

The Future of International Crimes: Feasibility of Adapting the Crime of Aggression to Counter Artificial Intelligence

 **Mohammad Ali Ardabili**

Professor, Faculty of Law, Shahid Beheshti University, Tehran, Iran. (Corresponding Author)
m-ardebili@sbu.ac.ir

 **Alireza Noorian**

Ph.D. in Criminal Law and Criminology, Faculty of Law, Edalat University, Tehran, Iran
m-ardebili@sbu.ac.ir



Abstract

The concurrent rise of state cyber capabilities and the potential (mis)use of Artificial Intelligence (AI) to advance malicious state objectives pose the critical question: Is the International Criminal Court (ICC) equipped to counter AI-driven cyber attacks perpetrated by and against states? Or does conduct via AI risk creating a legal vacuum, thereby shielding human actors who ordered its use from responsibility? In response, by outlining and explicating the “Responsibility Gap” discourse, this article analyzes how AI impacts the essential elements of international crimes namely, the material (*Actus Reus*) and mental (*Mens Rea*) elements from the perspective of the ICC Statute. Specifically, by examining the concept of “Cyber Aggression,” which has recently gained attention in legal scholarship, the study assesses the efficacy of the current text of the Rome Statute and its associated interpretations in establishing international criminal responsibility in cases where AI causes cyber aggression. This article explores a spectrum in which potential acts of cyber aggression may be reducible to human activity thus transferring

Journal of Research and
Development in Criminal Law and
Criminology

Iranian Law and Legal Research
Institute

Vol. 2 | No. 4 | Fall 2025 and
Winter 2026
(Original Article)

www.jclc.illrc.ac.ir

DOI:
10.22034/jclc.2026.735000

criminal responsibility to the human trainer of the AI versus scenarios where the committed act is perhaps too remote from human intervention to justify criminal responsibility based on the mental state of a culpable human agent. To engage in this discussion, the article begins with a brief overview of the Crime of Aggression, followed by the introduction of the emerging concept of cyber aggression. Subsequently, the challenges posed by applying AI-based aggression to the conventional elements of international criminal responsibility are examined. Furthermore, solutions proposed in International Criminal Law scholarship are described. It is argued that the elements of criminal responsibility for an act of aggression, within the current structure and interpretation of the ICC Statute, lack the necessary readiness and capacity to adapt to the ambiguous consequences of cyber aggression committed through state-sponsored AI systems. Finally, prior to the conclusion, an additional approach is proposed.

Keywords: International Criminal Court (ICC); Artificial Intelligence (AI); Cyber Aggression; Criminal Responsibility; Responsibility Gap.





آینده جرایم بین‌المللی؛ امکان‌سنجی تطبیق جرم تجاوز به منظور مقابله با هوش مصنوعی

استاد دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران (نویسنده
مسئول)

m-ardebili@sbu.ac.ir

دکترای حقوق کیفری و جرم‌شناسی دانشگاه عدالت، تهران، ایران
noorian@rocketmail.com

محمد علی اردبیلی 

علیرضا نوریان 



دوفصلنامه تحقیق و توسعه در حقوق کیفری و
جرم‌شناسی

پژوهشکده حقوق و قانون ایران

دوره ۲ | شماره ۴ | پاییز و زمستان ۱۴۰۴
(مقاله پژوهشی)

www.jclc.illrc.ac.ir

DOI:

10.22034/jclc.2026.735000

چکیده

افزایش هم‌زمان قابلیت‌های سایبری دولت‌ها و استفاده‌های (سوء) بالقوه از هوش مصنوعی برای پیشبرد اهداف مضر دولتی، این سوال را مطرح می‌کند که آیا دادگاه بین‌المللی کیفری آماده است تا با حملات سایبری مبتنی بر هوش مصنوعی که توسط و علیه دولت‌ها انجام می‌شود، مقابله کند؟ یا اینکه رفتار از طریق هوش مصنوعی، خطر افتادن در یک خلأ قانونی را به همراه دارد و بازیگران انسانی را که دستور استفاده از آن را داده‌اند از مسئولیت مصون می‌دارد؟ این مقاله در پاسخ، با طرح و تشریح گفتمان «شکاف مسئولیت»، به تحلیل چگونگی تأثیر هوش مصنوعی بر عناصر اساسی جرایم بین‌المللی، یعنی الزامات عناصر مادی و معنوی از منظر اساسنامه دادگاه بین‌المللی کیفری می‌پردازد و به‌طور خاص، با بررسی مفهوم تجاوز سایبری که اخیراً در نوشتگان حقوقی مورد توجه قرار گرفته است، اثربخشی متن فعلی اساسنامه دیوان و تفاسیر مرتبط با آن را در تعیین مسئولیت کیفری بین‌المللی در مواردی که هوش مصنوعی باعث تجاوز سایبری می‌شود، بررسی می‌نماید. این مقاله طیفی را بررسی می‌کند که در آن اعمال بالقوه

تجاوز سایبری، ممکن است به فعالیت انسانی تقلیل داده شوند بنابراین، مسئولیت کیفری به مرتبی انسانی هوش مصنوعی منتقل می‌شود؛ در مقابل حالتی که عمل ارتكابی شاید بیش از حد از مداخله انسانی دور است تا مسئولیت کیفری را تحت وضعیت روانی عامل انسانی دارای تقصیر توجیه کند. برای ورود به چنین بحثی، مقاله با مروری مختصر بر جرم تجاوز آغاز می‌شود و با معرفی مفهوم نوظهور تجاوز سایبری ادامه می‌یابد. سپس، چالش‌های اعمال تجاوز مبتنی بر هوش مصنوعی برای عناصر متعارف مسئولیت کیفری بین‌المللی بررسی می‌شود. در ادامه، راه‌حل‌های مطرح شده در نوشتگان حقوق بین‌الملل کیفری شرح داده می‌شوند و استدلال می‌شود که عناصر مسئولیت کیفری یک عمل تجاوز، در ساختار و تفسیر فعلی اساسنامه دیوان بین‌المللی کیفری در مواجهه با پیامدهای مبهم تجاوز سایبری انجام شده از طریق سیستم‌های هوش مصنوعی تحت حمایت دولت، آمادگی و ظرفیت لازم را برای تطبیق ندارند و در نهایت و پیش از ارائه برآمد، یک رویکرد اضافی پیشنهاد می‌گردد.

کلیدواژه‌ها: دادگاه بین‌المللی کیفری، هوش مصنوعی، تجاوز

سایبری، مسئولیت کیفری، شکاف مسئولیت

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

مقدمه

در سال ۲۰۱۷، گروه لازاروس^۱، حملهٔ بدافزار WannaCry را انجام داد که از نوعی ویروس کامپیوتری به نام کرم‌زننگاری شده برای آلوده کردن صدها هزار کامپیوتر در بیش از ۱۵۰ کشور استفاده کرد و تقریباً چهارمیلیارد دلار ضرر در سطح جهانی به بار آورد و صنایع مختلف، از مخابرات گرفته تا مراقبت‌های پزشکی اورژانسی را مختل کرد (What was the WannaCry., 2024).

در همان سال، گروه هکری روسی به نام Sandworm نیز از بدافزار مبتنی بر هوش مصنوعی برای انجام حملهٔ سایبری NotPetya استفاده کرد. گد مورد استفاده برای این حمله، به طور خودکار، سریع و بدون تبعیض اهداف پخش شد و در مجموع ده میلیارد دلار خسارت به بار آورد زیرا داده‌های شرکت‌های چندملیتی، شرکت‌های دولتی و مراکز اصلی برای حمل و نقل گرفته تا مراقبت‌های بهداشتی را از بین برد (Greenberg, 2018). به گفته کارشناسان، این حمله «تقریباً با هر تعریفی، یک جنگ سایبری بود. جنگی که احتمالاً حتی از آنچه سازندگان آن در نظر داشتند، انفجاری‌تر بود» (Ibid). در حالی که اوکراین به عنوان هدف این حمله در نظر گرفته شده بود، اما این بدافزار به سرعت در دیگر شبکه‌های رایانه‌ای پخش شد و میلیاردها دلار خسارت در سراسر جهان، از بیمارستان‌های پنسیلوانیا (ایالات متحده) گرفته تا یک کارخانهٔ شکلات‌سازی در تاسمانی (استرالیا) ایجاد کرد (Ibid).

همان‌طور که این مثال‌ها نشان می‌دهند قابلیت‌های سایبری می‌توانند ابزارهای قدرتمندی باشند که در یک حمله به کار گرفته می‌شوند، از جمله از طریق تلاش‌های تحت حمایت دولت یا به سفارش نهادهای خصوصی. علاوه بر این، همان‌طور که در ادامه مورد بحث قرار خواهد گرفت، نشانه‌های فزاینده‌ای وجود دارد که حملات سایبری تحت حمایت دولت، ممکن است طبق حقوق بین‌الملل، اقدامات تجاوزکارانه محسوب شوند.

چنین حملاتی پیش از این، محققان حقوق بین‌الملل، دولت‌ها و متخصصان را به طور یکسان آسیب‌ده کرده بود و اکنون نیز به نظر می‌رسد پیشرفت مداوم فناوری، ما را از یافتن پاسخ دورتر می‌کند، نه نزدیک‌تر. با گسترش سریع هوش مصنوعی که به طور فزاینده‌ای پیچیده و در دسترس قرار می‌گیرد، تعیین اینکه سوءرفتار انسانی در پس یک

۱. یک گروه مخفی از مجرمان سایبری که توسط دولت کره شمالی اداره می‌شود.

حمله سایبری به کجا ختم می‌شود و رفتار خود هوش مصنوعی از کجا آغاز می‌شود، به طور هم‌زمان چالش برانگیزتر خواهد شد. اخیراً در فوریه ۲۰۲۴، محققان دریافته‌اند که هوش مصنوعی مولد^۱ می‌تواند برای اجرای حملات سایبری با استفاده از کرم‌های رمزنگاشته، همان‌نوع بدافزاری را که مسئول حمله WannaCry بود مورد استفاده قرار دهد (Burges, 2024). مطالعه آنها پیش‌بینی کرد که این‌نوع کرم‌های رمزنگاشته، طی دو تا سه‌سال آینده مهارناشدنی خواهند بود (Ibid). این تحولات به این معنی است که حملات سایبری به‌طور فزاینده‌ای خود-توانمند و غیرقابل‌پیش‌بینی بوده و مقاومت در برابر آنها دشوار خواهد شد. هم‌زمان، کشورها نیز در حال سرمایه‌گذاری منابع و نیروی انسانی در قابلیت‌های عملیات سایبری خود هستند، هم به‌عنوان وسیله‌ای برای محافظت در برابر عملیات سایبری (ابوذری، ۱۴۰۲: ۱۹) و هم برای انجام آنها علیه سایر کشورها. در واقع، همان‌طور که «ینس استولتنبگ»^۲، دبیرکل سابق ناتو، در سخنرانی خود در کنفرانس تعهد دفاع سایبری ناتو در سال ۲۰۲۲ بیان داشت «سایبر، اکنون حوزه‌ای از عملیات است، برابر با عملیات زمینی، دریایی، هوایی و فضایی» (NATO Secretary General., 2022).

این افزایش هم‌زمان در قابلیت‌های سایبری دولت‌ها و در (سوء)استفاده‌های بالقوه از هوش مصنوعی برای پیشبرد اهداف مضر دولتی، این سوال را مطرح می‌کند که آیا دادگاه بین‌المللی کیفری آماده است تا با حملات سایبری مبتنی بر هوش مصنوعی که توسط و علیه دولت‌ها انجام می‌شود، مقابله کند؟ آیا رفتار هوش مصنوعی، خطر افتادن در یک خلأ قانونی را به‌همراه دارد و از مسئولیت بازیگران انسانی که دستور استفاده از آن را داده‌اند، محافظت می‌کند؟ در همین راستا، چگونه ممکن است حقوق بین‌الملل، نهادها و دست‌اندرکاران آن برای تعامل بهتر با آینده‌ای که در آن انسان‌ها لزوماً بازیگران اصلی پشتیبان (سوء)رفتار دولت‌ها نیستند، سازگار شوند؟

پرداختن به این نگرانی‌ها مهم است زیرا به توانایی مسئولیت‌کیفری بین‌المللی در رسیدگی به نقض‌های شدید صلح و امنیت بین‌المللی مربوط می‌شود و تعیین می‌کند که آیا جرایم بین‌المللی، به شکلی که در حال حاضر نوشته شده‌اند، ممکن است جرایم سایبری

۱. در حالی که تعاریف زیادی وجود دارد، در اینجا منظور از هوش مصنوعی مولد، یک مدل یادگیری ماشینی است که برای ایجاد داده‌های جدید آموزش دیده است، نه اینکه در مورد یک مجموعه داده خاص پیش‌بینی کند. یک سیستم هوش مصنوعی مولد، سیستمی است که یاد می‌گیرد اشیاء بیشتری تولید کند که شبیه داده‌هایی هستند که براساس آنها آموزش دیده است (Zewe, 2023).

2. Jens Stoltenberg

قابل توجهی را دربرگیرند یا خیر؟ اگر مجموعه‌ای از حملات بین‌المللی سایبری بتوانند از صلاحیت کیفری بین‌المللی فرار کنند، این امر کیفیت عدالتی را که دیوان بین‌المللی کیفری می‌تواند یا باید بتواند برای جرایم بین‌المللی معاصر ارائه دهد، به خطر می‌اندازد. برعکس، پرداختن مستقیم به این مسائل می‌تواند «به هم‌سو نمودن کار دیوان بین‌المللی کیفری با یکی از چالش‌های جدیدتر پیش‌روی جامعه بین‌المللی در قرن بیست و یکم کمک کند و بدین ترتیب، اهمیت دیوان را به‌شيوه‌ای که قبلاً تصور نمی‌شد، مجدداً تأیید کند» (Tarhan, 2021: 1134).

