Received: 14 /12/2025
Review: 19/02/2026
Accepted: 17 /03/2026
DOI: 10.22054/jocl.2025.8563. 6210

Journal of Cyber Law
No(4),Vol(2), 31-45.
ISSN: 0972-6934
www.jocl.ir

Attribution of Artificial Intelligence-Based Cyberattacks in the Absence of Direct Human Agent in International Law

Kian Jafari [1], Masoud Raei dehaghi [2*], Alireza Ansarimahyari[3]

1- Phd Student, Department Of Law, Na.C, Islamic Azad University, Najafabad, Iran
2*- Professor, Department Of Law, Na.C, Islamic Azad University, Najafabad, Iran
3- Assistant Professor, Department of Law, Na.C, Islamic Azad University, Najafabad, Iran

ABSTRACT

The legal examination of the attribution of cyberattacks based on artificial intelligence in the absence of a direct human agent in international law is an emerging and complex issue that has received special attention due to the nature of the technology and its specific technical and legal challenges. In the field of international law, attribution of an act to a specific state or actor is possible when the responsibility of the subject or human agent can be established; however, in automated cyberattacks based on artificial intelligence, the direct lack of a human agent and machine decision-making pose serious ambiguities regarding the extent of responsibility and the method of attribution.Using a descriptive-analytical method, the author has concluded that the method of attributing cyberattacks based on artificial intelligence to states is the main challenge in this field. Under the 2001 draft, the attribution factors in the case of States are the conduct of official organs of the State or of persons acting under the direction or control of the State and their acts are attributable to the State in their official capacity. The unlawful act or omission of organs and representatives of the State will give rise to the international responsibility of the State. In the 2011 draft for international organizations, the attribution of acts to the organization is based on their more limited structure and legal personality and includes conduct carried out by official organs and representatives of the organization, but attention is paid to the structural differences and fewer resources of organizations compared to States.

Keywords:
Cyber attacks, artificial intelligence, legal attribution, state responsibility, international law.

Article Type:Research Article

How to Cite: Jafari,K., Raei dehaghi,M. and Ansarimahyari,A. (2026). Attribution of Artificial Intelligence-Based Cyberattacks in the Absence of Direct Human Agent in International Law. *Journal of Cyber Law (JOCL)*, 2(4),31-45.doi: 10.22054/jocl.2025.8563.6210

)Corresponding Author: masoud.raei@iau.ir

نشریه حقوق سایبری
شماره (٤) ٤٥-٣١
دوره ١٤٠٤

تاریخ دریافت: ١٤٠٤/٠٩/٢٣
تاریخ اصلاح: ١٤٠٤/١١/٣٠
تاریخ پذیرش: ١٤٠٤/١٢/٢٧

انتساب حملات سایبری مبتنی بر هوش مصنوعی در غیاب عامل انسانی مستقیم در حقوق بین‌الملل

کیان جعفری [1]، مسعود راعی دهقی [2*]، علیرضا انصاری مهیاری [3]

۱- دانشجوی دکترا، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

۲- استاد، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

۳- استادیار، گروه حقوق، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

چکیده

بررسی حقوقی انتساب حملات سایبری مبتنی بر هوش مصنوعی در غیاب عامل انسانی مستقیم در حقوق بین‌الملل، مسئله ای نوظهور و پیچیده است که به دلیل ماهیت فناوری و چالشهای فنی و حقوقی خاص خود، مورد توجه ویژه قرار گرفته است. در حوزه حقوق بین‌الملل، انتساب عمل به دولت یا بازیگر مشخص، زمانی امکانپذیر است که بتوان مسئولیت فاعل یا عامل انسانی را احراز کرد؛ اما در حملات سایبری خودکار مبتنی بر هوش مصنوعی، فقدان مستقیم عامل انسانی و تصمیم گیری ماشینی، میزان مسئولیت و نحوه انتساب را با ابهامات جدی مواجه می کند. نگارنده با استفاده از روش توصیفی تحلیلی به این نتیجه رسیده است که نحوه انتساب حملات سایبری مبتنی بر هوش مصنوعی به دولتها، اصلی ترین چالش در این زمینه می باشد. بر اساس پیش نویس سال ۲۰۰۱، عوامل انتساب در مورد دولت‌ها، رفتار ارگان های رسمی دولت یا افرادی است که تحت هدایت یا کنترل دولت عمل می کنند و اعمال آنها به دولت در مقام رسمی‌شان قابل انتساب است. فعل یا ترک فعل غیرقانونی ارگان‌ها و نمایندگان دولت، مسئولیت بین‌المللی دولت را به دنبال خواهد داشت. در پیش‌نویس سال ۲۰۱۱ سازمان‌های بین‌الملل ی، انتساب اعمال به سازمان بر اساس ساختار و شخصیت حقوقی محدودتر آنها است و شامل رفتاری می‌شود که توسط ارگان های رسمی و نمایندگان سازمان انجام می‌شود، اما به تفاوت های ساختاری و منابع کمتر سازمان‌ها در مقایسه با دولت‌ها توجه شده است.

کلیدواژه‌ها:

حملات سایبری، هوش مصنوعی، انتساب حقوقی، مسئولیت دولت، حقوق بین‌الملل.

نوع مقاله: پژوهشی

نحوه استناد:

جعفری, کیان, راعی دهقی, مسعود و انصاری مهیاری, علیرضا. (۱۴۰۴). انتساب حملات سایبری مبتنی بر هوش مصنوعی در غیاب عامل انسانی مستقیم در حقوق بین‌الملل. حقوق سایبری , ۲(۴), ۴۵-۳۱.

[1] ایمیل نویسنده مسئول: masoud.raei@iau.ir

۱. مقدمه

بررسی حقوقی انتساب حملات سایبری مبتنی بر هوش مصنوعی در غیاب عامل انسانی مستقیم در حقوق بین‌الملل، موضوعی نوظهور و چالش‌برانگیز است که به دلیل پیشرفت‌های فناوری و کاربرد گسترده هوش مصنوعی در فضای مجازی، اهمیت زیادی یافته است. هوش مصنوعی با توانایی پردازش کلان‌داده و یادگیری خودکار، قادر به اجرای حملات سایبری پیچیده بدون دخالت مستقیم انسان است که ماهیت آن از نظر حقوقی و فنی کاملاً متفاوت از حملات سنتی است. این امر چالشی اساسی برای نظام‌های حقوقی بین‌المللی ایجاد کرده است، زیرا اصول متعارف انتساب حملات به یک دولت یا عامل خاص، مستلزم حضور یک عامل انسانی مسئول است. در حقوق بین‌الملل، مسئولیت یک دولت در قبال حملات سایبری به رابطه کنترل و نفوذ بر عامل اجراکننده حمله متکی است. با این حال، در حملات مبتنی بر هوش مصنوعی که تصمیمات به صورت مستقل و خودکار گرفته می‌شوند، تعیین این رابطه و انتساب مسئولیت پیچیده است. این وضعیت منجر به شکاف‌های قانونی و لزوم بازتعریف اصول و قواعد موجود، از جمله منشور سازمان ملل متحد، اصل ممنوعیت استفاده از زور و حق دفاع از خود شده است. علاوه بر این، مشکلات فنی در تشخیص و تحلیل حملات سایبری هوشمند، پیچیدگی وظیفه را برای نهادهای قضایی و بین‌المللی افزایش می‌دهد و نیاز به همکاری بین وکلا، متخصصان فناوری و سیاست‌گذاران بین‌المللی را برای شکل‌دهی چارچوب‌های قانونی انعطاف‌پذیر و مؤثر تشدید می‌کند. تدوین مقررات جدید و قوانین به‌روز شده در مورد انتساب می‌تواند ابزاری کلیدی برای پاسخگویی حقوقی منصفانه در مواجهه با تهدیدات سایبری جدید باشد. بنابراین، بررسی حقوقی این موضوع باید با دیدگاهی میان‌رشته‌ای و تطبیقی انجام شود تا تعادلی بین امنیت سایبری، پاسخگویی دولت و حفاظت از حقوق اساسی در فضای بین‌المللی برقرار شود و از ایجاد شکاف‌های قانونی که امکان سوءاستفاده را فراهم می‌کنند، جلوگیری شود. علاوه بر این، پیچیدگی‌های فنی مرتبط با هوش مصنوعی، فرآیند تحلیل و شناسایی عامل حمله را دشوارتر و زمان‌برتر کرده است، زیرا حملات سایبری خودکار توانایی تغییر رفتار خود را بر اساس محیط و بازخورد دارند و شناسایی منشأ آنها را به چالش بزرگی تبدیل می‌کنند. همچنین، سیستم‌های هوشمند ممکن است طوری برنامه‌ریزی شوند که عمداً عامل انسانی را پنهان کنند یا فعالیت‌های خود را به گونه‌ای انجام دهند که انتساب به یک نهاد خاص را غیرممکن کند. این شرایط نیاز به تقویت سازوکارهای فنی و حقوقی برای حفظ شفافیت و پاسخگویی را افزایش می‌دهد. در این راستا، حقوق بین‌الملل باید به گونه‌ای تنظیم شود که بتواند به تحولات سریع فناوری پاسخ دهد و همزمان منافع دولت‌ها و جامعه بین‌المللی را حفظ کند. همچنین توجه به اصول اخلاقی و حقوق بشر، به ویژه در زمینه حفظ حریم خصوصی و جلوگیری از سوءاستفاده، باید به عنوان بخش جدایی‌ناپذیر چارچوب حقوقی در نظر گرفته شود. در نهایت، فضای بین‌المللی نیازمند تعمیق همکاری‌های چندجانبه، اشتراک‌گذاری اطلاعات و تبادل تجربیات برای مدیریت بهتر تهدیدات سایبری و هوشمند به منظور حفظ امنیت و ثبات جهانی و جلوگیری از نقض حقوق بین‌الملل است.

