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

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

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

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.

آیندهٔ جرایم بین‌المللی؛ امکان‌سنجی تطبیق جرم تجاوز به‌منظور مقابله با هوش مصنوعی

محمدعلی اردبیلی
استاد دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران (نویسنده مسئول)
m-ardebili@sbu.ac.ir

علیرضا نوریان
دکترای حقوق کیفری و جرم شناسی دانشگاه عدالت، تهارن، ایران
noorian@rocketmail.com

دوفصلنامه تحقیق و توسعه در حقوق کیفری و جرم‌شناسی
پژوهشکده حقوق و قانون ایران

دوره۲| 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 هوش‌مصنوعی برای پیشبرد اهداف مضرّ دولتی، این سوال را مطرح می‌کند که آیا دادگاه بین‌المللی کیفری آماده است تا با حملات سایبری مبتنی‌بر هوش‌مصنوعی که توسط و علیه دولت‌ها انجام می‌شود، مقابله کند؟ یا اینکه رفتار از طریق هوش‌مصنوعی، خطرِ افتادن در یک خلأ قانونی را به‌همراه دارد و بازیگران انسانی را که دستور استفاده از آن را داده‌اند از مسئولیت مصون می‌دارد؟ این مقاله در پاسخ، با طرح و تشریح گفتمانِ «شکافِ مسئولیت»، به تحلیل چگونگی تأثیر هوش‌مصنوعی بر عناصر اساسی جرایم بین‌المللی، یعنی الزامات عناصر مادّی و معنوی از منظر اساسنامهٔ دادگاه بین‌المللی کیفری می پردازد و به‌طور خاص، با بررسی مفهوم تجاوز سایبری که اخیراً در نوشتگان حقوقی مورد توجه قرار گرفته‌است، اثربخشی متن فعلی اساسنامهٔ دیوان و تفاسیر مرتبط‌با آن را در تعیین مسئولیت‌کیفری بین‌المللی در مواردی که هوش‌مصنوعی باعث تجاوز سایبری می‌شود، بررسی می‌نماید. این‌مقاله طیفی را بررسی می‌کند که در و آن اَعمال بالقوهٔ

تجاوز سایبری، ممکن است به فعالیت انسانی تقلیل‌داده‌شوند بنابراین، مسئولیت‌کیفری به مربّی انسانیِ هوش‌مصنوعی منتقل می‌شود؛ در مقابلِ حالتی‌که عمل ارتکابی شاید بیش‌از حدّ از مداخلهٔ انسانی دور است تا مسئولیت‌کیفری را تحت وضعیت روانیِ عامل انسانیِ دارای‌تقصیر توجیه کند. برای ورود به چنین‌بحثی، مقاله با مروری مختصر بر جرم تجاوز آغاز می شود و با معرفی مفهوم نوظهور تجاوز سایبری ادامه‌می‌یابد. سپس، چالش‌های اِعمال تجاوز مبتنی‌بر هوش‌مصنوعی برای عناصر متعارف مسئولیت کیفری بین‌المللی بررسی می‌شود. در ادامه، راه‌حل‌های مطرح‌شده 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 سایبریِ انجام‌شده از طریق سیستم‌های هوش‌مصنوعیِ تحت‌حمایت 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، هوش‌مصنوعی، تجاوز سایبری، مسئولیت کیفری، شکاف مسئولیت

مقدمه

در سال۲۰۱۷، گروه لازاروس،[۱] حملهٔ بدافزارِ WannaCry را انجام‌داد که از نوعی ویروس‌کامپیوتری به‌نام کِرم‌رمزنگاری‌شده برای آلوده‌کردن صدهاهزار کامپیوتر در بیش‌از ۱۵۰کشور استفاده‌کرد و تقریباً چهارمیلیارد دلار ضرر در سطح‌جهانی به‌بارآورد و صنایع‌مختلف، از مخابرات گرفته تا مراقبت‌های پزشکی اورژانسی را مختل‌کرد (What was the WannaCry., 2024).

در همان‌سال، گروه هکری روسی به‌نام Sandworm نیز از بدافزار مبتنی‌بر هوش‌مصنوعی برای انجام حملهٔ سایبری NotPetya استفاده‌کرد. کُد مورد استفاده برای این‌حمله، به‌طور خودکار، سریع و بدون تبعیضِ اهداف پخش‌شد و درمجموع ده‌میلیارد دلار خسارت به‌بار آورد زیرا داده‌های شرکت‌های چندملّیتی، شرکت‌های‌دولتی و مراکز اصلی برای حمل‌ونقل گرفته تا مراقبت‌های بهداشتی را از بین بُرد (Greenberg, 2018). به گفتهٔ کارشناسان، این‌حمله «تقریباً با هر تعریفی، یک جنگ سایبری بود. جنگی‌که احتمالاً حتی‌از آنچه سازندگان آن در نظرداشتند، انفجاری‌تر بود» (Ibid). درحالی‌که اوکراین به‌عنوان هدف این‌حمله در نظر گرفته‌شده‌بود، امّا این‌بدافزار به‌سرعت در دیگر شبکه‌های رایانه‌ای پخش‌شد و میلیاردها دلار خسارت در سراسر جهان، از بیمارستان‌های پنسیلوانیا (ایالات‌متحده) گرفته تا یک کارخانهٔ شکلات‌سازی در تاسمانی (استرالیا) ایجاد کرد (Ibid).

همان‌طور که این‌مثال‌ها نشان می‌دهند قابلیت‌های سایبری می‌توانند ابزارهای قدرتمندی باشند که در یک حمله به کار گرفته می‌شوند، از جمله ازطریق تلاش‌های تحت‌حمایت دولت یا به سفارش نهادهای خصوصی. علاوه‌براین، همانطور که در ادامه موردبحث قرارخواهدگرفت، نشانه‌های فزاینده‌ای وجود دارد که حملات سایبری تحت‌حمایت دولت، ممکن‌است طبق حقوق بین‌الملل، اقدامات تجاوزکارانه محسوب‌شوند.

چنین‌حملاتی پیش‌از این، محققان حقوق بین‌الملل، دولت‌ها و متخصصان را به‌طور یکسان آسیمه کرده بود و اکنون نیز به‌نظر می‌رسد پیشرفت مداوم فنّاوری، ما را از یافتن پاسخ دورتر می‌کند، نَه نزدیک‌تر. با گسترش سریع هوش‌مصنوعی که به‌طور فزاینده‌ای پیچیده و در دسترس قرار می گیرد، تعیین اینکه سوءرفتار انسانی در پسِ یک

[۱]. یک گروه مخفی از مجرمان سایبری که توسط دولت کرهٔشمالی اداره می‌شود.

حملهٔ‌سایبری به‌کجا ختم می‌شود و رفتار خودِ هوش‌مصنوعی از کجا آغاز می‌شود، به‌طور هم‌زمان چالش‌برانگیزتر خواهدشد. اخیراً در فوریه۲۰۲۴، محققان دریافته‌اند که هوش‌مصنوعیِ مولد[1] می‌تواند برای اجرای حملات سایبری با استفاده‌از کرم‌های رمزنگاشته ، همان‌نوع بدافزاری را که مسئول حمله WannaCry بود مورداستفاده قرار دهد (Burges, 2024). مطالعهٔ آنها پیش‌بینی کرد که این‌نوع کرم‌های رمزنگاشته ، طی دو تا سه‌سال آینده مهارناشدنی خواهندبود (Ibid). این‌تحولات به‌این‌معنی است که حملات سایبری به‌طور فزاینده‌ای خود-توانمند و غیرقابل‌پیش‌بینی بوده و مقاومت در برابر آنها دشوار خواهد شد. هم‌زمان، کشورها نیز درحال سرمایه‌گذاری منابع و نیروی‌انسانی 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 استولتنبرگ»[2]، دبیرکل سابق ناتو، در سخنرانی خود در کنفرانس تعهد دفاع سایبری ناتو در سال۲۰۲۲ بیان‌داشت «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 هوش‌مصنوعی برای پیشبرد اهداف مضرّ دولتی، این سوال را مطرح می‌کند که آیا دادگاه بین‌المللی کیفری آماده است تا با حملات سایبری مبتنی‌بر هوش‌مصنوعی که توسط و علیه دولت‌ها انجام می‌شود، مقابله کند؟ آیا رفتار هوش‌مصنوعی، خطرِ افتادن در یک خلأ قانونی را به‌همراه دارد و از مسئولیت بازیگران انسانی که دستور استفاده از آن را داده‌اند، محافظت می‌کند؟ در همین‌راستا، چگونه ممکن‌است حقوق بین‌الملل، نهادها و دست‌اندرکاران آن برای تعامل بهتر با آینده‌ای که در آن انسان‌ها لزوماً بازیگران اصلی پشتیبانِ (سوء)رفتار دولت‌ها نیستند، سازگار شوند؟

پرداختن‌به این‌نگرانی‌ها مهم است زیرا به توانایی مسئولیت‌کیفری بین‌المللی در رسیدگی‌به نقض‌های شدید صلح‌وامنیت بین‌المللی مربوط می‌شود و تعیین می‌کند که آیا جرایم بین‌المللی، به شکلی که درحال‌حاضر نوشته شده‌اند، ممکن است جرایم سایبری

---

۱. در حالی‌که تعاریف زیادی وجود دارد، در اینجا منظور از هوش‌مصنوعی مولّد، یک مدل یادگیری ماشینی است که برای ایجاد داده‌های جدید آموزش دیده‌است، نَه اینکه در مورد یک مجموعه دادهٔ خاص پیش‌بینی کند. یک سیستم هوش‌مصنوعی مولّد، سیستمی‌است که یاد می‌گیرد اشیاء بیشتری تولید کند که شبیه داده‌هایی هستند که براساس آنها آموزش دیده‌است (Zewe, 2023).

2. Jens Stoltenberg

قابل‌توجهی را دربَرگیرند یا خیر؟ اگر مجموعه‌ای از حملات بین‌المللی سایبری بتوانند از صلاحیت کیفری بین‌المللی فرار کنند، این‌اَمر کیفیت عدالتی را که دیوان بین‌المللی کیفری می‌تواند یا باید بتواند برای جرایم بین‌المللیِ معاصر ارائه دهد، به‌خطر می‌اندازد. برعکس، پرداختن مستقیم به این مسائل می‌تواند «به هم‌سو نمودن کار دیوان بین‌المللی کیفری با یکی از چالش‌های جدیدتر پیشِ‌روی جامعهٔ بین‌المللی در قرن بیست‌ویکم کمک کند و بدین‌ترتیب، اهمیت دیوان را به‌شیوه‌ای که قبلاً تصور نمی‌شد، مجدداً تأیید کند» (Tarhan, 2021 : 1134).