این مقاله با هدف پرداختن به این پرسش‌ها، به جرم بین‌المللی تجاوز به‌عنوان یک مطالعه موردی^۱ تکیه می‌کند تا نشان دهد چگونه قابلیت‌های هوش مصنوعی ممکن است ارزیابی مجدد عناصر اساسی جرایم بین‌المللی، یعنی الزامات عنصر مادی و عنصر معنوی جرم را ضروری سازد. این مقاله به‌طور خاص با بررسی مفهوم «تجاوز سایبری»، به بررسی اثربخشی متن و تفسیر فعلی اساسنامه دیوان بین‌المللی کیفری در تطبیق مسئولیت کیفری بین‌المللی در مواردی که هوش مصنوعی باعث تجاوز سایبری می‌شود، می‌پردازد. در انجام این کار، مقاله به‌دنبال پاسخ به این سوال است که آیا می‌توان «رهبران»^۲ را در چارچوب جرم تجاوز سایبری به‌خاطر اقدامات هوش مصنوعی پاسخگو دانست؟

لازم به‌ذکر است که هرچند این تحقیق از دیگر شاخه‌های حقوق بین‌الملل برای ارائه پیشینه‌ای در مورد تأثیر هوش مصنوعی بر حقوق کیفری بین‌المللی بهره می‌برد، لکن بحث در این مقاله، از دو جهت کلیدی با آنچه در آثار حقوق بین‌الملل بشردوستانه در مورد «سیستم‌های سلاح‌های خودمختار کشنده»^۳ رایج شده است، متمایز می‌باشد. نخست اینکه، معیار بررسی و تجزیه و تحلیل در این مقاله، مسئولیت کیفری بین‌المللی است که علی‌رغم هم‌پوشانی در برخی زمینه‌ها با حقوق بین‌الملل بشردوستانه، یک نهاد حقوقی

۱. به این سبب، جنایت تجاوز به‌عنوان مطالعه موردی انتخاب شده است که برخلاف دیگر جرایم بین‌المللی، ارکان یک عمل تجاوز غیرقانونی، معمولاً گسسته‌تر و بنابراین قابل جداسازی‌تر از سایر جرایم بین‌المللی است و این امر، بحث در مورد تأثیر هوش مصنوعی بر هر عنصر جرم را ساده‌تر می‌کند. این در حالی است که تأثیر متغیرهای مخدوش‌کننده بر هرگونه نتیجه‌گیری را نیز محدود می‌کند.

۲. به‌طور کلی، افرادی که عموماً در جایگاه ممتاز زمامداری، رهبری و فرماندهی قرار دارند.

مجزا با عناصر مختص به خود برای مسئولیت است. دوم، هنگام بحث در مورد حملات مبتنی بر هوش مصنوعی در حقوق بین‌الملل بشردوستانه، تمرکز عمدتاً بر حملات جنبشی^۱ (یا حملاتی که به‌منظور ایجاد اثرات جنبشی صورت می‌پذیرد) است که با استفاده از سیستم‌های سلاح‌های خودمختار کشنده انجام می‌شوند. برعکس، پژوهش حاضر شامل بحث در مورد اعمالی است که با تکیه بر هوش مصنوعی برای انجام حملات غیرجنبشی در قالب جنگ سایبری انجام می‌شوند، که لایه‌ای از چالش‌ها را به‌ویژه در رابطه با شناسایی عامل اصلی مربوطه اضافه می‌کند.

در این مقاله، استدلال می‌شود که عناصر مسئولیت کیفری یک عمل تجاوزکارانه، در ساختار و تفسیر فعلی خود در اساسنامه دیوان، در مواجهه با پیامدهای مبهم تجاوز سایبری انجام‌شده از طریق سیستم‌های هوش مصنوعی تحت حمایت دولت، ظرفیت لازم را ندارند.

برای ورود به بحث، پس از تشریح مختصر جرم تجاوز و معرفی مفهوم نوظهور تجاوز سایبری (گفتار نخست)، چالش‌های اعمال تجاوزکارانه مبتنی بر هوش مصنوعی برای عناصر متعارف مسئولیت کیفری بین‌المللی بررسی می‌شود (گفتار دوم). سپس راه‌حل‌های مطرح‌شده در نوشتگان حقوقی شرح داده می‌شود و یک رویکرد اضافی پیشنهاد می‌شود (گفتار سوم) و در نهایت، نتیجه‌گیری ارائه می‌گردد.

گفتار نخست. جرم تجاوز

جنایت تجاوز، برای نخستین بار، پس از جنگ دوم جهانی در محاکمات نورنبرگ به‌عنوان یک جرم بین‌المللی که مسئولیت فردی به همراه دارد، شناخته شد. دادگاه نظامی بین‌المللی نورنبرگ^۲ «جنایات علیه صلح را در حوزه صلاحیت خود قرار داد، یعنی برنامه‌ریزی، آماده‌سازی، شروع یا اجرای جنگ تجاوزکارانه یا جنگی که ناقض معاهدات، توافق‌نامه‌ها یا تضمین‌های بین‌المللی باشد، و یا مشارکت در یک طرح یا توطئه مشترک برای انجام هریک از موارد فوق» (Tsilonis, 2024: 165-184). دادگاه نظامی بین‌المللی

1. kinetic attacks

2. International Military Tribunal at Nuremberg

نورنبرگ جرم تجاوز را «جنایت برتر بین‌المللی» می‌دانست که «تنها از این نظر با سایر جنایات متفاوت است که شرّ انباشته‌شده از کل را در خود جای داده است».^۱ با این حال، پس از دادگاه نورنبرگ و نیز دادرسی‌های کیفری بین‌المللی در توکیو نزد دادگاه نظامی بین‌المللی برای خاور دور^۲، «جنایت تجاوز از نقشه حقوق بین‌الملل ناپدید شد» (Cassese, 2007: 843-844). البته چند استثنا وجود داشت. از جمله، این مفهوم توسط مجمع عمومی سازمان ملل متحد در ۱۹۷۴، زمانی که قطعنامه‌ای را برای تعریف تجاوز تصویب کرد، قدری توسعه یافت (Tsilonis, op. cit.: 171). سپس، در ۱۹۸۵، شورای امنیت سازمان ملل متحد چندین اقدام دولتی را به‌عنوان اقدامات تجاوزکارانه محکوم کرد از جمله حمله هوایی اسرائیل به تأسیسات سازمان آزادی‌بخش فلسطین در تونس و حمله آفریقای جنوبی به آنگولا.^۳

متعاقباً در تابستان ۱۹۹۸ و پس از مذاکراتی طولانی، جرم تجاوز در اساسنامه رم، سند مؤسس دادگاه بین‌المللی کیفری، گنجانده شد و در فهرست جرایم بین‌المللی قرار گرفت. لکن اساسنامه مقرر داشت که تعریف جرم تجاوز در تاریخ‌دیگری تعیین شود. این امر در ۲۰۱۰ حادث شد، یعنی زمانی که کنفرانس بررسی در کامپالا برای تصمیم‌گیری در مورد تعریفی برای جرم تجاوز، که از طریق ماده ۸ مکرر در اساسنامه رم گنجانده شد، برگزار گردید. در نهایت مقرر شد که پس از اصلاحیه، صلاحیت دیوان «برای آن دسته از کشورهای عضو که اصلاحیه را یک سال پس از تودیع اسناد تصویب یا پذیرش خود پذیرفته‌اند» لازم‌الاجرا شود (اساسنامه دیوان بین‌المللی کیفری، ماده ۵(د) و ۱۲۱(۵)). برعکس، «در مورد کشوری که اصلاحیه را نپذیرفته‌است، دیوان صلاحیت خود را در مورد جرمی که مشمول اصلاحیه است، در صورتی که توسط اتباع آن کشور یا در قلمرو آن ارتکاب یابد، اعمال نخواهد کرد» (اساسنامه دیوان بین‌المللی کیفری، ماده ۱۲۱(۵)).

1. Judgment, United States of America et al. V. Goering et al, International Military Tribunal, 30 September to 1 October 1946, p.172.

2. International Military Tribunal for the Far East

3. SC Res. 573, 4 October 1985; and SC Res. 577, 6 December 1985.

تقریباً یک‌دهه بعد، در اواخر ۲۰۱۷، در شانزدهمین جلسه مجمع کشورهای عضو در نیویورک، زمانی که تعریفی از این جرم در اساسنامه دیوان بین‌المللی کیفری گنجانده شد، جرم تجاوز «فعال» گردید و بدین ترتیب، «به‌مثابه یک جرم واقعی از نظر قانونی تثبیت شد» (Tsilonis, op. cit.: 166) و در ۱۷ جولای ۲۰۱۸ لازم‌الاجرا گردید (Kreß, 2018: 15). ماده ۸ مکرر اساسنامه رم، جنایت تجاوز را برنامه‌ریزی، آماده‌سازی، شروع یا اجرای یک عمل تجاوز توسط شخصی که در موقعیتی است که به‌طور مؤثر می‌تواند بر اقدام سیاسی یا نظامی یک کشور کنترل یا هدایت کند، تعریف می‌کند که از نظر ماهیت، شدت و مقیاس، نقض آشکار منشور سازمان ملل متحد محسوب می‌شود.

الف. عناصر مسئولیت کیفری بین‌المللی برای جرم تجاوز

مانند سایر جرایم بین‌المللی مندرج در اساسنامه رم، جرم تجاوز نیز شامل دو عنصر کلیدی مادی و معنوی است. عنصر مادی، به رفتار (اعم از فعل، ترک فعل یا جرم فعل ناشی از ترک فعل)، حالت، و یا اوضاع و احوالی اشاره دارد که تجلی نیت مجرمانه و یا تقصیر جزایی است (اردبیلی، ۱۴۰۳: ۱ / ۱۳۵-۱۴۱) در اینجا، عنصر مادی جرم تجاوز در ماده ۸ مکرر اساسنامه رم، برنامه‌ریزی، آماده‌سازی، شروع یا اجرای یک عمل تجاوز توسط شخصی است که در موقعیتی است که به‌طور مؤثر کنترل یا هدایت اقدام سیاسی یا نظامی یک دولت را بر عهده دارد. پس تحقق عنصر مادی، مستلزم آن است که عمل تجاوزکارانه توسط شخصی که در موقعیت هدایت اقدام سیاسی یا نظامی یک دولت قرار دارد، انجام شود (Hajdin, 2021: 492).

عنصر روانی، به وضعیت روانی، خواست یا اراده اشاره دارد که مرتکب باید هنگام وقوع عنصر مادی داشته باشد تا در نتیجه ارتکاب جرم، مسئول شناخته شود (پیشین: ۱۷۰). عنصر روانی جنایت تجاوز، از ماده ۳۰ اساسنامه دیوان بین‌المللی کیفری گرفته می‌شود که عناصر روانی مورد نیاز برای آن دسته از جرایم در اساسنامه رم که وجه تمایز آنها ذکر عنصر روانی است، ارائه می‌دهد. بندهای (۲) و (۳) این ماده، به قصد در مورد رفتار مرتکب و آگاهی از شرایط پیرامونی و نتیجه، که شامل زمینه عمل تجاوز دولت نیز می‌شود، اشاره

دارد. این امر نشان از دیدگاه غالب در حقوق کیفری بین‌المللی معاصر است که به‌طور کلی، «کسی نمی‌تواند عملی را انجام دهد یا نتیجه‌ای را عمداً ایجاد کند مگر اینکه از شرایطی که آن عمل یا نتیجه در آن ارتکاب یافته است نیز آگاهی داشته باشد» (Greipl, 2023: 1106).

در مورد عنصر روانی، این الزام به قصد و آگاهی نسبت به اجزای جرم، به‌سمت استانداردهای سنگین‌تر متمایل است و بنابراین، اثبات آن چالش‌برانگیزتر است. این معیار با دیدگاه اکثریت اندیشمندان حقوق بین‌الملل نیز هم‌راستا است که حالات روانی خفیف‌تر را برای تحقق ماده ۳۰ اساسنامه رم کافی نمی‌دانند (Clark, 2001: 314-315; Ambos, 1999: 21-22). در حالی که برخی از محققان مخالفند و استدلال می‌کنند که یک حالت روانی خفیف‌تر، مانند بی‌پروایی^۱ نیز باید کافی باشد، که البته رویه فعلی دیوان بین‌المللی کیفری نشان می‌دهد که دیدگاه اخیر با رویکرد دیوان مطابقت ندارد.^۲ جمله‌بندی ماده ۳۰ اساسنامه نیز به‌سختی جایی برای تفسیری باقی می‌گذارد که شامل بی‌پروایی باشد (Eser, 2002: 915; Poro, 2014: 179).