۱. خصوصیات حملات سایبری مبتنی بر هوش مصنوعی

حملات سایبری مبتنی بر هوش مصنوعی ویژگی‌های متمایزی دارند که آنها را نسبت به حملات سنتی، پیچیده‌تر و هوشمندانه‌تر می‌کند (قمری و مرادی، ۱۴۰۳: ۰۶). اولاً، آنها کاملاً خودکار هستند؛ یعنی الگوریتم‌های هوش مصنوعی می‌توانند فرآیند شناسایی اهداف، تجزیه و تحلیل آسیب‌پذیری‌ها و اجرای حملات را به طور مستقل مدیریت کنند و به

نظارت انسانی کم یا بدون نیاز به نظارت انسانی نیاز دارند (عبداللهی و همکاران[1]، ۲۰۲۵: ۷۱). ثانیاً، آنها از جمع‌آوری داده‌های با دقت و سرعت بالا بهره‌مند می‌شوند؛ هوش مصنوعی می‌تواند حجم عظیمی از اطلاعات را از منابع عمومی مانند شبکه‌های اجتماعی و وب‌سایت‌ها استخراج کرده و از آن برای هدف قرار دادن دقیق افراد یا سازمان‌ها استفاده کند (گومبه و همکاران[2]، ۲۰۲۲: ۰۶). یکی دیگر از ویژگی‌های آنها شخصی‌سازی حملات است.

۱-۱. خودکارسازی و استقلال عملکرد

حملات سایبری مبتنی بر هوش مصنوعی دارای ویژگی‌های اتوماسیون و خودمختاری هستند که آنها را از نظر عملیاتی کاملاً متمایز و پیچیده می‌کند. اولاً، این حملات به صورت خودکار و بدون نیاز به مداخله مداوم انسان انجام می‌شوند، به این معنی که الگوریتم‌های هوش مصنوعی می‌توانند به طور مستقل فرآیند تحقیق در مورد هدف، شناسایی آسیب‌پذیری‌ها، برنامه‌ریزی و اجرای حمله را مدیریت کنند. این اتوماسیون سرعت و مقیاس حملات را افزایش می‌دهد و مهاجمان قادرند به طور همزمان به صدها یا هزاران هدف حمله کنند (عبدالله و همکاران[3]، ۲۰۲۱: ۷۵). به عنوان مثال، در مرحله تشخیص[4]، هوش مصنوعی قادر است با جمع‌آوری و تجزیه و تحلیل داده‌های عمومی مانند شبکه‌های اجتماعی یا وب‌سایت‌های شرکت‌ها، اهداف ارزشمند را به طور خودکار پیدا کند و اطلاعات دقیق‌تری در مورد شبکه‌ها، کارمندان کلیدی و دارایی‌های حساس، بدون نیاز به عملیات دستی، به دست آورد. ثانیاً، یادگیری تقویتی[5] و مدل‌های خود تطبیقی به هوش مصنوعی اجازه می‌دهند تا رفتار خود را در طول حمله به صورت بلادرنگ مطابق با واکنش سیستم‌های دفاعی تغییر دهد تا از شناسایی و مقابله جلوگیری کند. این خودمختاری عمل، به حملات اجازه می‌دهد تا هوشمند و پویا باشند و به آنها اجازه می‌دهد تا به سرعت از اقدامات امنیتی عبور کنند و حتی روش‌های جدیدی برای نفوذ و تخریب ابداع کنند (کلودی و لی[6]، ۲۰۲۰: ۱۱۱). یکی دیگر از ویژگی‌های این است که حملات هوش مصنوعی مستقل می‌توانند کاملاً مستقل از طریق شبکه حرکت کنند، پشتیبان‌گیری‌های مخفی[7] ایجاد کنند، داده‌ها را استخراج یا دستکاری کنند و سیستم‌ها را مختل کنند، در حالی که به حداقل یا بدون دخالت انسان نیاز دارند. این خودمختاری حملات، پیش‌بینی، تشخیص و پاسخ به آنها را برای سازمان‌ها و دولت‌ها دشوارتر می‌کند. علاوه بر این، سیستم‌های خودکار مبتنی بر هوش مصنوعی در حملات سایبری توانایی تولید محتوای جعلی، مانند ایمیل‌های فیشینگ بسیار واقع‌گرایانه و سفارشی را دارند که تشخیص آنها را برای کاربران و سیستم‌های امنیتی بسیار دشوار می‌کند. این حملات با جمع‌آوری خودکار داده‌ها، پیام‌های هدفمند و شخصی‌سازی‌شده‌ای ایجاد می‌کنند که اثربخشی مهندسی اجتماعی را به میزان قابل توجهی افزایش می‌دهد (امامعلیف و قلدوشف[8]، ۲۰۲۵: ۲۱۱). از منظر دفاعی، این اتوماسیون و استقلال در عملیات حملات، نیاز به توسعه چارچوب‌های امنیتی پیشرفته، برنامه‌های نظارتی پویا و همکاری بین‌المللی بیشتر برای همگام شدن با سرعت و پیچیدگی این حملات را ایجاد می‌کند.

---

[1] Abdullahi et al
[2] Guembe et al
[3] Abuodeh et al
[4] Reconnaissance
[5] Reinforcement Learning
[6] Kaloudi & Li
[7] Backdoor
[8] Imamaliyev & Quldoshev

