیم کلاسیک جنگ را دگرگون کرده‌اند، بلکه در سطح حقوقی نیز موجب ایجاد چالش‌هایی اساسی در حوزه مسئولیت بین‌المللی شده‌اند.در این میان، کاربرد هوش مصنوعی در اجرای حملات سایبری، به‌واسطه ویژگی‌هایی نظیر سرعت بالا، تصمیم‌گیری مستقل و گستره نفوذ، ابعاد پیچیده‌تری به موضوع داده است. از جمله مسائل اساسی، تعیین حدود مسئولیت دولت‌ها در قبال اقدامات مخرب در فضای مجازی، شناسایی عاملان واقعی و انتساب اقدامات به اشخاص یا نهادهای دولتی است. در چنین فضایی، قواعد سنتی حقوق بین‌الملل با پرسش‌هایی جدی مواجه شده‌اند که پاسخ به آن‌ها نیازمند بازنگری در مبانی موجود و تدوین اصول جدید است. این مقاله در پی آن است که ابعاد مختلف این چالش حقوقی را بررسی و تحلیل نماید.

۱-تعاریف و تاریخچه

۱-۱-تعریف هوش مصنوعی

هوش مصنوعی به مجموعه‌ای از فناوری‌ها و سامانه‌ها اطلاق می‌شود که توانایی انجام وظایف شناختی مشابه انسان، مانند یادگیری، استدلال، تحلیل داده، تصمیم‌گیری و حل مسئله را دارند. این سیستم‌ها بر اساس پردازش داده‌های گسترده و مدل‌سازی رفتارهای منطقی، قادر به انجام عملکردهایی هستند که پیش‌تر تنها از عهده انسان برمی‌آمد. در حوزه نظامی و امنیتی، هوش مصنوعی به عنوان ابزاری برای تحلیل سریع اطلاعات، هدایت سامانه‌های خودکار، شناسایی تهدیدات و حتی اجرای عملیات سایبری به کار گرفته می‌شود و همین امر موجب طرح مسائل پیچیده‌ای در زمینه مسئولیت‌پذیری و کنترل حقوقی بر آن شده است(جوادی، فاطمه السادات، ۱۴۰۰: ص۶۲).

۱-۲-چیستی جنگ سایبری و تمایز آن با دیگر اشکال جنگ

جنگ سایبری به مجموعه‌ای از اقدامات تهاجمی یا تدافعی در فضای مجازی اطلاق می‌شود که با هدف آسیب‌زدن به زیرساخت‌های حیاتی، اختلال در نظام‌های اطلاعاتی، سرقت داده‌ها یا تضعیف توان دفاعی و اقتصادی یک کشور توسط دولت‌ها یا عوامل وابسته به آن‌ها صورت می‌گیرد. برخلاف اشکال سنتی جنگ که معمولاً با استفاده از نیروی نظامی، اشغال سرزمین یا درگیری فیزیکی همراه است، جنگ سایبری در محیطی غیرفیزیکی و نامرئی انجام می‌شود و اغلب بدون نشانه‌های آشکار یا تلفات انسانی مستقیم ظاهر می‌گردد. این تفاوت‌های ماهوی، شناسایی عامل حمله، تعیین زمان وقوع جنگ و اعمال قواعد کلاسیک حقوق مخاصمات مسلحانه را با چالش‌هایی اساسی مواجه ساخته است(پاکزاد، بتول،۱۳۹۰: ص۴۳).

۱-۳-مروری بر تاریخچه استفاده از فناوری در جنگ‌های نوین

با آغاز قرن بیستم و به‌ویژه در جریان جنگ‌های جهانی اول و دوم، فناوری به عاملی تعیین‌کننده در تغییر چهره جنگ تبدیل شد. استفاده از ماشین‌آلات سنگین، هواپیما، رادار، و در نهایت سلاح هسته‌ای نشان داد که توسعه فناوری نه‌تنها ابزارهای نبرد، بلکه استراتژی‌های نظامی و شیوه‌های تصمیم‌گیری را نیز دگرگون می‌سازد. در دوره جنگ سرد، فناوری اطلاعات و ارتباطات نیز به یکی از ابعاد حیاتی در رقابت‌های نظامی میان قدرت‌های بزرگ تبدیل شد و مفاهیم نوینی چون جنگ الکترونیک و اطلاعات‌محور پدیدار شدند.با ورود به قرن بیست‌ویکم، جنگ‌های نوین بیش از پیش به فناوری‌های دیجیتال، شبکه‌های رایانه‌ای و سامانه‌های هوشمند وابسته شده‌اند. عملیات نظامی به تدریج به فضاهای سایبری گسترش یافته و دامنه تهدیدات نیز از جبهه‌های فیزیکی به زیرساخت‌های نرم‌افزاری، اطلاعاتی و ارتباطی کشیده شده است. در این میان، هوش مصنوعی به‌عنوان پیشرفته‌ترین ابزار فناورانه، نقش فزاینده‌ای در طراحی، اجرا و حتی تصمیم‌گیری در عملیات‌های سایبری یافته و این روند، مرز میان فناوری و مسئولیت حقوقی را بیش از پیش مخدوش کرده است(آقابابایان دامغانی و همکاران، ۱۳۹۸: ص۴).