این‌مقاله با هدف پرداختن‌به این پرسش‌ها، به جرم بین‌المللی تجاوز به‌عنوان یک مطالعهٔ موردی[1] تکیه می‌کند تا نشان دهد چگونه قابلیت‌های هوش‌مصنوعی ممکن‌است ارزیابی مجددِ عناصر اساسی جرایم بین‌المللی، یعنی الزامات عنصر مادّی و عنصر معنوی جرم را ضروری سازد. این‌مقاله به‌طور خاص با بررسی مفهوم «تجاوز سایبری»، به بررسی اثربخشی متن و تفسیر فعلی اساسنامهٔ دیوان بین‌المللی کیفری در تطبیق مسئولیت‌کیفری بین‌المللی در مواردی که هوش‌مصنوعی باعثِ تجاوز سایبری می‌شود، می‌پردازد. در انجام این کار، مقاله به‌دنبال پاسخ به این‌سوال است که آیا می‌توان «رهبران»[2] را در چارچوب جرم تجاوز سایبری به‌خاطر اقدامات هوش‌مصنوعی پاسخگو دانست؟

لازم‌به‌ذکراست که هرچند این‌تحقیق از دیگر شاخه‌های حقوق بین‌الملل برای ارائه پیشینه‌ای در مورد تأثیر هوش‌مصنوعی بر حقوق کیفری بین‌المللی بهره می‌برَد، لکن بحث در این‌مقاله، از دو جهتِ کلیدی با آنچه در آثار حقوق بین‌الملل بشردوستانه در مورد «سیستم‌های سلاح‌های خودمختار کشنده»[3] رایج‌شده‌است، متمایز می‌باشد. نخست اینکه، معیار بررسی و تجزیه و تحلیل در این‌مقاله، مسئولیت کیفری بین‌المللی است که علی‌رغم هم‌پوشانی در برخی زمینه‌ها با حقوق بین‌الملل بشردوستانه، یک نهاد حقوقی

---

۱. به‌این‌سبب، جنایت تجاوز به‌عنوان مطالعهٔ موردی انتخاب شده‌است که برخلاف دیگر جرایم بین‌المللی، ارکان یک عمل تجاوز غیرقانونی، معمولاً گسسته‌تر و بنابراین قابلِ جداسازی‌تر از سایر جرایم بین‌المللی است و این‌اَمر، بحث درمورد تأثیر هوش‌مصنوعی بر هر عنصرِ جرم را ساده‌تر می‌کند. این در حالی‌است‌که 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.

3. Lethal Autonomous Weapon Systems

مجزا با عناصر مختص به خود برای مسئولیت است. دوم، هنگام بحث در مورد حملات مبتنی‌بر هوش‌مصنوعی در حقوق بین‌الملل بشردوستانه، تمرکز عمدتاً بر حملات‌جنبشی[1] (یا حملاتی که به‌منظور ایجاد اثرات جنبشی صورت می‌پذیرد) است که با استفاده‌از سیستم‌های سلاح‌های خودمختار کشنده انجام می‌شوند. برعکس، پژوهش حاضر شامل بحث در مورد اَعمالی است که با تکیه‌بر هوش‌مصنوعی برای انجام حملات غیرجنبشی در قالب جنگ سایبری انجام می‌شوند، که لایه‌ای از چالش‌ها را به‌ویژه در رابطه با شناساییِ عامل اصلی مربوطه اضافه می‌کند.

در این‌مقاله، استدلال می‌شود که عناصر مسئولیت کیفری یک عمل تجاوزکارانه، در ساختار و تفسیر فعلی خود در اساسنامهٔ دیوان، در مواجههٔ با پیامدهای مبهم تجاوز سایبریِ انجام‌شده از طریق سیستم‌های هوش‌مصنوعی تحت‌حمایت دولت، ظرفیت لازم را ندارند.

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

گفتار نخست. جرم تجاوز

جنایت تجاوز، برای نخستین‌بار، پس‌از جنگ دوم جهانی در محاکمات نورنبرگ به‌عنوان یک جرم بین‌المللی که مسئولیت فردی به همراه دارد، شناخته شد. دادگاه نظامی بین‌المللی نورنبرگ[2]«جنایات علیه صلح را در حوزهٔ 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 یک‌طرح یا توطئهٔ 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 این‌نظر با سایر جنایات متفاوت است که شرّ انباشته‌شده از کل را در خود جای‌داده‌است».[1]

با این‌حال، پس‌از دادگاه نورنبرگ و نیز دادرسی‌های کیفری بین‌المللی در توکیو نزد دادگاه نظامی بین‌المللی برای خاور دور[2]، «جنایت‌تجاوز از نقشهٔ حقوق بین‌الملل ناپدید شد» (Cassese, 2007: 843-844). البته چند استثنا وجود داشت. از جمله، این‌مفهوم توسط مجمع‌عمومی سازمان ملل متحد در۱۹۷۴، زمانی‌که قطعنامه‌ای را برای تعریف تجاوز تصویب کرد، قدری توسعه یافت (Tsilonis, op. cit.: 171). سپس، در۱۹۸۵، شورای‌امنیت سازمان‌ملل‌متحد چندین اقدام دولتی را به‌عنوان اقدامات تجاوزکارانه محکوم کرد از جمله حملهٔ هوایی اسرائیل به تأسیسات سازمان آزادی‌بخش فلسطین در تونس و حملهٔ آفریقای‌جنوبی به آنگولا.[3]

متعاقباً در تابستان۱۹۹۸ و پس‌از مذاکراتی طولانی، جرم تجاوز در اساسنامهٔ رم، سند موسس دادگاه بین‌المللی کیفری، گنجانده‌شد و در فهرست جرایم بین‌المللی قرارگرفت. لکن اساسنامه مقرر داشت که تعریف جرم تجاوز در تاریخ‌دیگری تعیین‌شود. این‌اَمر در۲۰۱۰ حادث شد، یعنی زمانی‌که کنفرانس بررسی در کامپالا برای تصمیم‌گیری در مورد تعریفی برای جرم تجاوز، که از طریق مادهٔ۸ مکرّر در اساسنامهٔ رم گنجانده شد، برگزار گردید. در نهایت مقرر شد که پس‌از اصلاحیه، صلاحیت دیوان «برای آن‌دسته از کشورهای عضو که اصلاحیه را یک سال پس‌از تودیع اَسناد تصویب یا پذیرش‌خود پذیرفته‌اند» لازم‌الاجرا شود (اساسنامهٔ دیوان بین‌المللی کیفری، موادّ ۵(د) و ۱۲۱(۵)). برعکس، «در مورد کشوری که اصلاحیه را نپذیرفته‌است، دیوان صلاحیت خود را درمورد جرمی که مشمول اصلاحیه است، در صورتی‌که توسط اتباع آن کشور یا در قلمرو آن ارتکاب‌یابد، اِعمال نخواهد کرد» (اساسنامهٔ دیوان بین‌المللی کیفری، مادّه 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 اواخر۲۰۱۷، در شانزدهمین جلسهٔ مجمع کشورهای عضو در نیویورک، زمانی‌که تعریفی از این‌جرم در اساسنامهٔ دیوان بین‌المللی کیفری گنجانده‌شد، جرم تجاوز «فعّال» گردید و بدین‌ترتیب، «به‌مثابهٔ یک جرم واقعی از نظر قانونی تثبیت شد» (Tsilonis,op. cit.: 166) و در ۱۷ جولای۲۰۱۸ لازم‌الاجرا گردید (Kreß, 2018: 15). مادهٔ۸ مکرر اساسنامهٔ رم، جنایت تجاوز را برنامه‌ریزی، آماده‌سازی، شروع یا اجرای یک عمل تجاوز توسط شخصی‌که در موقعیتی‌است که به‌طور مؤثر می‌تواند بر اقدام سیاسی یا نظامی یک‌کشور کنترل یا هدایت کند، تعریف می‌کند که از نظر ماهیت، شدّت و مقیاس، نقض آشکار منشور سازمان‌ملل‌متحد محسوب‌می‌شود.

الف. عناصر مسئولیت کیفری بین‌المللی برای جرم تجاوز

مانند سایر جرایم بین‌المللی مندرج در اساسنامهٔ رم، جرم تجاوز نیز شامل دو عنصر کلیدی مادّی و معنوی است. عنصر مادّی، به رفتار (اعمّ از فعل، ترک‌فعل یا جرم فعل ناشی‌از ترک‌فعل)، حالت، و یا اوضاع‌واحوالی اشاره‌دارد که تجلّی نیّت مجرمانه و یا تقصیر جزایی است (اردبیلی، ۱۴۰۳: ۱/ ۱۳۵-۱۴۱) در اینجا، عنصر مادّی جرم تجاوز در مادهٔ۸ مکرّر اساسنامهٔ رم، برنامه‌ریزی، آماده‌سازی، شروع یا اجرای یک عمل تجاوز توسط شخصی است که در موقعیتی‌است که به‌طور مؤثر کنترل یا هدایت اقدام سیاسی یا نظامی یک دولت را بر عهده دارد. پس تحقق عنصر مادّی، مستلزم آن‌است که عمل تجاوزکارانه توسط شخصی‌که 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 مادّی داشته‌باشد تا در نتیجهٔ ارتکاب‌جرم، مسئول شناخته شود (پیشین: ۱۷۰). عنصر روانی جنایت تجاوز، از مادهٔ ۳۰ اساسنامهٔ دیوان بین‌المللی کیفری گرفته می‌شود که عناصر روانی موردنیاز برای آن‌دسته از جرایم در اساسنامهٔ رم که وجه‌تمایز آنها ذکر عنصر روانی است، ارائه می‌دهد. بندهای (۲)و(۳) این‌مادّه، به قصد در مورد رفتار مرتکب و آگاهی‌از شرایط پیرامونی و نتیجه، که شامل زمینهٔ عمل‌تجاوز دولت نیز می‌شود، اشاره

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

در مورد عنصر روانی، این‌الزام به قصد و آگاهی نسبت به اجزای جرم، به‌سَمت استانداردهای سنگین‌تر متمایل است و بنابراین، اثبات آن چالش‌برانگیزتر است. این‌معیار با دیدگاه اکثریت اندیشمندان حقوق بین‌الملل نیز هم‌راستا است که حالات روانی خفیف‌تر را برای تحقق مادهٔ ۳۰ اساسنامهٔ رم کافی نمی‌دانند (Clark, 2001 : 314-315; Ambos, 1999 : 21-22). در حالی‌که برخی‌از محققان مخالفند و استدلال می‌کنند که یک حالت روانی خفیف‌تر، مانند بی‌پروایی[1] نیز باید کافی‌باشد، که البته رویهٔ فعلی دیوان بین‌المللی کیفری نشان می‌دهد که دیدگاه اخیر با رویکرد دیوان مطابقت ندارد.[2] جمله‌بندی مادهٔ ۳۰ اساسنامه نیز به‌سختی جایی برای تفسیری باقی‌می‌گذارد 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 حوزهٔ مطالعاتی نسبتاً جدید در حقوق بین‌الملل است، به اَعمال تجاوزکارانه‌ای اشاره‌دارد که در فضای‌مجازی با نقض حقوق بین‌الملل انجام می‌شوند. این‌تصور که پیشرفت‌های فنّاوری ممکن‌است ما را ملزم به بازنگریِ مفاهیم متعارف در حقوق بین‌الملل کند، جدید نیست (Tsilonis, op. cit.: 315). در طول دو دههٔ گذشته، نمونه‌های زیادی از دولت‌هایی که حملات سایبری را علیه کشورهای‌دیگر 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 این‌حال، ادبیات این‌حوزه 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 این‌حملات، حتی بدون کمک هوش‌مصنوعی، با تعریف جرم تجاوز روبرو بوده است.[1]

در سال‌های اخیر، دولت‌ها شروع به ارائهٔ مواضع رسمی خود در مورد کاربرد حقوق بین‌الملل در فضای‌مجازی نموده‌اند. سی‌وهشت دولت (و هم‌چنان درحال افزایش) که تا به‌امروز چنین موضعی را بیان‌داشته‌اند، به اتفاق آراء معتقدند که قوانین و هنجارهای حقوق بین‌الملل در فضای‌سایبری اِعمال می‌شود (Carpenter and Hollis, 2023) و در نتیجه، حقوق کیفری بین‌الملل را به‌طور گسترده دربَرمی‌گیرد.