ب. ظهور تجاوز سایبری و بحران هویت آن به‌عنوان یک جرم بین‌المللی

تجاوز سایبری، که حوزه مطالعاتی نسبتاً جدید در حقوق بین‌الملل است، به اعمال تجاوزکارانه‌ای اشاره دارد که در فضای مجازی با نقض حقوق بین‌الملل انجام می‌شوند. این تصور که پیشرفت‌های فناوری ممکن است ما را ملزم به بازنگری مفاهیم متعارف در حقوق بین‌الملل کند، جدید نیست (Tsilonis, op. cit.: 315). در طول دو دهه گذشته، نمونه‌های زیادی از دولت‌هایی که حملات سایبری را علیه کشورهای دیگر یا در قلمرو دیگر کشورها (Zetter, 2013) و یا با هدف ایجاد اختلال در صنایع اساسی در یک کشور انجام داده‌اند، وجود داشته‌است (Davis, 2007). با این حال، ادبیات این حوزه با چالش‌های

¹. dolus eventualis; recklessness

². Decision of the Pre-Trial Chamber, Bemba Gombo (ICC-01/05-01/08-424), 15 June 2009, § 368; Judgment, Lubanga (ICC-01/04-01/06-2842), Trial Chamber, 14 March 2012, § 1011.

زیادی در تطبیق این حملات، حتی بدون کمک هوش مصنوعی، با تعریف جرم تجاوز روبرو بوده است.^۱

در سال‌های اخیر، دولت‌ها شروع به ارائه مواضع رسمی خود در مورد کاربرد حقوق بین‌الملل در فضای مجازی نموده‌اند. سی‌وهشت دولت (و هم‌چنان در حال افزایش) که تا به امروز چنین موضعی را بیان داشته‌اند، به اتفاق آراء معتقدند که قوانین و هنجارهای حقوق بین‌الملل در فضای سایبری اعمال می‌شود (Carpenter and Hollis, 2023) و در نتیجه، حقوق کیفری بین‌الملل را به‌طور گسترده دربرمی‌گیرد.

با این حال، اگرچه در مورد اعمال حقوق بین‌الملل در فضای سایبری تاحدودی اجماع وجود دارد اما ادبیات موجود در حقوق کیفری بین‌الملل در مورد چگونگی و اینکه تحت چه شرایطی ممکن است حمله سایبری به یک عمل تجاوز منجر شود، نامشخص است. دو چالش خاص در اینجا برجسته است: نخست اینکه، آیا یک حمله سایبری می‌تواند به سطح جنایت تجاوز برسد؟ دوم اینکه، آیا مرتکب چنین حمله‌ای می‌تواند الزام شرط رهبری مندرج در جنایت تجاوز را برآورده کند؟

در مورد چالش نخست، این مقاله به‌سرعت خاطر نشان می‌کند که در تطبیق یک حمله سایبری مشخص با معنای یک عمل تجاوز، موارد فراوانی مربوط به «تعریف» وجود دارد. در این مورد، توجه به توسعه دستورالعمل‌های تالین (۱/۰ و ۲/۰)، که توسط گروهی از کارشناسان بین‌المللی در حقوق بین‌الملل و امنیت سایبری به‌میزبانی مرکز عالی دفاع سایبری مشترک ناتو در تالین (استونی) ایجاد گردیده، حائز اهمیت است (اردبیلی و دیگران، ۲۰۲۱: ۱۴۰۲-۱۵۳۷-۱۵۵۹). این گروه، دو کتابچه راهنما منتشر کرد که در مورد چارچوب قانونی عملیات سایبری در حقوق بین‌الملل و حقوق درگیری‌های مسلحانه راهنمایی ارائه می‌دادند؛ یکی در ۲۰۱۳ و دیگری در ۲۰۱۷. در کتابچه راهنمای تالین ۲۰۰، حمله سایبری به‌عنوان «عملیاتی سایبری [...] که به‌طور منطقی انتظار می‌رود

۱. باید توجه داشت که این گفتار و در واقع این مقاله، محدود به بحث در مورد حملات سایبری به‌عنوان اقدام تهاجمی است. لذا شامل سایر جرایم سایبری، از جمله جاسوسی سایبری نمی‌شود. برای بحث در مورد تفاوت‌های بین این جرایم (Weissbrodt, 2013: 347-387).

باعث آسیب یا مرگ افراد یا آسیب یا تخریب اشیاء شود» تعریف شده است (Schmitt, 2017: 126). جنگ سایبری نیز به‌عنوان استفاده از حمله سایبری، چه در چارچوب درگیری مسلحانه و چه بدون آن، به شیوه‌ای تعریف شد که اثراتی معادل^۱ یک حمله مسلحانه متعارف داشته باشد (Ibid). این موضوع در دکترین (Weissbrodt, op. cit.: 369; Ambos,) و در بین کشورها (Carpenter and Hollis, op. cit.: supra; Greco, 2020: 44; 495-504; 2016) در مورد اینکه مصادیق «اثر معادل» چه می‌تواند باشد، مورد بحث قرار گرفته است، (note 37) در مورد اینکه مصادیق «اثر معادل» چه می‌تواند باشد، مورد بحث قرار گرفته است، اما درک برجسته‌ای وجود دارد که برای مثال، حمله سایبری به تأسیسات هسته‌ای، شبکه‌های برق، بیمارستان‌ها یا سایر زیرساخت‌های ضروری می‌تواند به‌عنوان یک حمله مسلحانه انجام شده از طریق ابزارهای سایبری شناخته شود (Trahan, op. cit.: 1136).

از سوی دیگر، طرح‌های استراتژیک که به‌طور متناوب توسط دفتر دادستانی دیوان بین‌المللی کیفری منتشر می‌شوند نیز هنوز به این سؤالات نپرداخته‌اند. تمرکز طرح ۲۰۱۶-۲۰۱۸ «به صورت تک‌بُعدی بر نیاز به استفاده بیشتر از فناوری‌های دیجیتالی جدید برای شناسایی، جمع‌آوری و ارائه شواهد از طریق فناوری» قرار گرفته است و تنها اشاره‌ای مبهم به نیاز فوری در به‌دست آوردن «بینش در مورد احتمالات و تهدیدهای جدید ناشی از تکامل فناوری» دارد (Office of the Prosecutor, Strategic Plan 2016-2018). به‌همین ترتیب، طرح ۲۰۲۳-۲۰۲۵ که با هدف «نهایی کردن یک بررسی جامع و تثبیت چارچوب سیاست خود در مورد شدت/اولویت‌بندی/تکمیل تحقیقات» است نیز معتقد است که «سایر سیاست‌های جدیدی که در طول دوره اجرای این طرح استراتژیک تکمیل خواهند شد، به حوزه‌هایی از جمله جرایم سایبری خواهند پرداخت [...]» (Office of the Prosecutor, Strategic Plan 2023-2025).

«کریم.ا.ا.خان»، دادستان دیوان بین‌المللی کیفری، در ژانویه ۲۰۲۴ اظهار داشت که جرایم سایبری «در صورت برآورده شدن الزامات اساسنامه رم، ممکن است در صلاحیت دیوان بین‌المللی کیفری قرار گیرند» (Statement by ICC Prosecutor., 2024) و «دفتر من [دادستانی] می‌تواند چنین رفتارهایی را بررسی یا تحت پیگرد قانونی قرار دهد» (K.A.A.).

1. equivalent effects

Khan KC., 2023).^۱ براین اساس، توجه نهادین به چالش‌های تفسیری تطبیق رفتار حملات سایبری با پارامترهای جرایم بین‌المللی، ممکن است به‌زودی صورت گیرد، اما هنوز به آن توجه وافی نشده است.

در مورد چالش دوم، حملات سایبری با حملاتی که از طریق ابزارهای سنتی جنگ انجام می‌شوند، متفاوت‌اند. زیرا در مورد اخیر، شناسایی مهاجم، اغلب چالش برانگیز نیست، چه‌رسد به اینکه بتوان ارتکاب حمله را به یک فرد به اندازه کافی عالی‌رتبه که قادر به انجام یک عمل تجاوزکارانه است، نسبت داد. در این خصوص، استدلال شده است که به‌عنوان یک مسئله آستانه‌ای^۲، درجه ناشناس بودن که توسط حملات سایبری ممکن می‌شود، توانایی شناسایی مجرم را برای اعطای مسئولیت کیفری به فرد از هر نوع، به چالش می‌کشد (Chaumette, 2018: 18; Tsagourias and Farrell, 2020: 941-967). به عبارت دیگر، در حالی که ردیابی یک حمله [سایبری] امکان‌پذیر است، بیشتر ردیابی‌ها به ISP ختم می‌شوند [...] و ردیابی بیشتر نیاز به همکاری ISP‌ها دارد (نوریان، ۱۳۹۵: ۴۴۱) و البته، برای اینکه مسئولیت یک عمل تجاوزکارانه به آن نسبت داده شود، یک حمله سایبری مبتنی بر هوش مصنوعی باید نه‌تنها به یک بازیگر (Ophardt, 2010: 10-11) در دستگاه دولت، بلکه به یک مقام عالی‌رتبه، مانند یک رهبر سیاسی یا نظامی نیز منتسب گردد (پیری، ۱۴۰۴: ۱۸۲). در این مورد، اتکای دولت‌ها به هکرهای قراردادی و یا سایر طرف‌های خارجی، با تقویت این موضوع با انتساب، نه‌تنها به یک دولت بلکه به یک رهبر خاص در درون دولت، مسئولیت تحت جرم تجاوز را به چالش می‌کشد (Greco, op. cit.: 44).

^۱. گفتنی است که در این مقاله کم‌بازدید در «فارین پالیسی آنالیتیکس»، دادستان دیوان، چارچوب قواعد ایجادشده توسط اساسنامه رم را برای رسیدگی به فعالیت‌های سایبری، بدون نیاز به ایجاد قواعد جدید، به اندازه کافی، گسترده و انعطاف‌پذیر می‌داند.

^۲. Gravity threshold

در خصوص مفهوم آستانه‌شدت در تجاوز سایبری، باید گفت هر زمان که وضعیت خاصی از سوی شورای امنیت به دادستان دیوان ارجاع شود یا دولت‌ها و یا به ابتکار خود دادستان قضیه‌ای شناسایی گردد، دادستان باید مبنای معقولی در تصمیم‌گیری در خصوص تعقیب یا عدم آن اتخاذ نماید. مرحله اول، براساس صلاحیت‌ها، و مرحله دوم، از حیث داشتن شدت کافی یا آستانه شدت براساس بند (د) ماده ۱۷ اساسنامه دیوان (اردبیلی و دیگران، پیشین: ۱۵۴۷).

هم‌چنین تعریف جرم تجاوز، مسئولیت کیفری فردی را در مورد حملات سایبری انجام‌شده توسط بازیگران غیردولتی که به یک‌دولت قابل‌انتساب نیستند، غیرممکن می‌کند (Buchan and Tsagourias, 2016: 377-381; Schmitt and Watts, 2016: 595-611). مطمئناً این‌آمر، مسئله‌ای منحصر به تجاوز سایبری نیست، زیرا حقوق کیفری بین‌الملل مدت‌هاست که با نحوه رسیدگی به جرایم بین‌المللی ارتکاب‌یافته توسط بازیگران غیردولتی، دست‌وپنجه نرم می‌کند (Acquaviva, 2011: Ch 13; Steer, 2011: Ch 19). پس، حملات سایبری، مسئله انتساب را تشدید می‌کنند، زیرا دولت‌ها بارها برای انجام عملیات سایبری خود به نهادهای ظاهراً غیردولتی متکی بوده‌اند. لذا تلاش‌ها برای پیگرد قانونی تجاوز سایبری در سطح بین‌کشورها، احتمالاً مسئله انتساب را به‌عنوان یک مسئله آستانه‌ای دربرمی‌گیرد.

برآورده کردن شرط (الزام) رهبری مندرج در بند (۱) ماده ۸ مکرر، ممکن است با تشکیل روزافزون بخش‌های تخصصی توسط کشورهای مختلف که وظیفه انجام عملیات سایبری، چه دفاعی و چه تهاجمی، را بر عهده‌دارند، کمتر اهمیت پیدا کند.^۱ در اینجا، محققان، رهبری را به «وظایف نظارتی یک مافوق مرتبط در چارچوب دکترین مسئولیت فرماندهی» تشبیه کرده‌اند (Ambos, op. cit.). طبق پرونده «بمبا گمبو»^۲ پاسخ مافوق به اقدامات نظامی یک زیردست می‌تواند فرمانده را در صورتی که «از رفتار مطلع بوده یا باید مطلع می‌بود» و «توانایی مادی برای جلوگیری یا سرکوب ارتکاب جرایم یا ارائه موضوع به مقامات جزء» را داشته باشد، در معرض مسئولیت قرار دهد.^۳ دستورالعمل تالین ۲/۰ به‌طور مشابه بیان می‌کند که مسئولیت کیفری برای فرماندهان و مافوق‌ها در زمینه جنایات جنگی وجود دارد که در آن «آنها می‌دانستند [...] یا باید می‌دانستند که زیردستانشان مرتکب جرم می‌شوند، در شرف ارتکاب آن هستند یا مرتکب شده‌اند» و «از انجام تمام اقدامات معقول

^۱. مثال نخست، مربوط است به استراتژی جامع سایبری وزارت جنگ (وزارت دفاع سابق) ایالات متحده و

واحد عملیاتی آن: U.S. Cyber Command (2024); and UK's National Security Cyber Center (2024).

^۲. بمبا گمبو، تبعه کنگو و فرمانده نظامی نیروهایی بود که به درخواست رییس‌جمهور وقت آفریقای مرکزی، از کنگو به سوی این کشور گسیل شدند و از اکتبر ۲۰۰۲ تا مارچ ۲۰۰۳ به سرکوب مخالفان رییس‌جمهور مذکور پرداختند.

^۳. Judgment of the Trial Chamber, Bemba Gombo (ICC-01/05-01/08-2170), 21 March 2016, §§ 170, 183.