۱-۲. سرعت

حملات سایبری مبتنی بر هوش مصنوعی ویژگی‌های متمایزی دارند که آنها را نسبت به حملات سنتی، پیچیده‌تر و هوشمندانه‌تر می‌کند. اولاً، این حملات با اتوماسیون کامل اجرا می‌شوند؛ یعنی الگوریتم‌های هوش مصنوعی می‌توانند فرآیند شناسایی اهداف، تجزیه و تحلیل آسیب‌پذیری‌ها و اجرای حمله را به طور مستقل مدیریت کنند و به نظارت انسانی حداقلی یا بدون نظارت نیاز دارند. ثانیاً، این حملات از جمع‌آوری دقیق و سریع داده‌ها بهره می‌برند؛ هوش مصنوعی قادر است حجم عظیمی از اطلاعات را از منابع عمومی مانند شبکه‌های اجتماعی و وب‌سایت‌ها استخراج کرده و از آن برای هدف قرار دادن دقیق افراد یا سازمان‌ها استفاده کند. ویژگی دیگر، شخصی‌سازی حمله است؛ این حملات می‌توانند پیام‌ها و بدافزارهای خود را به شیوه‌ای بسیار سفارشی و متناسب با ویژگی‌های هدف طراحی کنند که در حملات فیشینگ بسیار مؤثر است و با استفاده از مهندسی اجتماعی پیشرفته همراه است (سارکر[1]، ۲۰۲۳: ۱۵۸). همچنین، حملات هوش مصنوعی از یادگیری تقویتی برای تغییر رفتار خود در زمان واقعی در طول حمله استفاده می‌کنند تا از شناسایی و اقدامات متقابل جلوگیری کنند و آنها را بسیار پویاتر و سازگارتر می‌کنند. ویژگی دیگر، استفاده از جعل عمیق و محتوای جعلی زنده مانند صدا و تصویر است که اثربخشی حملات مهندسی اجتماعی را افزایش می‌دهد و می‌تواند افراد را برای افشای اطلاعات حساس فریب دهد. همچنین، ظهور سرویس‌های جنایی مبتنی بر هوش مصنوعی به افراد غیرمتخصص اجازه می‌دهد تا حملات پیچیده را با حداقل دانش فنی انجام دهند (داش و همکاران[2]، ۲۰۲۳: ۱۹). به طور خلاصه، این حملات به دلیل سرعت عمل، دقت بالا، خودمختاری کامل و توانایی یادگیری و تغییر رفتار، تهدیدی بسیار جدی برای امنیت سایبری ملی و سازمانی محسوب می شوند و مقابله با آنها نیازمند فناوریهای شناسایی پیچیده، چارچوبهای امنیتی بهروز و همکاریهای بین‌المللی گسترده است.

۱-۳. سازگاری

سازگاری یکی از مهم‌ترین ویژگی‌های حملات سایبری مبتنی بر هوش مصنوعی است که تشخیص و مقابله با آنها را به طور قابل توجهی پیچیده‌تر و دشوارتر می‌کند. هوش مصنوعی با توانایی یادگیری و تجزیه و تحلیل مداوم کلان‌داده‌ها، می‌تواند به صورت پویا و در لحظه با تغییرات در محیط حمله، پاسخ‌های سیستم دفاعی و اقدامات متقابل سازگار شود (وارنابوا[3]، ۲۰۲۵: ۱۶۳). برخلاف سیستم‌های سنتی که به الگوهای ثابت متکی هستند، الگوریتم‌های هوش مصنوعی تمایل دارند الگوهای حمله جدید و متنوع را یاد بگیرند و رفتار خود را با استفاده از یادگیری ماشینی و یادگیری تقویتی متناسب با موقعیت بهینه کنند. این سازگاری به مهاجمان اجازه می‌دهد تا حملات را به روشی هدفمند و شخصی‌سازی شده طراحی کنند، به طوری که پیام‌ها و بدافزارها متناسب با ویژگی‌های خاص هر هدف اصلاح شوند (ساهانی[4]، ۲۰۲۴: ۷۸). به عنوان مثال، استفاده از جعل عمیق و محتوای جعلی زنده برای مهندسی اجتماعی بسیار مؤثر می‌شود، زیرا سیستم هوش مصنوعی می‌تواند بازخورد قربانی را تجزیه و تحلیل کرده و استراتژی حمله را بهبود بخشد. همچنین، توانایی تغییر رفتار در لحظه به حملات سایبری مبتنی بر هوش مصنوعی اجازه می‌دهد تا از تشخیص و اقدامات امنیتی فرار کنند یا حتی پس از تشخیص اولیه، روش‌های خود را به سرعت تغییر دهند. این ویژگی حملات را بسیار پویا و غیرقابل پیش‌بینی

---

[1] Sarker
[2] Dash et al
[3] Varbanova
[4] Sahani

می‌کند و برای مقابله با آنها به فناوری‌ها و چارچوب‌های امنیتی پیشرفته و انعطاف‌پذیر نیاز دارد (یوکسل و همکاران[1]، ۲۰۲۰: ۳۳۶). علاوه بر این، هوش مصنوعی می‌تواند با تجزیه و تحلیل مداوم روندهای گذشته و داده‌های تهدید، پیش‌بینی کند که حملات آینده چگونه رخ خواهند داد و در نتیجه، اقدامات متقابل واکنشی را به سمت رویکردهای پیشگیرانه تغییر دهد. این نشان می‌دهد که سازگاری نه تنها در اجرای حملات، بلکه در توسعه مداوم استراتژی‌های حمله نیز مهم است. برای مدیران و سیاست‌گذاران امنیتی، این سازگاری به معنای نیاز به تقویت مداوم سیستم‌های دفاعی، به‌روزرسانی قوانین و مقررات و افزایش همکاری‌های بین‌المللی برای مقابله با تهدیدات جدید است. سازگاری حملات هوش مصنوعی یک چالش فنی و حقوقی است که نیازمند رویکردهای چند رشته‌ای در زمینه‌های فناوری، قانون و سیاست است.

٤-۱. پنهان سازی

پنهان‌سازی یک ویژگی حیاتی و پیشرفته در حملات سایبری مبتنی بر هوش مصنوعی است که به مهاجمان اجازه می‌دهد عملیات مخرب خود را به صورت کاملاً مخفیانه و غیرقابل ردیابی انجام دهند. در این حملات، هوش مصنوعی با استفاده از الگوریتم‌های پیچیده یادگیری عمیق و شبکه‌های عصبی مصنوعی، قادر به ایجاد ترافیک مشکوک و رفتارهای مخرب به روشی جعلی است که شبیه رفتارهای طبیعی کاربران شبکه است. این روش باعث می‌شود ابزارهای امنیتی و سیستم‌های تشخیص نفوذ نتوانند بین ترافیک عادی و مخرب تمایز قائل شوند و شناسایی دقیق منبع و زمان حمله را بسیار دشوار می‌کند (بهروزیان، ۱۴۰۴: ۰۱). یکی از تکنیک‌های مهم در پنهان‌سازی، تولید ترافیک جعلی است که باعث سردرگمی و خطا در تجزیه و تحلیل داده‌ها برای سیستم‌های دفاعی می‌شود. هوش مصنوعی می‌تواند الگوریتم‌های خود را به طور مداوم به‌روزرسانی کند تا از اقدامات متقابل موجود عبور کند و حتی در برابر پاسخ‌های امنیتی خودکار مقاومت کند. همچنین، حملات چند مرحله‌ای با رمزگذاری پیچیده و اختلالات شبکه، تحلیلگران امنیتی را در تشخیص زودهنگام حملات به چالش می‌کشد. سیستم‌های هوشمند مبتنی بر هوش مصنوعی می‌توانند مخفیانه در شبکه‌ها حرکت کنند، درهای پشتی ایجاد کنند و داده‌ها را بدون جلب توجه مدافعان استخراج یا دستکاری کنند.

از سوی دیگر، این حملات ممکن است به گونه‌ای برنامه‌ریزی شوند که فعالیت خود را در زمان‌ها و شرایط خاص پنهان کنند و با تقلید از رفتار نرم‌افزارهای قانونی، ترافیک طبیعی را بازسازی کنند. علاوه بر این، استفاده از محتوای جعلی بسیار واقع‌گرایانه مانند دیپ‌فیک (تصاویر و ویدیوهای جعلی)، صداهای مصنوعی و پیام‌های فیشینگ پیشرفته، ابزاری مؤثر برای پنهان کردن هویت مهاجم و فریب کاربران انسانی است. به عنوان یک چالش بزرگ، مبهم‌سازی نه تنها یک ویژگی فنی، بلکه یک مسئله امنیتی و حقوقی نیز هست (عبدیوا-علیوا و همکاران[2]، ۲۰۲۱: ۱۱). این ویژگی، شناسایی دقیق منبع حمله و نسبت دادن مسئولیت به بازیگران یا دولت‌ها را بسیار پیچیده می‌کند، که مستلزم توسعه روش‌های جدید رهگیری، همکاری بین متخصصان فناوری و حقوقی و توسعه چارچوب‌های حقوقی و فنی پیشرفته است. (محمد[3]، ۲۰۲۵: ۱۴). این ویژگی‌ها، مقابله با حملات سایبری مبتنی بر هوش مصنوعی را نه تنها به یک مسئله فنی، بلکه به یک چالش قانونی و سیاسی تبدیل می‌کند که نیازمند همکاری چند رشته‌ای و چندجانبه است.