۱-۴-ورود هوش مصنوعی به عرصه جنگ سایبری و پیامدهای اولیه حقوقی

ورود هوش مصنوعی به عرصه جنگ سایبری، نقطه عطفی در تحول منازعات مدرن محسوب می‌شود. سامانه‌های هوشمند امروزه قادرند بدون دخالت مستقیم انسان، عملیات شناسایی، نفوذ، تخریب و حتی دفاع سایبری را با سرعت و دقت بالا انجام دهند. استفاده از این ابزارها توسط دولت‌ها یا عوامل وابسته، موجب شکل‌گیری نوعی از مخاصمه شده است که کنترل، ردیابی و مهار آن به‌مراتب دشوارتر از اشکال سنتی جنگ است. به‌ویژه اینکه بسیاری از این سامانه‌ها به‌گونه‌ای طراحی می‌شوند که خودمختارانه عمل کرده و در شرایط خاص، تصمیم‌گیری مستقل داشته باشند.پیامدهای حقوقی اولیه ناشی از این تحول، نظام مسئولیت بین‌المللی دولت‌ها را با پرسش‌های بنیادین مواجه ساخته است. از جمله اینکه در صورت بروز حمله سایبری توسط سامانه‌ای مبتنی بر هوش مصنوعی، چگونه می‌توان عمل انجام‌شده را به یک دولت خاص منتسب کرد، یا دولت مزبور تا چه میزان مسئولیت پیشگیری، کنترل و پاسخ‌دهی به اقدامات مخرب چنین سامانه‌هایی را برعهده دارد. در شرایطی که قواعد سنتی حقوق بین‌الملل عمدتاً بر مبنای رفتار انسانی تنظیم شده‌اند، ورود فناوری‌هایی با قابلیت تصمیم‌گیری مستقل، ضرورت بازاندیشی در مبانی انتساب، مسئولیت و پاسخگویی را به‌وضوح آشکار ساخته است(خلیلی پور رکن آبادی و نور علی وند، ۱۳۹۱: ص ۱۷۸).

۲- جایگاه حقوق بین‌الملل در مواجهه با جنگ‌های سایبری مبتنی بر هوش مصنوعی

حقوق بین‌الملل، به‌ویژه در قالب منشور ملل متحد و اصول کلی حقوق بین‌الملل عرفی، چارچوب‌هایی برای تنظیم روابط میان دولت‌ها در شرایط صلح و جنگ فراهم آورده است. اصولی مانند منع توسل به زور، احترام به حاکمیت ملی، و عدم مداخله در امور داخلی دولت‌ها، ستون‌های اصلی این نظام حقوقی را تشکیل می‌دهند. با این حال، ظهور جنگ‌های سایبری به‌ویژه آن دسته که با بهره‌گیری از هوش مصنوعی صورت می‌گیرند، نشان داده است که این چارچوب‌ها برای پاسخ‌گویی به تحولات فناورانه معاصر کفایت لازم را ندارند.

یکی از چالش‌های مهم در این زمینه، شناسایی مصداق توسل به زور در فضای سایبری و تعیین نقطه آغاز مخاصمه در غیاب خشونت فیزیکی آشکار است(فقیه حبیبی، علی، ۱۳۹۵: ص۹۶).

افزون بر آن، حقوق بین‌الملل بشردوستانه و قواعد حاکم بر مخاصمات مسلحانه نیز با پرسش‌هایی تازه مواجه شده‌اند؛ از جمله چگونگی تطبیق اصل تفکیک میان اهداف نظامی و غیرنظامی، تناسب در حملات، و رعایت حداقل خسارت انسانی در شرایطی که تصمیم‌گیری به سامانه‌های هوش‌مصنوعی واگذار شده است. همچنین، چالش‌هایی مانند عدم شفافیت در عملکرد این سامانه‌ها و دشواری در احراز مسئولیت دولت‌ها، نظام پاسخگویی بین‌المللی را به‌شدت تضعیف کرده است. بدین ترتیب، جایگاه حقوق بین‌الملل در مواجهه با این نوع از مخاصمات، در وضعیتی گذار و نیازمند بازنگری و توسعه جدی قرار دارد.

۲-۱-اصول بنیادین منشور ملل متحد و تحدید استفاده از زور

اصل منع توسل به زور که در ماده ۲ بند ۴ منشور ملل متحد تصریح شده، یکی از اصول بنیادین حقوق بین‌الملل معاصر است و دولت‌ها را از تهدید یا استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی سایر کشورها منع می‌کند. این اصل، مبنایی برای حفظ صلح و امنیت بین‌المللی تلقی می‌شود و تنها در دو حالت محدود قابل نقض است: دفاع مشروع طبق ماده ۵۱ منشور و مجوز شورای امنیت تحت فصل هفتم. در زمینه جنگ‌های سایبری مبتنی بر هوش مصنوعی، چالش اصلی آن است که آیا یک حمله سایبری می‌تواند مصداق «توسل به زور» تلقی شود؛ به‌ویژه زمانی که این حمله منجر به خسارات فیزیکی گسترده، تلفات انسانی یا اختلال اساسی در عملکرد زیرساخت‌های حیاتی گردد. در نبود تعریف صریح از «زور» در بستر سایبری، تفسیر این اصل در مواجهه با فناوری‌های نوین همچنان محل مناقشه و تحلیل‌های گوناگون حقوقی است(فقیه حبیبی، علی، ۱۳۹۵: ص۹۰).