و موجود برای جلوگیری از ارتکاب آنها یا مجازات مسئولان آن کوتاه‌ی کرده‌اند» (Schmitt, (op. cit.: 396-397(Rule 85).

بنابراین و به‌عنوان مسئله‌ای حائز اهمیت، مقاله حاضر این دیدگاه را اتخاذ می‌کند که مسئولیت جرم تجاوز می‌تواند، و در واقع باید، برای پاسخگو کردن رهبران سیاسی و نظامی یک کشور در جایی که فرمانبران ایشان برای ارتکاب عمل تجاوز علیه کشور دیگر به عملیات سایبری متکی هستند، در دسترس باشد. ضرورت اتخاذ این دیدگاه ممکن است به‌طور فزاینده‌ای اهمیت یابد، زیرا این پژوهش، در مورد در دسترس بودن جرم تجاوز برای مقابله با حملات سایبری انجام‌شده توسط بازیگران دولتی بحث می‌کند، در حالی که خطر ناشی از این حملات هم‌چنان به‌سرعت در حال گسترش است. هوش مصنوعی، در حال حاضر برای افزایش سرعت، دامنه و مقیاس تخریب ناشی از حملات سایبری استفاده می‌شود و این در حالی است که شناسایی، ردیابی و قطع این حملات را دشوارتر می‌کند (Greenberg, op. cit.: supra note 3) و همان‌طور که هوش مصنوعی، حملات سایبری را تأثیرگذارتر و قابل دسترس‌تر می‌نمایند^۱ با همان نسبت، انطباق آنها با عناصر مسئولیت کیفری بین‌المللی را دشوارتر می‌سازد.

گفتار دوم. تطبیق تجاوز سایبری مبتنی بر هوش مصنوعی با عناصر متعارف مسئولیت کیفری بین‌المللی

در این گفتار، مقاله نشان خواهد داد که حتی با فرض اینکه حمله سایبری با اثرات غیرجنبشی^۲ می‌تواند جرم تجاوز محسوب گردد، مسائل منحصر به فردی هنگام ارتکاب چنین اعمالی با استفاده از هوش مصنوعی ایجاد می‌شود.

هوش مصنوعی، چالش‌های بیشتری را در رابطه با الزامات عنصر مادی و عنصر معنوی ایجاد می‌کند. این مشکل در نوشتگان حقوقی مرتبط با مسئولیت کیفری بین‌المللی برای اعمالی که با (یا توسط؟) هوش مصنوعی انجام می‌شود با عنوان «شکاف مسئولیت»^۳

۱. از آنجا که موانع استفاده از هوش مصنوعی از نظر نیروی انسانی، مالی و سایر منابع، بسیار کمتر از دستگاه‌های نظامی سنتی است.

2. non-kinetic effects

3. responsibility gap

مورد بحث قرار گرفته است. این اصطلاح که ابتدائاً توسط «آندریاس ماتیاس» ابداع شد، به موارد زیر اشاره دارد:

«در این دسته روبرشد از اقدامات ماشینی، روش‌های سنتی انتساب مسئولیت با حس عدالت ما و چارچوب اخلاقی جامعه سازگار نیست، زیرا هیچ‌کس کنترل کافی بر اعمال ماشین ندارد تا بتواند مسئولیت آنها را بر عهده بگیرد. در زمینه استفاده از هوش مصنوعی برای ارتکاب جرم تجاوز سایبری [...] شکاف مسئولیت، ممکن است برای توصیف خلاء قانونی استفاده شود که طی آن هوش مصنوعی به اندازه کافی مسئول یک عمل باشد یا به اندازه کافی تصمیم‌به اقدام بگیرد تا تصمیم‌گیرنده انسانی را در قبال آسیب ایجادشده مسئول نداند» (Matthias, 2004: 180).

«ماتیاس» در بررسی چگونگی اعمال «شکاف مسئولیت» در مورد تجاوز ناشی از هوش مصنوعی، از نوشتگان حقوقی غنی‌تری که جنایات جنگی ناشی از هوش مصنوعی و در دسترس بودن آنها برای مسئولیت کیفری بین‌المللی را تجزیه و تحلیل می‌کند، راهنمایی می‌گیرد. در آنجا، محققان، چالش‌ها و محدودیت‌های اعمال عناصر موجود در جرایم بین‌المللی را مورد بحث قرار داده‌اند و راه‌حل‌های متنوعی را برای از بین بردن شکاف مسئولیت بالقوه بین جرایم جنگی مبتنی بر هوش مصنوعی و مسئولیت کیفری بین‌المللی ارائه داده‌اند. در عین حال، استدلال شده است که مسئله شکاف مسئولیت، به آن اندازه که در آثار حقوقی پیش‌بینی شده، شایع نیست و در واقع، این مسائل «فقط در برخی موقعیت‌ها، یعنی موقعیت‌هایی که نتیجه، محصول بی‌دقتی یا سوءنیت نیست، مطرح می‌شوند» (Königs, 2022: 4).

باری، ادامه این گفتار به تحلیل این موضوع خواهد پرداخت که چگونه عناصر مسئولیت کیفری بین‌المللی، ممکن است تحت تأثیر تفاوت‌های ظریف مربوط به استفاده از هوش مصنوعی در اقدامات مرتبط با تجاوز سایبری قرار گیرند، که نمونه دیگری از مفهوم «شکاف مسئولیت» را شکل می‌دهد.

الف. عنصر مادی

در ارزیابی عنصر مادی، با این سوال اساسی شروع می‌کنیم که چه کسی هنگام وقوع یک حمله سایبری مبتنی بر هوش مصنوعی، عامل است؟ به‌دیگر بیان، چه کسی (یا چه چیزی) را می‌توان مسئول آن آسیب دانست؟ به‌طور معمول، جرایم به یک عامل انسانی نیاز دارند،

همان‌طور که «سیستم‌های حقوق کیفری مدرن و مفاهیم مسئولیت کیفری، حول محور اعمال و ارادهٔ انسانی ساخته شده‌اند» (Gaeta, 2023: 1038). البته، از برخی جهات، شخصیت حقوقی به سایر عاملان،^۱ یعنی اشخاص حقوقی نیز تعمیم داده شده است، اما حتی در این شرایط، وقتی صحبت از مسئولیت کیفری می‌شود، کسانی که در رأس یک شخص حقوقی هستند، هم‌چنان به‌عنوان عامل مسئولیت کیفری برای آسیب‌های ناشی از سوءرفتار جدی شخص حقوقی در نظر گرفته می‌شوند (Press Release: Former CEO., 2018)؛ به این دلیل مهم که اسناد تقصیر به شخص حقوقی ناممکن است (اردیبه‌لی، ۱۴۰۳: ۱۵/۲). این رویکرد در حقوق کیفری بین‌المللی نیز منعکس شده است، آنجایی که کسانی که اعمال مجرمانهٔ یک دولت را هدایت می‌کنند، کسانی هستند که شخصاً مسئول شناخته می‌شوند (اساسنامهٔ دیوان بین‌المللی کیفری، مادهٔ ۸ مکرر).

بنابراین، هوش مصنوعی با ایجاد یک عامل دیگر، که به‌طور بالقوه جایگزین می‌شود و قادر به تصمیم‌گیری مستقل^۲ است، این ساختار متعارف را که زیربنای حقوق جزا و مسئولیت کیفری است مخدوش می‌کند (Ex-Google Officer Finally., 2023). این امر باعث شده است که برخی اندیشمندان، گسترش شخصیت حقوقی به سیستم‌های هوش مصنوعی را ممکن بدانند و در نتیجه، آنها را قادر و مشمول عاملان مسئول کیفری قلمداد کنند (Lagioia and Sartor, 2020: 433).

با این حال، دیدگاه اخیر، اغلب رد می‌شود. زیرا سیستم‌های هوش مصنوعی فاقد جنبه‌های حیاتی شخصیت هستند که عملی را منجر به تحقق مسئولیت کیفری می‌کند. از این گذشته، مسئولیت کیفری حتی درجایی که رفتار یک انسان غیرارادی باشد،^۳ منتسب نمی‌شود. زیرا این امر، مختصات و کیفیات اساسی مدنظر برای یک عمل مجرمانه را که محصول ارادهٔ آزاد خود انسان، و بنابراین، آگاهی است تضعیف می‌کند (Moore, 2010: 115). سیستم‌های هوش مصنوعی، به‌عنوان یک فناوری برنامه‌ریزی شده تلقی می‌شوند و فاقد این درجه از خودمختاری هستند که به فرد اجازه می‌دهد استدلال کند

^۱. actors

^۲. و شاید حتی قادر به فکر و احساس، به گفته برخی از تأثیرگذارترین سازندگان هوش مصنوعی.

^۳. به‌عنوان مثال، جایی که متهم در هنگام خواب‌گردی، یا در حالت مستی غیرارادی مرتکب جرم شده است.

که برنامه‌نویسان یا کاربران انسانی هم‌چنان بازیگران واقعی در پس‌پردهٔ یک جرم مبتنی بر هوش مصنوعی هستند و به عبارت بهتر، عدم پیش‌بینی‌پذیری در چگونگی دستیابی هوش مصنوعی به اهداف مندرج در گد خود، «تجلی‌ای از کنش هوشمندانه» نیست (Gaeta, op. cit.: 1040). بنابراین، اگرچه در برخی از تکرارهای آینده، سیستم‌های هوش مصنوعی ممکن است به درجه‌ای از استقلال واقعی لازم برای در نظرگرفتن عاملان دارای مسئولیت کیفری دست یابند، اما نمی‌توان آنها را در وضعیت فعلی‌شان چنین در نظر گرفت (Lina, 2018: 682).

پس به‌عنوان تحلیل بیشتر، این‌مقاله با این‌دیدگاه موافق است که سیستم‌های هوش مصنوعی را نمی‌توان در حال حاضر به عنوان عاملان دارای مسئولیت کیفری در نظر گرفت. بنابراین، درجایی که قوانین بین‌المللی توسط یک سیستم هوش مصنوعی نقض می‌شود، می‌توان به‌طور دقیق‌تر گفت که «صرفاً» با استفاده از یک سیستم هوش مصنوعی نقض شده است. بنابراین، این سؤال باقی می‌ماند که آیا تصمیم‌گیرندهٔ انسانی آن سوی هوش مصنوعی، شامل توسعه‌دهنده، برنامه‌نویس، کاربر و غیره، می‌تواند به‌عنوان «عامل» در راستای تحقق مسئولیت کیفری در نظر گرفته شود یا خیر؟ پاسخ به این پرسش نیز نامشخص است. برای این منظور، بهتر است از سامانه‌های تسلیحاتی خودمختار هوشمند^۱ مبتنی بر هوش مصنوعی صحبت کرد.

در خصوص اعمال انجام‌شده توسط سیستم‌های تسلیحاتی خودمختار^۲ باید گفت که «این سیستم‌های تسلیحاتی پس از فعال شدن، بدون نظارت یا کنترل کاربر، در انجام وظایف و کارکردهای محوله خود عمل می‌کنند یا می‌توانند عمل کنند [...] با توجه به ویژگی‌های خاص الگوریتم‌ها، مبتنی بر روش‌های خودآموزی، نحوهٔ انجام وظایف و کارکردهای محوله توسط سیستم نمی‌تواند به‌طور کامل توسط برنامه‌نویس یا کاربر پیش‌بینی شود. این سامانه‌ها با خطری بالایی که از غیرقابل‌پیش‌بینی بودن در اجرای کارکردهای حیاتی در

1. intelligent AWS

۲. سیستم‌های هوشمندی که برای هدف‌گیری، یعنی تشخیص و ردیابی و تعامل با هدف، تعریف شده‌اند و پس از فعال شدن می‌توانند بدون دخالت انسان، اهداف را انتخاب و با آنها درگیر شوند. این تسلیحات با عنوان ربات قاتل نیز شناخته می‌شوند.

چرخه هدف‌گیری از خود نشان می‌دهند، می‌توانند بی‌هدف باشند و به همین دلیل توسط حقوق بین‌الملل بشردوستانه ممنوع شده‌اند» (Gaeta, op. cit.: 1034). بنابراین، «با توجه به غیرقابل‌پیش‌بینی بودن ذاتی نحوه انجام عملکرد و وظیفه محوله توسط این سیستم»، این امر «عدم امکان واگذاری مسئولیت به برنامه‌نویس یا کاربر» را در پی دارد (Ibid: 1035). بیان این نکته لازم است که این شق از مقوله انتساب، با آنچه در بالا مورد بحث قرار گرفت، متفاوت است. در آنجا، مسئله انتساب، بر چالش شناسایی مرتکب جرایم سایبری به دلیل ناشناس بودن عامل آن متمرکز بود، لکن در اینجا، هویت عامل انسانی اولیه، قابل‌شناسایی است اما سوال این است که سیستم‌های مورد بحث، تا چه اندازه خودمختار در نظر گرفته می‌شوند تا بر مبنای آن، قانون بتواند شرایط مورد نیاز برای فاعل اصلی جرم را به آن تصمیم‌گیرنده انسانی نسبت دهد؟

باری، محققان در این باره اتفاق نظر ندارند که در نظر گرفتن انسان در پس یک سیستم هوش مصنوعی به عنوان عامل مرتبط برای اهداف مسئولیت، ممکن است چالش‌برانگیز باشد. بلکه برعکس، استدلال شده است که حفظ استقلال و غیرقابل‌پیش‌بینی بودن^۱ یک سیستم هوش مصنوعی، به معنای عدم مسئولیت برنامه‌نویس آن نیست و بنابراین، اقدامات یا غفلت‌های تصمیم‌گیرندگان انسانی آن سوی سیستم‌های هوش مصنوعی، ممکن است به عنوان عاملان مرتبط برای مسئولیت در نظر گرفته شود (Königs, op. cit.: 4).