با این‌حال، اگرچه در مورد اِعمال حقوق بین‌الملل در فضای‌سایبری تاحدودی اجماع وجود دارد امّا ادبیات موجود در حقوق کیفری بین‌الملل درمورد چگونگی و اینکه تحت چه‌شرایطی ممکن‌است حملهٔ سایبری به یک عمل تجاوز منجر شود، نامشخص است. دو چالش خاص در اینجا برجسته است: نخست اینکه، آیا یک حملهٔ سایبری می‌تواند به سطح جنایت تجاوز برسد؟ دوم اینکه، آیا مرتکب چنین حمله‌ای می‌تواند الزام شرطِ رهبری مندرج در جنایت تجاوز را برآورده کند؟

در مورد چالش‌نخست، این‌مقاله به‌سرعت خاطرنشان می‌کند که در تطبیق یک حملهٔ سایبریِ مشخص با معنای یک‌عمل تجاوز، موارد فراوانی مربوطبه «تعریف» وجود دارد. دراین‌مورد، توجه به توسعهٔ دستورالعمل‌های تالین (۱٫۰ و ۲٫۰)، که توسط گروهی‌از 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، ۱۴۰۲: ۱۵۳۷-۱۵۵۹). این‌گروه، دو کتابچهٔ راهنما منتشر کرد که در مورد چارچوب قانونی عملیات سایبری در حقوق بین‌الملل و حقوق درگیری‌های مسلحانه راهنمایی ارائه می‌دادند؛ یکی در۲۰۱۳ و دیگری در۲۰۱۷. در کتابچهٔ راهنمای تالین ۲.۰، حملهٔ سایبری به‌عنوان «عملیاتی سایبری [...] که به‌طور منطقی انتظار می‌رود

---

۱. باید توجه داشت که این‌گفتار و در واقع این‌مقاله، محدود به بحث درمورد حملات سایبری به‌عنوان اقدام تهاجمی است. لذا شامل سایر جرایم سایبری، ازجمله جاسوسی‌سایبری نمی‌شود. برای‌بحث در مورد تفاوت‌های بین این جرایم (Weissbrodt, 2013 : 347-387).

باعث آسیب یا مرگ افراد یا آسیب یا تخریب اشیاء شود» تعریف‌شده‌است (Schmitt, 2017: 126). جنگ‌سایبری نیز به‌عنوان استفاده از حملهٔ سایبری، چه در چارچوب درگیری مسلحانه و چه بدون آن، به شیوه‌ای تعریف شد که اثراتی معادل[1] یک حملهٔ مسلحانهٔ متعارف داشته‌باشد (Ibid). این موضوع در دکترین (Weissbrodt, op. cit.: 369; Ambos, 2016: 495-504; Greco, 2020: 44) و در بین کشورها (Carpenter and Hollis, op. cit.: supra note 37) درمورد اینکه مصادیق «اثر معادل» چه‌می‌تواند باشد، مورد بحث قرارگرفته‌است، اما درک برجسته‌ای وجود دارد که برای‌مثال، حملهٔ سایبری به تأسیسات هسته‌ای، شبکه‌های‌برق، بیمارستان‌ها یا سایر زیرساخت‌های ضروری می‌تواند به‌عنوان یک حملهٔ مسلحانهٔ انجام‌شده ازطریق ابزارهای سایبری شناخته‌شود (Trahan, op. cit.: 1136).

ازسوی‌دیگر، طرح‌های استراتژیک که به‌طور متناوب توسط دفتر دادستانی دیوان بین‌المللی کیفری منتشر می‌شوند نیز هنوز به این سؤالات نپرداخته‌اند. تمرکز طرح۲۰۱۶-۲۰۱۸ «به صورت تک‌بُعدی بر نیاز به استفادهٔ بیشتر از فنّاوری‌های دیجیتال جدید برای شناسایی، جمع‌آوری و ارائهٔ شواهد از طریق فنّاوری» قرارگرفته‌است و تنها اشاره‌ای مبهم به نیاز فوری در به‌دست‌آوردن «بینش درمورد احتمالات و تهدیدهای جدید ناشی‌از تکامل فناوری» دارد (Tsilonis, op. cit.: 324; Office of the Prosecutor, Strategic Plan 2016-2018). به‌همین‌ترتیب، طرح۲۰۲۳-۲۰۲۵ که با هدف «نهایی‌کردن یک بررسی جامع و تثبیت چارچوب سیاست خود درمورد شدت/اولویت‌بندی/تکمیل تحقیقات» است نیز معتقد است که «سایر سیاست‌های جدیدی که در طول دورهٔ اجرای این‌طرح استراتژیک تکمیل خواهند شد، به حوزه‌هایی ازجمله جرایم سایبری خواهندپرداخت [...]» (Office of the Prosecutor, Strategic Plan 2023-2025). «کریم‌ا.ا.خان»، دادستان دیوان بین‌المللی کیفری، در ژانویهٔ۲۰۲۴ اظهار داشت که جرایم سایبری «درصورت برآورده‌شدن الزامات اساسنامهٔ رم، ممکن‌است در صلاحیت دیوان بین‌المللی کیفری قرارگیرند» (Statement by ICC Prosecutor., 2024) و «دفتر من [دادستانی] می‌تواند چنین رفتارهایی را بررسی یا تحت‌پیگردقانونی قراردهد» (K.A.A.

1. equivalent effects

(Khan KC., 2023).[1] براین‌اساس، توجه نهادین به چالش‌های تفسیریِ تطبیق رفتار حملات سایبری با پارامترهای جرایم بین‌المللی، ممکن‌است به‌زودی صورت گیرد، اما هنوز به آن توجه وافی نشده‌است.

در مورد چالش‌دوم، حملات سایبری با حملاتی‌که ازطریق ابزارهای سنتیِ جنگ انجام می‌شوند، متفاوت‌اند. زیرا در مورد اخیر، شناسایی مهاجم، اغلب چالش‌برانگیز نیست، چه‌رسد به اینکه بتوان ارتکاب حمله را به یک فردِ به اندازهٔ کافی عالی‌رتبه که قادر به انجام یک عمل تجاوزکارانه است، نسبت داد. دراین‌خصوص، استدلال شده است که به‌عنوان یک مسئلهٔ آستانه‌ای[2]، درجهٔ ناشناس بودنی 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). به‌عبارت‌دیگر، در حالی‌که ردیابی یک‌حملهٔ [سایبری] امکان‌پذیر است، بیشتر ردیابی‌ها به ISP ختم می‌شوند [...] و ردیابیِ بیشتر نیاز به همکاری ISPها دارد (نوریان، ۱۳۹۵: ۴۴۱) و البته، برای اینکه مسئولیت یک عمل تجاوزکارانه به آن نسبت داده شود، یک حملهٔ سایبری مبتنی‌بر هوش‌مصنوعی باید نَه‌تنها به یک بازیگر (Ophardt, 2010 : 10-11) در دستگاه دولت، بلکه به یک مقام‌عالی‌رتبه، مانند یک رهبر سیاسی یا نظامی نیز منتسب گردد (پیری، ۱۴۰۴: ۱۸۲). در این‌مورد، اتکای دولت‌ها به هکرهای قراردادی و یا سایر طرف‌های خارجی، با تقویت این‌موضوع با انتساب، نَه‌تنها به یک دولت بلکه به یک رهبر خاص در درون دولت، مسئولیتْ تحت جرم تجاوز را به چالش می‌کشد (Greco, op. cit. : 44).

---

[1] .گفتنی‌است که در این مقالهٔ کم‌بازدید در «فارین پالیسی آنالیتیکس»، دادستان دیوان، چارچوب قواعد ایجادشده توسط اساسنامهٔ رم را برای رسیدگی به فعالیت‌های سایبری، بدون نیاز به ایجاد قواعد جدید، به اندازهٔ کافی، گسترده و انعطاف‌پذیر می‌دانَد.

[2]. Gravity threshold

در خصوص مفهوم آستانهٔ‌شدت در تجاوز سایبری، باید گفت هر زمان‌که وضعیت‌خاصی ازسوی شورای‌امنیت به دادستان دیوان ارجاع شود یا دولت‌ها و یا به ابتکار خود دادستان قضیه‌ای شناسایی گردد، دادستان باید مبنای معقولی در تصمیم‌گیری درخصوص تعقیب یا عدم‌آن اتخاذ نماید. مرحلهٔ اول، براساس صلاحیت‌ها، و مرحلهٔ دوم، از حیث داشتنِ شدت‌کافی یا آستانهٔ شدت براساس بند (د) مادهٔ۱۷ اساسنامهٔ دیوان (اردبیلی و دیگران، پیشین: ۱۵۴۷).

هم‌چنین تعریف جرم تجاوز، مسئولیت کیفری فردی را در مورد حملات سایبریِ انجام‌شده توسط بازیگران غیردولتی که به یک‌دولت قابل‌انتساب نیستند، غیرممکن می‌کند (Buchan and Tsagourias, 2016: 377-381; Schmitt and Watts, 2016: 595-611). مطمئناً این‌اَمر، مسئله‌ای منحصر به تجاوز سایبری نیست، زیرا حقوق کیفری بین‌الملل مدت‌هاست که با نحوهٔ رسیدگی‌به جرایم بین‌المللیِ ارتکاب‌یافته توسط بازیگران غیردولتی، دست‌وپنجه نرم‌می‌کند (Acquaviva, 2011: Ch 13; Steer, 2011: Ch 19). پس، حملات سایبری، مسئلهٔ انتساب را تشدید می‌کنند، زیرا دولت‌ها بارها برای انجام عملیات سایبریِ خود به نهادهای ظاهراً غیردولتی متکی‌بوده‌اند. لذا تلاش‌ها برای پیگرد قانونی تجاوز سایبری در سطح بین کشورها، احتمالاً مسئلهٔ انتساب را به‌عنوان یک مسئلهٔ آستانه‌ای دربَرمی‌گیرد.

برآورده‌کردن شرط (الزام) رهبری مندرج در بند(۱) مادهٔ۸ مکرّر، ممکن‌است با تشکیل روزافزون بخش‌های تخصصی توسط کشورهای مختلف که وظیفهٔ 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» تشبیه‌کرده‌اند (Ambos, op. cit.). طبق پروندهٔ «بِمبا گمبو»[۲] پاسخ مافوق به اقدامات نظامی یک زیردست می‌تواند فرمانده را در صورتی‌که «از رفتار مطلع بوده یا باید مطلع می‌بود» و «توانایی مادّی برای جلوگیری یا سرکوب ارتکاب جرایم یا ارائهٔ موضوع به مقامات جزء» را داشته باشد، در معرض‌مسئولیت قرار دهد.[۳] دستورالعمل تالین ۲٫۰ به‌طورمشابه بیان می‌کند که مسئولیت‌کیفری برای فرماندهان و مافوق‌ها در زمینهٔ جنایات‌جنگی وجود دارد که در آن «آنها می‌دانستند [...] یا باید می‌دانستند که زیردستانشان مرتکب جرم می‌شوند، در شُرف ارتکاب آن هستند یا مرتکب شده‌اند» و «از انجام تمام اقدامات معقول

---

[۱]. مثال نخست، مربوط‌است به استراتژی جامع سایبری وزارت جنگ (وزارت دفاع سابق) ایالات‌متحده و واحد عملیاتی آن: U.S. Cyber Command (2024); and UK's National Security Cyber Center (2024)

[۲]. بمبا گُمبو، تبعهٔ کنگو و فرماندهٔ نظامی نیروهایی بود که به درخواست رییس‌جمهور وقت آفریقای مرکزی، از کنگو به‌سوی این کشور گسیل شدند و از اکتبر۲۰۰۲ تا مارچ۲۰۰۳ به سرکوب مخالفان رییس‌جمهور مذکور پرداختند.