۲-۲-کاربرد حقوق بین‌الملل بشردوستانه در فضای مجازی

حقوق بین‌الملل بشردوستانه که اساس آن بر رعایت اصول تفکیک، تناسب و ضرورت استوار است، به‌طور سنتی برای تنظیم رفتار طرفین در جنگ‌های مسلحانه به کار می‌رود. این حقوق به‌ویژه در جنگ‌های کلاسیک، برای جلوگیری از آسیب به غیرنظامیان و حفاظت از اهداف غیرنظامی طراحی شده است. اما در جنگ‌های سایبری، با توجه به طبیعت دیجیتال و نامرئی این حملات، اعمال این اصول به چالش کشیده شده است. برای مثال، تعیین این که یک حمله سایبری چه تأثیری بر غیرنظامیان دارد یا آیا حمله به یک شبکه دیجیتال در واقع معادل حمله به یک هدف نظامی است یا خیر، از پیچیدگی‌های ویژه‌ای برخوردار است. بنابراین، ضروری است که حقوق بشردوستانه در فضای مجازی تطبیق یابد و به‌ویژه درباره نحوه برخورد با سامانه‌های هوش مصنوعی که به‌طور خودکار عملیات جنگی را انجام می‌دهند، دقت بیشتری به خرج داده شود(ابراهیم زاده و ملکی زاده، ۱۴۰۰: ص۸۶).

یکی از چالش‌های اصلی در کاربرد حقوق بشردوستانه در فضای مجازی، مسئله انتساب و شناسایی طرف‌های درگیر است. در جنگ‌های سایبری، تعیین اینکه آیا حمله‌ای توسط یک دولت، گروه غیر دولتی یا بازیگران غیرمستقیم انجام شده، بسیار دشوار است. از سوی دیگر، مفهوم «ضرورت» در

عملیات‌های سایبری نیز نیاز به بازنگری دارد؛ چرا که گاهی اوقات حملات سایبری بدون هیچ آسیب جسمانی، می‌توانند به شدت زیرساخت‌های حیاتی کشورها را مختل کنند، که پیامدهای غیرقابل پیش‌بینی و وسیعی دارد. بنابراین، با توجه به سرعت پیشرفت فناوری، نیاز به تدوین قوانین و رویه‌های جدید در راستای تطبیق اصول حقوق بشردوستانه با فضای دیجیتال به وضوح احساس می‌شود.

۲-۳-چالش‌های شناسایی عامل در عملیات سایبری با واسطه هوش مصنوعی

در جنگ‌های سایبری مبتنی بر هوش مصنوعی، یکی از چالش‌های اساسی، شناسایی و انتساب دقیق عامل حمله است. با استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی، عملیات‌های سایبری می‌توانند بدون نیاز به دخالت مستقیم انسان یا از طریق سامانه‌های خودمختار صورت گیرند. این امر موجب می‌شود که شناسایی عامل واقعی حمله پیچیده‌تر از جنگ‌های سنتی شود، جایی که غالباً شواهد فیزیکی و ملموس وجود داشت. در فضای سایبری، حملات ممکن است از سوی یک دولت، گروه‌های غیردولتی، یا حتی هکرهای مستقل صورت گیرد و این حملات می‌توانند از شبکه‌های پراکنده و پیچیده‌ای استفاده کنند که ردیابی منشأ آن‌ها را دشوار می‌سازد. به‌ویژه زمانی که هوش مصنوعی در طراحی حملات سایبری به کار می‌رود، مشخص کردن نقش انسان‌ها و نهادهای دخیل در تصمیم‌گیری‌های آن سیستم‌ها به مسأله‌ای بغرنج تبدیل می‌شود(میربدو همکاران، ۱۳۹۸: ص۲۴۹).

یکی دیگر از ابعاد چالش‌برانگیز در شناسایی عامل، موضوع "نقاب‌پوشی" یا "پوشش مخفی" در فضای سایبری است که می‌تواند از طریق تکنیک‌های پیشرفته مانند تغییر نشانه‌های دیجیتال، استفاده از **VPN**ها، یا مسیرهای پنهانی برای انحراف مسیر ردیابی اعمال شود. در این شرایط، حتی اگر یک حمله سایبری با بهره‌گیری از هوش مصنوعی صورت گیرد، شواهد دیجیتال ممکن است کاملاً ساختگی یا مخدوش شده باشند، که شناسایی و اثبات مسئولیت را غیرممکن می‌سازد. این پیچیدگی‌ها نه‌تنها کار را برای تحلیلگران اطلاعاتی دشوار می‌کند، بلکه بر مبنای حقوقی و اعمال مسئولیت بین‌المللی نیز تأثیرگذار است. تا زمانی که این مسائل به‌طور موثر حل نشوند، دولت‌ها و نهادهای بین‌المللی با مشکلات جدی در خصوص پاسخگویی و برخورد با حملات سایبری مواجه خواهند بود.

