مسئولیت کیفری ناشی از حملات مبتنی بر اینترنت اشیا به مثابه جنایت جنگی در پرتو حقوق بین‌الملل کیفری

سیده مهشید میری بالاجورشری[۱]، امیررضا محمودی*[۲]، بابک پورقهرمانی[۳]

چکیده

گسترش فناوری‌های مبتنی بر اینترنت اشیا و پیوند روزافزون سامانه‌های دیجیتال با زیرساخت‌های فیزیکی، ابعاد نوینی از عملیات سایبری و سایبر-فیزیکی را در مخاصمات مسلحانه پدید آورده است. این تحول، پرسش‌های مهمی را درباره امکان انطباق عملیات مبتنی بر اینترنت اشیا با عناوین جنایات جنگی، حدود مسئولیت کیفری بازیگران انسانی و چگونگی انتساب رفتار مجرمانه در محیط‌های دیجیتال مطرح می‌سازد. در عین حال، ناشناسی سایبری، استفاده از سامانه‌های نیمه‌خودکار، حضور بازیگران خصوصی و دشواری تفکیک میان انتساب فنی، دولتی و کیفری، چالش‌های جدی در اعمال قواعد حقوق بین‌الملل کیفری ایجاد کرده است. هدف این پژوهش، بررسی ظرفیت و چگونگی اعمال قواعد حقوق بین‌الملل کیفری، به‌ویژه مقررات اساسنامه رم، بر عملیات مبتنی بر اینترنت اشیا در مخاصمات مسلحانه و تحلیل مبانی انتساب مسئولیت کیفری برای اشخاص دخیل در این عملیات است. این پژوهش با روش توصیفی-تحلیلی و با بهره‌گیری از منابع کتابخانه‌ای و تحلیل مقررات اساسنامه رم انجام شده است. یافته‌های پژوهش نشان می‌دهد در عملیات مبتنی بر اینترنت اشیا رفتارهایی نظیر حملات کور، حمله به زیرساخت‌های غیرنظامی و مراکز درمانی، یا تخریب گسترده اموال می‌توانند مشمول عناوین جنایات جنگی قرار گیرند و مهم‌ترین چالش در این حوزه، مسئله انتساب مسئولیت کیفری و بازسازی زنجیره تصمیم‌گیری و کنترل در محیط‌های دیجیتال و متصل است. نتایج پژوهش حاکی از آن است که تحول فناوری، شیوه ارتکاب و سازمان‌دهی عملیات نظامی را تغییر داده است و پاسخ حقوقی مناسب در توسعه تفسیرهای تخصصی، تقویت سازوکارهای انتساب، ارتقای استانداردهای ادله دیجیتال و حفظ زنجیره انسانی تصمیم‌گیری در عملیات مبتنی بر اینترنت اشیا نهفته است.

واژگان کلیدی: اینترنت اشیا، جنایات جنگی، مسئولیت کیفری، حقوق بین‌الملل کیفری.

[۱]. گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. s.miribalajorshari@iau.ac.ir

[۲]. گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. (نویسنده مسئول) dr.mahmoudi@iau.ac.ir

[۳]. گروه حقوق کیفری و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران. pourghahramani@iau.ac.ir

مقدمه

تحول شتابان فناوری‌های دیجیتال در دهه‌های اخیر، ساختار بسیاری از روابط اجتماعی، اقتصادی، امنیتی و نظامی را دگرگون کرده است. در این میان، اینترنت اشیا[4] به‌عنوان یکی از مهم‌ترین جلوه‌های همگرایی فضای سایبری و محیط فیزیکی، زمینه اتصال گسترده دستگاه‌ها، سامانه‌ها و زیرساخت‌های حیاتی را فراهم ساخته است. اینترنت اشیا صرفاً محدود به ابزارهای مصرفی و خدمات روزمره نیست، بلکه به‌تدریج در حوزه‌های حساس و راهبردی همچون زیرساخت‌های انرژی، سامانه‌های حمل‌ونقل، تجهیزات پزشکی، صنایع دفاعی، شبکه‌های کنترل صنعتی و ساختارهای فرماندهی و کنترل نظامی نیز نفوذ کرده است. این تحول، ضمن ایجاد ظرفیت‌های گسترده عملیاتی، مخاطرات نوینی را نیز در بستر مخاصمات مسلحانه پدید آورده است؛ به‌گونه‌ای که حمله به سامانه‌های متصل می‌تواند بدون استفاده از ابزارهای متعارف خشونت، آثار انسانی و مادی گسترده‌ای برجای گذارد. گسترش عملیات سایبری و سایبر-فیزیکی در سال‌های اخیر نشان داده است که محیط‌های متصل و زیرساخت‌های مبتنی بر اینترنت اشیا، به اهداف بالقوه عملیات نظامی و امنیتی تبدیل شده‌اند. در چنین شرایطی، پرسش‌های مهمی درباره امکان انطباق این عملیات با عناوین موجود جنایات جنگی، حدود مسئولیت کیفری اشخاص دخیل، نحوه اعمال اصول بنیادین حقوق بشردوستانه و چگونگی انتساب رفتار مجرمانه در محیط‌های پیچیده دیجیتال مطرح می‌شود. هرچند حقوق بین‌الملل کیفری بر مبنای رفتارهای سنتی و عمدتاً فیزیکی شکل گرفته است، اما تحول فناوری ضرورت بازخوانی و تفسیر قواعد موجود در پرتو ویژگی‌های عملیات مبتنی بر اینترنت اشیا را اجتناب‌ناپذیر ساخته است. در این میان، یکی از مهم‌ترین چالش‌ها، مسئله انتساب مسئولیت کیفری در محیط‌های چندلایه و غیرمتمرکز دیجیتال است. در بسیاری از عملیات مبتنی بر اینترنت اشیا، نتیجه زیان‌بار حاصل تعامل مجموعه‌ای از عوامل انسانی و فنی، از جمله فرماندهان، اپراتورها، برنامه‌نویسان، شرکت‌های خصوصی، سامانه‌های نیمه‌خودکار، بدافزارها و زیرساخت‌های ابری است. افزون بر این، ناشناسی سایبری، عملیات پرچم دروغین، استفاده از شبکه‌های واسط و بهره‌گیری از دستگاه‌های آلوده متعلق به اشخاص ثالث، فرایند شناسایی مرتکب واقعی و اثبات رابطه میان رفتار و نتیجه را با دشواری جدی مواجه می‌سازد. ازاین‌رو، تفکیک میان انتساب فنی، انتساب دولتی و انتساب کیفری فردی، در تحلیل مسئولیت کیفری ناشی از عملیات مبتنی بر اینترنت اشیا، اهمیتی بنیادین پیدا می‌کند. از سوی دیگر، استفاده روزافزون از سامانه‌های خودکار و نیمه‌خودکار در عملیات نظامی، پرسش‌هایی اساسی درباره حدود کنترل انسانی، مسئولیت فرماندهان و جایگاه عنصر روانی در حقوق بین‌الملل کیفری ایجاد کرده است. اگرچه ماشین و الگوریتم واجد مسئولیت کیفری نیستند، اما پیچیدگی فنی سامانه‌ها ممکن است زنجیره تصمیم‌گیری انسانی را مبهم ساخته و خطر ایجاد شکاف پاسخگویی را افزایش دهد. در نتیجه، بررسی قابلیت اعمال مواد ۲۵ و ۲۸ اساسنامه رم بر عملیات سایبری- فیزیکی و اینترنت اشیا، به یکی از مباحث مهم و نوظهور در حقوق بین‌الملل کیفری تبدیل شده است.