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

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

بنابراین و به‌عنوان مسئله‌ای حائز اهمیت، مقالۀحاضر این‌دیدگاه را اتخاذ می‌کند که مسئولیت جرم تجاوز می‌تواند، و در واقع باید، برای پاسخگوکردن رهبران سیاسی و نظامی یک کشور در جایی‌که فرمانبَران ایشان برای ارتکاب عمل تجاوز علیه کشور دیگر به عملیات سایبری متکی هستند، در دسترس باشد. ضرورت اتخاذ این‌دیدگاه ممکن است به‌طور فزاینده‌ای اهمیت یابَد، زیرا این پژوهش، در مورد در دسترس‌بودن جرم تجاوز برای مقابله با حملات سایبری انجام‌شده توسط بازیگران دولتی بحث می‌کند، در حالی‌که خطر ناشی از این‌حملات هم‌چنان به‌سرعت درحال گسترش است. هوش‌مصنوعی، درحال‌حاضر برای افزایش‌سرعت، دامنه و مقیاس تخریب ناشی‌از حملات سایبری استفاده می‌شود و این درحالی‌است که شناسایی، ردیابی و قطع این حملات را دشوارتر می‌کند (Greenberg, op. cit.: supra note 3) و همان‌طور که هوش‌مصنوعی، حملات سایبری را تأثیرگذارتر و قابل‌دسترس‌تر می‌نمایاند[1] با همان‌نسبت، انطباق آنها با عناصر مسئولیت کیفری بین‌المللی را دشوارتر می‌سازد.

گفتار دوم. تطبیق تجاوز سایبری مبتنی‌بر هوش‌مصنوعی با عناصر متعارف مسئولیت کیفری بین‌المللی

در این‌گفتار، مقاله نشان خواهد داد که حتی با فرض اینکه حملۀ سایبری با اثرات غیرجنبشی،[2] می‌تواند جرم تجاوز محسوب گردد، مسائل منحصربه‌فردی هنگام‌ارتکاب چنین اَعمالی با استفاده‌از هوش‌مصنوعی ایجاد می‌شود.

هوش‌مصنوعی، چالش‌های بیشتری را در رابطه با الزامات عنصر مادّی و عنصر معنوی ایجاد می‌کند. این‌مشکل در نوشتگان حقوقی مرتبط‌با مسئولیت کیفری بین‌المللی برای اَعمالی که با (یا توسط؟) هوش‌مصنوعی انجام می‌شود با عنوان «شکافِ مسئولیت»[3]

---

[1]. از آنجا که موانع استفاده‌از هوش‌مصنوعی از نظر نیروی انسانی، مالی و سایر منابع، بسیار کمتر از دستگاه‌های نظامی سنّتی است.

2. non-kinetic effects

3. responsibility gap

مورد بحث قرار گرفته‌است. این‌اصطلاح که ابتدائاً توسط «آندریاس ماتیاس» ابداع شد، به موارد زیر اشاره دارد:

«در این دستهٔ روبه‌رشد از اقدامات ماشینی، روش‌های سنتیِ انتساب مسئولیت با حسّ عدالت ما و چارچوب اخلاقی جامعه سازگار نیست، زیرا هیچ‌کس کنترل کافی بر اَعمال ماشین ندارد تا بتواند مسئولیت آنها را بر عهده بگیرد. در زمینهٔ استفاده‌از هوش‌مصنوعی برای ارتکاب جرم تجاوز سایبری [...] شکاف مسئولیت، ممکن است برای توصیف خلاء قانونی استفاده شود که طی‌آن هوش‌مصنوعی به‌اندازهٔ‌کافی مسئول یک عمل باشد یا به‌اندازهٔ‌کافی تصمیم‌به اقدام بگیرد تا تصمیم‌گیرندهٔ انسانی را در قِبال آسیبِ ایجادشده مسئول ندانَد» (Matthias, 2004 : 180).

«ماتیاس» در بررسی چگونگی اِعمال «شکاف مسئولیت» درمورد تجاوز ناشی‌از هوش‌مصنوعی، از نوشتگان حقوقی غنی‌تری که جنایات‌جنگی ناشی‌از هوش‌مصنوعی و در دسترس‌بودن آنها برای مسئولیت کیفری بین‌المللی را تجزیه‌وتحلیل می‌کند، راهنمایی می‌گیرد. در آنجا، محققان، چالش‌ها و محدودیت‌های اِعمال عناصر موجود در جرایم بین‌المللی را مورد بحث قرار داده‌اند و راه‌حل‌های متنوعی را برای از بین‌بردن شکاف مسئولیتِ بالقوّه بین جرایم‌جنگی مبتنی‌بر هوش‌مصنوعی و مسئولیت کیفری بین‌المللی ارائه‌داده‌اند. درعین‌حال، استدلال شده است که مسئلهٔ شکاف مسئولیت، به‌آن‌اندازه که در آثار حقوقی پیش‌بینی‌شده، شایع نیست و در واقع، این‌مسائل «فقط در برخی موقعیت‌ها، یعنی موقعیت‌هایی که نتیجه، محصولِ بی‌دقتی یا سوءنیت نیست، مطرح می‌شوند» (Königs, 2022 : 4).

باری، ادامهٔ این‌گفتار به‌تحلیل این‌موضوع خواهد پرداخت که چگونه عناصر مسئولیت کیفری بین‌المللی، ممکن‌است تحت‌تأثیر تفاوت‌های ظریف مربوط به استفاده از هوش‌مصنوعی در اقدامات مرتبط با تجاوز سایبری قرار گیرند، که نمونهٔ دیگری از مفهوم «شکاف مسئولیت» را شکل می‌دهد.

الف. عنصر مادّی

در ارزیابی عنصر مادّی، با این سوال اساسی شروع می‌کنیم که چه‌کسی هنگام وقوع یک حملهٔ سایبری مبتنی‌بر هوش‌مصنوعی، عامل است؟ به‌دیگر بیان، چه‌کسی (یا چه‌چیزی) 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، حولِ محور اَعمال و ارادهٔ انسانی ساخته شده‌اند» (Gaeta, 2023 : 1038). البته، از برخی جهات، شخصیت حقوقی به سایر عاملان،[1] یعنی اشخاص‌حقوقی نیز تعمیم داده‌شده‌است، امّا حتّی در این‌شرایط، وقتی صحبت از مسئولیت کیفری می‌شود، کسانی‌که در رأس یک شخص‌حقوقی هستند، هم‌چنان به‌عنوان عاملِ مسئولیت کیفری برای آسیب‌های ناشی‌از سوءرفتار جدّی شخص‌حقوقی در نظر گرفته‌می‌شوند (Press Release : Former CEO., 2018)؛ به‌این‌دلیلِ مهم که اِسناد تقصیر به شخص‌حقوقی ناممکن است (اردبیلی، ۱۴۰۳: ۲/ ۱۵). این‌رویکرد در حقوق کیفری بین‌المللی نیز منعکس شده‌است، آنجایی که کسانی‌که اَعمال مجرمانهٔ یک دولت را هدایت می‌کنند، کسانی‌هستند که شخصاً مسئول شناخته می‌شوند (اساسنامهٔ دیوان بین‌المللی کیفری، مادّهٔ ۸ مکرّر).

بنابراین، هوش‌مصنوعی با ایجاد یک عاملِ دیگر، که به‌طور بالقوه جایگزین می‌شود و قادر به تصمیم‌گیری مستقل[2] است، این ساختارِ متعارف را که زیربنای حقوق جزا و مسئولیت کیفری است مخدوش می‌کند (Ex-Google Officer Finally., 2023). این‌اَمر باعث شده است که برخی اندیشمندان، گسترشِ شخصیت‌حقوقی به سیستم‌های هوش‌مصنوعی را ممکن بدانند و درنتیجه، آنها را قادر و مشمول عاملانِ مسئول کیفری قلمداد کنند (Lagioia and Sartor, 2020 : 433).

با این‌حال، دیدگاه اخیر، اغلب رد می‌شود. زیرا سیستم‌های هوش‌مصنوعی فاقد جنبه‌های حیاتیِ شخصیت هستند که عملی را منجر به تحقق مسئولیت کیفری می‌کند. از این گذشته، مسئولیت‌کیفری حتی درجایی‌که رفتار یک انسان غیرارادی باشد،[3] منتسب نمی‌شود . زیرا این‌اَمر، مختصات و کیفیات اساسیِ مدّنظر برای یک عمل‌مجرمانه را که محصول ارادهٔ آزاد خودِ انسان، و بنابراین، آگاهی است تضعیف می‌کند (Moore, 2010 : 115). سیستم‌های هوش‌مصنوعی، به‌عنوان یک فناوریِ برنامه‌ریزی‌شده تلقی می‌شوند و فاقد این درجه از خودمختاری هستند که به فرد اجازه می‌دهد استدلال کند

[1]. actors

[2]. و شاید حتی قادر به فکر و احساس، به گفته برخی از تأثیرگذارترین سازندگان هوش مصنوعی.

[3]. به‌عنوان‌مثال، جایی‌که متهم در هنگام خوابگردی، یا در حالت مستی غیرارادی مرتکب‌جرم شده‌است.

که برنامه‌نویسان یا کاربران انسانی هم‌چنان بازیگران واقعیِ درپس‌پردهٔ یک جرم مبتنی‌بر هوش‌مصنوعی هستند و به عبارت بهتر، عدم پیش‌بینی‌پذیری در چگونگی دستیابی هوش‌مصنوعی به اهداف مندرج در کُد خود، «تجلّی‌ای از کنش هوشمندانه» نیست (Gaeta, op. cit.: 1040). بنابراین، اگرچه در برخی‌از تکرارهای آینده، سیستم‌های هوش‌مصنوعی ممکن‌است به درجه‌ای از استقلال واقعیِ لازم برای در نظرگرفتن عاملانِ دارای مسئولیت‌کیفری دست یابند، اما نمی‌توان آنها را در وضعیت فعلی‌شان چنین درنظرگرفت (Lina, 2018: 682).