پژوهش حاضر با این دیدگاه موافق است و یافتن برنامه‌نویس در واحد سایبری ارتش یک کشور به عنوان عاملی در پس آسیب‌های ناشی از یک حمله سایبری مبتنی بر هوش مصنوعی را که با استفاده از گد‌های وی انجام می‌شود بدون مشکل می‌داند. این دیدگاه توسط فلسفه حقوقی‌ای که زیربنای مفهوم عمل مجرمانه در حقوق جزای مدرن است و نیز توسط منافع سیاسی در معرض خطر در ادامه عملکرد حقوق کیفری بین‌الملل در مواجهه با پیشرفت‌های تکنولوژیکی در درگیری‌های بین کشورها پشتیبانی می‌شود. درباره مورد نخست، منصفانه است که توسعه‌دهنده، برنامه‌نویس یا کاربر انسانی

1. autonomy and unpredictability

در پس یک سیستم هوش مصنوعی را تحت یک نظریه نمایندگی، مشابه آنچه که از آن طریق، رهبران سیاسی یا نظامی مسئول اعمال زبردستان خود شناخته می‌شوند، مسئول بدانیم (اساسنامه دیوان بین‌المللی کیفری، بند (۱) ماده ۸ مکرر). در خصوص مورد دوم، حقوق کیفری بین‌الملل تمایل دارد تا از اینکه کاربران انسانی پشت‌پرده سیستم‌های هوش مصنوعی به خودی خود نتوانند عامل اصلی یک جرم بین‌المللی محسوب شوند، جلوگیری کند و در نتیجه، رفتار مجرمانه را بدون مرتکب باقی نگذارد.

از باب تأکید، هم‌چنان که پیشتر بحث شد، جنایت تجاوز شامل این شرط است که «یک رهبر سیاسی یا نظامی» در برنامه‌ریزی، آماده‌سازی، شروع یا اجرای آن دخیل باشد. هرچند توسط برخی نویسندگان، بحث مفصلی در مورد شرایطی که ممکن است الزام رهبری برای یک عمل تجاوز سایبری لحاظ شود، ارائه شده است (Ambos, op. cit.: 498-499) اما کافی است بگوییم که نسخه‌های مختلف این تحلیل‌ها معمولاً به سؤالات مربوط به «کنترل»، به‌ویژه در مفهوم نظامی، می‌پردازند. بنابراین، یک رهبر سیاسی یا نظامی که قادر به کنترل ارتکاب یک حمله سایبری است، احتمالاً می‌تواند به‌عنوان عامل در پس‌پرده یک تجاوز سایبری در نظر گرفته شود.^۱

در ادامه این تحلیل، پژوهش حاضر، بر این فرض استوار است که «عنصر مادی» توسط عامل انسانی که مسبب استفاده از یک سیستم هوش مصنوعی در ارتکاب یک جرم بین‌المللی است، محقق گردد. لذا به «عنصر معنوی» پرداخته می‌شود.

ب. عنصر معنوی

عنصر معنوی تمام جنایات عمدی در صلاحیت دیوان، در ماده ۳۰ اساسنامه دیوان بین‌المللی کیفری تبیین شده است. این ماده به‌مثابه قاعده‌ای عمومی است و در مورد تمام جنایات در صلاحیت دیوان، به‌استثنای مواردی که به غیرعمد بودن آنها تصریح شده،

۱. مفهوم اعمال کنترل بر جنایت، بر این‌اندیشه استوار است که فاعلان اصلی یک جنایت، فقط کسانی نیستند که عناصر عینی جرم را مادماً مرتکب می‌شوند، بلکه کسانی هم که با وجود بُعد مسافت و دوری از صحنه جنایت آن را کنترل و یا ارتکاب آن را هدایت می‌کنند، فاعلان اصلی به‌شمار می‌روند چون درباره وقوع جنایت و نحوه ارتکاب آن تصمیم می‌گیرند (اردبیلی، ۱۳۹۷: ۶۵۸).

اعمال می‌شود (قیاسی و محترم‌قلاتی، پیشین: ۱۵۶). در حالی که ماده ۳۰ اساسنامه، مستلزم قصد و آگاهی مرتکب، اعم از خاص یا عام است،^۱ مسئله اصلی در خصوص پرسش این مقاله، آن است که با توجه به ماده مذکور، آیا مسئول دانستن عامل انسانی در پس‌پرده یک سیستم هوش مصنوعی، در جایی که این عامل انسانی صرفاً آگاه است که رفتار مجرمانه می‌تواند رخ دهد یا حتی رخ خواهد داد، غیرممکن می‌شود؟

ظاهراً اساسنامه رم، قادر به پرداختن به جنایات بین‌المللی ناشی از هوش مصنوعی که حالات روانی آنها در ماده ۳۰ تعریف شده، نیست زیرا «الزام اینکه رفتار ممنوعه عمداً انجام شود [...] به نظر می‌رسد آشکال ریسک‌پذیری مسئولیت کیفری را مستثنی می‌کند» (Bo, 284: 2021). به بیان دیگر، در حالی که برخی نظریات برای گنجاندن مفاهیمی مانند ریسک‌پذیری آگاهانه^۲ یا بی‌پروایی در عنصر معنوی جرایم بین‌المللی وجود دارد، «دیدگاه پیشرو در رویه اولیه دیوان بین‌المللی کیفری، اتخاذ تفسیری محدودکننده است» (Trahan, op. cit.: 1150). این حمایت از تفسیر مضیق، در حکم «بمبا گمبو» یافت می‌شود و بعداً در حکم تجدیدنظر «توماس لوبانگا دیلو»^۳ تأکید شد که مطابق آن، «معیار پیش‌بینی‌پذیری رویدادها، قریب‌به یقین (تقریباً قطعی بودن) است».^۴

استفاده عمدی دولت‌ها از حملات سایبری، سابقه متقنی در انتشار تأثیر آنها فراتر از هدف موردنظر یا حتی پیش‌بینی شده، یا ایجاد آسیب‌هایی که به‌طور خاص توسط مرتکب مشخص نشده‌اند دارد. بر این مبنا، عنصر معنوی موردنیاز برای جنایت تجاوز، ناهماهنگی قابل توجهی بین حملات سایبری که رنگ‌وبوی یک عمل تجاوزکارانه دارند، با قابلیت انتساب مسئولیت کیفری بین‌المللی به آن عاملان ایجاد می‌کند.

۱. در این‌بخش از مقاله، سند عناصر جرایم (ICC, Elements of Crimes, U.N. Doc.) نیز علاوه بر اساسنامه رم، مورد ملاحظه قرار گرفته‌است. PCNICC/2000/1/Add.2

2. conscious risk-taking

۳. لوبانگا، تبعه کنگو و رهبر گروه نظامی اتحادیه میهن‌پرستان کنگو بود که در دادگاه بین‌المللی کیفری به اتهامات جنایت جنگی و به‌کارگیری کودکان زیرپانزده‌سال در مخاصمات مسلحانه محاکمه گردید.

۴. «the standard for the foreseeability of events is virtual certainty». Judgment, Lubanga (ICC-01/04-01/06-3121), Appeals Chamber, 1 December 2014, § 447.

این استفاده (یا سوءاستفاده) عمدی از عملیات سایبری برای انجام حمله علیه یک هدف تقریباً غیرقطعی، دو نوع مشکل تعریف‌محور را از نظر آثار حملات ایجاد می‌کند: یکی مربوط به هویت و دیگری مربوط به قلمرو جغرافیایی. در مورد هویت، حمله سایبری ممکن است برای افراد یا نهادهای خاصی در کشور هدف در نظر گرفته شده باشد اما به دلیل اتصال یکپارچه شبکه‌های رایانه‌ای می‌تواند به راحتی به اهداف ناخواسته دیگری منتقل شود (Bo, op. cit.: 278).^۱ در مورد جغرافیا، اتصال شبکه‌های رایانه‌ای به هیچ وجه مرزهای ملی را رعایت نمی‌کند. به این معنی که یک حمله سایبری که برای یک کشور در نظر گرفته شده است، می‌تواند شامل حمله به کشورهای دیگر، تقریباً به طور همزمان نیز باشد. هر دوی این مشکلات، در حمله بدافزار WannaCry (به شرح مقدمه این مقاله) به نمایش گذاشته شدند؛ حمله‌ای که عمدتاً قربانیان آن شامل اهداف ناخواسته‌ای مانند وزارت کشور روسیه و چندین شرکت جهانی بودند (Ghafur et al., 2017: 1-7). هدف کلی حمله، قلمرو چندین کشور در سراسر جهان بود اما تعیین هدف خاص اینکه کدام کشورها و با چه ظرفیتی مورد حمله قرار گیرند، به خود بدافزار واگذار شد.

این مسئله با آنچه که در مقالات علمی تحت عنوان «اثر جعبه سیاه هوش مصنوعی»^۲ توصیف می‌شود، پیچیده تر می‌گردد. این اثر می‌گوید که ابهام کُد هوش مصنوعی، به معنی توضیح اینکه چرا هوش مصنوعی به شیوه‌ای خاص رفتار کرده است، چه به عنوان محصول نقص در کُد آن، نقص در فرآیند توسعه یا آسیب عمدی از سوی کاربر انسانی، آسان نیست (Wendehorst, 2020: 152). این امر، آگاهی از وضعیت روانی مجرم در مورد یک حمله سایبری خاص، در این خصوص که حمله تا چه اندازه طبق برنامه انجام شده است، یا اینکه هوش مصنوعی در مورد مقیاس آسیب یا وضعیت تحت تأثیر، آزادی‌های اخلاقانه‌ای داشته است یا خیر را دچار ابهام می‌کند. بنابراین، با توجه به ضرورت اثبات قصد و آگاهی

۱. «یو»، با بحث در زمینه سلاح‌های خودکار مورد استفاده برای ارتکاب جنایات جنگی، این مشکل را به عنوان «خلاء ناشی از عدم جرم‌انگاری حملاتی که عمداً علیه غیرنظامیان انجام نمی‌شوند، اما در عوض از تمایز بین اهداف قانونی و غیرقانونی کوتاهی می‌کنند، جایی که خطری در مورد احتمال حمله به غیرنظامیان در نظر گرفته می‌شود»، توصیف می‌کند.

2. black box effect of AI

مرتکب (به شرح ماده ۳۰ اساسنامه رم) هوش مصنوعی رویکردهای واجد این حالات روانی را مختل می‌کند.

و باز هم تأکید می‌شود که انتساب مسئولیت در جنایت تجاوز، مستلزم آن است که جرم به یک رهبر نظامی یا سیاسی مربوط شود. در اینجا، یک رهبر سیاسی یا نظامی، ممکن است استدلال نماید که به دلیل عدم درک فنی از ماهیت پیچیده حمله سایبری، نمی‌تواند سوءنیت لازم برای عمل تجاوز سایبری را داشته باشد. البته محققان توافق کرده‌اند که این دفاع برای ایشان کافی نیست تا از مسئولیت کیفری تحت ماده ۸ مکرر شانه‌خالی کنند. همانطور که استدلال شده است شخصی که در موقعیتی است که می‌تواند دستور انجام دادن یک عمل تجاوزکارانه را صادر کند و به‌طور مؤثر برنامه تجاوز را کنترل نماید، نیازی به دانستن جزئیات فنی عملکرد ابزارهای به‌کاررفته برای اجرای دستور خود ندارد و کافی است که بداند که دستور او اجرا خواهد شد و عواقب مضرّی برای افراد یا اشیاء مورد هدف ایجاد خواهد کرد (Kai Ambos, op. cit.: 503-504).

در زمینه مسئولیت فرمانده برای جنایات جنگی، دستورالعمل تالین ۲/۰ نیز این دیدگاه را تقویت می‌کند که پیچیدگی فنی ابزارهای عمل مجرمانه، سپری برای مسئولیت قلمداد نمی‌شود (Schmitt, op. cit.: 399).

گفتار سوم. تطبیق‌ها و راه‌حل‌های پیشنهادی

گروهی از محققان حقوق بین‌الملل کیفری، روش‌هایی را برای پرداختن به «شکاف مسئولیت» در مورد مسئولیت ناشی از آسیب‌های هوش مصنوعی پیشنهاد کرده‌اند. این بخش از پژوهش، برخی از این موارد را مورد بحث قرار می‌دهد (الف) و النهایه، راه حل بالقوه خود را مطرح می‌کند (ب).

الف. پیشنهادهایی از نوشتگان حقوقی موضوع

محققانی که به دنبال پرداختن به «شکاف مسئولیت» هستند، تمایل دارند بر عنصر روانی جرایم بین‌المللی تمرکز کنند. نخستین گروه از محققان، حالات روانی خفیف‌تر، از جمله بی‌پروایی را به عنوان جایگزین مناسب‌تری مطرح می‌کنند. به عنوان مثال، در مواردی که از یک سیستم هوش مصنوعی برای ایجاد نقض‌های ناخواسته قواعد حقوق بین‌الملل

بشردوستانه استفاده می‌شود (Bo, op. cit.: 275) حتی با اشاره به قصد خاص در جایی که هنوز صرف آسیب عمومی مدنظر است. باید توجه داد که این مقاله برخی از این پیشنهادها را به‌عنوان استدلال در نظر می‌گیرد و بدان می‌پردازد، زیرا همان‌طور که شرح آن گذشت، بسیاری از نویسندگان به صراحت اتفاق نظر دارند که حالات روانی خفیف‌تر، مانند بی‌پروایی و غیره، عامدانه از اساسنامه رم مستثنی شده‌اند. لذا با این رویکرد، این بخش از مقاله، پیشنهادهای صاحبان نظری را بررسی می‌کند که حتی بسا سهواً، با قرائت سخت‌گیرانه ماده ۳۰ اساسنامه رم مخالف هستند.