۲-۴-تعهدات دولت‌ها در پیشگیری از حملات سایبری در قلمرو خود

دولت‌ها مطابق با اصول حقوق بین‌الملل، به‌ویژه در چارچوب منشور ملل متحد و دیگر توافقات بین‌المللی، موظف به اتخاذ تدابیر مؤثر برای پیشگیری از حملات سایبری در قلمرو خود هستند. این تعهدات شامل ایجاد و تقویت زیرساخت‌های امنیتی دیجیتال، تصویب و اجرای قوانین مرتبط با جرایم سایبری، و همکاری با دیگر دولت‌ها و سازمان‌های بین‌المللی برای مقابله با تهدیدات مشترک است. علاوه بر این، دولت‌ها باید مکانیزم‌های نظارتی و پاسخگویی مؤثری را برای شناسایی و جلوگیری از فعالیت‌های مخرب سایبری که ممکن است از قلمرو آن‌ها نشأت گیرد، ایجاد کنند. در صورتی که دولت‌ها نتوانند به این تعهدات عمل کنند، ممکن است به‌عنوان عامل

تسهیل‌کننده حملات سایبری تلقی شوند و مسئولیت بین‌المللی برای پیامدهای ناشی از آن‌ها به‌عهده آن‌ها قرار گیرد. این مسئولیت‌ها همچنین به دولت‌ها این الزامات را تحمیل می‌کند که از وقوع حملات سایبری از سوی بازیگران غیردولتی یا گروه‌های تروریستی در خاک خود جلوگیری کنند(محمدحسینی و همکاران، ۱۳۹۹: ص۴۰).

۳-مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری هوش‌مصنوعی‌محور

مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری هوش مصنوعی‌محور، یکی از چالش‌های حقوقی پیچیده در عصر فناوری‌های نوین است. طبق اصول حقوق بین‌الملل، دولت‌ها موظفند از قلمرو خود برای انجام اقدامات مخرب در فضای سایبری جلوگیری کنند و از آنجا که هوش مصنوعی می‌تواند به‌طور خودمختار و بدون دخالت مستقیم انسان حملات سایبری را طراحی و اجرا کند، مسئولیت دولت‌ها در این زمینه به‌ویژه در ارتباط با استفاده از این فناوری‌ها پیچیده‌تر می‌شود. اگر حمله سایبری به‌طور مستقیم یا غیرمستقیم از قلمرو یک دولت انجام شود یا دولت‌ها قادر به کنترل و نظارت بر فعالیت‌های فضای مجازی در خاک خود نباشند، آن دولت می‌تواند مسئولیت بین‌المللی در قبال خسارت‌های وارده به دولت دیگر را برعهده گیرد. این مسئولیت می‌تواند شامل جبران خسارت، توقف فعالیت‌های مخرب و اتخاذ تدابیر پیشگیرانه برای جلوگیری از وقوع حملات مشابه در آینده باشد. در این راستا، نیاز به تدوین و تطبیق اصول حقوقی جدید و شفاف برای مقابله با تهدیدات سایبری و تعیین دقیق مسئولیت‌ها بیش از پیش احساس می‌شود(رحمتی، رضا،۱۳۹۶: ص۵۵).

۳-۱-ارکان تحقق مسئولیت بین‌المللی (رفتار منتسب و تخلف از تعهد بین‌المللی)

ارکان تحقق مسئولیت بین‌المللی در حقوق بین‌الملل شامل دو عنصر اصلی است: رفتار منتسب و تخلف از تعهد بین‌المللی.

۱.رفتار منتسب: اولین رکن برای تحقق مسئولیت بین‌المللی، باید یک رفتار خاص (اعم از عمل یا ترک فعل) وجود داشته باشد که به یک دولت یا نهاد دولتی نسبت داده شود. این رفتار می‌تواند شامل اقدامات مثبت یا منفی باشد که به‌طور مستقیم یا غیرمستقیم از سوی دولت، مقامات دولتی، یا گروه‌های وابسته به آن انجام شده باشد. در زمینه حملات سایبری، اگر یک حمله سایبری از قلمرو یک دولت آغاز شود یا توسط بازیگران غیر دولتی که تحت حمایت آن دولت قرار دارند انجام شود، این رفتار به دولت مربوطه منتسب خواهد شد(نعمتی و صادقی نشاط، ۱۳۹۶: ص۱۷۰).

۲.تخلف از تعهد بین‌المللی: دومین رکن این است که رفتار منتسب، نقض یک تعهد بین‌المللی موجود باشد. این تعهد می‌تواند از منابع مختلفی ناشی شود، از جمله معاهدات، عرف بین‌المللی یا اصول بنیادین حقوقی مانند اصول منع توسل به زور و احترام به حاکمیت ملی. در صورتی که یک دولت از تعهدات خود در قبال سایر دولت‌ها، مانند جلوگیری از حملات سایبری یا جلوگیری از استفاده از فناوری‌های مخرب، تخلف کند، این نقض تعهد موجب مسئولیت بین‌المللی آن دولت خواهد شد. در حملات سایبری مبتنی بر هوش مصنوعی، تخلف از این تعهدات می‌تواند شامل عدم نظارت بر فضای مجازی، عدم پیشگیری از فعالیت‌های مخرب در قلمرو خود، یا بی‌توجهی به تعهدات امنیت سایبری باشد(همان منبع).

این دو رکن در مجموع مسئولیت بین‌المللی دولت‌ها را در برابر نقض حقوق و قوانین بین‌المللی به‌ویژه در زمینه تهدیدات سایبری، ایجاد می‌کنند.