---

[1] Yüksel et al
[2] Abdiyeva-Aliyeva et al
[3] Mohammed

۲. تحلیل حقوقی انتساب در حقوق بین‌الملل

تحلیل حقوقی انتساب در حقوق بین‌الملل، مجموعه‌ای از قواعد و اصولی است که مسئولیت یک دولت یا نهاد بین‌المللی را برای اعمال خاص ارتکابی توسط افراد، گروه‌ها یا مأموران در قلمرو یا تحت کنترل آن تعیین می‌کند (استریکوفسکا[1]، ۲۰۱۸: ۱۴۹). در این زمینه، انتساب به معنای نسبت دادن یک فعل یا ترک فعل به یک دولت است که برای آن مسئولیت بین‌المللی ایجاد شده است. از منظر حقوق بین‌الملل، معیار اساسی برای انتساب دو عامل کلیدی است: کنترل مؤثر دولت بر مرتکب عمل، و ارتباط مستقیم یا غیرمستقیم آن عمل با اقدامات دولت (آسپرمونت و همکاران[2]، ۲۰۱۵: ۵۳). به عنوان مثال، اعمال افراد خصوصی به خودی خود قابل انتساب به دولت نیستند، مگر اینکه دولت کنترل کاملی بر آنها داشته باشد یا حداقل آنها را هدایت و حمایت کند یا در پاسخ به اقدامات آنها از اقدام خودداری کند. این امر به ویژه در زمینه حملات سایبری اهمیت دارد، زیرا انتساب یک حمله سایبری به یک دولت پیچیدگی‌های خاصی را به همراه دارد.

۲-۱. چالش‌های انتساب

انتساب در حقوق بین‌الملل به معنای انتساب یک فعل یا ترک فعل خاص به یک دولت یا نهاد بین‌المللی است که منجر به مسئولیت قانونی آن دولت می‌شود. این مفهوم مبنای تعیین مسئولیت بین‌المللی است و به تعیین اینکه کدام دولت یا نهاد قانونی باید مسئول عواقب رفتار غیرقانونی بین‌المللی شناخته شود، کمک می‌کند (نایتینگ موز[3]، ۲۰۲۵: ۰۶). معیارهای اصلی انتساب شامل انتساب اعمال ارگان‌های رسمی دولت، نمایندگان یا کارگزاران رسمی و همچنین گروه‌ها یا افرادی است که تحت کنترل مؤثر دولت عمل می‌کنند. کنترل «مؤثر» به این معنی است که دولت قادر به هدایت یا نظارت بر رفتار بازیگر یا گروه مربوطه است، حتی اگر کنترل کامل و جزئی نباشد (تساگوریاس و فارل[4]، ۲۰۲۰: ۹۴۷). مفهوم «کنترل کلی» نیز تعریف شده است که معیار وسیع‌تری است و به سطح کلی فرماندهی و پشتیبانی دولت بر گروه‌ها اشاره دارد. انتساب چالش‌های خاصی را در زمینه حملات سایبری ایجاد می‌کند.

۲-۱-۱. غیاب عامل انسانی مستقیم

فقدان عامل انسانی مستقیم یکی از چالش‌های عمده در انتساب مسئولیت در حملات سایبری است که تعیین دقیق منشأ و عامل حمله را پیچیده می‌کند (صادقیان لمراسکی و همکاران، ۱۴۰۴: ۰۶). در حملات سایبری متعارف، حضور عامل انسانی از طریق رفتار و خطاهای انسانی قابل ردیابی و شناسایی است، اما در حملات مبتنی بر هوش مصنوعی و فناوری‌های پیشرفته، حملات به صورت خودکار و بدون دخالت مستقیم انسان انجام می‌شوند، یا انسان‌ها فقط در طراحی اولیه دخیل هستند و در عملیات روزانه حضور ندارند. این امر «انتساب مستقیم» به عامل انسانی را که معمولاً مبنای مسئولیت قانونی است، دشوار یا غیرممکن می‌کند (سوات و همکاران[5]، ۲۰۲۴: ۰۳). از سوی دیگر، این فقدان عامل انسانی مستقیم، امکان اثبات «کنترل مؤثر» یا «هدایت» توسط یک دولت یا یک بازیگر خاص را پیچیده می‌کند، زیرا اثبات رابطه بین دولت و عملیات حمله نیاز به شواهد دقیق و قابل اعتماد از تماس و نظارت مستقیم انسان دارد که در حملات خودکار قابل مشاهده نیست. همچنین، فقدان عامل انسانی ملموس، استفاده از روش‌های فرار و فریب مانند

---

[1] Stryjkowska
[2] Aspremont et al
[3] Ntiting Mose
gj [4] Tsagourias & Farrell
[5] Swate

سرقت هویت و عملیات پرچم دروغین را تسهیل می‌کند و منجر به تحقیقات فنی و حقوقی گمراه‌کننده می‌شود. علاوه بر این، عدم وجود عامل انسانی مستقیم در فرآیند اجرا، مانعی برای جمع‌آوری شواهد قانونی قابل قبول برای اثبات مسئولیت می‌شود، مشکلی بزرگ به ویژه در حقوق بین‌الملل که نیازمند استانداردهای سختگیرانه‌ای برای اثبات است. پیچیدگی فنی و سرعت بالای حملات خودکار ناشی از هوش مصنوعی نیز فرصت پاسخ سریع و مؤثر را کاهش می‌دهد (ابو علید و ابو الطالیبه[1]، ۲۰۲۳: ۰۵). عدم وجود عامل انسانی مستقیم، نیاز به توسعه رویکردهای جدید در حقوق بین‌الملل، از جمله استفاده از اقدامات کنترلی مؤثر غیرمستقیم، تجزیه و تحلیل پیشرفته داده‌های فنی و همکاری گسترده بین‌المللی برای اثبات انتساب را افزایش می‌دهد.

۲-۱-۲. پیچیدگی فنی و جعل هویت

پیچیدگی فنی و جعل هویت از جمله چالش‌های اساسی در حوزه انتساب حملات سایبری هستند که شناسایی دقیق عامل یا منبع حمله را بسیار دشوار می‌کند. جعل هویت به معنای تظاهر به یک منبع معتبر است تا مهاجم بتواند با پنهان کردن ردپای واقعی خود به سیستم‌ها نفوذ کند یا کاربران را فریب دهد. حملات جعل هویت می‌تواند شامل جعل ایمیل، یا حتی وب‌سایت‌های جعلی باشد که برای سرقت اطلاعات حساس یا انتشار بدافزار با هدف فریب کاربران استفاده می‌شوند (صلاحی و کشفی، ۱۳۹۵: ۱۹). این حملات به دلیل استفاده از تکنیک‌های فنی پیشرفته و قابلیت سازگاری با محیط‌های مختلف، به راحتی توسط کاربران یا حتی سیستم‌های امنیتی قابل تشخیص نیستند (فائوتو و همکاران[2]، ۲۰۲۴: ۷۹). پیچیدگی فنی در این حوزه به دلیل لایه‌های مختلف پوشش و فریب ایجاد شده توسط مهاجمان است. آنها معمولاً از فناوری‌های ناشناس‌سازی مانند شبکه‌های پروکسی چندگانه، شبکه‌های خصوصی مجازی[3] و فناوری‌هایی مانند مرورگر تور[4] برای پنهان کردن مسیر حمله استفاده می‌کنند. همچنین استفاده از حملات چند مرحله‌ای و ترکیب فناوری‌های پیچیده رمزنگاری، ردیابی و تجزیه و تحلیل ردپاهای فنی حمله را بسیار دشوار می‌کند. این امر علاوه بر ایجاد ابهام در شناسایی منبع حمله، چالش بزرگی را در ارائه شواهد قانونی مستند برای اثبات مسئولیت ایجاد می‌کند (تگ و همکاران[5]، ۲۰۲۳: ۷۹). از سوی دیگر، جعل هویت به مهاجمان اجازه می‌دهد پیام‌ها یا درخواست‌هایی را ارسال کنند که به نظر می‌رسد از یک منبع قابل اعتماد، مانند یک فرد یا سازمان شناخته شده، ارسال شده‌اند که تحلیلگران امنیتی و حتی مقامات اجرای قانون را گمراه می‌کند. در نتیجه، شناسایی دقیق منشأ یک حمله و نسبت دادن آن به یک نهاد یا دولت خاص به یک مشکل پیچیده حقوقی و فنی تبدیل می‌شود. همچنین، ارائه شواهد کافی و قابل قبول برای اثبات ارتباط بین مهاجم و یک دولت یا گروه خاص، با توجه به پیچیدگی فنی این روش‌ها، به یکی از بزرگترین موانع در فرآیند نسبت دادن تبدیل شده است (دنیل سون و ویکتور ساموئل[6]، ۲۰۲۴: ۱۷۲۵). این چالش‌ها مستلزم استفاده از فناوری‌های پیشرفته تحلیل داده‌ها، همکاری بین‌المللی و چارچوب‌های قانونی دقیق به منظور ارائه پاسخی مؤثر و قانونی به حملات سایبری است.