«مارتا بو»، با بحث در زمینه استفاده از سیستم‌های تسلیحاتی خودمختار در ارتکاب جنایات جنگی، استدلال می‌کند که جایی برای تفسیر الزام عنصر روانی برای جنایت جنگی حمله به غیرنظامیان در اساسنامه رم وجود دارد تا شامل اشکالی از ریسک‌پذیری رفتار مجرمانه مانند بی‌پروایی شود. این تفسیر، انتساب مسئولیت کیفری برای حملات کورکورانه، در جایی که اپراتور انسانی که از سیستم‌های تسلیحاتی خودمختار استفاده یا آنها را مستقر می‌کند، خطر هدایت حملات علیه افراد یا اشیاء مصون از حمله را پیش‌بینی می‌کند و با وجود این، تصمیم به ادامه حمله می‌گیرد امکان‌پذیر می‌سازد (Ibid.: 278-279). او همچنین اظهار می‌دارد که این امر، قابل‌تصور و نیز امکان‌پذیر است و استدلال می‌کند در حالی که بی‌پروایی در ماده ۳۰ اساسنامه دادگاه بین‌المللی کیفری گنجانده نشده است، اما به دلیل ابهام موجود در بند (۲)(b) این ماده در مورد اینکه آیا سطح آگاهی موردنیاز، این است که یک «پیامد»^۱ قطعاً رخ خواهد داد (خواستن نتیجه) یا اینکه پیامد احتمال دارد یا ممکن است در جریان عادی وقایع و در پی رخدادهای معمول واقع شود، می‌توان ادعا کرد که بی‌پروایی وجود دارد. (Ibid.: 286)

مورد اخیر ممکن است راه را برای لحاظ بی‌پروایی به‌عنوان عنصر معنوی باز بگذارد. البته ایرادهای «کونیگز» به مقوله شکاف مسئولیت، به در دسترس بودن بی‌پروایی یا سهل‌انگاری^۲ به‌عنوان حالات ذهنی موجود برای مسئول دانستن سازنده، برنامه‌نویس،

1. consequence

2. negligence

اپراتور و غیره در جایی که سوءرفتاری مضرّ از یک سیستم هوش مصنوعی رخ می‌دهد، بستگی دارد (6). (Königs, op. cit. : 6).

به‌هر ترتیب و با لحاظ آنچه که مورد بحث قرار گرفت، مسئله در مورد امکان لحاظ بی‌پروایی به‌عنوان وجهی از عنصر معنوی جنایت موضوع این مقاله هم‌چنان پابرجاست. پذیرفتن نظر دوم نیز مستلزم آن است که عامل بتواند خطر را درک کند اما به‌سادگی بدان بی‌اعتنا باشد یا آن را نادیده بگیرد (115 : Fletcher, 1998). با توجه به اینکه مبرهن است استعداد و توانایی هوش مصنوعی برای تجزیه و تحلیل داده‌ها، هدف‌گیری و سایر تصمیمات، در حال حاضر بسیار فراتر از توانایی‌های انسانی‌ست، توانایی عامل انسانی برای درک یک خطر مشخص در رفتار هوش مصنوعی، به گونه‌ای که بتوان آن را مصداق بی‌پروایی دانست، جای سوال است!

هم‌چنین شایان ذکر است که عنصر معنوی سهل‌انگاری کیفری،^۱ ممکن است در شرایطی که از سیستم‌های هوش مصنوعی برای ارتکاب تجاوز استفاده می‌شود، از بین برود. سهل‌انگاری کیفری، مستلزم نقض شدید وظیفه مراقبت معقول فرد است، اما در مواردی که هوش مصنوعی به‌طور غیرقابل پیش‌بینی عمل کرده باشد، این امر ممکن است سطوح مناسب مراقبت انجام‌شده را مختل کند. یک رژیم سهل‌انگاری کیفری تلاش می‌کند تا عاملانی را که نتوانسته‌اند خطر قابل پیش‌بینی را درک کنند و به‌عنوان یک فرد معقول عمل کرده تا از بروز چنین خطراتی جلوگیری شود، مجازات کند (American Law Institute, 2017, § 2.02(2)(d); Baron, 2020 : 86).

همگی این خواسته‌ها ممکن است برآورده شوند و یک سیستم هوش مصنوعی به‌گونه‌ای عمل نماید که نتیجه‌ای را ایجاد کند که مستلزم مسئولیت باشد. این امر به‌ویژه در زمینه جنایت تجاوز جالب توجه است، زیرا در اینجا عنصر معنوی باید به آستانه خاصی برسد تا به‌عنوان نقض آشکار^۲ منشور سازمان ملل در نظر گرفته شود و در نتیجه، ماده ۸ مکرر از نقض کند. در واقع، اعمال مداخله‌ای سطح پایین‌تر در یک کشور خارجی، به‌عنوان اعمال

3. criminal negligence

2. manifest violation

ممنوعه بین‌المللی مانند حمله مسلحانه تلقی نشده‌اند (Schmitt, op. cit. : 334). به عبارت دیگر «با رعایت قاعده حداقلی، [عملیات سایبری] که صرفاً باعث تشویش خاطر یا تحریک می‌شوند، هرگز [به عنوان توسل به زور] تلقی نمی‌شوند» (Ibid : 328-356).

در نمونه‌های موجود از بیانیه‌های هنجار سایبری، کشورها تمایل دارند توافق کنند که مداخله سایبری سطح پایین، نقض اصول حقوقی بین‌المللی محسوب نمی‌شود. برای مثال، موضع استرالیا این است که اگر یک فعالیت سایبری، به آستانه یک حمله جنبشی، تحت حقوق بین‌الملل بشردوستانه برسد، قوانین حاکم بر چنین حملاتی در طول درگیری‌های مسلحانه، بر آن نوع فعالیت‌های سایبری اعمال خواهد شد.^۱ هم‌چنین موضع کاستاریکا این است که در فضای دیجیتال، عبور از آستانه استفاده از زور، نه به ابزارهای دیجیتال به کار رفته، بلکه به آثار عملیات سایبری بستگی دارد و عملیات سایبری انجام شده توسط یک دولت علیه دولت دیگر، در صورتی که آثار آن مشابه آثار ناشی از استفاده از سلاح‌های متعارف باشد، ممنوعیت استفاده از زور را نقض می‌کند.^۲

بنابراین، در جایی که مداخله سطح پایین‌تر با استفاده از هوش مصنوعی، در نظر گرفته شده و یا انجام شده باشد، اما آسیب در مقیاس بزرگ‌تری وارد شود، عامل احتمالاً مراقبت لازم برای مسئول قلمداد شدن تحت‌استاندارد سهل‌انگاری کیفری را نخواهد داشت. در جایی که یک عامل می‌تواند مراقبت لازم را ابراز کند و نتیجه، هم‌چنان خسارات گسترده‌ای را در یک کشور خارجی ایجاد کند، همان «شکاف مسئولیت» در مسئولیت کیفری بین‌المللی حاصل می‌شود.

«آکواویوا» استدلال می‌کند که ممکن است حقوق بین‌الملل کیفری، ارتباط بالقوه بین کنترل تحت حقوق بین‌الملل کیفری (که همان ارتباط علی ضروری‌ای است که مسئولیت کیفری را ایجاد می‌کند) و کنترل معنادار انسانی در چارچوب حقوق بین‌الملل بشردوستانه (یعنی میزان دخالت انسانی که برای اطمینان از مجاز بودن یک فرد به

1. available online at : https://cyberlaw.ccdcoe.org/wiki/National_position_of_Australia (2020)

2. available online at : https://docs-library.unoda.org/Costa_Rica's_Position_on_the_Application_of_International_Law_in_Cyberspace (2021).

استفاده از سیستم‌های تسلیحاتی خودکار توسط حقوق بین‌الملل بشردوستانه کافی تلقی می‌شود) را بررسی کند (Acquaviva, 2023 : 1003). در واقع وی، به تشریح چارچوبی برای خطای انسانی، مشابه بی‌پروایی، می‌پردازد و چنین پیشنهاد می‌دهد که شاید راه حل استفاده از سیستم‌های تسلیحاتی خودکار، از درک واقعی این گزاره شروع شود که وقتی از برخی ساختارها سود می‌بریم،^۱ مجبور به پذیرش این نتیجه هستیم که وقتی این ساختارها باعث آسیبی می‌شوند که مستقیماً قصد آن را نداشته‌ایم، اما وجود این آن را همراه با نفع موردانتظار پذیرفته‌ایم، پس مسئول هستیم (Ibid : 1002).

«گریپل»، با روی برگرداندن از پیامدهای ناخواسته استفاده از سیستم‌های هوش مصنوعی، استدلال می‌کند که سیستم‌های هوش مصنوعی ناگزیر با هدف «ارتکاب یا تسهیل» جنایات جنگی و سایر «تهدیدات مخرب علیه اهداف دنیای واقعی» مورد استفاده قرار خواهند گرفت (Greipl, op. cit.: 1098). در مواردی که این رفتار عمدی منجر به آسیب پیش‌بینی‌نشده یا به‌طور خاص، آسیب به یک هدف ناخواسته شود، «گریپل» استدلال می‌کند که دکترین شَر انتقال‌یافته^۲ در حقوق جزای داخلی، می‌تواند راه‌حلی برای شکاف مسئولیت ناشی از آن ارائه دهد (Ibid : 1099).

ملاحظه می‌شود راه‌حل‌های زیادی برای پُرکردن شکاف مسئولیتی که برای حملات مبتنی بر هوش مصنوعی وجود دارد، به‌ویژه در مورد جنایات جنگی، پیشنهاد شده است، اما هم‌چنان اقدامات مرتبط با تجاوز سایبری، این راه‌حل‌ها را مختل می‌کند. به‌هر روی مقاله حاضر، گزینه دیگری را با دو پیش‌فرض ارائه می‌دهد. اولاً اینکه، مقالات پیشتر مورد بحث، دقت زیادی به خرج دادند تا نشان دهند که چگونه تفسیرهای پیشنهادی‌شان، به‌ویژه در مورد عنصر روانی، به‌طور عملی در لسان موجود اساسنامه رم و رویه قضایی دیوان بین‌المللی کیفری به‌کار گرفته شده‌اند، موضوعی که مقاله حاضر عمدتاً به این دلیل که اثبات آن ممکن نیست، چنین تلاشی نمی‌کند. ثانیاً، این مقاله استدلال می‌کند از آنجا که مسئولیت کیفری مدرن تا به امروز بر این پیش‌فرض بنا شده است که عامل متفکر موجود برای مسئولیت، انسان است، ورود هوش مصنوعی به این معادله، مستلزم تفکر خلاقانه‌ای

۱. هوش مصنوعی و سامانه‌های تسلیحاتی خودکار، ساختارهایی قابل مشاهده و ملموس هستند.

2. transferred intent

است که توسط ساختار قوانین موجود محدود نشود، یعنی قوانینی که زمانی نوشته شده‌اند که آن پیش‌فرض، کاملاً درست و موجه بوده‌است. براین اساس، این سوال مطرح است که در خصوص پرسش تحقیق، کدام‌یک از آستانه‌های موجود برای مسئولیت، هنگام بررسی از میان مجموعه‌ای نامحدود از گزینه‌ها و راه‌حل‌ها می‌تواند بهتر اعمال شود؟ به‌عنوان پیشنهاد خود: مسئولیت مطلق.

ب. جایگزین دیگر: مسئولیت مطلق

دکترین مسئولیت مطلق، نوعی مسئولیت بدون تقصیر (اردبیلی، ۱۴۰۴: ۷۸)، بیان می‌کند که مسئولیت می‌تواند از یک عمل آسیب‌زا ناشی شود، صرف‌نظر از سوءنیت یا تقصیر خاص عامل. در یک رژیم سهل‌انگاری استاندارد، عناصر موردنیاز شامل اثبات وظیفه مراقبت عامل، نقض وظیفه مذکور و اثبات اینکه این نقض باعث آسیب خاصی شده‌است، می‌باشد. مسئولیت مطلق، الزام به اثبات نقض وظیفه را از این زنجیره حذف می‌کند و در عوض، فقط مستلزم آن است که نشان داده شود عامل، رفتار مرتبیطی را انجام داده و این رفتار باعث آسیب موردنظر شده‌است.

از منظر سیاست‌گذاری، مسئولیت مطلق به این‌گزاره اشاره دارد که قانون برای فعالیت‌های ذاتاً خطرناک، به این موضوع که فرد تاچه‌اندازه وظیفه مراقبت خود را در انجام برخی اعمال رعایت می‌کند، توجهی ندارد و لذا درجایی که این اعمال انجام می‌شوند و آسیبی که مشخصه آن اعمال است حادث می‌شود، عامل [حمله] صرف‌نظر از سطح مراقبتش، مسئول آن آسیب است (Wendehorst, op. cit.: 159). این رویکرد برای حملات سایبری مبتنی بر هوش مصنوعی مناسب است که بدون تردید به دلیل غیرقابل پیش‌بینی بودن و غیرقابل مهاربودنشان که باعث می‌شود آسیب‌هایی فراتر از محدوده، حتی هدف موردنظر و به‌همان اندازه غیرقانونی وارد کنند، ذاتاً خطرناک به‌شمار می‌روند. این حملات نه مرزهای حاکمیتی را رعایت می‌کنند و نه شبکه‌های رایانه‌ای را که هدف قرار می‌دهند. این واقعیتی است که توسط کسانی که اقدام به استقرار آنها می‌کنند و تصمیم می‌گیرند دامنه و سرعت آثار خود را با هوش مصنوعی افزایش دهند، به‌خوبی شناخته شده‌است.