پژوهش حاضر با رویکردی توصیفی- تحلیلی و با تکیه بر قواعد حقوق بشردوستانه، مقررات اساسنامه رم و رویه و ادبیات موجود در حوزه حقوق بین‌الملل کیفری، درصدد بررسی این پرسش است که عملیات مبتنی بر اینترنت اشیا تحت چه شرایطی می‌تواند مشمول عناوین جنایات جنگی قرار گیرد و مسئولیت کیفری اشخاص دخیل در این عملیات بر چه مبانی و معیارهایی قابل انتساب است. همچنین، این پژوهش می‌کوشد با تحلیل چالش‌های انتساب، کنترل مؤثر، ادله دیجیتال و نقش بازیگران خصوصی و سامانه‌های نیمه‌خودکار، ظرفیت‌ها و محدودیت‌های چارچوب کنونی حقوق بین‌الملل کیفری را در مواجهه با تحولات فناورانه ارزیابی کند.

[4] Internet of Things (IoT)

۱. مفهوم‌شناسی اینترنت اشیا و سامانه‌های سایبری- فیزیکی در بستر مخاصمات مسلحانه

براساس تعریف اتحادیه بین المللی مخابرات[5]، اینترنت اشیا زیرساختی برای راه‌اندازی یک شبکه جهانی پویا همراه با قابلیت خودپیکربندی می‌باشد و مبتنی بر پروتکل‌های ارتباطی استاندارد و سازگار با سایر بخش‌های شبکه است. در این زیرساخت، اشیای فیزیکی و مجازی دارای هویت مستقل، ویژگی‌های فیزیکی مشخص و شخصیت مجازی بوده و از طریق واسط‌های هوشمند، با شبکه اطلاعاتی یکپارچه شده‌اند. به عبارت دیگر اینترنت اشیا زیرساختی جهانی برای جامعه اطلاعاتی است که با بهره‌گیری از تعامل و ارتباط میان اشیای فیزیکی و مجازی، امکان ارائه خدمات نوین و پیشرفته را فراهم می‌سازد. (ITU-T Y2060, 2012) در این تعریف، اینترنت اشیا به‌عنوان بستری پویا و در حال تکامل معرفی می‌شود که قادر است از ظرفیت‌های موجود در فناوری‌های اطلاعاتی و ارتباطی برای ایجاد ارتباطات هوشمند میان افراد، اشیا و سامانه‌ها استفاده کند.

از سوی دیگر، سازمان همکاری و توسعه اقتصادی در تعریفی، اینترنت اشیا را مجموعه‌ای از دستگاه‌ها و اشیایی معرفی می‌کند که وضعیت یا حالت آن‌ها می‌تواند از طریق شبکه اینترنت، با یا بدون دخالت مستقیم انسان، تغییر کند. (OECD, 2023: 12)