پس به‌عنوان تحلیل بیشتر، این‌مقاله با این‌دیدگاه موافق است که سیستم‌های هوش‌مصنوعی را نمی‌توان درحال‌حاضر به عنوان عاملان دارای مسئولیت کیفری درنظرگرفت. بنابراین، درجایی‌که قوانین بین‌المللی توسط یک سیستم هوش‌مصنوعی نقض می‌شود، می‌توان به‌طور دقیق‌تر گفت که «صرفاً» با استفاده از یک سیستم هوش‌مصنوعی نقض شده‌است. بنابراین، این‌سؤال باقی می‌مانَد که آیا تصمیم‌گیرندهٔ انسانی آن‌سوی هوش‌مصنوعی، شامل توسعه‌دهنده، برنامه‌نویس، کاربر و غیره، می‌تواند به‌عنوان «عامل» در راستای تحقق مسئولیت کیفری در نظر گرفته‌شود یا خیر؟ پاسخ به‌این پرسش نیز نامشخص است. برای این‌منظور، بهتر است از سامانه‌های تسلیحاتی خودمختار هوشمند[1] مبتنی‌بر هوش‌مصنوعی صحبت‌کرد.

درخصوص اَعمال انجام‌شده توسط سیستم‌های تسلیحاتی خودمختار[2] باید گفت که «این سیستم‌های تسلیحاتی پس از فعال‌شدن، بدون نظارت یا کنترل کاربر، در انجام وظایف و کارکردهای محولهٔ خود عمل می‌کنند یا می‌توانند عمل کنند [...] با توجه به ویژگی‌های خاصّ الگوریتم‌ها، مبتنی‌بر روش‌های خودآموزی، نحوهٔ انجام وظایف و کارکردهای محوله توسط سیستم نمی‌تواند به‌طور کامل توسط برنامه‌نویس یا کاربر پیش‌بینی شود. این سامانه‌ها با خطر بالایی که از غیرقابل‌پیش‌بینی‌بودن 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 پس‌از فعال‌شدن می‌توانند بدون دخالت انسان، اهداف را انتخاب و با آنها درگیر شوند. این‌تسلیحات با عنوانِ ربات قاتل نیز شناخته‌می‌شوند.

چرخهٔ هدف‌گیری از خود نشان می‌دهند، می‌توانند بی‌هدف باشند و به‌همین‌دلیل توسط حقوق بین‌الملل بشردوستانه ممنوع شده‌اند» (Gaeta, op. cit.: 1034). بنابراین، «با توجه‌به غیرقابل‌پیش‌بینی‌بودن ذاتی نحوهٔ انجام عملکرد و وظیفهٔ محوله توسط این سیستم»، این‌اَمر «عدم امکان واگذاری مسئولیت به برنامه‌نویس یا کاربر» را در پی دارد (Ibid: 1035). بیان این نکته لازم است که این‌شِق از مقولهٔ انتساب، با آنچه در بالا موردبحث قرارگرفت، متفاوت است. در آنجا، مسئلهٔ انتساب، بر چالشِ شناسایی مرتکب جرایم سایبری به‌دلیل ناشناس‌بودنِ عامل آن متمرکز بود، لکن در اینجا، هویت عاملِ انسانی اولیه، قابل‌شناسایی است امّا سوال این‌است که سیستم‌های مورد بحث، تا چه‌اندازه خودمختار در نظر گرفته‌می‌شوند تا برمبنای آن، قانون بتواند شرایط موردنیاز برای فاعل اصلی جرم را به آن تصمیم‌گیرندهٔ انسانی نسبت دهد؟

باری، محققان دراین‌باره اتفاق‌نظر ندارند که درنظرگرفتن انسانِ درپَس یک سیستم هوش‌مصنوعی به‌عنوان عامل مرتبط برای اهداف مسئولیت، ممکن‌است چالش‌برانگیز باشد. بلکه برعکس، استدلال شده است که حفظ استقلال و غیرقابل‌پیش‌بینی‌بودن[1] یک‌سیستم هوش‌مصنوعی، به‌معنای عدم مسئولیت برنامه‌نویس آن نیست و بنابراین، اقدامات یا غفلت‌های تصمیم‌گیرندگان انسانیِ آن‌سوی سیستم‌های هوش‌مصنوعی، ممکن است به‌عنوان عاملان مرتبط برای مسئولیت درنظرگرفته شود (Königs, op. cit.: 4).

پژوهش حاضر با این‌دیدگاه موافق است و یافتن برنامه‌نویس در واحد سایبری ارتش یک‌کشور به‌عنوان عاملی در پسِ آسیب‌های ناشی‌از یک حملهٔ سایبری مبتنی‌بر هوش‌مصنوعی را که با استفاده از کُدهای وی انجام می‌شود بدون‌مشکل می‌داند. این‌دیدگاه توسط فلسفه حقوقی‌ای که زیربنای مفهوم عمل مجرمانه در حقوق جزای مدرن است و نیز توسط منافع سیاسیِ در معرض‌خطر در ادامهٔ عملکرد حقوق کیفری بین‌الملل در مواجهه با پیشرفت‌های تکنولوژیکی در درگیری‌های بین کشورها پشتیبانی می‌شود. دربارهٔ مورد نخست، منصفانه است که توسعه‌دهنده، برنامه‌نویس یا کاربر انسانی

1. autonomy and unpredictability

در پَس یک سیستم هوش‌مصنوعی را تحت یک نظریهٔ نمایندگی، مشابه آنچه که از آن‌طریق، رهبران سیاسی یا نظامیْ مسئول اَعمال زیردستان خود شناخته می‌شوند، مسئول بدانیم (اساسنامهٔ دیوان بین‌المللی کیفری، بند(۱) مادّهٔ۸ مکرّر). درخصوص مورد دوم، حقوق کیفری بین‌الملل تمایل دارد تا از اینکه کاربران انسانیِ پشت‌پردهٔ سیستم‌های هوش‌مصنوعی به‌خودی‌خود نتوانند عامل اصلی یک جرم بین‌المللی محسوب شوند، جلوگیری کند و درنتیجه، رفتار مجرمانه را بدون مرتکب باقی نگذارد.

از باب تأکید، هم‌چنان‌که پیشتر بحث‌شد، جنایت تجاوز شامل این‌شرط است که «یک رهبر سیاسی یا نظامی» در برنامه‌ریزی، آماده‌سازی، شروع یا اجرای آن دخیل باشد. هرچند توسط برخی نویسندگان، بحث مفصلی درمورد شرایطی که ممکن است الزام رهبری برای یک عمل تجاوز سایبری لحاظ شود، ارائه‌شده‌است (Ambos, op. cit.: 498-499) امّا کافی‌است بگوییم که نسخه‌های مختلف این‌تحلیل‌ها معمولاً به سؤالات مربوط‌به «کنترل»، به‌ویژه در مفهوم نظامی، می‌پردازند. بنابراین، یک رهبر سیاسی یا نظامی که قادر به کنترلِ ارتکاب یک حملهٔ سایبری است، احتمالاً می‌تواند به‌عنوان عامل در پَس‌پردهٔ یک تجاوز سایبری در نظر گرفته‌شود.[۱]

در ادامهٔ این‌تحلیل، پژوهش حاضر، بر این فرض استوار است که «عنصر مادّی» توسط عامل انسانی که مسبّب استفاده از یک سیستم هوش‌مصنوعی 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 مادهٔ ۳۰ اساسنامهٔ دیوان بین‌المللی کیفری تبیین‌شده‌است. این‌مادّه به‌مثابهٔ قاعده‌ای عمومی است و درمورد تمام جنایات در صلاحیت دیوان، به‌استثنای مواردی‌که به غیرعمدبودن آنها تصریح‌شده،

۱. مفهوم اِعمال کنترل بر جنایت، بر این‌اندیشه استوار است که فاعلان اصلی یک جنایت، فقط کسانی نیستند که عناصر عینی جرم را مادتاً مرتکب می‌شوند، بلکه کسانی هم که با وجود بُعد مسافت و دوری از صحنهٔ جنایت آن را کنترل و یا ارتکاب آن را هدایت می‌کنند، فاعلان اصلی به‌شمار می‌روند چون دربارهٔ وقوع جنایت و نحوهٔ ارتکاب آن تصمیم می‌گیرند (اردبیلی، ۱۳۹۷: ٦٥٨).

اِعمال می‌شود (قیاسی و محترم‌قلاتی، پیشین: ۱۵۶). درحالی‌که مادۀ ۳۰ اساسنامه، مستلزم قصد و آگاهی مرتکب، اعمّ از خاص یا عام است،[۱] مسئلۀ اصلی درخصوص پرسشِ این مقاله، آن است که با توجه به مادۀمذکور، آیا مسئول دانستنِ عامل انسانیِ درپَس‌پردۀ یک سیستم هوش‌مصنوعی، درجایی‌که این عامل انسانی صرفاً آگاه است که رفتار مجرمانه می‌تواند رخ دهد یا حتی رخ‌خواهد داد، غیرممکن می‌شود؟

ظاهراً اساسنامۀ رم، قادر به پرداختن‌به جنایات بین‌المللی ناشی‌از هوش‌مصنوعی که حالات روانی آنها در مادۀ ۳۰ تعریف‌شده، نیست زیرا «الزام اینکه رفتار ممنوعه عمداً انجام شود [...] به‌نظر می‌رسد اَشکال ریسک‌پذیریِ مسئولیت‌کیفری را مستثنی می‌کند» (Bo, 2021 : 284). به بیان دیگر، درحالی‌که برخی نظریات برای گنجاندن مفاهیمی مانند ریسک‌پذیری آگاهانه[۲] یا بی‌پروایی در عنصر معنوی جرایم بین‌المللی وجود دارد، «دیدگاه پیشرو در رویۀ اولیۀ دیوان بین‌المللی کیفری، اتخاذ تفسیری محدودکننده است» (Trahan, op. cit.: 1150). این‌حمایت از تفسیر مضیّق، در حکم «بِمبا 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]

استفادۀ عمدی دولت‌ها از حملات سایبری، سابقۀ متقنی در انتشار تأثیر آنها فراتر از هدف موردنظر یا حتی پیش‌بینی‌شده، یا ایجاد آسیب‌هایی که به‌طور خاص توسط مرتکب مشخص نشده‌اند دارد. براین‌مبنا، عنصر معنوی موردنیاز برای جنایت تجاوز، ناهماهنگی قابل‌توجهی 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. PCNICC/2000/1/Add.2) نیز علاوه‌بر اساسنامۀ رم، مورد ملاحظه قرار گرفته‌است.

2. conscious risk-taking

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

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

این‌استفاده (یا سوءاستفاده) عمدی از عملیات سایبری برای انجام حمله علیه یک‌هدفِ تقریباً غیرقطعی، دو نوع مشکلِ تعریف‌محور را از نظر آثار حملات ایجاد می‌کند: یکی مربوط‌به هویت و دیگری مربوط به قلمرو جغرافیایی . درمورد هویت، حملهٔ سایبری ممکن‌است برای افراد یا نهادهای خاصی در کشور هدف در نظر گرفته‌شده‌باشد اما به‌دلیل اتصال یکپارچه شبکه‌های رایانه‌ای می‌تواند به‌راحتی به اهداف ناخواستهٔ دیگری منتقل شود (Bo, op. cit.: 278).[1] درمورد جغرافیا، اتصال شبکه‌های رایانه‌ای به‌هیچ‌وجه مرزهای ملّی را رعایت نمی‌کند. به‌این‌معنی‌که یک حملهٔ سایبری که برای یک‌کشور درنظرگرفته‌شده‌است، می‌تواند شامل حمله به کشورهای دیگر، تقریباً به‌طور همزمان نیز باشد. هر دوی این‌مشکلات، در حملهٔ بدافزار WannaCry (به‌شرح مقدمهٔ این‌مقاله) به‌نمایش گذاشته‌شدند؛ حمله‌ای که عمدتاً قربانیان آن شامل اهداف ناخواسته‌ای مانند وزارت کشور روسیه و چندین شرکت جهانی بودند (Ghafur et al., 2017: 1-7). هدف کلّی حمله، قلمرو چندین کشور در سراسر جهان بود اما تعیین هدفِ خاص اینکه کدام کشورها و با چه ظرفیتی مورد حمله قرارگیرند، به خودِ بدافزار واگذار شد.