---

[1] Abu Alead & AB ALTALIBE

[2] Faotu et al

[3] شبکه خصوصی مجازی (VPN) یک فناوری است که اتصال امن و رمزگذاری شده بین دستگاه شما و اینترنت ایجاد می‌کند. این فناوری با ایجاد یک تونل خصوصی برای داده‌های شما، حریم خصوصی و امنیت آنلاین شما را افزایش می‌دهد و امکان دسترسی به منابع یا محتوای محدود شده را فراهم می‌کند.

[4] تور (Tor) یک نرم‌افزار آزاد و متن باز است که برای ناشناس ماندن کاربران در محیط اینترنت به کار می‌رود. تور بر پایه نرم‌افزار کارخواه (Client) و شبکه‌ای از سرویس دهنده‌ها (سرورها) بنا می‌شود و می‌تواند داده‌هایی از کاربران را مانند موقعیت مکانی و نشانی آی‌پی پنهان کند.

[5] Tag et al

[6] Daniel Sontan & Victor Samuel

۲-۱-۳. عدم وجود معیار مشخص برای فناوری‌های نوین

امروزه حملات سایبری یک کشور علیه کشور دیگر در طول جنگ یا برای مقابله با درگیری‌های سیاسی امری رایج است و نمونه‌های زیادی از این حملات در سراسر جهان دیده می‌شود. حملات سایبری به عنوان یکی از مظاهر جدید دخالت سایبری شناخته شده‌اند (توحیدی و سیجانی، ۱۳۹۸: ۵۲). حملات سایبری اقداماتی هستند که توسط یک کشور برای هدف قرار دادن زیرساخت‌های اساسی یک کشور، از جمله سیستم‌های بانکی، انرژی و حمل و نقل عمومی که به یک شبکه رایانه‌ای متصل هستند، انجام می‌شوند (انصاری مهیاری و حسینی، ۱۴۰۲: ۰۳). فقدان یک استاندارد مشخص برای فناوری‌های جدید، به‌ویژه در حوزه حملات سایبری و فضای سایبری، یکی از چالش‌های اصلی و پیچیده در فرآیند انتساب مسئولیت در حقوق بین‌الملل است. این چالش از چندین عامل کلیدی ناشی می‌شود:

-اول، فناوری‌های جدید، مانند هوش مصنوعی، اینترنت اشیا و شبکه‌های نظیر به نظیر، اغلب دارای ویژگی‌ها و رفتارهای جدیدی هستند که قوانین و معیارهای سنتی انتساب برای آنها طراحی نشده یا سازگار نیستند. در نتیجه، بسیاری از قوانین موجود نمی‌توانند به طور مناسب به پیچیدگی‌ها و ویژگی‌های خاص این فناوری‌ها، مانند خودکارسازی حملات، سرعت بسیار بالا، رفتارهای دائماً در حال تغییر و پنهان‌کاری پیشرفته، پاسخ دهند (سیورلینه[1]، ۲۰۲۴: ۳۹)؛

-دوم، فقدان استانداردهای مشخص برای اثبات رابطه بین مهاجم (چه انسان و چه سیستم خودکار) و دولت یا نهاد بین‌الملل ی، فرآیند حقوقی را با ابهامات زیادی مواجه می‌کند. به عنوان مثال، در حملات مبتنی بر هوش مصنوعی، عدم وجود عامل انسانی مستقیم و استقلال عملکرد سیستم‌ها، تعیین «کنترل مؤثر» یا «جهت» دولت را دشوار و گاهی غیرممکن می‌کند. این امر معیارهای متعارف مانند «کنترل کامل» یا «کنترل مؤثر» را ناکافی و نیازمند تعریف مجدد یا تکمیل می‌کند (ایلیاشنکو و همکاران[2]، ۲۰۲۳: ۱۰۵).

-سوم، فضای مجازی که عرصه تعامل بین فناوری‌های مختلف و بازیگران متنوع (دولتی و غیردولتی) است، ماهیتی ناشناخته، پیچیده و چندلایه دارد که به سرعت تغییر می‌کند. این بدان معناست که تکیه صرف بر شواهد فنی یا روش‌های مرسوم جمع‌آوری داده‌ها نمی‌تواند منجر به قطعیت در انتساب شود و تحلیل‌های حقوقی و سیاسی دقیق‌تری مورد نیاز است (بورامدان[3]، ۲۰۲۳: ۱۴).

-چهارم، فقدان معیارهای مشخص به دولت‌ها یا سایر بازیگران اجازه می‌دهد تا از پذیرش مسئولیت طفره بروند یا به بهانه فقدان قوانین حقوقی روشن، از فضای مبهم برای عملیات مخرب سوءاستفاده کنند. این وضعیت، نظم حقوقی بین‌المللی را شکننده و همکاری بین‌المللی برای مقابله با تهدیدات جدید را دشوارتر می‌کند (هی و همکاران[4]، ۲۰۲۱: ۱۴۰۳). بنابراین، چالش فقدان معیارهای مشخص در فناوری‌های جدید، نیازمند تلاش‌های چندجانبه برای توسعه چارچوب‌های حقوقی جدید، تحقیق و تبیین معیارهای مشخص بر اساس ماهیت فناوری‌های جدید است.

۲-۲. راهکارهای پیشنهادی

در زمینه بررسی حقوقی انتساب حملات سایبری مبتنی بر هوش مصنوعی در غیاب عامل انسانی مستقیم، چندین راه‌حل کلیدی در حقوق بین‌الملل پیشنهاد شده است. اول، توسعه و به‌روزرسانی معیارهای انتساب به گونه‌ای که ویژگی‌های

[1] Čiurlienė
[2] Illiashenko et al
[3] Bouramdane
[4] He et al

فناوری‌های جدید مانند اتوماسیون و یادگیری خودکار سیستم‌ها را در بر بگیرد، مهم است؛ به طوری که معیارهای سنتی مانند «کنترل مؤثر» باید با شاخص‌های غیرمستقیم‌تر و تحلیل فنی همراه باشد (مافی و یزدانی، ۱۳۹۳: ۱۵۸). دوم، استفاده از فناوری‌های پیشرفته در جمع‌آوری و تحلیل شواهد دیجیتال، از جمله ردیابی داده‌های زنده و تحلیل الگوهای رفتاری هوش مصنوعی، برای تقویت اسناد فنی انتساب ضروری است. سوم، همکاری بین‌المللی گسترده برای تبادل اطلاعات و همسویی قانونی بین کشورها، پایه مهمی برای مقابله با حملات پیچیده و ناشناس محسوب می‌شود (فکوری سرشت، ۱۴۰۲: ۰۶). علاوه بر این، با توجه به فقدان عامل انسانی مستقیم، راه‌حل‌هایی مانند اعترافات فنی سیستم‌ها (مانند گزارش‌ها و داده‌های خودکار سیستم‌های هوش مصنوعی)، تحلیل رفتارهای مشابه در حملات مختلف و مدل‌های پیش‌بینی ریسک توسط هوش مصنوعی پیشنهاد شده است. چارچوب‌های قانونی باید امکان پیگیری مسئولیت را برای بازیگران انسانی درگیر در استفاده و مدیریت هوش مصنوعی، حتی در صورت عدم دخالت مستقیم در حمله، گسترش دهند (صوفی و صالح نژاد بهرستاقی، ۱۴۰۲: ۰۶). تأکید بر تدوین و اجرای مقررات بین‌المللی شفاف و منسجم در مورد استفاده از هوش مصنوعی در عملیات سایبری، از جمله مسئولیت ناشی از استفاده و سوءاستفاده از این فناوری، به کاهش شکاف‌های قانونی فعلی کمک خواهد کرد.