در این پژوهش، اینترنت اشیا نه در معنای ابزارهای مصرفی، بلکه به‌عنوان اکوسیستمی پیچیده از حسگرها، عملگرها و سامانه‌های پردازش داده در کالبد سامانه‌های سایبری- فیزیکی تحلیل می‌شود. در این سامانه‌ها، پردازش دیجیتال و کنش فیزیکی چنان در هم تنیده‌اند که رفتار سامانه حاصل تعامل مستمر این دو قلمرو است. (Greer, et al. 2019: 10) اهمیت این پیوند برای حقوق بین‌الملل کیفری در قابلیت تبدیلِ داده به اثر عینی نهفته است؛ جایی که دستکاری داده‌های ورودی (حسگرها) یا فرامین خروجی (عملگرها) می‌تواند به نتایج مجرمانه‌ای همچون حمله به اهداف غیرنظامی، انفجار زیرساخت‌های حیاتی یا مرگ بیماران در مراکز درمانی متصل منجر شود. (McKenzie, 2021: 1166) از منظر حقوقی، معیار شمول قواعد بر این فناوری، وابستگی آن به اینترنت عمومی یا پروتکل‌های متعارف نیست؛ بلکه در کاربردهای نظامی و صنعتی، ملاک اصلی تحقق عناصر جرم، احراز رابطه سببیت میان دستورات دیجیتال و نتایج فیزیکی، و نقش عامل انسانی در این زنجیره است. (ENISA, 2020: 10)

اینترنت اشیا دارای ویژگی‌هایی است که تحلیل حقوقی آن را در بستر مخاصمات مسلحانه پیچیده می‌سازد. نخست، اتصال‌پذیری و وابستگی متقابل میان دستگاه‌ها، حسگرها و سامانه‌های پردازشی موجب می‌شود حمله به یک جزء، آثار خود را به زیرساخت‌های وابسته غیرنظامی مانند شبکه‌های درمانی، انرژی، آب و حمل‌ونقل نیز تسری دهد. دوم، در این سامانه‌ها داده صرفاً کارکرد اطلاعاتی ندارد، بلکه می‌تواند منشأ آثار فیزیکی باشد؛ ازاین‌رو، دستکاری داده‌ها ممکن است رفتار سامانه‌ها یا تصمیمات انسانی را تغییر داده و مرز میان حمله به داده و حمله به اشیای فیزیکی را مبهم سازد. سوم، ساختار چندلایه و چندبازیگری اینترنت اشیا، شامل تولیدکنندگان تجهیزات، توسعه‌دهندگان نرم‌افزار، ارائه‌دهندگان خدمات و بهره‌برداران، مسئله انتساب و تعیین مسئولیت را پیچیده می‌کند. چهارم، خودکار یا نیمه‌خودکار بودن این سامانه‌ها، اگرچه مسئولیت کیفری را متوجه ماشین نمی‌سازد، اما کانون مسئولیت انسانی را به مراحل طراحی، استقرار، نظارت و کنترل عملیات منتقل می‌کند. (Sebestyen, et al. 2025: 14) افزون بر این، اینترنت اشیا در مخاصمات مسلحانه می‌تواند به‌عنوان ابزار ارتکاب جرم، موضوع حمله، محیط عملیاتی و نیز منبع ادله ایفای نقش کند. بر این اساس، اینترنت اشیا باید به‌عنوان سامانه‌ای سایبری- فیزیکی و چندلایه تحلیل شود که در آن رفتار مجرمانه ممکن است از سطح داده آغاز شده و به پیامدهای فیزیکی و انسانی منتهی گردد؛ وضعیتی که تفکیک میان ابعاد فنی، عملیاتی و کیفری مسئولیت را ضروری می‌سازد.

---

[5] International Telecommunication Union (ITU)

۲. قابلیت اعمال حقوق بشردوستانه بین‌المللی بر عملیات مبتنی بر اینترنت اشیا

پیش از آنکه بتوان عملیات مبتنی بر اینترنت اشیا را جنایت جنگی دانست، باید جایگاه آن در حقوق بشردوستانه بین‌المللی روشن شود. حقوق بین‌الملل کیفری در حوزه جنایات جنگی بر نقض‌های جدی حقوق بشردوستانه بنا شده است. (ساعد، ۱۳۹۳: ۳۱) بنابراین، نمی‌توان مستقیماً از نفوذ به سامانه متصل یا دستکاری حسگر به جنایت جنگی گذر کرد؛ مرحله میانی آن است که رفتار در بستر مخاصمه مسلحانه و در چارچوب قواعد حقوق بشردوستانه تحلیل شود. حقوق بشردوستانه از حیث ابزار ارتکاب، نظامی بسته و ایستا نیست. قواعد بنیادین آن به تفنگ، توپخانه، موشک یا بمب اختصاص ندارد. هر وسیله یا روش جنگی، اعم از قدیم یا جدید، اگر در مخاصمه مسلحانه به کار رود، باید با قواعد تمایز، تناسب، احتیاط، ضرورت نظامی و انسانیت سنجیده شود. (ممتاز و شایگان، ۱۳۹۷: ۲۲)

شرط اساسی برای اعمال حقوق بین‌الملل بشردوستانه، وجود مخاصمه مسلحانه و احراز ارتباط عملیات با آن است. ازاین‌رو، هر حمله سایبری یا عملیات مبتنی بر اینترنت اشیا، صرف‌نظر از میزان خسارت یا آثار زیان‌بار آن، لزوماً جنایت جنگی محسوب نمی‌شود؛ بلکه باید در بستر یک مخاصمه مسلحانه بین‌المللی یا غیربین‌المللی ارتکاب یافته و با آن دارای پیوند کافی باشد. احراز این پیوند می‌تواند بر اساس عواملی نظیر هدف عملیات، زمینه وقوع، آثار و نتایج رفتار، هویت طرف‌های درگیر و کارکرد عملیاتی آن صورت گیرد. (ممتاز و رنجبریان، ۱۳۹۵: ۳۴) در این میان، محل فیزیکی مرتکب نیز نقش تعیین‌کننده‌ای ندارد؛ بنابراین، حتی اگر عملیات از قلمرو دولت ثالث یا از طریق زیرساخت‌های فراملی انجام شود، در صورت وجود ارتباط واقعی و مؤثر با مخاصمه، قواعد حقوق بین‌الملل بشردوستانه بر آن حاکم خواهد بود. (ICC, 2013: 24)