این مسئله با آنچه که در مقالات علمی تحت‌عنوان «اثر جعبه‌سیاهِ هوش‌مصنوعی»[2] توصیف می‌شود، پیچیده‌تر می‌گردد. این‌اَثر می‌گوید که ابهام کُد هوش‌مصنوعی، به‌معنی توضیح اینکه چرا هوش‌مصنوعی به شیوه‌ای خاص رفتار کرده است، چه به‌عنوان محصول نقص در کُد آن، نقص در فرآیند توسعه یا آسیب عمدی ازسوی کاربر انسانی، آسان نیست (Wendehorst, 2020: 152). این‌اَمر، آگاهی‌از وضعیت روانیِ مجرم درمورد یک حملهٔ سایبری خاص، در این‌خصوص که حمله تا چه‌اندازه طبق‌برنامه انجام‌شده‌است، یا اینکه هوش‌مصنوعی درمورد مقیاس آسیب یا وضعیت تحت‌تأثیر، آزادی‌های خلاقانه‌ای داشته‌است یا خیر را دچار ابهام می‌کند. بنابراین، با توجه‌به ضرورت اثبات قصد و آگاهی

---

[1]. «بو»، با بحث در زمینهٔ سلاح‌های خودکار مورداستفاده برای ارتکاب جنایات جنگی، این‌مشکل را به‌عنوان «خلاء ناشی‌از عدم جرم‌انگاری حملاتی که عمداً علیه غیرنظامیان انجام نمی‌شوند، اما درعوض از تمایز بین اهداف قانونی و غیرقانونی کوتاهی می‌کنند، جایی‌که خطری درمورد احتمال حمله به غیرنظامیان درنظرگرفته‌می‌شود»، توصیف می‌کند.

2. black box effect of AI

مرتکب (به‌شرح مادهٔ ۳۰ اساسنامهٔ رم) هوش‌مصنوعی رویکردهای واجد این‌حالات روانی را مختل می‌کند.

و باز هم تأکید می‌شود که انتساب مسئولیت در جنایت تجاوز، مستلزم آن‌است‌که جرم به یک رهبر نظامی یا سیاسی مربوط شود. در اینجا، یک رهبر سیاسی یا نظامی، ممکن است استدلال نماید که به‌دلیل عدم درک فنّی از ماهیت پیچیدهٔ حمله سایبری، نمی‌تواند سوءنیت لازم برای عمل تجاوز سایبری را داشته‌باشد. البته محققان توافق کرده‌اند که این دفاع برای ایشان کافی نیست تا از مسئولیت کیفری تحت مادّه۸ مکرّر شانه‌خالی کنند. همانطور که استدلال‌شده‌است شخصی‌که در موقعیتی‌است که می‌تواند دستور انجام دادن یک عمل تجاوزکارانه را صادر کند و به‌طورمؤثر برنامه تجاوز را کنترل نماید، نیازی‌به دانستن جزئیات فنّی 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 خواهدکرد (Kai Ambos, op. cit.: 503-504).

در زمینهٔ مسئولیت فرمانده برای جنایات جنگی، دستورالعمل تالین ۲٫۰ نیز این‌دیدگاه را تقویت می‌کند که پیچیدگی فنّی ابزارهای عمل مجرمانه، سپری برای مسئولیت قلمداد نمی‌شود (Schmitt, op. cit.: 399).

گفتار سوم. تطبیق‌ها و راه‌حل‌های پیشنهادی

گروهی‌از محققان حقوق بین‌الملل کیفری، روش‌هایی را برای پرداختن به «شکاف مسئولیت» درمورد مسئولیت ناشی‌از آسیب‌های هوش‌مصنوعی پیشنهاد کرده‌اند. این‌بخش از پژوهش، برخی‌از این‌موارد را موردبحث قرار می‌دهد (الف) و النهایه، راه‌حل بالقوهٔ خود را مطرح می‌کند (ب).

الف. پیشنهادهایی از نوشتگان حقوقیِ موضوع

محققانی که به‌دنبال 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 به‌عنوان جایگزین مناسب‌تری مطرح می‌کنند. به‌عنوان مثال، در مواردی‌که از یک سیستم هوش‌مصنوعی برای ایجاد نقض‌های ناخواستهٔ قواعد حقوق بین‌الملل

بشردوستانه استفاده می‌شود (Bo, op. cit.: 275) حتی با اشاره به قصد خاص در جایی‌که هنوز صِرف آسیب عمومی مدّنظر است. باید توجه داد که این‌مقاله برخی‌از این پیشنهادها را به‌عنوان استدلال درنظرمی‌گیرد و بدان می‌پردازد، زیرا همان‌طور که شرح آن گذشت، بسیاری‌از نویسندگان به‌صراحت اتفاق‌نظر دارند که حالات روانی خفیف‌تر، مانند بی‌پروایی و غیره، عامدانه از اساسنامۀ رم مستثنی شده‌اند. لذا با این‌رویکرد، این بخش‌از مقاله، پیشنهادهای صاحبان‌نظری را بررسی می‌کند که حتی بسا سهواً، با قرائت سخت‌گیرانه مادۀ ۳۰ اساسنامۀ رم مخالف هستند.

«مارتا بو»، با بحث در زمینۀ استفاده‌از سیستم‌های تسلیحاتی خودمختار در ارتکاب جنایات جنگی، استدلال می‌کند که جایی برای تفسیر الزام عنصر روانی برای جنایت جنگی حمله به غیرنظامیان در اساسنامۀ رم وجود دارد تا شامل اَشکالی از ریسک‌پذیری رفتار مجرمانه مانند بی‌پروایی شود. این‌تفسیر، انتساب مسئولیت کیفری برای حملات کورکورانه، در جایی‌که اُپراتور 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 وجوداین ، تصمیم به ادامۀ حمله می‌گیرد امکان‌پذیر می‌سازد (Ibid.: 278-279). او هم‌چنین اظهار می‌دارد که این‌اَمر، قابل‌تصور و نیز امکان‌پذیر است و استدلال می‌کند درحالی‌که بی‌پروایی در مادۀ ۳۰ اساسنامۀ دادگاه بین‌المللی کیفری گنجانده نشده‌است، امّا به‌دلیل ابهام موجود در بند(۲)(b) این‌مادّه درمورد اینکه آیا سطح آگاهی موردنیاز، این است که یک «پیامد»[1] قطعاً رخ خواهد داد (خواستنِ نتیجه) یا اینکه پیامد احتمال دارد یا ممکن‌است در جریان عادّی وقایع و در پیِ رخدادهای معمول واقع شود، می‌توان ادعا کرد که بی‌پروایی وجود دارد. (Ibid.: 286)

مورد اخیر ممکن‌است راه را برای لحاظِ بی‌پروایی به‌عنوان عنصر معنوی باز بگذارد. البته ایرادهای «کونیگز» به مقولۀ شکاف مسئولیت، به در دسترس‌بودن بی‌پروایی یا سهل‌انگاری[2] به‌عنوان حالات ذهنیِ موجود برای مسئول‌دانستنِ سازنده، برنامه‌نویس،

1. consequence

2. negligence

اپراتور و غیره در جایی‌که سوءرفتاری مضرّ از یک سیستم هوش‌مصنوعی رخ می‌دهد، بستگی دارد (Königs, op. cit.: 6).

به‌هر ترتیب و با لحاظ آنچه که موردبحث قرارگرفت، مسئله درمورد اِمکان لحاظ بی‌پروایی به‌عنوان وجهی‌از عنصر معنوی جنایت موضوع این‌مقاله هم‌چنان پابرجاست. پذیرفتن نظر دوم نیز مستلزم آن است که عاملْ بتواند خطر را درک کند امّا به‌سادگی بدان بی‌اعتنا باشد یا آن را نادیده بگیرد (Fletcher, 1998: 115). با توجه‌به اینکه مبرهن است استعداد و توانایی هوش‌مصنوعی برای تجزیه‌وتحلیل داده‌ها، هدف‌گیری و سایر تصمیمات، درحال‌حاضر بسیار فراتر از توانایی‌های انسانی‌ست، توانایی عاملِ انسانی برای درک یک خطرِ مشخص در رفتار هوش‌مصنوعی، به گونه‌ای که بتوان آن را مصداق بی‌پروایی دانست، جای سوال است!

هم‌چنین شایان‌ذکراست که عنصر معنوی سهل‌انگاری کیفری،[1] ممکن است در شرایطی که از سیستم‌های هوش‌مصنوعی برای ارتکاب تجاوز استفاده می‌شود، از بین برود. سهل‌انگاری کیفری، مستلزم نقض شدید وظیفهٔ مراقبت معقولِ فرد است، اما درمواردی‌که هوش‌مصنوعی به‌طور غیرقابل‌پیش‌بینی عمل کرده باشد، این‌اَمر ممکن است سطوح مناسب مراقبت انجام‌شده را مختل کند. یک رژیم سهل‌انگاری کیفری تلاش می‌کند تا عاملانی را که نتوانسته‌اند خطر قابل‌پیش‌بینی را درک‌کنند 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 این‌خواسته‌ها ممکن‌است برآورده شوند و یک سیستم هوش‌مصنوعی به‌گونه‌ای عمل نماید که نتیجه‌ای را ایجاد کند که مستلزم مسئولیت باشد. این‌اَمر به‌ویژه در زمینهٔ جنایت تجاوز جالب‌توجه است، زیرا در اینجا عنصر معنوی باید به آستانهٔ خاصی برسد تا به‌عنوان نقض آشکار[2] منشور سازمان‌ملل درنظرگرفته‌شود و در نتیجه، مادهٔ ۸ مکرّر را نقض کند. در واقع، اَعمال مداخله‌ایِ سطح پایین‌تر در یک کشور خارجی، به‌عنوان اَعمال

3. criminal negligence

2. manifest violation

ممنوعهٔ بین‌المللی مانند حملهٔ مسلحانه تلقی نشده‌اند (Schmitt, op. cit.: 334). به‌عبارت دیگر «با رعایت قاعدهٔ حداقلی، [عملیات سایبری] که صرفاً باعث تشویش‌خاطر یا تحریک می‌شوند، هرگز [به عنوان توسل به زور] تلقی نمی‌شوند» (Ibid: 328-356).