۳-۲-مسئولیت مستقیم، غیرمستقیم و مشارکتی در حملات سایبری

در حقوق بین‌الملل، مسئولیت دولت‌ها در قبال حملات سایبری می‌تواند به سه دسته اصلی تقسیم شود: مسئولیت مستقیم، غیرمستقیم و مشارکتی. هر کدام از این انواع مسئولیت دارای ویژگی‌ها و شرایط خاص خود هستند که در خصوص حملات سایبری مبتنی بر هوش مصنوعی نیز قابل اعمال هستند.

۱.مسئولیت مستقیم: مسئولیت مستقیم زمانی تحقق می‌یابد که یک دولت به‌طور مستقیم مسئول انجام یا تسهیل یک حمله سایبری باشد. این حملات می‌تواند به‌طور مستقیم از سوی مقامات دولتی یا سازمان‌های وابسته به آن‌ها صورت گیرد. در این حالت، دولت به‌طور روشن مسئول حمله‌ای است که تحت کنترل و هدایت مستقیم آن قرار دارد. برای مثال، اگر یک دولت از فناوری‌های هوش مصنوعی برای حمله به زیرساخت‌های حیاتی کشور دیگر استفاده کند، مسئولیت مستقیم بر عهده آن دولت است. در این نوع مسئولیت، انتساب رفتار به دولت به‌طور کامل مشخص است و دولت مسئول باید برای جبران خسارت‌ها اقدام کند.

۲.مسئولیت غیرمستقیم: مسئولیت غیرمستقیم زمانی مطرح می‌شود که یک دولت به‌طور غیرمستقیم و از طریق حمایت یا تسهیل حمله سایبری توسط گروه‌ها یا افراد غیردولتی، مسئول شناخته می‌شود. به‌عبارت دیگر، اگر یک دولت با اعطای پناهگاه، منابع مالی، آموزش یا امکانات فنی به گروه‌های تروریستی یا هکرهای مستقل کمک کند تا حملات سایبری علیه دولت دیگر انجام دهند، آن دولت مسئول شناخته خواهد شد، حتی اگر به‌طور مستقیم خود اقدام به حمله نکرده باشد. این نوع مسئولیت در حملات سایبری مبتنی بر هوش مصنوعی پیچیده‌تر می‌شود زیرا بازیگران غیر دولتی می‌توانند با استفاده از فناوری‌های پیشرفته و خودمختار بدون نیاز به دخالت مستقیم دولت‌ها، حملاتی را طراحی کنند.

۳.مسئولیت مشارکتی: مسئولیت مشارکتی زمانی ایجاد می‌شود که دو یا چند دولت به‌طور مشترک در انجام یک حمله سایبری نقش داشته باشند. در این حالت، هر یک از دولت‌ها به‌طور مشترک مسئول حمله سایبری هستند که نتیجه همکاری آن‌ها بوده است. برای مثال، اگر دو دولت با همکاری یکدیگر به طراحی و اجرای یک حمله سایبری مبتنی بر هوش مصنوعی بپردازند، هر دو دولت به‌طور مشترک مسئول شناخته می‌شوند. در این نوع مسئولیت، تعیین سهم هر دولت در ایجاد حمله و نقض حقوق بین‌الملل به دشواری صورت می‌گیرد، به‌ویژه زمانی که عملیات‌های پیچیده‌ای مانند حملات سایبری ترکیب شده با هوش مصنوعی انجام شده باشد.

این سه نوع مسئولیت، به‌ویژه در زمینه حملات سایبری که با استفاده از هوش مصنوعی انجام می‌شود، می‌تواند به چالش‌های جدی در تعیین مسئولیت و پاسخگویی بین‌المللی منجر شود. با توجه به پیچیدگی‌های موجود، نیاز به تدوین قواعد جدید و شفاف در حقوق بین‌الملل احساس می‌شود.

۴- الزامات حقوقی و چالش‌های پیش‌رو در تنظیم قواعد بین‌المللی

الزامات حقوقی و چالش‌های پیش رو در تنظیم قواعد بین‌المللی در حوزه جنگ‌های سایبری مبتنی بر هوش مصنوعی، به‌ویژه در زمینه مسئولیت دولت‌ها، یکی از مسائل پیچیده و نوظهور در عرصه حقوق بین‌الملل است. همانطور که فناوری‌های جدید، به‌ویژه هوش مصنوعی، به طور فزاینده‌ای در عرصه امنیت سایبری و جنگ‌های دیجیتال به کار گرفته می‌شوند، نیاز به تدوین و به‌روزرسانی قوانین بین‌المللی برای پاسخگویی به این تهدیدات جدی‌تر از همیشه احساس می‌شود. الزامات حقوقی برای تنظیم قواعد بین‌المللی در این حوزه شامل نیاز به تعریف دقیق‌تری از مفاهیم اصلی همچون «توسل به زور»، «حمله سایبری»، «دفاع مشروع» و «مسئولیت بین‌المللی» در دنیای سایبری است. در این راستا، باید اصول حقوق بشر دوستانه و دیگر مقررات بین‌المللی برای فضای سایبری تطبیق داده شوند تا تضمین‌کننده حقوق بشر و جلوگیری از سوءاستفاده‌های احتمالی باشند(مولوی، حانیه، ۱۴۰۲: ص۱۸).