اینترنت اشیا در مخاصمات مسلحانه می‌تواند به‌عنوان وسیله یا روش جنگی مورد استفاده قرار گیرد؛ زیرا در این سامانه‌های سایبری- فیزیکی، دستکاری داده قادر است فرایندهای فیزیکی را تغییر دهد و آثار واقعی ایجاد کند. (Greer, et al. 2019: 11) با این حال، یکی از مسائل مهم در این زمینه، تفسیر مفهوم «حمله» است. مطابق ماده ۴۹ پروتکل الحاقی اول به کنوانسیون‌های ژنو، حمله به معنای اعمال خشونت علیه دشمن در وضعیت آفندی یا پدافندی است. (AP I, 1977: art. 49) در محیط اینترنت اشیا، این خشونت لزوماً به‌صورت متعارف و از طریق انفجار یا استفاده از سلاح‌های سنتی ظاهر نمی‌شود، بلکه ممکن است از طریق دستکاری داده حسگرها، آلودگی سفت‌افزار یا ارسال فرمان‌های دیجیتال به سامانه‌های متصل تحقق یابد. هرگاه چنین اقداماتی به مرگ، جراحت، تخریب یا ازکارافتادگی شدید منتهی شود، امکان تحلیل آن در قلمرو مفهوم حمله تقویت می‌شود.

اصل تمایز در عملیات مبتنی بر اینترنت اشیا دو بعد دارد: تمایز میان اشخاص و تمایز میان اشیا. از نظر اشخاص، غیرنظامیان فقط زمانی و برای مدتی حمایت خود در برابر حمله را از دست می‌دهند که مستقیماً در مخاصمات شرکت کنند. در محیط دیجیتال، کارکنان شرکت‌های فناوری، مهندسان شبکه، اپراتورهای بیمارستان یا کاربران دستگاه‌های متصل صرفاً به دلیل حضور در زنجیره فنی هدف مشروع حمله نمی‌شوند. (AP I, 1977: art. 48) از نظر اشیا نیز باید میان اهداف نظامی و اموال غیرنظامی تفکیک شود. سامانه‌های شهری، درمانی، صنعتی، ابری یا ارتباطی ممکن است کارکرد دوگانه داشته باشند و همین امر تحلیل را دشوار می‌کند. زیرساخت‌های دوگانه از مهم‌ترین مسائل اینترنت اشیا هستند. شبکه برق، مخابرات، حمل‌ونقل، آب‌رسانی، مراکز داده، سامانه‌های ابری و شبکه‌های حسگر شهری ممکن است هم به نظامیان و هم به غیرنظامیان خدمت دهند. وجود استفاده نظامی محدود، حمله به کل زیرساخت را مجاز نمی‌کند. (Henckaerts, Doswald-Beck, 2005: Rules 7-8)

منع حملات کور در عملیات مبتنی بر اینترنت اشیا از اهمیت ویژه‌ای برخوردار است؛ زیرا ابزارهایی که امکان هدایت دقیق یا محدودسازی آثار آن‌ها وجود ندارد، ممکن است با اصل تمایز تعارض پیدا کنند. در این چارچوب، بدافزارهای خودانتشار و حملاتی که توان تفکیک میان اهداف نظامی و غیرنظامی را ندارند، خطر نقض ممنوعیت حملات کور را افزایش می‌دهند.

اهمیت این مسئله در محیط اینترنت اشیا بیشتر است؛ زیرا سامانه‌های متصل علاوه بر پردازش داده، کنترل فرایندهای فیزیکی را نیز برعهده دارند و اختلال در آن‌ها می‌تواند پیامدهای مستقیم انسانی و خسارات فیزیکی گسترده ایجاد کند. (AP I, 1977: art. 51(4))

اصل تناسب در بستر عملیات مبتنی بر اینترنت اشیا باید با درنظرگرفتن ماهیت به‌شدت به‌هم‌پیوسته و وابسته زیرساخت‌ها تفسیر شود. در چنین محیطی، ارزیابی آثار یک حمله صرفاً به پیامدهای مستقیم بر هدف نظامی محدود نمی‌ماند، بلکه شامل پیامدهای غیرمستقیم و زنجیره‌ای (آثار آبشاری[6]) نیز می‌شود. (شریفی طرازکوهی و صیادنژاد، ۱۳۹۹: ۵۶۰) برای مثال، حمله به شبکه برق یا سامانه‌های حمل‌ونقل هوشمند می‌تواند موجب اختلال گسترده در خدمات حیاتی نظیر بیمارستان‌ها، سامانه‌های امدادی و زنجیره تأمین دارو شود. (ICRC, 2024: 10) بر این اساس، در چارچوب حقوق بین‌الملل بشردوستانه، ارزیابی تناسب در عملیات مبتنی بر اینترنت اشیا مستلزم لحاظ کلیه آثار قابل پیش‌بینی، اعم از مستقیم و غیرمستقیم، بر جمعیت و زیرساخت‌های غیرنظامی است. (رنجبریان و بذّار، ۱۳۹۷: ۷۱)