در نمونه‌های موجود از بیانیه‌های هنجار سایبری، کشورها تمایل دارند توافق‌کنند که مداخلهٔ سایبری سطح پایین، نقض اصول حقوقی بین‌المللی محسوب نمی‌شود. برای‌مثال، موضع استرالیا این‌است که اگر یک فعالیت سایبری، به آستانهٔ یک حملهٔ جنبشی، تحت حقوق بین‌الملل بشردوستانه برسد، قوانین حاکم‌بر چنین حملاتی در طول درگیری‌های مسلحانه، بر آن‌نوع فعالیت‌های سایبری اِعمال خواهد شد.[1] هم‌چنین موضع کاستاریکا این‌است که در فضای دیجیتال، عبور از آستانهٔ استفاده از زور، نَه به ابزارهای دیجیتال به‌کار رفته، بلکه به آثار عملیات سایبری بستگی دارد و عملیات سایبری انجام‌شده توسط یک دولت علیه دولت دیگر، در صورتی‌که آثار آن مشابه آثار ناشی‌از استفاده از سلاح‌های متعارف باشد، ممنوعیت استفاده از زور را نقض می‌کند.[2]

بنابراین، در جایی‌که مداخلهٔ سطح پایین‌تر با استفاده‌از هوش‌مصنوعی، در نظر گرفته‌شده و یا انجام شده‌باشد، اما آسیب در مقیاس بزرگ‌تری وارد شود، عاملْ احتمالاً مراقبت‌لازم برای مسئول‌قلمدادشدن تحت‌استاندارد سهل‌انگاری کیفری را نخواهد داشت. درجایی‌که یک عاملْ 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 ممکن‌است حقوق بین‌الملل کیفری، ارتباط بالقوهٔ بین کنترل تحت حقوق بین‌الملل کیفری (که همان ارتباط علّی ضروری‌ای است که مسئولیت کیفری را ایجاد می‌کند) و کنترل معنادار انسانی در چارچوب حقوق بین‌الملل بشردوستانه (یعنی میزان دخالت انسانی که برای اطمینان‌از مجازبودن یک‌فرد 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).

استفاده‌از 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 راه‌حلِ استفاده‌از سیستم‌های تسلیحاتی خودکار، از درک‌واقعی این‌گزاره شروع شود که وقتی از برخی ساختارها سود می‌بریم، [1] مجبور به پذیرش این‌نتیجه هستیم که وقتی این‌ساختارها 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 روی‌برگرداندن از پیامدهای ناخواستهٔ استفاده‌از سیستم‌های هوش‌مصنوعی، استدلال می‌کند که سیستم‌های هوش‌مصنوعی ناگزیر با هدفِ «ارتکاب یا تسهیل» جنایات جنگی و سایر «تهدیدات مخرب علیه اهداف دنیای واقعی» مورداستفاده قرارخواهندگرفت (Greipl, op. cit. : 1098). درمواردی‌که این رفتار عمدی منجر به آسیب پیش‌بینی‌نشده یا به‌طورخاص، آسیب به یک هدفِ ناخواسته شود، «گریپل» استدلال می‌کند که دکترین شرّ انتقال‌یافته [2] در حقوق جزای داخلی، می‌تواند راه‌حلی برای شکاف مسئولیت ناشی‌از آن ارائه‌دهد (Ibid : 1099).

ملاحظه می‌شود راه‌حل‌های زیادی برای پُرکردن شکاف مسئولیتی که برای حملات مبتنی‌بر هوش‌مصنوعی وجود دارد، به‌ویژه در مورد جنایات‌جنگی، پیشنهاد شده است، اما هم‌چنان اقدامات مرتبط‌با تجاوز سایبری، این راه‌حل‌ها را مختل می‌کند. به‌هر روی مقالهٔ حاضر، گزینهٔ دیگری را با دو پیش‌فرض ارائه می‌دهد. اولاً اینکه، مقالات پیشتر موردبحث ،دقت زیادی به خرج دادند تا نشان دهند که چگونه تفسیرهای پیشنهادی‌شان، به‌ویژه درمورد عنصر روانی، به‌طورعملی در لسانِ موجود اساسنامهٔ رم و رویهٔ قضایی دیوان بین‌المللی کیفری به‌کار گرفته شده‌اند، موضوعی که مقالهٔ حاضر عمدتاً به‌این‌دلیل که اثبات آن ممکن نیست، چنین تلاشی نمی‌کند. ثانیاً، این‌مقاله استدلال می‌کند از آنجا که مسئولیت کیفری مدرن تا به‌امروز بر این پیش‌فرض بنا شده‌است که عاملِ متفکر موجود برای مسئولیت، انسان است، ورود هوش‌مصنوعی به این معادله، مستلزم تفکّر خلاقانه‌ای

---

[1]. هوش‌مصنوعی و سامانه‌های تسلیحاتی خودکار، ساختارهایی قابل‌مشاهده و ملموس هستند.

2. transferred intent

است که توسط ساختار قوانین موجود محدود نشود، یعنی قوانینی‌که زمانی نوشته شده‌اند که آن پیش‌فرض، کاملاً درست و موجّه بوده‌است. براین‌اساس، این‌سوال 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 اِعمال شود؟ به‌عنوان پیشنهادِ خود: مسئولیت مطلق.

ب. جایگزین دیگر: مسئولیت مطلق

دکترین مسئولیت مطلق، نوعی مسئولیتِ بدون تقصیر (اردبیلی، ۱۴۰۴: ۷۸)، بیان می‌کند که مسئولیت می‌تواند از یک عمل آسیب‌زا ناشی‌شود، صرف‌نظر از سوءنیت یا تقصیر خاصّ عامل. در یک رژیم سهل‌انگاریِ استاندارد، عناصر موردنیاز شامل اثبات وظیفهٔ مراقبتِ عامل، نقض‌وظیفهٔ مذکور و اثبات اینکه این‌نقض باعث آسیب خاصی شده‌است، می‌باشد. مسئولیت‌مطلق، الزام‌به اثبات نقض وظیفه را از این زنجیره حذف می‌کند و در عوض، فقط مستلزم آن‌است که نشان داده‌شود عامل، رفتار مرتبطی را انجام داده و این‌رفتار باعث آسیب موردنظر شده‌است.

از منظر سیاست‌گذاری، مسئولیت‌مطلق به این‌گزاره اشاره دارد که قانون برای فعالیت‌های ذاتاً خطرناک، به این‌موضوع که فرد تاچه‌اندازه وظیفهٔ مراقبت خود را در انجام برخی اَعمال رعایت می‌کند، توجهی ندارد و لذا درجایی‌که این‌اَعمال انجام می‌شوند و آسیبی که مشخصهٔ آن اَعمال است حادث می‌شود، عامل [حمله] صرف‌نظر از سطح مراقبتش، مسئول آن آسیب است (Wendehorst, op. cit.: 159). این‌رویکرد برای حملات سایبری مبتنی‌بر هوش‌مصنوعی مناسب است که بدون‌تردید به‌دلیل غیرقابل پیش‌بینی‌بودن و غیرقابل مهاربودنشان که باعث می‌شود آسیب‌هایی فراتر از محدوده، حتی هدف موردنظر و به‌همان‌اندازه غیرقانونی وارد کنند، ذاتاً خطرناک به‌شمار می‌روند. این‌حملات نَه مرزهای حاکمیتی را رعایت می‌کنند و نَه شبکه‌های رایانه‌ای را که هدف قرار می‌دهند. این واقعیتی‌است که توسط کسانی‌که اقدام به استقرار آنها می‌کنند و تصمیم می‌گیرند دامنه و سرعت آثار خود را با هوش‌مصنوعی افزایش دهند، به‌خوبی شناخته شده‌است.

مسئولیت‌مطلق، علاوه‌بر اینکه درمورد یک فعالیت منحصراً خطرناک مناسب است، درمواردی‌که به‌طور معمول اثبات عناصر سهل‌انگاری بسیار دشوار است نیز مفید خواهدبود تا به انجا که نگرانی‌ای جدّی درمورد عدم اجرای کامل قانون ایجاد می‌کند و «هم‌چنین می‌تواند پاسخی مناسب باشد در جایی‌که اثبات چنین عناصری برای قربانی بسیار دشوار باشد، به‌طوری که الزام‌به چنین اثباتی منجر به ناکارآمدی شود» (Ibid: 159-160). این ممیّزه، با نمونه‌های موجود از حملات سایبری بزرگ و تحت‌حمایت دولت، مانند حملهٔ NotPetya سازگار است (Greenberg, op. cit.: note 3).

همان‌طور که در گزارش مربوط‌به آن آمده است: حتی بیش‌از یک‌سال پس‌از گسترش فاجعه‌بار این‌حمله، هنوز کارشناسان امنیت سایبری درمورد اسرار NotPetya بحث می‌کنند. نیت واقعی هکرها چه بود؟ کارکنان شرکت امنیتی ISSP در کی‌یف [...] معتقدند که این‌حمله نَه‌تنها برای تخریب، بلکه به‌عنوان تلاشی برای پاکسازی درنظرگرفته‌شده‌بود. از این گذشته، هکرهایی که ابتدا آن را راه‌اندازی کردند ماه‌ها دسترسی نامحدود به شبکه‌های قربانیان داشتند. علاوه‌بر وحشت و اختلالی که ایجاد کرد، NotPetya ممکن‌است شواهد جاسوسی یا حتی شناسایی برای خرابکاری‌های آینده را نیز از بین بُرده‌باشد (Ibid).

این نگرانی‌های دوگانه، یعنی خطر منحصربه‌فرد و ذاتی در به‌کارگیری هوش‌مصنوعی برای دخالت و یا آسیب‌رساندن به یک کشور خارجی، و چالش اثبات این سوءرفتار هنگامی‌که از طریق یک حملهٔ سایبری مبتنی‌بر هوش‌مصنوعی انجام می‌شود، مسئولیت‌مطلق را به یک راه‌حل جذاب برای شکاف مسئولیتیِ ایجادشده در رابطه‌با تجاوز سایبری مبتنی‌بر هوش‌مصنوعی تبدیل می‌کند.

این‌رویکرد، معیار مسئولیت استفاده‌از هوش‌مصنوعی را در ارتکاب تجاوز سایبری - آنچه‌که حقوق بین‌الملل کیفری به پیشگیری از آن علاقه دارد - بسیار حداقلی تعیین می‌کند و هدفِ تشویق به عدم‌استفاده از هوش‌مصنوعی در این‌زمینه را پیش‌می‌برَد. البته با این‌پیش‌فرض که اجتناب از استفاده از هوش‌مصنوعی در ارتکاب اَعمال مرتبط‌با تجاوز سایبری، نتیجهٔ مطلوبی است.

در اینجا نکته‌ای کلیدی وجود دارد. اینکه زمینهٔ تجاوز سایبری با زمینهٔ سیستم‌های تسلیحاتی خودمختار در تضاد است. برخی معتقدند که استفاده‌از هوش‌مصنوعی در اجرای فعالیت‌های نظامی مزایای ویژه‌ای دارد. برای مثال، مطالعات (Galliott 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.[1] اما در زمینهٔ جنایت تجاوز، این‌تعادل بین آسیب‌ها و مزایا قابل اِعمال نیست. مشارکت در رفتاری‌که منجر به جرم‌تجاوز می‌شود، آن‌چیزی‌است که قانونْ علاقهٔ وافری به منع آن دارد، زیرا هیچ شرایطی وجود ندارد که آن رفتار طبق حقوق بین‌الملل، عملی موجّه تلقی گردد. به‌این‌ترتیب، هیچ نگرانی درمورد کم‌اثر یا ناکارآمدکردن عملی که فی‌نفسه غیرقابل‌توجیه است وجود ندارد. این‌اَمر به‌ویژه با توجه‌به آنچه که درحال‌حاضر درمورد تأثیر هوش‌مصنوعی بر درگیری‌های بین کشورها می‌دانیم صادق است؛ اینکه اهداف بیشتری را با سرعت بیشتر تخریب می‌کند، دامنهٔ 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.