یکی از چالش‌های اصلی در تنظیم قواعد بین‌المللی در این زمینه، پیچیدگی و ابهام در شناسایی و انتساب مسئولیت به دولت‌ها و بازیگران غیردولتی است. با توجه به طبیعت نامرئی و گسترده حملات سایبری و استفاده از هوش مصنوعی در این حملات، بسیار دشوار است که مشخص شود کدام دولت یا نهاد مسئول ایجاد یک حمله سایبری خاص است. همچنین، بسیاری از اصول حقوق بین‌الملل، مانند ممنوعیت مداخله در امور داخلی کشورها و احترام به حاکمیت ملی، در فضای سایبری ممکن است با چالش‌های جدی مواجه شوند. علاوه بر این، نبود اجماع جهانی بر سر قوانین جامع در مورد جنگ سایبری و مسئولیت دولت‌ها، می‌تواند منجر به تفاوت‌های اساسی در تفسیر و اجرای این قوانین در سطح بین‌المللی شود. این مشکلات به‌ویژه در زمانی که فناوری‌های هوش مصنوعی و الگوریتم‌های خودمختار قادر به انجام حملات پیچیده می‌شوند، تبدیل به یک معضل حقوقی و اجرایی بزرگ می‌شود(مصطفوی اردبیلی و همکاران، ۱۴۰۲: ص۸۹).

۴-۱-نیاز به تدوین معاهدات خاص در زمینه هوش مصنوعی و جنگ سایبری

نیاز به تدوین معاهدات خاص در زمینه هوش مصنوعی و جنگ سایبری یکی از مهم‌ترین مسائلی است که در دنیای امروز و با توجه به تحولات سریع فناوری‌های نوین، بیش از پیش احساس می‌شود. جنگ‌های سایبری به‌ویژه زمانی که از هوش مصنوعی بهره می‌برند، چالش‌های قابل توجهی را برای حقوق بین‌الملل به همراه دارند. این حملات، نه‌تنها قدرت نظامی و امنیتی کشورها را تهدید می‌کنند، بلکه می‌توانند منجر به تخریب زیرساخت‌های حیاتی، تلفات انسانی و اختلالات اقتصادی گسترده‌ای شوند که تأثیرات آنها از هر جنگ فیزیکی فراتر است. در این شرایط، تدوین معاهدات خاص برای تنظیم و پاسخگویی به تهدیدات ناشی از حملات سایبری، به‌ویژه آنهایی که با استفاده از هوش مصنوعی انجام می‌شود، به شدت ضروری است(میرزا آقایی،مهدی، ۱۴۰۱: ص۴۳).

معاهدات خاص می‌توانند در زمینه‌های مختلفی همچون تعیین مسئولیت دولت‌ها در قبال حملات سایبری، مقررات استفاده از هوش مصنوعی در عملیات‌های نظامی، و تدوین قواعد خاص برای جلوگیری از تشدید بحران‌های سایبری در

سطح بین‌المللی عمل کنند. این معاهدات می‌توانند از طریق ایجاد یک چارچوب قانونی مشترک برای پیشگیری از جنگ‌های سایبری، تدوین قواعد مربوط به دفاع مشروع در فضای سایبری، و تبیین مسئولیت‌های دولت‌ها در قبال گروه‌های غیردولتی، به کاهش خطرات و تهدیدات ناشی از فناوری‌های نوین کمک کنند. علاوه بر این، معاهدات خاص می‌توانند به ایجاد سازوکارهایی برای حل اختلافات و ایجاد نهادهای نظارتی و اجرایی بین‌المللی در این زمینه کمک کنند. همچنین، با توجه به ماهیت پیچیده و تغییرپذیر تهدیدات سایبری، این معاهدات باید انعطاف‌پذیر و به‌روز باشند تا بتوانند به‌طور مؤثر با تحولات سریع در این حوزه هماهنگ شوند(زر رخ، احسان، ۱۳۸۹: ص۶۸).

۴-۲-نقش سازمان‌های بین‌المللی و اجماع جهانی در تنظیم مقررات

نقش سازمان‌های بین‌المللی و اجماع جهانی در تنظیم مقررات مربوط به جنگ‌های سایبری و استفاده از هوش مصنوعی، از اهمیت ویژه‌ای برخوردار است. تهدیدات سایبری، به دلیل ماهیت فرامرزی و تأثیرات جهانی آن‌ها، نمی‌توانند تنها در محدوده یک کشور مدیریت شوند و نیازمند همکاری گسترده بین‌المللی هستند. سازمان‌های بین‌المللی مانند سازمان ملل متحد، اتحادیه بین‌المللی ارتباطات و سازمان امنیت و همکاری در اروپا نقش اساسی در تدوین استانداردها و مقررات جهانی ایفا می‌کنند. این سازمان‌ها قادرند با ایجاد چارچوب‌های مشترک و قوانین بین‌المللی، اصولی را برای پیشگیری از حملات سایبری، تنظیم استفاده از هوش مصنوعی در جنگ‌ها و تعیین مسئولیت دولت‌ها در قبال نقض حقوق بین‌الملل به تصویب برسانند(جعفری، کامران، ۱۳۹۱: ص۵۳).