در نهایت، حمایت ویژه از بیمارستان‌ها، تجهیزات پزشکی متصل و اشیای ضروری برای بقای جمعیت غیرنظامی در این حوزه اهمیت مضاعف دارد؛ زیرا امروزه کارکرد بسیاری از این زیرساخت‌ها به سامانه‌های متصل و خدمات دیجیتال وابسته شده است و حمله به لایه دیجیتال آن‌ها می‌تواند همان آثار حمله مستقیم فیزیکی را ایجاد کند. (Schmitt, 2017: 50) بنابراین، عملیات مبتنی بر اینترنت اشیا در صورت وجود مخاصمه و ارتباط کافی با آن، مشمول قواعد حقوق بین‌الملل بشردوستانه خواهد بود، هرچند صرف نقض این قواعد به‌تنهایی برای تحقق جنایت جنگی کافی نبوده و باید امکان انطباق رفتار با عناوین مقرر در ماده ۸ اساسنامه رم نیز بررسی شود.

۳. امکان تحقق جنایات جنگی موضوع ماده ۸ اساسنامه رم از طریق عملیات مبتنی بر اینترنت اشیا

تحلیل جنایات جنگی در بستر اینترنت اشیا، مستلزم تطبیق این فناوری با عناوین موجود در ماده ۸ اساسنامه رم است، نه ابداع جرایم جدید. نقطه عزیمت این تحلیل، اصل قانونی بودن است. ماده ۲۲ اساسنامه رم مقرر می‌کند که شخص فقط زمانی مسئول است که رفتار او در زمان ارتکاب، جرم داخل در صلاحیت دیوان باشد و تعریف جرم باید مضیق تفسیر شود. (Rome Statute, 1998: art. 22) با این حال، تفسیر مضیق به معنای انجماد مفاهیم نیست و عناوین ماده ۸ از حیث ابزار ارتکاب به شیوه‌های سنتی محدود نشده‌اند. بر این اساس، عملیات مبتنی بر اینترنت اشیا در صورتی جنایت جنگی محسوب می‌شود که علاوه بر احراز رابطه با مخاصمه، عناصر مادی و روانی یکی از عناوین ذیل را محقق سازد.

نخستین عنوان قابل طرح، حمله عمدی علیه غیرنظامیان است. هرگاه عملیات مبتنی بر اینترنت اشیا با هدف مستقیم آسیب به غیرنظامیان، مانند اختلال در تجهیزات پزشکی یا سامانه‌های شهری، انجام شود، می‌تواند ذیل این عنوان قرار گیرد. عنصر اساسی در اینجا، جهت‌گیری عمدی حمله به سوی غیرنظامیان است.[7] (Rome Statute, 1998: art. 8(2)(b)(i))

دومین عنوان، حمله عمدی علیه اموال غیرنظامی است. زیرساخت‌ها و سامانه‌های متصل، از جمله شبکه‌های برق، حمل‌ونقل، تجهیزات درمانی و مراکز داده، در صورت نداشتن وصف هدف نظامی، اموال غیرنظامی محسوب می‌شوند و حمله عمدی به

---

[6] cascade effect

[7]. ماده ۸(۲)(ب)(۱) اساسنامه رم «حملات عمدی بر علیه غیرنظامیان با قصد حمله علیه آنان، یا افراد غیرنظامی که مستقیماً در این مخاصمات شرکت ندارند» را در مخاصمات مسلحانه بین‌المللی جنایت جنگی می‌داند.

آن‌ها می‌تواند جنایت جنگی باشد. در زیرساخت‌های دوگانه نیز صرف استفاده نظامی محدود، حمله به کل سامانه را توجیه نمی‌کند. (Rome Statute, 1998: art. 8(2)(b)(ii))[۸]

سومین عنوان، حمله نامتناسب است. مطابق ماده ۸(۲)(ب)(۴)، حمله‌ای که با علم به ایجاد خسارات تبعی آشکارا بیش از حد نسبت به مزیت نظامی مورد انتظار انجام شود، جنایت جنگی محسوب می‌شود. اینترنت اشیا به دلیل آثار آبشاری، بستر مهمی برای این عنوان است؛ زیرا اختلال در یک زیرساخت، مانند شبکه برق، می‌تواند به آسیب گسترده خدمات غیرنظامی منجر شود. در اینجا، احراز علم مرتکب به خسارات نامتناسب اهمیت اساسی دارد. (Rome Statute, 1998: art. 8(2)(b)(iv))[۹]

چهارمین عنوان، تخریب گسترده اموال بدون وجود ضرورت نظامی است. در عملیات مبتنی بر اینترنت اشیا، حمله به زیرساخت‌های متصل مانند شبکه‌های انرژی، آب‌رسانی یا سامانه‌های صنعتی می‌تواند موجب ازکارافتادگی گسترده اموال حمایت‌شده شود. با این حال، صرف اختلال موقت کافی نیست و تحقق این عنوان مستلزم احراز خسارت گسترده و فقدان ضرورت نظامی است. (Rome Statute, 1998: art. 8(2)(a)(iv))[۱۰]

پنجمین عنوان، قتل عمدی و ایراد رنج شدید یا آسیب جدی است. دستکاری دستگاه‌های تنفس مصنوعی، پمپ‌های تزریق، تجهیزات مراقبت ویژه، سامانه‌های حمل‌ونقل خودکار، شبکه‌های هشدار یا سامانه‌های ایمنی صنعتی می‌تواند به مرگ یا آسیب شدید منتهی شود. (Rome Statute, 1998: arts. 8(2)(a)(i), 8(2)(a)(iii), 8(2)(c)(i))[۱۱]