مسئولیت مطلق، علاوه بر اینکه در مورد یک فعالیت منحصرأً خطرناک مناسب است، در مواردی که به طور معمول اثبات عناصر سهل‌انگاری بسیار دشوار است نیز مفید خواهد بود تا به آنجا که نگرانی‌ای جدی در مورد عدم اجرای کامل قانون ایجاد می‌کند و «هم‌چنین می‌تواند پاسخی مناسب باشد در جایی که اثبات چنین عناصری برای قربانی بسیار دشوار باشد، به طوری که الزام به چنین اثباتی منجر به ناکارآمدی شود» (Ibid : 159-160). این ممیزه، با نمونه‌های موجود از حملات سایبری بزرگ و تحت حمایت دولت، مانند حملهٔ NotPetya سازگار است (Greenberg, op. cit.: note 3).

همان‌طور که در گزارش مربوط به آن آمده است: حتی بیش از یک‌سال پس از گسترش فاجعه‌بار این حمله، هنوز کارشناسان امنیت سایبری در مورد اسرار NotPetya بحث می‌کنند. نیت واقعی هکرها چه بود؟ کارکنان شرکت امنیتی ISSP در کی‌یف [...] معتقدند که این حمله نه‌تنها برای تخریب، بلکه به‌عنوان تلاشی برای پاکسازی در نظر گرفته شده بود. از این گذشته، هک‌هایی که ابتدا آن را راه‌اندازی کردند ماه‌ها دسترسی نامحدود به شبکه‌های قربانیان داشتند. علاوه بر وحشت و اختلالی که ایجاد کرد، NotPetya ممکن است شواهد جاسوسی یا حتی شناسایی برای خرابکاری‌های آینده را نیز از بین برده باشد (Ibid).

این نگرانی‌های دوگانه، یعنی خطر منحصر به فرد و ذاتی در به‌کارگیری هوش مصنوعی برای دخالت و یا آسیب‌رساندن به یک کشور خارجی، و چالش اثبات این سوءرفتار هنگامی که از طریق یک حملهٔ سایبری مبتنی بر هوش مصنوعی انجام می‌شود، مسئولیت مطلق را به یک راه‌حل جذاب برای شکاف مسئولیتی ایجاد شده در رابطه با تجاوز سایبری مبتنی بر هوش مصنوعی تبدیل می‌کند.

این رویکرد، معیار مسئولیت استفاده از هوش مصنوعی را در ارتکاب تجاوز سایبری - آنچه که حقوق بین‌الملل کیفری به پیشگیری از آن علاقه دارد - بسیار حداقلی تعیین می‌کند و هدف تشویق به عدم استفاده از هوش مصنوعی در این زمینه را پیش می‌برد. البته با این پیش‌فرض که اجتناب از استفاده از هوش مصنوعی در ارتکاب اعمال مرتبط با تجاوز سایبری، نتیجهٔ مطلوبی است.

در اینجا نکته‌ای کلیدی وجود دارد. اینکه زمینه تجاوز سایبری با زمینه سیستم‌های تسلیحاتی خودمختار در تضاد است. برخی معتقدند که استفاده از هوش مصنوعی در اجرای فعالیت‌های نظامی مزایای ویژه‌ای دارد. برای مثال، مطالعات (Galliot and Wyatt, 2020: 25) نشان داده‌اند که بخش‌های دفاع ملی، سامانه‌های تسلیحاتی خودکار را به‌عنوان ابزاری برای کاهش آسیب پرسنل و هم‌چنین غیرنظامیان، کاهش هزینه‌ها و آسیب‌های زیست‌محیطی و درعین‌حال افزایش قابلیت‌های نظامی می‌دانند.^۱ اما در زمینه جنایت تجاوز، این تعادل بین آسیب‌ها و مزایا قابل‌اعمال نیست. مشارکت در رفتاری که منجر به جرم تجاوز می‌شود، آن چیزی است که قانون علاقه‌افری به منع آن دارد، زیرا هیچ شرایطی وجود ندارد که آن رفتار طبق حقوق بین‌الملل، عملی موجه تلقی گردد. به این ترتیب، هیچ نگرانی درمورد کم‌اثر یا ناکارآمد کردن عملی که فی‌نفسه غیرقابل توجیه است وجود ندارد. این امر به‌ویژه با توجه به آنچه که در حال حاضر درمورد تأثیر هوش مصنوعی بر درگیری‌های بین‌کشورها می‌دانیم صادق است؛ اینکه اهداف بیشتری را با سرعت بیشتر تخریب می‌کند، دامنه حمله را گسترش می‌دهد و در نتیجه، باعث آسیب بیشتر و افزایش تلفات می‌شود. بنابراین، یک رژیم مسئولیت مطلق که منجر به تخفیف این نتایج گردد، یک مزیت محسوب می‌شود.

این سوال عملی باقی می‌ماند که دقیقاً چه زمانی یک عمل تجاوزکارانه که از هوش مصنوعی استفاده می‌کند، وارد قلمرو مسئولیت مطلق می‌شود؟ به‌ویژه با ادغام بیشتر هوش مصنوعی در زندگی روزمره و گنجاندن آن در ابزارهای فناورانه، این سوال قابل توجه است.

برای رسیدن به پاسخی دقیق، تحقیقات بیشتری لازم است، اما این مقاله پیشنهاد می‌کند که در مواردی که میزان استفاده از هوش مصنوعی منجر به حمله‌ای فوق‌العاده خطرناک می‌شود، مسئولیت مطلق اعمال گردد. با وام‌گرفتن از قانون مسئولیت مدنی ایالات متحده (U.S. Restatement., 2025)، این امر می‌تواند مستلزم آن باشد که دادگاه، موارد زیر را در نظر بگیرد: (۱) خطر اینکه آسیب ناشی از حمله زیاد باشد، (۲) ناتوانی متهم در

۱. بحث درمورد اینکه آیا یک رژیم مسئولیت سختگیرانه برای سایر جنایات بین‌المللی، یعنی جنایات جنگی که با هوش مصنوعی انجام می‌شود، منطقی‌ست یا خیر، فراتر از محدوده این مقاله است.

از بین بردن خطر از طریق اعمال مراقبت معقول و (۳) میزانی که فعالیت مورد نظر، امری رایج و مرسوم نیست. در مواردی که نقش هوش مصنوعی در یک حمله منجر به این شود که میزان آسیب ایجاد شده به‌طور قابل توجهی بیشتر از آن چیزی باشد که بدون استفاده از هوش مصنوعی ممکن بود، یا در مواردی که استفاده از هوش مصنوعی، حمله را از توانایی متهم برای مهار آن خارج کرده باشد نیز این امر باعث ایجاد مسئولیت مطلق می‌شود.

نتیجه‌گیری

در این پژوهش، بررسی کردیم که چگونه حملات سایبری مبتنی بر هوش مصنوعی ممکن است به‌عنوان یک عمل تجاوزکارانه در نظر گرفته شوند. سپس به بررسی موانعی که بر سر راه مسئولیت کیفری بین‌المللی ناشی از این رفتار وجود دارد پرداختیم. در این راستا، اینکه تا چه حد می‌توان یک عمل تجاوزکارانه انجام شده توسط یک سیستم هوش مصنوعی را به‌عنوان فعل مجرمانه در نظر گرفت، جای سوال است.

چالش برانگیزتر از آن، ناسازگاری تجاوز سایبری با عنصر روانی مسئولیت کیفری در پرتو ماده ۳۰ اساسنامه دیوان بین‌المللی کیفری است. از آنجایی که عنصر روانی جرم تجاوز، ترکیبی از قصد و آگاهی است، بسیاری از صاحب‌نظران استدلال می‌کنند که قابل انطباق با حملات سایبری مبتنی بر هوش مصنوعی نیست. در پاسخ، دیگر محققان، حالات روانی خفیف‌تر نظیر بی‌پروایی را پیشنهاد کرده‌اند که به‌طور عملی‌تری، حالت روانی یک عامل را که با تکیه بر هوش مصنوعی حمله سایبری انجام می‌دهد به تصویر می‌کشد.

علاوه بر راه‌حل‌های موجود در آثار حقوقدانان بین‌المللی کیفری، این مقاله با پیشنهاد یک سیستم مسئولیت مطلق برای اعمال تجاوز سایبری انجام شده با هوش مصنوعی، یک گام فراتر رفت. این امر چالش فنی شناسایی وضعیت روانی عامل انسانی (در فرض کنش‌گری انسان) را با توجه به غیرقابل پیش‌بینی بودن و ابهام هوش مصنوعی برطرف می‌کند. هم‌زمان، این امر به نفع سیاست‌گذاری‌ای است که حملات سایبری مبتنی بر هوش مصنوعی به کشورهای خارجی را به‌عنوان فعالیت ذاتاً خطرناک که فی‌نفسه مسئولیت‌کاربر انسانی را به همراه دارد، در نظر می‌گیرد. هم‌چنین این پیشنهاد ممکن است باعث کاهش انگیزه استفاده از هوش مصنوعی در ارتکاب تجاوز سایبری، به‌عنوان رفتاری همواره نامطلوب گردد.

اگرچه پیشنهاد کاربردی این پژوهش، با محدودیت‌ها و چشم‌اندازهای موهومی در موقع اعمال همراه است و این مقاله تلاش نمود تا موانع مفهومی را از گزینه‌های مرسوم دور کند، زیرا هوش مصنوعی، درک رایج از نقش انسان‌ها در اعمال غیرقانونی بین‌المللی را مختل نموده است، اما از برآیند آنچه شرح داده شد این نتیجه به دست می‌آید که عناصر مسئولیت کیفری یک عمل تجاوزکارانه به شرح اساسنامه دیوان بین‌المللی کیفری، در ساختار و تفسیر فعلی خود، ظرفیت لازم را برای تطبیق با تجاوز سایبری انجام‌شده از طریق سیستم‌های مبتنی بر هوش مصنوعی تحت حمایت دولت ندارند.

به عبارت دیگر، هر چند موضوع صلاحیت دیوان بین‌المللی کیفری، در حال گسترش است و نه کاهش و اساسنامه دیوان نیز آماده اصلاح، تغییر، توسعه، تعریف و بازتعریف جرایم جدید و آینده است و این امر به صراحت در سند تأسیس دیوان منظور شده است (Morris, 598: 2002) و صرف نظر از ابهام در مورد عنصر مادی و سخت‌گیری درباره عنصر معنوی (با لحاظ برخی نظریات که بیان می‌دارد باید عنصر معنوی تجاوز سایبری را به دلیل پیچیدگی مرتبط با ضریب خطر، تقلیل داد که البته این اظهار، در تعارض با اصول قانونی بودن و تفسیر مضیق مندرج در ماده ۲۲(۲) اساسنامه رم قرار دارد، به شرحی که در مقاله گذشت)، این امکان وجود دارد که میان تعقیب حمله سایبری مبتنی بر هوش مصنوعی تحت عنوان تجاوز، با دکتین صلاحیت دیوان بین‌المللی کیفری در تعقیب اشخاص حقیقی (مندرج در ماده ۲۵ اساسنامه رم) نیز ناسازگاری‌های مفهومی پدید آید. هم‌چنین حمله سایبری، صرف نظر از خشونت نهفته در آن که از بسیاری جهات می‌تواند مورد بررسی و تحلیل قرار گیرد (مهر و کارگری، ۱۴۰۱: ۶۸۱-۷۰۱) غالباً نه از رهگذر فعلی معین، که در نتیجه نقش‌آفرینی مجموعه‌ای از عوامل حادث می‌شود و در نتیجه، وظیفه دادستان در اثبات مجرمیت متهم از طریق جمع‌آوری ادله و احراز رابطه سببیت میان فعل ارتكابی و خسارت‌وارده بسیار دشوار خواهد بود.

و اینکه در نهایت، توسل به سازکار عدالت کیفری بین‌المللی، باید به عنوان هسته سخت و آخرین راه حل در مواجهه با نقض ممنوعیت‌های پذیرفته‌شده باشد، به خصوص به دلیل قوانین سایبری متناسب، واجد اثر و کاربردی در حقوق داخلی، که مانع از بی‌کیفری متجاوزان سایبری است و دامنه مسئولیت در نتیجه این مقررات، بسط پیدا می‌کند (نوریان، ۱۳۹۶: ۲۷-۳۰).