اجماع جهانی نیز در این زمینه اهمیت زیادی دارد، چرا که در دنیای دیجیتال امروز، تهدیدات سایبری و حملات مبتنی بر هوش مصنوعی می‌توانند تمامی کشورها را تحت تأثیر قرار دهند. بدون همکاری بین‌المللی و توافقات جهانی، مقابله مؤثر با این تهدیدات دشوار خواهد بود. دستیابی به اجماع جهانی در خصوص تدوین مقررات واحد در این زمینه، به دولت‌ها کمک می‌کند تا در برابر تهدیدات سایبری و استفاده نادرست از هوش مصنوعی در جنگ‌ها، اقداماتی مؤثر و هماهنگ انجام دهند. در نتیجه، سازمان‌های بین‌المللی و اجماع جهانی برای ایجاد یک فضای قانونی و حقوقی منسجم، ضروری به نظر می‌رسند.

۴-۳-آینده‌پژوهی حقوقی در مواجهه با پیشرفت‌های سریع فناوری نظامی

آینده‌پژوهی حقوقی در مواجهه با پیشرفت‌های سریع فناوری نظامی، به‌ویژه در حوزه جنگ‌های سایبری و استفاده از هوش مصنوعی، نیازمند تحلیل و پیش‌بینی چالش‌ها و تحولات احتمالی در دنیای دیجیتال و نظامی است. با توجه به سرعت بالای پیشرفت فناوری‌های نوین، نظیر سیستم‌های هوش مصنوعی خودمختار، ربات‌های جنگی، و حملات سایبری پیچیده، قوانین و مقررات حقوقی موجود ممکن است به‌زودی از توانایی مقابله با تهدیدات جدید باز بمانند. در این راستا، حقوق‌دانان و کارشناسان باید به تدوین اصول و استانداردهای جدیدی برای تنظیم استفاده از این فناوری‌ها در جنگ‌ها بپردازند. همچنین، توجه به ابعاد اخلاقی و انسانی این فناوری‌ها، به‌ویژه در زمینه حملات سایبری و نقش دولت‌ها

در پیشگیری از تهدیدات، باید در فرآیند تدوین قوانین جدید قرار گیرد. پیش‌بینی آینده حقوقی در این زمینه نیازمند همکاری بین‌المللی و اجماع جهانی است تا از ایجاد خلاءهای قانونی و سوءاستفاده‌های احتمالی جلوگیری شود و یک نظام حقوقی جامع و منسجم برای مقابله با تهدیدات نظامی نوین شکل گیرد.

نتیجه‌گیری

در مواجهه با پیشرفت‌های سریع فناوری‌های نظامی، به‌ویژه در زمینه جنگ‌های سایبری و استفاده از هوش مصنوعی، نیاز به بازنگری در قوانین و مقررات بین‌المللی به‌وضوح احساس می‌شود. تهدیدات جدید ناشی از این فناوری‌ها می‌توانند تهدیدات پیچیده و فراگیرتری نسبت به جنگ‌های سنتی ایجاد کنند که دامنه و تأثیرات آن‌ها به مرزهای ملی محدود نمی‌شود. حملات سایبری می‌توانند به‌طور گسترده‌ای به زیرساخت‌های حیاتی، سیستم‌های مالی و خدمات دولتی آسیب بزنند و علاوه بر آن، کاربردهای خودمختار هوش مصنوعی در عرصه نظامی می‌توانند به پیچیدگی‌های جدیدی در شناسایی مسئولیت و تعیین نقش دولت‌ها در نقض حقوق بین‌المللی منجر شوند. بنابراین، ضرورت دارد که جامعه جهانی به‌ویژه سازمان‌های بین‌المللی، در تدوین و به‌روزرسانی مقررات بین‌المللی و معاهدات خاص، به‌طور مؤثری عمل کنند.سازمان‌های بین‌المللی، همچون سازمان ملل متحد و اتحادیه بین‌المللی ارتباطات ، نقش محوری در تنظیم این مقررات دارند و می‌توانند با ارائه چارچوب‌های حقوقی مشترک، اقداماتی برای کاهش تهدیدات سایبری و استفاده نادرست از هوش مصنوعی در جنگ‌ها انجام دهند. این مقررات می‌توانند بر اساس اصول حقوق بشر و موازین امنیت بین‌المللی شکل گیرند و مسئولیت‌های دولت‌ها را در قبال تهدیدات سایبری و جنگ‌های دیجیتال مشخص کنند. همچنین، تأکید بر اصل پیشگیری و ترویج همکاری‌های بین‌المللی به‌منظور نظارت بر فعالیت‌های فضای سایبری، می‌تواند از بروز بحران‌ها و سوءاستفاده‌ها جلوگیری کند و روند تأمین امنیت جهانی را تسهیل نماید.

در نهایت، با توجه به پیچیدگی و سرعت تحولات فناوری در حوزه نظامی، به‌ویژه در زمینه‌های هوش مصنوعی و جنگ‌های سایبری، تدوین معاهدات خاص و ایجاد سازوکارهای نظارتی و اجرایی برای مدیریت این تهدیدات ضروری است. حقوق بین‌الملل باید به‌طور مستمر با تغییرات سریع فناوری هماهنگ شود تا بتواند به‌طور مؤثر به تهدیدات ناشی از این فناوری‌ها پاسخ دهد. این امر نیازمند همکاری و اجماع جهانی در سطح بین‌المللی است تا از هرگونه بحران و آسیب‌های ناشی از سوءاستفاده از فناوری‌های پیشرفته جلوگیری شود.