ششمین عنوان قابل طرح، حمله به بیمارستان‌ها و واحدهای درمانی است. امروزه کارکرد بیمارستان‌ها به‌طور گسترده به زیرساخت‌های دیجیتال و سامانه‌های متصل وابسته شده است. ازاین‌رو، حمله به لایه دیجیتال یا سامانه‌های متصل یک مرکز درمانی، هرگاه موجب اختلال در ارائه خدمات پزشکی و کارکرد درمانی آن شود، می‌تواند در حکم حمله به واحد درمانی حمایت‌شده تلقی گردد. (Rome Statute, 1998: arts. 8(2)(b)(ix), 8(2)(e)(iv))[۱۲]

هفتمین عنوان، محروم‌سازی جمعیت غیرنظامی از اشیای ضروری برای بقاست. آب‌رسانی هوشمند، سامانه‌های تصفیه، کشاورزی هوشمند، زنجیره غذا و دارو، شبکه انرژی و لجستیک غذا همگی به اینترنت اشیا وابسته‌اند. حمله به لایه دیجیتال این سامانه‌ها اگر با هدف محروم‌سازی غیرنظامیان از آب، غذا، دارو یا خدمات حیاتی انجام شود، می‌تواند در چارچوب جنایت جنگی بررسی شود. (Rome Statute, 1998: arts. 8(2)(b)(xxv), Amendment to article 8, 2019: art. 8(2)(e)(xix))[۱۳]

---

[۸]. ماده ۸(۲)(ب)(۲) اساسنامه رم «حملات عمدی علیه اهداف غیرنظامی، یعنی اهدافی که دارای کاربرد نظامی نیستند» را در مخاصمات مسلحانه بین‌المللی جنایت جنگی می‌داند.

[۹]. ماده ۸(۲)(ب)(۴) اساسنامه رم «آغاز عمدی حمله با علم به اینکه چنین حمله‌ای باعث تلفات یا صدمات به افراد غیرنظامی یا تخریب اهداف غیرنظامی یا خسارات شدید، گسترده و دراز مدت به محیط زیست می‌شود که در مقایسه با مجموع منافع نظامی مستقیم و قطعی پیش بینی شده، آشکارا بیش از حد باشد» را در مخاصمات مسلحانه بین‌المللی جنایت جنگی می‌داند.

[۱۰]. ماده ۸(۲)(الف)(۴) اساسنامه رم «تخریب و تصرف اموال در سطح گسترده، که به صورت غیرقانونی و مغرضانه انجام گیرد و نتوان آن را به دلیل ضرورت نظامی توجیه نمود» را در زمره نقض‌های فاحش کنوانسیون‌های ژنو جنایت جنگی می‌داند.

[۱۱]. ماده ۸(۲)(الف)(۱) اساسنامه رم «قتل عمدی» و ماده ۸(۲)(الف)(۳) اساسنامه رم «وارد آوردن عمدی رنج شدید یا صدمه جدی به جسم یا سلامت افراد» را در زمره نقض‌های فاحش کنوانسیون‌های ژنو جنایت جنگی می‌داند.

ماده ۸(۲)(ج)(۱) اساسنامه رم «اعمال خشونت علیه حیات و تمامیت جسمانی، به‌ویژه هر نوع قتل، قطع عضو، رفتار بی‌رحمانه و شکنجه» در مخاصمات مسلحانه غیربین‌المللی، نسبت به اشخاصی که مستقیماً در مخاصمات شرکت ندارند یا از رزم خارج شده‌اند، را جنایت جنگی می‌داند.

[۱۲]. ماده ۸(۲)(ب)(۹) و ماده ۸(۲)(هـ)(۴) اساسنامه رم «حملات عمدی به ساختمان های مذهبی، آموزشی، هنری، علمی یا خیریه، بناهای تاریخی، بیمارستان‌ها و مکان‌هایی که افراد بیمار و مجروح در آن‌ها گردآوری می‌شوند، مشروط بر اینکه این اماکن اهداف نظامی نباشند» را به‌ترتیب در مخاصمات مسلحانه بین‌المللی و غیربین‌المللی جنایت جنگی می‌داند.

[۱۳]. ماده ۸(۲)(ب)(۲۵) اساسنامه رم «تحمیل گرسنگی اجباری بر غیرنظامیان به عنوان یک حربه نظامی، از طریق محروم ساختن این افراد از لوازم حیاتی که برای بقای آن‌ها ضروری است، از جمله جلوگیری عمدی از ارسال کمک‌های امدادی، آن‌گونه که در کنوانسیون‌های ژنو مقرر شده است» را در مخاصمات مسلحانه بین‌المللی جنایت جنگی می‌داند. عنوان مشابه در مخاصمات مسلحانه غیربین‌المللی، به موجب اصلاحیه ۶ دسامبر ۲۰۱۹، به‌عنوان ماده ۸(۲)(هـ)(۱۹) به اساسنامه افزوده شد.