فهرست منابع

فارسی

- ۱- ابوذری، مهرانوش، (۱۴۰۲) حقوق و هوش مصنوعی، تهران: نشر میزان، چاپ سوم.
- ۲- اردبیلی، محمدعلی، علیرضا محقق‌هرچگان، ابراهیم بیگزاده و محمدعلی مهدوی‌ثابت، (۱۴۰۳) «حقوق بین‌الملل سایبری و توسعه صلاحیت دیوان کیفری بین‌المللی (با تأکید بر مذاکرات تالین ۲۰۱۷ میلادی)»، مطالعات حقوق عمومی، ۵۳، ۳ (۱۴۰۲)، ۱۵۳۷-۱۵۵۹.
- ۳- اردبیلی، محمدعلی، حقوق جزای عمومی، جلد نخست، تهران: نشر میزان، ویراست پنجم، چاپ هفتاد و چهارم.
- ۴- اردبیلی، محمدعلی، (۱۴۰۳) حقوق جزای عمومی، جلد دوم، تهران: نشر میزان، ویراست ششم، چاپ شصت و پنجم.
- ۵- اردبیلی، محمدعلی، (۱۳۹۷) «دیوان کیفری بین‌المللی و نظریه کنترل بر جنایت»، دایرةالمعارف علوم جنایی، کتاب سوم (علوم جنایی حقوقی)، تهران: نشر میزان، ۶۷۳-۶۵۵.
- ۶- اردبیلی، محمدعلی، (۱۴۰۱)، مسئولیت کیفری، تهران: پژوهشکده حقوقی شهردانش.
- ۷- پیبری، حیدر، (۱۴۰۱)، «مسئولیت بین‌المللی دولت‌ها در ارتباط با کاربست سلاح‌های مبتنی بر هوش مصنوعی در درگیری‌های مسلحانه»، حقوق فناوری‌های نوین، ۶، ۱۲، ۱۶۹-۱۹۳.
- ۸- قیاسی، جلال‌الدین و ایمان محترم‌قلاتی، (۱۳۹۳)، «تحلیل عنصر محور رکن معنوی جنایات عمدی در صلاحیت دیوان کیفری بین‌المللی»، پژوهش حقوق کیفری، ۶، ۲۱، ۱۵۵-۱۹۶.
- ۹- مهرا، نسرین و نوروز کارگری، «روانشناسی مرتکبان اقدامات تروریستی»، در حقوق کیفری پویا (مجموعه مقاله‌ها در پاسداشت استاد دکتر محمدعلی اردبیلی)، ۶۸۱-۷۰۱، به کوشش نسرین مهرا و امیرحسن نیازپور، تهران: بنیاد حقوقی میزان، ۱۴۰۱.
- ۱۰- نوریان، علیرضا، آیین دادرسی جرایم رایانه‌ای و مخابراتی، تهران: نشر میزان، ۱۳۹۶.
- ۱۱- نوریان، علیرضا، «مستندسازی ادله الکترونیکی در تحقیقات پیش‌دادرسی کیفری از نگاه رویه قضایی»، در مجموعه مقالات اولین همایش ملی رویارویی با جرایم سایبری؛ چالش‌ها و راهکارها، جلد اول، تهران: دانشگاه علوم انتظامی امین، ۱۳۹۵، ۴۳۸-۴۵۲.

انگلیسی

- 1- Acquaviva, Guido, "Crimes without Humanity? Artificial Intelligence, Meaningful Human Control, and International Criminal Law", *Journal of International Criminal Justice*, vol.21, 2023, 981-1004.
- 2- . Acquaviva, Guido, "Non-State Actors from the Perspective of International Criminal Tribunals", in Jean D'Aspremont, Math Noortmann and W. Michael Reisman (eds), *Participants in the International Legal System*, London : Routledge, 2011.
- 3- . American Law Institute, *Model Penal Code and Commentaries*, Philadelphia, 2017.
- 4- . Ambos, kai, "Individual Criminal Responsibility for Cyber Aggression", *Journal of Conflict & Security Law*, vol.21, n 3, 2016, 495-504.
- 5- . Ambos, Kai, "General Principles of Criminal Law in the Rome Statute", *Criminal Law Forum*, vol.10, 1999, 1-32.
- 6- . Baron, Marcia, "Negligence, Mens Rea, and What We Want the Element of Mens Rea to Provide", *Criminal Law and Philosophy*, vol.14, n¹, 2020, 69-89.
- 7- . Bo, Marta, "Autonomous Weapons and the Responsibility Gap in the Light of the Mens Rea of War Crime of Attacking Civilians in the ICC Statute", *Journal of International Criminal Justice*, vol.19, n 2, 2021, 275-299.
- 8- . Buchan, Russell and Nicholas Tsaourias, "Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence", *Journal of Conflict & Security Law*, vol.21, n 3, 2016, 377-381.
- 9- . Cassese, Antonio, "On Some Problematical Aspects of the Crime of Aggression", *Leiden Journal of International Law*, vol.20, n 4, 2007, 841-849.
- 10- . Chaumette, Anne-Laure, "International Criminal Responsibility of Individuals in Case of Cyberattacks", *International Criminal Law Review*, vol.18, n¹, 2018, 1-35.

- 11- . Clark, Roger S., "The Mental Element in International Criminal Law : The Rome Statute of the International Criminal Court and the Elements of Offences", Criminal Law Forum, vol.12, 2001, 291-334.
- 12- . Eser, Albin, "Mental Elements-Mistake of Fact and Mistake of Law", in Antonio Cassese, Paola Gaeta and John R.W.D. Jones (eds), The Rome Statute of the International Criminal Court: A Commentary, vol.1, Oxford University Press, 2002.
- 13- . Fletcher, George P., Basic Concepts of Criminal Law, Oxford University Press, 1998.
- 14- . Gaeta, Paola, "Who Acts When Autonomous Weapons Strike? The Act Requirement for Individual Criminal Responsibility and State Responsibility", Journal of International Criminal Justice, vol.21, n 5, 2023, 1033-1055.
- 15- . Galliot, Jai and Austin Wyatt, "Risks and Benefits of Autonomous Weapon Systems : Perceptions among Future Australian Defence Force Officers", Journal of Indo-Pacific Affairs, vol.3, 2020, 17-34.
- 16- . Ghafur Shayer, Søren Rud Kristensen, Kate Honeyford, Greg Martin, Ara Drazi and Paul Aylin, "A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS", Nature partner journals, vol.98, 2019, 1-7.
- 17- . Greco, Gianpiero, "Cyberattacks as Aggression Crimes in Cyberspace in the Context of International Criminal Law", European Journal of Political Science Studies, vol.4, n 1, 2020, 40-47.
- 18- . Greipl, Anna Rosalie, "Data-Driven Learning Systems and the Commission of International Crimes: Concerns for Criminal Responsibility?", Journal of International Criminal Justice, vol.21, n 5, 2023, 1097-1118.
- 19- . Hajdin, Nikola R., "The Actus Reus of the Crime of Aggression", Leiden Journal of International Law, vol.34, 2021, 489-504.
- 20- . Königs, Peter, "Artificial Intelligence and Responsibility Haps: What is the Problem?", 24 Ethics and Information Technology, vol.24, n 36, 2022, 1-11.

- 21- . Kreß, Claus, “On the Activation of ICC Jurisdiction over the Crime of Aggression”, *Journal of International Criminal Justice*, vol.16, 2018, 1-17.
- 22- . Lagioia, Francesca and Giovanni Sartor, “AI Systems under Criminal Law: A Legal Analysis and a Regulatory Perspective”, *Philosophy & Technology*, vol.33, 2020, 433-465.
- 23- . Lina, Dafni, “Could AI Agents Be Held Criminally Liable: Artificial Intelligence and the Challenges for Criminal Law”, *South Carolina Law Review*, vol.69, n 3, 2018, 677-696.
- 24- . Morris, Madeline, “The Democratic Dilemma of the International Criminal Court”, *Buffalo Criminal Law Review*, vol.5, 2002, 591-600.
- 25- . Matthias, Andreas, “The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata”, *Ethics and Information Technology*, vol.6, 2004, 175-183.
- 26- . Moore, Michael S., *Act and Crime: The Philosophy of Action and its Implications for Criminal Law*, Oxford University Press, 2010.
- 27- . Ophardt, Jonathan A., “Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow’s Battlefield”, *Duke Law & Technology Review*, vol.9, n 3, 2010, 1-27.
- 28- . Porro, Sara, *Risk and Mental Element: An Analysis of National and International Law on Core Crimes*, DPhil Thesis, University of Hamburg, 2014.
- 29- . Schmitt, Michael N. and Sean Watts, “Beyond State-Centrism: International Law and Non-State Actors in Cyberspace”, *Journal of Conflict & Security Law*, vol.21, n 3, 2016, 595-611.
- 30- . Schmitt, Michael N., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2 ed., Cambridge University Press, 2017.
- 31- . Steer, Cassandra, “Non-State Actors in International Criminal Law”, in Jean D’Aspremont, Math Noortmann and W. Michael Reisman (eds), *Participants in the International Legal System*, London: Routledge, 2011.

- 32- . Trahan, Jennifer, "The Criminalization of Cyber-Operations Under the Rome Statute", *Journal of International Criminal Justice*, vol.19, n°5, 2021, 1133-1164.
- 33- . Tsgourias, Nicholas and Michael Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges", *European Journal of International Law*, vol.31, n 3, 2020, 941-967.
- 34- . Tsilonis, Victor P., *The Jurisdiction of the International Criminal Court*, Cham: Springer, 2 ed., 2024.
- 35- . Weissbrodt, David, "Cyber-Conflict, Cyber-Crime, and Cyber-Espionage", *Minnesota Journal of International Law*, vol.22, 2013, 347-387.
- 36- . Wendehorst, Christiane, "Strict Liability for AI and other Emerging Technologies", *Journal of European Tort Law*, vol.11, n 2, 2020, 150-180.

أسناد و دعاوی

- 37- . Office of the Prosecutor, *Strategic Plan 2016-2018* (2015), §§ 63, 65.
- 38- . Office of the Prosecutor, *Strategic Plan 2023-2025* (2023), § 57.
- 39- . ICC-01/05-01/08-424, 15 June 2009, § 368.
- 40- . ICC-01/04-01/06-2842, 14 March 2012, § 1011.
- 41- . ICC-01/04-01/06-3121, 1 December 2014, § 447.
- 42- . ICC-01/05-01/08-2170, 21 March 2016, §§ 170, 183.
- 43- . ICC, *Elements of Crimes*, U.N. Doc. PCNICC/2000/1/Add.2
- 44- . SC Res. 573, 4 October 1985.
- 45- . SC Res. 577, 6 December 1985.
- 46- . UN General Assembly Resolution 3314,
- 47- . United States of America et al. V. Goering et al, *International Military Tribunal*, 30 September to 1 October 1946.

منابع اینترنتی

- 48- . Burges, Matt, "Here Come the AI Worms", WIRED, 1 March 2024,
- 49- available online at: www.wired.com/story/here-come-the-ai-worms (visited 27 March 2024).
- 50- . Carpenter, Chris and Duncan B. Hollis, "A Victim's Perspective on International Law in Cyberspace", Lawfare, 28 August 2023,
- 51- available online at: www.lawfaremedia.org/article/a-victim-s-perspective-on-international-law-in-cyberspace (visited 6 March 2024).
- 52- . Davis, Joshua, "Hackers Take Down the Most Wired Country in Europe", WIRED, 21 August 2007,
- 53- available online at: www.wired.com/politics/security/magazine/15-09/ff_estonia (visited 6 March 2024).
- 54- . "Ex-Google Officer Finally Speaks Out on The Dangers Of AI! -Mo Gawdat", Diary of a CEO, Episode 252, 1 June 2023,
- 55- available online at: www.youtube.com/watch?v=bk-nQ7HF6k4 (visited 22 March 2024).
- 56- . Greenberg, Andy, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", WIRED, 22 August 2018,
- 57- available online at: www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world (visited 13 March 2024).
- 58- . K.A.A. Khan KC, "Technology Will Not Exceed Our Humanity", Foreign Policy, 20 August 2023,
- 59- available online
- 60- at: <https://digital.frontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/> (visited 21 November 2024).
- 61- . NATO Secretary General Jens Stoltenberg at the NATO Cyber Defense Pledge Conference in Italy, 10 November 2022,
- 62- available online
- 63- at: www.nato.int/cps/en/natohq/opinions_208925.htm (visited 27 November 2024).

- 64- . “Press Release : Former CEO of Volkswagen AG Charged with Conspiracy and Wire Fraud in Diesel Emissions Scandal”, U.S. Department of Justice, 3 May 2018,
- 65- available online at: www.justice.gov/opa/pr/former-ceo-volkswagen-ag-charged-conspiracy-and-wire-fraud-diesel-emissions-scandal (visited 16 October 2024).
- 66- . “Statement by ICC Prosecutor Karim A.A. Khan KC on conference addressing cyber-enabled crimes through the Rome Statute system, International Criminal Court”, 22 January 2024,
- 67- available online at: www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through (visited 21 November 2024);
- 68- . UK’s National Security Cyber Center (NSCC), “What We Do”,
- 69- available online at: www.ncsc.gov.uk/section/about-ncsc/what-we-do (visited 20 November 2024)
- 70- . U.S. Cyber Command (USCYBERCOM), “Our Vision and Mission”,
- 71- available online at: www.cybercom.mil/About/Mission-and-Vision (visited 20 November 2024)
- 72- . “What was the WannaCry ransomware attack?”, Cloudflare,
- 73- available online
- 74- at: www.cloudflare.com/learning/security/ransomware/wannacry-ransomware (visited 15 April 2024).
- 75- . Zetter, Kim, “Logic Bomb Set Off South Korea Cyberattack”, WIRED, 21 March 2013,
- 76- available online at: www.wired.com/2013/03/logic-bomb-south-korea-attack (visited 6 March 2024);
- 77- . Zewe, Adam, “Explained : Generative AI”, MIT News, 9 November 2023,
- 78- available online at: <https://news.mit.edu/2023/explained-generative-ai-1109> (visited 11 March 2024).