سپاسگزاری

از معاونت محترم پژوهشی به خاطر حمایت حمایت معنوی در اجرای پژوهش حاضر سپاسگزاری می‌شود.

از آقای دکتر عبدالله علیزاده به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.

از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.

نگارندگان بر خود لازم می‌دانند از آقای دکتر محمد رسول آهنگران به خاطر مطالعه متن مقاله حاضر و ارائه نظرهای ارزشمند سپاسگزاری نمایند.

منابع

کتاب‌ها

پاکزاد، بتول(۱۳۹۰)، تروریسم سایبری، تهران: انتشارات دانشگاه آزاد اسلامی، دفتر گسترش تولید علم معاونت پژوهشی دانشگاه آزاد اسلامی

جوادی، فاطمه سادات (۱۴۰۰)، فناوری‌های نوین و حقوق جزا: رویکردی به هوش مصنوعی، تهران: انتشارات دانشگاه تهران

مقالات

ابراهیم زاده، پوریا؛ ملکی زاده، امیرحسین(۱۴۰۰)، جایگاه دفاع پیش دستانه از منظر حقوق بین الملل با تأکید بر تبیین موانع حقوقی بین المللی اعمال آن جهت حفاظت از غیرنظامیان، نشریه مطالعات بین المللی، شماره۷۰،صص ۱۰۰-۸۳

آقابابایان دامغانی، حمیدرضا؛ عسگرخانی، ابومحمد؛ میرعباسی، سیدباقر، ۱۳۹۸، مسئولیت بین المللی در قبال حملات سایبری، مجله فقه و تاریخ تمدن، دوره ۵، شماره ۱، صص۵-۱

خلیلی پور رکن آبادی، علی؛ نور علی وند، یاسر، ۱۳۹۱، تهدیدات سایبری و تاثیر آن بر امنیت ملی، فصلنامه مطالعات راهبردی، شماره دوم، سال ۱۵، صص ۱۹۶-۱۶۷

فقیه حبیبی، علی(۱۳۹۵)، جایگاه حقوق بشر دوستانه در اسلام و اسناد بین المللی ، فصلنامه پژوهش‌های سیاسی جهان اسلام، سال ششم، شماره۲،صص ۱۰۳-۸۱

محمدحسینی، بابک؛ هادی زاده، مرتضی؛ قافله باشی، سید فهیم (۱۳۹۹)، پیشران‌های ارائه‌ی خدمات سایبری پایدار در دولت با تاکید بر حفظ امنیت از طریق هوش مصنوعی، دوفصلنامه آینده پژوهی ایران، سال پنجم، شماره دوم، صص ۶۵-۳۵

مصطفوی اردبیلی، سید محمد مهدی؛ تقی زاده انصاری، مصطفی؛ رحمتی فر، سمانه (۱۴۰۲)، تاثیر هوش مصنوعی بر نظام حقوق بشر بین الملل، نشریه حقوق فناوری‌های نوین، دوره ۴، شماره ۸، صص ۱۰۰-۸۵

مولوی، حانیه (۱۴۰۲)، مطالعه چالش‌های حقوق بشری هوش مصنوعی، پنجمین کنفرانس بین المللی علوم انسانی، حقوق، مطالعات اجتماعی و روانشناسی، صص ۱-۲۷

میربد، لیلا؛ سلیمی، صادق؛ نیاورانی، صابر؛ زمانی، سید قاسم (۱۳۹۸)، تروریسم سایبری؛ نقض حقوق بشر و آزادی‌های بنیادین، فصلنامه حقوق پزشکی، ویژه نامه حقوق بشر و شهروندی، شماره ۱۳، صص ۲۴۰-۲۲۴

نعمتی، نبی اله؛ صادقی نشاط، امیر، ۱۳۹۶، بررسی مسئولیت مدنی ناشی از نقض امنیت داده در تهدیدات سایبری، فصلنامه پژوهش‌های حفاظتی-امنیتی دانشگاه جامع امام حسین(ع)، سال ششم، شماره ۲۳، صص ۱۸۶-۱۵۷

پایان نامه‌ها

جعفری، کامران(۱۳۹۱)، جنگ سایبری در حقوق بین الملل، پایان نامه کارشناسی ارشد حقوق بین الملل، دانشکده حقوق دانشگاه پیام نور استان تهران

رحمتی، رضا،۱۳۹۶، فضای مجازی و امنیت سایبر در حقوق بین الملل، رساله برای اخذ درجه دکتری در رشته روابط بین الملل، دانشگاه تهران

زر رخ، احسان (۱۳۸۹)، جرم شناسی فضای مجازی، پایان نامه برای دریافت درجه کارشناسی ارشد، دانشگاه تهران

میرزا آقایی،مهدی، ۱۴۰۱، معیارهای تدوین نظام نامه پیشگیری اجتماعی از جرم سایبر (با استناد به اسناد ملی و بین‌المللی)، پایان نامه برای دریافت کارشناسی ارشد، دانشگاه آزاد اسلامی واحد الکترونیک