هشتمین عنوان، حمله به کارکنان، تأسیسات و وسایل مأموریت‌های بشردوستانه یا حافظ صلح است. کاروان‌های امدادی، تجهیزات پزشکی سیار، سامانه‌های موقعیت‌یابی و ارتباطات بشردوستانه ممکن است به اینترنت اشیا وابسته باشند. مختل کردن آگاهانه این سامانه‌ها برای جلوگیری از امدادرسانی یا قرار دادن کاروان‌های امدادی در معرض حمله، می‌تواند ذیل ماده ۸ مطرح شود.[۱۴] (Rome Statute, 1998: arts. 8(2)(b)(iii), 8(2)(e)(iii))

در مخاصمات غیر بین‌المللی نیز تحلیل مشابه است، هرچند عناوین دقیق ماده ۸ متفاوت‌اند. گروه‌های مسلح غیردولتی و هکرهای وابسته به آنان نیز می‌توانند در صورت تحقق عناصر لازم، مسئول جنایات جنگی شوند. اما باید آستانه مخاصمه غیربین‌المللی، سازمان‌یافتگی گروه، پیوند رفتار با مخاصمه و عناصر خاص جرم احراز شود. (Rome Statute, 1998: arts. 8(2)(c), 8(2)(e))

نتیجه این بخش آن است که عملیات مبتنی بر اینترنت اشیا می‌تواند در شرایط مشخص جنایت جنگی باشد؛ اما نه به دلیل جدید بودن فناوری، بلکه به دلیل تحقق عناصر جرایم موجود. هر هک، نفوذ، سرقت داده یا هر اختلال دیجیتال جنایت جنگی نیست؛ بلکه باید زمینه مخاصمه، عنوان دقیق ماده ۸، موضوع حمایت‌شده، شدت اثر، رابطه سببیت و عنصر روانی احراز گردد.

۴. اشکال مسئولیت کیفری فردی در جنایات جنگی مبتنی بر اینترنت اشیا: ماده ۲۵ اساسنامه رم

وقوع جنایت جنگی با انتساب آن به شخص حقیقی دو مرحله متفاوت است و ماده ۲۵ اساسنامه رم مبنای تحلیل مسئولیت فردی را فراهم می‌کند. این ماده اشکال مختلف مسئولیت فردی، از جمله ارتکاب مستقیم، ارتکاب از طریق دیگری، معاونت، مشارکت و شروع به جرم را پیش‌بینی می‌کند. در عملیات مبتنی بر اینترنت اشیا، نقش‌ها معمولاً میان بازیگران متعدد توزیع می‌شود؛ با این حال، هر نقش فنی یا سازمانی به‌تنهایی موجب مسئولیت کیفری نمی‌شود و احراز عنصر مادی، عنصر روانی و شکل خاص مسئولیت ضروری است. (Rome Statute, 1998: art. 25)

ارتکاب مستقیم در عملیات مبتنی بر اینترنت اشیا زمانی مطرح است که شخص خود عناصر مادی جرم را از طریق ابزارهای دیجیتال محقق کند؛ مانند فعال‌سازی بدافزار یا دستکاری سامانه‌های متصل، مشروط بر آنکه رفتار، قصد و نتیجه قابل‌انتساب باشد. (Trahan, 2021: 1134) ارتکاب مشترک نیز در عملیات مبتنی بر اینترنت اشیا به دلیل ماهیت شبکه‌ای و تقسیم‌شده این عملیات اهمیت ویژه‌ای دارد و مستلزم وجود طرح مشترک، مشارکت اساسی و آگاهی از ماهیت مجرمانه آن است. طراح معماری حمله، فراهم‌کننده دسترسی اختصاصی، اپراتور اجراکننده و فرمانده‌ی تأییدکننده ممکن است در قالب طرح مشترک عمل کنند. (ابوذری، برزگر و نادری، ۱۴۰۲: ۱۲۳) همچنین، ارتکاب از طریق دیگری در اینترنت اشیا در مواردی قابل‌تصور است که شخص از اپراتورها، گروه‌های نیابتی یا سامانه‌های خودکار به‌عنوان ابزار ارتکاب استفاده کند؛ هرچند سامانه خودکار به‌تنهایی موضوع مسئولیت کیفری نیست و مسئولیت متوجه عامل انسانی خواهد بود.[۱۵] (Rome Statute, 1998: art. 25(3)(a))

افزون بر این، دستور دادن و معاونت نیز در محیط اینترنت اشیا اهمیت دارد. معیار اصلی در دستور، محتوا و اثر مورد نظر آن است، نه قالب فنی یا زبانی آن؛ بنابراین استفاده از اصطلاحات فنی مانع مسئولیت کیفری نخواهد بود. (Rome Statute, 1998:

---

[۱۴]. ماده ۸(۲)(ب)(۳) و ماده ۸(۲)(هـ)(۳) اساسنامه رم «حملات عمدی علیه کارکنان، تأسیسات، تجهیزات، واحدها یا وسایل نقلیه مرتبط با مأموریت کمک‌رسانی بشردوستانه یا حفظ صلح مطابق با منشور ملل متحد، تا زمانی که به موجب حقوق بین‌الملل مخاصمات مسلحانه از حمایت اعطا شده به غیرنظامیان یا اموال غیرنظامی برخوردار باشند» را به‌ترتیب در مخاصمات بین‌المللی و غیربین‌المللی جنایت جنگی می‌داند.