۲-۲-۱. توسعه قواعد جدید

تدوین قوانین جدید برای ارزیابی حقوقی حملات سایبری مبتنی بر هوش مصنوعی به عنوان یک راه حل حیاتی پیشنهاد شده است که می‌تواند به چالش‌های جدید در این حوزه پاسخ دهد. فناوری‌های جدید مانند هوش مصنوعی و اتوماسیون حملات، ویژگی‌هایی مانند عدم وجود عامل انسانی مستقیم، پیچیدگی فنی و پنهان‌کاری پیشرفته دارند که قوانین سنتی انتساب در حقوق بین‌الملل را ناکافی یا ناکارآمد کرده است (هوینگ و همکاران[1]، ۲۰۲۴: ۷۳۵). بنابراین، نیاز به ایجاد قوانین و معیارهای جدیدی وجود دارد که ویژگی‌های خاص حملات سایبری هوشمند را در بر می‌گیرد و امکان انتساب دقیق‌تر و قابل تأییدتری را فراهم می‌کند. این قوانین جدید باید شامل معیارهای دقیق‌تر و محتاطانه‌تری برای تعریف «کنترل مؤثر» و «هدایت» باشند که بتوانند فراتر از تعامل معمول انسانی باشند و همچنین اقدامات سیستم‌های هوشمند و خودکار را پوشش دهند. علاوه بر این، باید سازوکارهایی برای پذیرش شواهد دیجیتال پیچیده و تحلیل رفتار هوش مصنوعی به عنوان دلایل قانونی قابل قبول در نظر گرفته شود. همچنین لازم است نقش‌های مختلف بازیگران انسانی درگیر در توسعه، استقرار و مدیریت فناوری‌های هوش مصنوعی، علیرغم عدم دخالت مستقیم آنها در حملات، در چارچوب مسئولیت قانونی جدید، دقیق‌تر تعریف شود (اوادلاهه و همکاران[2]، ۲۰۲۵: ۱۲۴). از سوی دیگر، این قوانین باید بتوانند به سرعت با تغییرات تکنولوژیکی و تهدیدات جدید سازگار شوند تا بتوانند به توسعه سریع فناوری‌های سایبری و هوش مصنوعی پاسخ دهند. تأکید بر همکاری‌های بین‌المللی برای تدوین این استانداردها، ایجاد سازوکارهای هماهنگی و تبادل اطلاعات بین کشورها و نهادهای بین‌المللی نیز از دیگر جنبه‌های مهم تدوین قوانین جدید است (نئوپانه و همکاران[3]، ۲۰۲۴: ۲۸۱). به طور خلاصه، تدوین قوانین حقوقی جدید می‌تواند با تعریف معیارهای انتساب متناسب با ویژگی‌های هوش مصنوعی، پذیرش شواهد فنی دیجیتال پیچیده و تأکید بر همکاری بین‌الملل ی، ضمن حفظ عدالت و

[1] Hoenig et al
[2] Awadallah et al
[3] Neupane et al

پاسخگویی، و تضمین امنیت سایبری بین‌الملل ی، چارچوبی مؤثر برای مقابله با تهدیدات پیچیده و خودکار حملات سایبری فراهم کند.

۲-۲-۲. اصلاح معیارهای انتصاب

اصلاح معیارهای انتساب به عنوان یکی از راه‌حل‌های پیشنهادی برای مقابله با حملات سایبری مبتنی بر هوش مصنوعی از اهمیت ویژه‌ای برخوردار است، زیرا معیارهای سنتی حقوق بین‌الملل برای تعیین مسئولیت دولت طراحی شده‌اند و نمی‌توانند به طور کافی چالش‌های فناوری‌های جدید مانند هوش مصنوعی را پوشش دهند (عمیدی مهر و سیفی؛ ۱۳۹۹: ۹۵). این اصلاح باید شامل تعریف مجدد دقیق‌تر و به‌روزتری از معیارهایی مانند «کنترل مؤثر» و «هدایت» باشد، به گونه‌ای که بتواند عدم دخالت مستقیم انسان و عملکردهای خودمختار هوش مصنوعی را نیز به عنوان عوامل انتساب در نظر بگیرد (نام اور جهرمی[1]، ۲۰۲۲: ۵۸). علاوه بر این، معیارهای جدید باید امکان پذیرش شواهد دیجیتال و تحلیل رفتارهای پیچیده هوش مصنوعی را به عنوان مبانی قانونی قابل قبول فراهم کنند. این به معنای استفاده از فناوری‌های پیشرفته ردیابی داده‌ها، تحلیل الگوهای رفتاری و خودآموزی در هوش مصنوعی برای مستندسازی مسئولیت حملات است. همچنین باید نقش‌های مختلف بازیگران انسانی در توسعه، پیاده‌سازی و مدیریت سیستم‌های هوش مصنوعی را در نظر بگیرد، حتی اگر آنها مستقیماً در اقدامات حمله دخیل نباشند. اصلاح معیارهای انتساب باید بتواند به سرعت با سرعت تغییر در فناوری‌های سایبری سازگار شود، زیرا حملات مبتنی بر هوش مصنوعی به سرعت در حال تکامل هستند (اصلانی و رنجبریان، ۱۳۹۴: ۲۵۹). این امر مستلزم توسعه قوانین و چارچوب‌های پویا و به‌روز است که بتوانند با انعطاف‌پذیری با تهدیدات جدید مقابله کنند. این اصلاحات همچنین باید بر همکاری بین‌المللی برای توسعه استانداردهای مشترک و قابل اجرا بین کشورها و کاهش شکاف‌های قانونی فعلی در زمینه انتساب در فضای مجازی تأکید کنند (سنویراتنا و همکاران[2]، ۲۰۲۵: ۹۵۳). تدوین چنین معیارهایی، امکان پاسخ دقیق‌تر، عادلانه‌تر و کارآمدتر به حملات سایبری مبتنی بر هوش مصنوعی را فراهم می‌کند.

۲-۲-۳. همکاری‌های بین‌المللی

همکاری بین‌المللی یک استراتژی کلیدی و ضروری در مبارزه با حملات سایبری مبتنی بر هوش مصنوعی است که به دلیل ماهیت فرامنطقه‌ای این تهدیدات، بدون هماهنگی و همکاری جهانی نمی‌توان به طور مؤثر با آنها مقابله کرد (ضیائی بیگدلی و ترازی، ۱۴۰۰: ۸۳). این همکاری، در قالب تبادل اطلاعات، تجربیات، فناوری‌ها و الگوهای تهدید، به دولت‌ها و سازمان‌های بین‌المللی کمک می‌کند تا تهدیدات را بهتر درک کرده و اقدامات هماهنگی را برای پیشگیری و مقابله با آنها انجام دهند. تشکیل ائتلاف‌ها و پروژه‌های مشترک، مانند پروژه اطلس جرایم سایبری که تخصص متخصصان امنیت سایبری از سراسر جهان را گرد هم می‌آورد، نمونه‌ای از این همکاری است که به ایجاد یک پایگاه داده بزرگ در مورد جرایم سایبری کمک می‌کند و شناسایی و مسدود کردن حملات را تسهیل می‌کند (برناندز و همکاران[3]، ۲۰۲۳: ۷۲). این پروژه‌ها اعتماد بین نهادهای دولتی و خصوصی و به اشتراک‌گذاری داده‌ها و فناوری‌های جدید را افزایش می‌دهند که در نهایت دفاع در برابر حملات پیچیده و خودکار مبتنی بر هوش مصنوعی را تقویت می‌کند. همکاری بین‌المللی همچنین زمینه را برای توسعه چارچوب‌های مشترک قانونی، اخلاقی و فنی در مورد نحوه مدیریت و پاسخ به حملات سایبری

[1] Namavar Jahromi
[2] Senevirathna et al
[3] Bernardez et al

فراهم می‌کند که برای مقابله با فناوری‌های نوظهور و چالش‌های خاص آنها، مانند عدم دخالت مستقیم انسان و خودکارسازی حملات، ضروری است. آموزش و افزایش آگاهی جهانی در مورد تهدیدها و اقدامات متقابل نیز بخش مهمی از این همکاری است (راجوب و همکاران[1]، ۲۰۲۳: ۵۲۳). به طور خلاصه، همکاری بین‌المللی شامل موارد ی از جمله تبادل اطلاعات و تجربیات در مورد تهدیدها و الگوهای حمله؛ توسعه و اجرای پروتکل‌ها و استانداردهای مشترک امنیت سایبری؛ مشارکت در پروژه‌ها و ائتلاف‌های تحقیقاتی و عملیاتی مشترک؛ هماهنگی قانونی و نظارتی برای پاسخگویی می باشد.