این‌سوال عملی باقی می‌مانَد که دقیقاً چه‌زمانی یک عمل تجاوزکارانه که از هوش‌مصنوعی استفاده می‌کند، وارد قلمرو مسئولیت‌مطلق می‌شود؟ به‌ویژه با ادغام بیشترِ هوش‌مصنوعی در زندگی روزمره و گنجاندن آن در ابزارهای فناورانه، این‌سوال قابل‌توجه است.

برای رسیدن‌به پاسخی دقیق، تحقیقات بیشتری لازم است، امّا این مقاله پیشنهاد می‌کند که در مواردی که میزان استفاده از هوش‌مصنوعی منجر به حمله‌ای فوق‌العاده خطرناک می‌شود، مسئولیت مطلق اِعمال گردد. با وام‌گرفتن از قانون مسئولیت‌مدنی ایالات‌متحده (U.S. Restatement., 2025)، این‌اَمر می‌تواند مستلزم آن باشد که دادگاه، موارد زیر را در نظر بگیرد: (۱) خطر اینکه آسیبِ ناشی از حمله زیاد باشد، (۲) ناتوانی متهم در

[1]. بحث درمورد اینکه آیا یک رژیم مسئولیت سختگیرانه برای سایر جنایات بین‌المللی، یعنی جنایات جنگی که با هوش‌مصنوعی انجام می‌شود، منطقی‌ست یا خیر، فراتر از محدودهٔ این‌مقاله است.

ازبین‌بردن خطر ازطریق اِعمال مراقبت معقول و (۳) میزانی که فعالیت موردنظر، اَمری رایج و مرسوم نیست. درمواردی‌که نقش هوش‌مصنوعی در یک حمله منجر به این شود که میزان آسیب ایجادشده به‌طور قابل‌توجهی بیشتر از آن چیزی باشد که بدون استفاده‌از هوش‌مصنوعی ممکن بود، یا در مواردی که استفاده‌از هوش‌مصنوعی، حمله را از توانایی متهم برای مهار آن خارج‌کرده‌باشد نیز این‌اَمر باعث ایجاد مسئولیت‌مطلق می‌شود.

نتیجه‌گیری

در این پژوهش، بررسی کردیم که چگونه حملات سایبری مبتنی‌بر هوش‌مصنوعی ممکن است به‌عنوان یک عمل تجاوزکارانه درنظرگرفته‌شوند. سپس به بررسی موانعی که بر سَر راه مسئولیت کیفری بین‌المللی ناشی‌از این رفتار وجود دارد پرداختیم. دراین‌راستا، اینکه تا چه‌حدّ می‌توان یک عمل تجاوزکارانهٔ انجام‌شده توسط یک سیستم هوش‌مصنوعی را به‌عنوان فعل مجرمانه درنظرگرفت، جای‌سوال است.

چالش‌برانگیزتر از آن، ناسازگاری تجاوز سایبری با عنصر روانیِ مسئولیت کیفری در پرتو مادهٔ ۳۰ اساسنامهٔ دیوان بین‌المللی کیفری است. از آنجایی که عنصر روانی جرم تجاوز، ترکیبی از قصد و آگاهی است، بسیاری‌از صاحب‌نظران استدلال می‌کنند که قابل‌انطباق با حملات سایبری مبتنی‌بر هوش‌مصنوعی نیست. در پاسخ، دیگر محققان، حالات روانی خفیف‌تر نظیر بی‌پروایی را پیشنهاد کرده‌اند که به‌طور عملی‌تری، حالت روانی یک عامل را که با تکیه‌بر هوش‌مصنوعی حملهٔ سایبری انجام می‌دهد به تصویر می‌کشد.

علاوه بر راه‌حل‌های موجود در آثار حقوقدانان بین‌الملل کیفری، این‌مقاله با پیشنهاد یک سیستم مسئولیت مطلق برای اَعمال تجاوز سایبری انجام‌شده با هوش‌مصنوعی، یک گام فراتر رفت. این‌اَمر چالش فنّیِ شناسایی وضعیت روانیِ عامل انسانی (در فرض کنش‌گریِ انسان) را با توجه به غیرقابل پیش‌بینی‌بودن و ابهام هوش‌مصنوعی برطرف می‌کند. هم‌زمان، این‌اَمر به نفع سیاست‌گذاری‌ای است که حملات سایبریِ مبتنی‌بر هوش‌مصنوعی به کشورهای خارجی را به‌عنوان فعالیتی ذاتاً خطرناک که فی‌نفسه مسئولیت کاربر انسانی را به همراه دارد، در نظر می‌گیرد. هم‌چنین این پیشنهاد ممکن است باعث کاهش انگیزهٔ استفاده از هوش‌مصنوعی در ارتکاب تجاوز سایبری، به‌عنوان رفتاری همواره نامطلوب گردد.

اگرچه پیشنهاد کاربردی این پژوهش، با محدودیت‌ها و چشم‌اندازهای موهومی در موقع اِعمال همراه است و این‌مقاله تلاش نمود تا موانع مفهومی را از گزینه‌های مرسوم دور کند، زیرا هوش‌مصنوعی، درک رایج از نقش انسان‌ها در اَعمال غیرقانونی بین‌المللی را مختل نموده‌است، امّا از برآیند آنچه شرح داده‌شد این نتیجه به‌دست می‌آید که عناصر مسئولیت کیفری یک‌عمل تجاوزکارانه به‌شرح اساسنامۀ دیوان بین‌المللی کیفری، در ساختار و تفسیر فعلی خود، ظرفیت لازم را برای تطبیق با تجاوز سایبریِ انجام‌شده از طریق سیستم‌های مبتنی‌بر هوش‌مصنوعیِ تحت‌حمایت دولت ندارند.

به‌عبارت دیگر، هرچند موضوع صلاحیت دیوان بین‌المللی کیفری، درحال گسترش است و نَه کاهش و اساسنامۀ دیوان نیز آمادۀ اصلاح، تغییر، توسعه، تعریف و بازتعریف جرایم جدید و آینده است و این‌اَمر به‌صراحت در سند تأسیس دیوان منظور شده‌است (Morris, 2002 : 598) و صرف‌نظر از ابهام درمورد عنصر مادّی و سخت‌گیری دربارۀ عنصر معنوی (با لحاظ برخی‌نظریات که بیان می‌دارد باید عنصر معنویِ تجاوز سایبری را به‌دلیل پیچیدگیِ مرتبط با ضریبِ خطر، تقلیل داد که البته این اظهار، در تعارض‌با اصول قانونی‌بودن و تفسیر مضیّق مندرج در مادّۀ ۲۲(۲) اساسنامۀ رم قرار دارد، به‌شرحی که در مقاله گذشت)، این اِمکان وجود دارد که میان تعقیب حملۀ سایبری مبتنی‌بر هوش‌منصوعی تحت‌عنوان تجاوز، با دکترین صلاحیت دیوان بین‌المللی کیفری در تعقیب اشخاص‌حقیقی (مندرج در مادۀ۲۵ اساسنامۀ رم) نیز ناسازگاری های مفهومی پدید آید.

هم‌چنین حملۀ سایبری، صرف‌نظر از خشونت نهفته در آن که از بسیاری جهات می‌تواند موردبررسی و تحلیل قرار گیرد (مهرا و کارگری، ۱۴۰۱: ۶۸۱-۷۰۱) غالباً نَه از رهگذر فعلیْ معیّن، که در نتیجۀ نقش‌آفرینیِ مجموعه‌ای از عوامل حادث می‌شود و در نتیجه، وظیفۀ دادستان در اثبات مجرمیت متهم از طریق جمع‌آوری ادلّه و احراز رابطۀ سببیت میان فعل ارتکابی و خسارت‌وارده بسیار دشوار خواهد بود.

و اینکه در نهایت، توسل‌به سازِکار عدالت کیفری بین‌المللی، باید به‌عنوان هستۀسخت و آخرین راه‌حل در مواجهه با نقض ممنوعیت‌های پذیرفته‌شده باشد، به‌خصوص به‌دلیل قوانین سایبریِ متناسب، واجدِ اثر و کاربردی در حقوق داخلی، که مانع‌از بی کیفری متجاوزان سایبری است و دامنۀ مسئولیت در نتیجۀ این مقررات، بسط پیدا می‌کند (نوریان، ۱۳۹۶: ۲۷-۳۰).

فهرست منابع

فارسی

۱- ابوذری، مهرنوش،(۱۴۰۲) حقوق و هوش‌مصنوعی، تهران: نشر میزان، چاپ سوم.

۲- .اردبیلی، محمدعلی، علیرضا محقق‌هرچگان، ابراهیم بیگ‌زاده و محمدعلی مهدوی‌ثابت، (۱۴۰۳)«حقوق بین‌الملل سایبری و توسعهٔ صلاحیت دیوان کیفری بین‌المللی (با تأکید بر مذاکرات تالین ۲۰۱۷میلادی)»، مطالعات حقوق عمومی، ۵۳، ۳ (۱۴۰۲)، ۱۵۳۷-۱۵۵۹.

۳- .اردبیلی، محمدعلی، حقوق جزای عمومی، جلد نخست، تهران: نشر میزان، ویراست‌پنجم، چاپ هفتادوچهارم.

۴- .اردبیلی، محمدعلی، (۱۴۰۳)حقوق جزای عمومی، جلد دوم، تهران: نشر میزان، ویراست‌ششم، چاپ شصت‌وپنجم.

۵- .اردبیلی، محمدعلی، (۱۳۹۷)«دیوان کیفری بین‌المللی و نظریهٔ 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- .پیری، حیدر، (۱۴۰۱)، «مسئولیت بین‌المللی دولت‌ها در ارتباط‌با کاربست سلاح‌های مبتنی‌بر هوش‌مصنوعی در درگیری‌های مسلحانه»، حقوق فناوری‌های نوین، ۶، ۱۲، ۱۶۹-۱۹۳.

۸- .قیاسی، جلال‌الدین و ایمان محترم قلاتی، (۱۳۹۳)، «تحلیل عنصرمحور 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 حقوق‌کیفری پویا (مجموعه مقاله‌ها در پاسداشت استاد دکتر محمدعلی اردبیلی)، ۶۸۱-۷۰۱، به‌کوشش نسرین مهرا و امیرحسن نیازپور، تهران: بنیادحقوقی میزان، ۱۴۰۱.

۱۰- .نوریان، علیرضا، آیین دادرسی جرایم رایانه‌ای و مخابراتی، تهران: نشر میزان، ۱۳۹۶.

۱۱-. نوریان، علیرضا، «مستندسازی ادلّهٔ الکترونیکی در تحقیقات پیش‌دادرسی کیفری از نگاه رویهٔقضایی»، در مجموعه مقالات اولین همایش ملّی رویارویی با جرایم سایبری؛ چالش¬ها و راهکارها، جلد اول، تهران: دانشگاه علوم‌انتظامی 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, n°1, 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 Tsagourias, "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, n°1, 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- . Galliott, 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- . Tsagourias, 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.

اَسناد 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-prose cutor-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 Mach 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).