نتیجه‌گیری

انتساب حقوقی حملات سایبری مبتنی بر هوش مصنوعی در غیاب عامل انسانی مستقیم، از جمله چالش‌های نوین و پیچیده حقوق بین‌الملل است که به دلیل ماهیت فناورانه و ویژگی‌های خاص این نوع حملات، قواعد موجود را با محدودیت‌های جدی مواجه ساخته است. ماهیت خودکار، توانایی سازگاری رفتاری، سرعت و دقت بالا، همراه با قابلیت پنهان‌سازی پیشرفته در این حملات، سبب شده است معیارهای سنتی انتساب مانند «کنترل مؤثر» و «کنترل کلی» در بسیاری از موارد ناکارآمد باشند و نتوانند رابطه میان دولت‌ها و عملیات تهاجمی را با قطعیت اثبات کنند. غیاب عامل انسانی مستقیم در فرآیند اجرا، علاوه بر دشوار کردن جمع‌آوری شواهد، امکان شناسایی منبع حمله را به نحو چشمگیری کاهش داده و اثبات مسئولیت بین‌المللی را با موانع فنی و حقوقی جدی روبه‌رو ساخته است. همچنین پیچیدگی‌های فنی نظیر جعل هویت، عملیات پرچم دروغین، رمزگذاری پیچیده و مهندسی اجتماعی پیشرفته، بر ابهام موجود افزوده و بازسازی مسیر حمله و انتساب آن به بازیگر یا دولت مشخص را دشوارتر کرده است. در چنین شرایطی، حفظ کارآمدی نظام مسئولیت بین‌المللی مستلزم بازنگری و اصلاح معیارهای انتساب به نحوی است که قابلیت پوشش‌دهی ویژگی‌های فناوری‌های نوین از جمله عملکرد خودمختار سیستم‌های هوش مصنوعی را داشته باشد. این بازنگری باید در کنار پذیرش شواهد دیجیتال پیچیده، تحلیل الگوهای رفتاری سامانه‌های هوشمند و شناسایی مسئولیت بازیگران انسانی دخیل در طراحی، توسعه و بهره‌برداری از فناوری، حتی بدون مداخله مستقیم در حمله، صورت گیرد. علاوه بر این، تدوین قواعد و استانداردهای جدید با هدف انطباق سریع با تهدیدات فناورانه، ضرورتی اجتناب‌ناپذیر است. این قواعد باید با مشارکت دولت‌ها، نهادهای بین‌المللی و جامعه علمی–فنی شکل گرفته و بتوانند چارچوبی شفاف و یکپارچه ایجاد کنند که مانع استفاده سوء از خلأهای حقوقی شود. همکاری‌های بین‌المللی نیز باید به‌عنوان رکن اساسی این فرآیند مورد تأکید قرار گیرد. تبادل اطلاعات فنی، همسان‌سازی رویه‌های اثبات، ایجاد سازوکارهای مشترک برای تحلیل داده‌ها و ارتقاء ظرفیت‌های حقوقی و فناورانه کشورها، پیش‌شرط دستیابی به نظام انتساب کارآمد محسوب می‌شود. در این میان، نقش سازمان ملل متحد و دیگر نهادهای بین‌المللی در تدوین اسناد الزام‌آور و هماهنگ‌سازی اقدامات، اهمیت ویژه‌ای دارد. پاسخ به چالش‌های ناشی از انتساب حملات سایبری مبتنی بر هوش مصنوعی، نیازمند رویکردی چندلایه و پویا است که همزمان سه بُعد فنی، حقوقی و سیاست‌گذاری را پوشش دهد.

[1] Rjoub et al

منابع

۱. منابع فارسی

مقالات

اصلانی، جبار؛ رنجبریان، امیرحسین (۱۳۹۴). بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه- کشورها و سازمان های بین‌المللی در حقوق بین‌الملل. مجله تحقیقات حقوقی، ۱۸: ۲۵۷-۲۸۹.

انصاری مهیاری، علیرضا؛ حسینی، زهراسادات (۱۴۰۲). نحوه انتساب جرایم سایبری به دولت ها. چهارمین کنفرانس ملی پدافند سایبری، ۰۱-۱۶.

بهروزیان، میثم (۱۴۰۴). هوش مصنوعی در دفاع سایبری: تشخیص، رهگیری و مقابله با تکنیک های پیشرفته مخفی سازی هکرها. منتشر شده در پایگاه مقالات سیویلیکا.

توحیدی، احمدرضا؛ سیجانی، محسن (۱۳۹۸). ارزیابی ماهیت حقوقی حملات سایبری با نگاهی به منشور سازمان ملل متحد. مجله پدافند غیرعامل، ۴۰:۴۷-۵۵.

صادقیان لمراسکی، محدثه؛ نقشین، مهدی؛ ابراهیمی، ابوالفضل (۱۴۰۴). جرایم سایبری مرتبط با هوش مصنوعی. اولین همایش ملی دستاوردها و چالشهای خانوادگی و فرهنگی از منظر روانشناسی حقوقی، ۰۱-۲۶.

صلاحی، سهراب؛ کشفی، سید مهدی (۱۳۹۵). جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تالین، فصلنامه علمی و پژوهشی مطالعات قدرت نرم، ۰۶: ۱۶-۲۵.

صوفی، سارا؛ صالح نژاد بهرستاقی، صابر (۱۴۰۲). تاثیر هوش مصنوعی در ارتکاب جرایم سایبری. مجله مطالعات حقوق، ۵۱: ۰۱-۱۸.

ضیائی بیگدلی، محمدرضا؛ ترازی، نسرین (۱۴۰۰). تحلیل قواعد انتساب در مسئولیت مشترک بین‌الملل ی. فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ۵۱: ۸۱-۱۰۲.

عمیدی مهر، الهام؛ سیفی، جمال (۱۳۹۹). رابطه حقوق بین‌الملل و حقوق داخلی در حوزه انتساب مسئولیت به دولت. پژوهشکده حقوق دانشگاه تهران، ۴: ۹۱-۱۱۷.

فکوری سرشت، مژگان (۱۴۰۲). نحوه انتساب و جبران خسارت در قبال حملات سایبری و مسئولیت بین‌المللی دولتها. هشتمین کنفرانس ملی پژوهش های نوین در حوزه علوم انسانی و مطالعات اجتماعی ایران، ۰۱-۲۲.

قمری، اسماعیل؛ مرادی، مجتبی (۱۴۰۳). بررسی تاثیر بکارگیری هوش مصنوعی در امنیت سایبری. دومین کنفرانس بین‌المللی حقوق، مدیریت، علوم تربیتی، روانشناسی و مدیریت برنامه ریزی آموزشی، ۰۱-۲۵.

مافی، همایون؛ یزدانی، سعید (۱۳۹۳). معیارهای انتساب اعمال شورشیان به دولت در حقوق بین‌الملل. پژوهشنامه حقوق تطبیقی، ۰۱: ۱۵۵-۱۷۴.

۲. منابع انگلیسی

Articles

Abuodeh, Muhammed & Adkins, Christian& Setayeshfar, Omid & Doshi, Prashant Lee, Kyu H. (2021). A Novel AI-based Methodology for Identifying Cyber Attacks in Honey Pots. Proceedings of the AAAI Conference on Artificial Intelligence, Vol. 35 No. 17: IAAI-21, EAAI-21, AAAI-21, 65-89.

Abu Alead, Rafeak M Salem & AB ALTALIBE, ALI AMHMED. (2023). Attribution Challenges in the Era of Cyber Warfare: Unraveling the Identity of Cyber-Attackers. Journal of the Higher Institute for Gender Studies, Volume 3, Issue 16,01-23.

Abdullahi, Mujaheed & Alhussian, Hitham & Aziz, Norshakirah & Abdulkadir, Said Jadid & Alwadain, Ayed & Muazu, Aminu Aminu. (2025). Comparison and Investigation of AI-Based Approaches for Cyberattack Detection in Cyber-Physical Systems. IEEE Access, Volume. 12, 65-89.

Awadallah, Abeer & Eledlebi, Khouloud & Zemerly, Mohamed Jamal & Puthal, Deepak & Damiani, Ernesto & Taha, Kamal. (2025). Artificial Intelligence-Based Cybersecurity for the Metaverse: Research Challenges and Opportunities. IEEE Communications Surveys & Tutorials (Volume: 27, Issue: 2, April 2025), 108 - 152.

Aspremont, Jean d’ & Nollkaemper, André & Plakokefalos, Ilias & Ryngaert, Cedric. (2015). Sharing Responsibility Between Non-State Actors and States in International Law: Introduction. Netherlands International Law Review, Volume 62, pages 49–67.

Abdiyeva-Aliyeva, Gunay & Hematyar, Mehran & Bakan, Sefa. (2021). Development of System for Detection and Prevention of Cyber Attacks Using Artificial Intelligence Methods. 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 01-25.

Bouramdane, Ayat-Allah. (2023). Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process. Laboratory of Renewable Energies and Advanced Materials (LERMA), College of Engineering and Architecture, International University of Rabat (IUR), IUR Campus, Technopolis Park, Rocade Rabat-Salé, Sala Al Jadida 11103, Morocco, 01-25.

Bernardez, Sergio Molina, Nespoli, Pantaleone & Gómez Mármol, Félix. (2023). Tackling Cyberattacks through AI-based Reactive Systems: A Holistic Review and Future Vision, Cornell Univerxity, Vo.6, 65-89.

Case Presecutor V. Tadic (1999) ILM. Vol, 38, P. 1518, at P 1541. and Para. 117.

Čiurlienė, Karina. (2024). Analysis of event and human factor-based decision-making in cybersecurity exercises using MCDM. Vilnius: Vilnius University Press, 2024, 36-70.

Daniel Sontan, Adewale & Victor Samuel, Segun. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews, 2024, 21(02), 1720–1736.

Dash, Bibhu & Ansari, Meraj Farheen & Sharma, Pawankumar & Ali, Azad. (2023). Threats and Opportunities with AI-Based Cyber Security Intrusion Detection: A Review. International Journal of Software Engineering & Applications (IJSEA), Vol.13, No.5, 14-36.

Faotu, Happy & Asheshemi, Oghenekevwe N. & Jeremiah T, Esite. (2024). Human Vulnerabilities in Cybersecurity: Analyzing Social Engineering Attacks and AI-Driven Machine Learning Countermeasures. Journal of Science and Technology. 30, 1 (Dec. 2024), 72–84. DOI:https://doi.org/10.20428/jst.v30i1.2597.

Guembe, Blessing & Azeta, Ambrose & Misra, Sanjay, Chukwudi Osamor, Victor & Fernandez-Sanz, Luis & Pospelova, Vera. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. Applied Artificial Intelligence An International Journal, 01-36.

He, Hongmei & Gray, John & Cangelosi, Angelo & Meng, Qinggang McGinnity, & T. Martin & Mehnen, Jörn. (2021). he Challenges and Opportunities of Human-Centered AI for Trustworthy Robots and Autonomous Systems, IEEE Transactions on Cognitive and Developmental Systems (Volume: 14, Issue: 4, December 2022), 1398 - 1412.

Hoenig, Amber & Roy, Kaushik & Takyiwaa Acquaah, Yaa & Yi, Sun & Desai, Salil S. (2024). Explainable AI for Cyber-Physical Systems: Issues and Challenges. IEEE Access, Volume: 12, 729 - 740

Illiashenko, Oleg & Kharchenko, Vyacheslav & Babeshko, Ievgen & Fesenko, Herman & Di Giandomenico, Felicita. (2023). Security-Informed Safety Analysis of Autonomous Transport Systems Considering AI-Powered Cyberattacks and Protection. Security Informed Safety Assessment and Assurance of Complex Critical Systems, Vol.25: 99-138.

Imamaliyev, Aybek & Quldoshev, Otabek. (2025). ARTIFICIAL INTELLIGENCE-BASED CYBERATTACKS AND THEIR PREVENTION. Лучшие интеллектуальные исследования, 39(1), 210–220. извлечено от https://inlibrary.uz/index.php/tbir/article/view/100261.

Kaloudi, Nektaria, Li, Jingyue. (2020). The AI-Based Cyber Threat Landscape: A Survey. ACM Computing Surveys,Vol. 53, No. 1, 01-34.

Plakokefalos, Ilias. (2017). The Use of Force by Non-State Actors and the Limits of Attribution of Conduct: A Reply to Vladyslav Lanovoy. European Journal of International Law, Volume 28: 587–593.

Mohammed, Anwar. (2025). Artificial Intelligence-Powered Cyber Attacks: Adversarial Machine Learning. Authorea. Innovative Science Publishers, 01-32.

Ntiting Mose, Theresa. (2025). Topic: Attribution and its Challenges and the Implications for State Responsibility Under International Cyber Security Law. Available at SSRN: https://ssrn.com/abstract=5087840 or http://dx.doi.org/10.2139/ssrn.5087840

Neupane, Subash & Mitra, Shaswata & Fernandez, Ivan A. & Sah, Swayamjit & Mittal, Sudip & Chen, Jingdao. (2024). Security Considerations in AI-Robotics: A Survey of Current Methods, Challenges, and Opportunities. IEEE Access, Volume: 12, 272 - 297.

Namavar Jahromi, Amir. (2022). AI-enabled Cybersecurity Framework for Industrial Control Systems. Doctoral thesis, University of Calgary, Calgary, Canada). Retrieved from https://prism.ucalgary.ca.

Rjoub, Gaith & Jamal, Bentahar & Abdel Wahab, Omar & Mizouni, Rabeb & Song, Alyssa & Cohen, Robin. (2023). A Survey on Explainable Artificial Intelligence for Cybersecurity. IEEE Transactions on Network and Service Management (Volume: 20, Issue: 4, December 2023), 515 - 540.

Sahani, Nitasha. (2024). AI-based Detection Against Cyberattacks in Cyber-Physical Distribution Systems. Virginia Tech, Vol. 01: 69-90.

Salem, Aya H. & Azzam, Safaa M. & Emam, O. E. & Abohany, Amr A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Springer Nature Link, Volume 11, 80-125.

Sarker, Iqbal H. (2023). Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. SECURITY AND PRIVACY, Volume6, Issue5, 154-170.

Swate, Clementine & Sithungu, Siphesihle & Lebea, Khutso (2024). An Analysis of Cyberwarfare Attribution Techniques and Challenges. Proceedings of the 23rd European Conference on Cyber Warfare and Security, ECCWS 2024, 01-08.

Senevirathna, Thulitha & La, Vinh Hoa & Marcha, Samuel & Siniarski, Bartlomiej & Liyanage, Madhusanka & Wang, Shen. (2025). A Survey on XAI for 5G and Beyond Security: Technical Aspects, Challenges and Research Directions. IEEE Communications Surveys & Tutorials (Volume: 27, Issue: 2, April 2025), 941-975.

Stryjkowska, Sylwia. (2018). The International Legal Issue of Attribution of Conduct to a State – The Case Law of the International Courts and Tribunals. Adam Mickiewicz University Law Review, Vol. 3: 143-156.

Tsagourias, Nicholas & Farrell, Michael. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. European Journal of International Law, Volume 31, Issue 3, August 2020, Pages 941–967.

Varbanova, Gergana. (2025). APPLICATION OF DEEP LEARNING IN ARTIFICIAL INTELLIGENCE SYSTEMS FOR CYBERATTACK IDENTIFICATION AND PREVENTION. Environment. Technology. Resources. Proceedings of the 16th International Scientific and Practical Conference. Volume 5, 158-189.

Yüksel, Benjamin & Schwarz, Klaus & Creutzburg, Reiner. (2020). AI-based anomaly detection for cyberattacks on Windows systems - Creation of a prototype for automated monitoring of the process environment. n Proc. IS&T Int'l. Symp. on Electronic Imaging: Mobile Devices and Multimedia: Technologies, Algorithms & Applications, 2020, pp 331 - 344.