[۱۵]. ماده ۲۵(۳)(الف) اساسنامه رم مقرر می‌دارد: «شخص زمانی واجد مسئولیت کیفری است که جرمی داخل در صلاحیت دیوان را به‌تنهایی، مشترکاً با شخص دیگر یا از طریق شخص دیگری مرتکب شود؛ اعم از اینکه شخصی که جرم از طریق او ارتکاب یافته است، خود دارای مسئولیت کیفری باشد یا نباشد»

art. 25(3)(b))[16] علاوه بر آن، معاونت از طریق تسهیل ارتکاب جرم یا فراهم کردن وسایل ارتکاب جرم در بستر عملیات مبتنی بر اینترنت اشیا باید مورد توجه قرار گیرد. در این چارچوب، رفتارهایی نظیر طراحی بدافزار اختصاصی برای دستگاه‌های پزشکی، ایجاد یا واگذاری دسترسی پنهانی به سامانه‌های حیاتی مانند آب‌رسانی، تأمین زیرساخت‌های فرماندهی و کنترل، یا حذف و تضعیف سازوکارهای ایمنی وحفاظتی[17]، در صورت انجام با قصد تسهیل جرم، می‌تواند مصداق معاونت باشد. (Rome Statute, 1998: art. 25(3)(c))[18] مشارکت در جرم گروهی نیز در مورد واحدهای سایبری، شبکه‌های نیابتی یا گروه‌های هکری، در صورت احراز مشارکت آگاهانه در هدف مجرمانه گروه قابل‌طرح است. (Rome Statute, 1998: art. 25(3)(d))[19]

شروع به جرم در عملیات مبتنی بر اینترنت اشیا اهمیت ویژه‌ای دارد؛ زیرا این عملیات غالباً پیش از تحقق نتیجه نهایی شناسایی یا متوقف می‌شوند. مطابق ماده ۲۵(۳)(و) اساسنامه رم، شروع به جرم زمانی محقق می‌شود که مرتکب با قصد ارتکاب جرم، اقداماتی انجام دهد که به‌طور عینی گام اساسی در جهت اجرای جرم محسوب شود، اما جرم به دلایل خارج از اراده او کامل نگردد. در این چارچوب، اقداماتی مانند استقرار کد مخرب در شبکه‌های حیاتی یا فعال‌سازی فرمان اجرایی برای ایجاد اختلال، در صورت عبور از مرحله آمادگی صرف، می‌توانند مصداق شروع به جرم باشند؛ هرچند ناکامی عملیات به علت مداخله عوامل خارجی مانع تحقق آن نیست و صرف انصراف داوطلبانه پیش از ورود به مرحله اجرا می‌تواند مانع مسئولیت شود. (Rome Statute, 1998: art. 25(3)(f))[20] در کنار آن، نقش بازیگران خصوصی در این نوع عملیات برجسته است. شرکت‌های فناوری، پیمانکاران و ارائه‌دهندگان خدمات ممکن است در زنجیره طراحی و اجرای عملیات نقش داشته باشند، اما اساسنامه رم مسئولیت کیفری اشخاص حقوقی را پیش‌بینی نکرده و نظام مسئولیت در آن بر مسئولیت کیفری فردی استوار است. بر این اساس، مدیران، کارشناسان یا سایر اشخاص حقیقی فعال در درون شرکت‌ها، در صورتی که با علم و قصد لازم در ارتکاب جرم مشارکت مؤثر داشته باشند، می‌توانند واجد مسئولیت کیفری بین‌المللی شناخته شوند. (Rome Statute, 1998: art. 25(1))[21]

برنامه‌نویسان و متخصصان داده صرفاً به سبب نگارش کد یا توسعه سامانه‌های نرم‌افزاری، واجد مسئولیت کیفری شناخته نمی‌شوند؛ مگر آنکه با علم یا قصد استفاده مجرمانه از محصول خود، در ارتکاب جرم مشارکت مؤثر داشته باشند و رفتار آنان ذیل یکی از اشکال مسئولیت ماده ۲۵ قابل‌انطباق باشد. (Greipl, 2023: 1099) بر این اساس، ماده ۲۵ ظرفیت بالایی برای تحلیل نقش‌های انسانی در عملیات مبتنی بر اینترنت اشیا دارد، اما انتساب مسئولیت مستلزم احراز دقیق نقش فرد، نوع مشارکت و عنصر روانی است و انتساب صرف به ابزار یا سامانه کفایت نمی‌کند.

---

[16]. ماده ۲۵(۳)(ب) اساسنامه رم مقرر می‌دارد: «شخصی که دستور ارتکاب جرمی داخل در صلاحیت دیوان را صادر کند، ارتکاب آن را درخواست نماید یا دیگری را به ارتکاب آن ترغیب کند، در صورتی مسئولیت کیفری خواهد داشت که جرم واقع شود یا دست‌کم شروع به ارتکاب آن صورت گیرد.»

[17] safeguards

[18]. ماده ۲۵(۳)(ج) اساسنامه رم مقرر می‌دارد: «هرگاه شخص با هدف تسهیل ارتکاب جرمی داخل در صلاحیت دیوان، در ارتکاب یا شروع به ارتکاب آن کمک، معاونت یا به هر نحو دیگری مساعدت کند، از جمله اینکه وسایل ارتکاب جرم را فراهم سازد، دارای مسئولیت کیفری خواهد بود.»

[19]. ماده ۲۵(۳)(د) اساسنامه رم مقرر می‌دارد: «شخصی که عمداً و به هر نحو دیگری در ارتکاب یا شروع به ارتکاب جرم توسط گروهی از اشخاص دارای هدف مشترک مشارکت کند، دارای مسئولیت کیفری می‌باشد. این مشارکت باید یا با هدف پیشبرد فعالیت یا مقصود مجرمانه گروه انجام شده باشد، مشروط بر آنکه فعالیت یا مقصود مزبور متضمن ارتکاب جرمی داخل در صلاحیت دیوان باشد، یا با آگاهی از قصد گروه برای ارتکاب آن جرم صورت گرفته باشد.»

[20]. ماده ۲۵(۳)(و) اساسنامه رم مقرر می‌دارد: «شخصی که با قصد ارتکاب جرمی داخل در صلاحیت دیوان، از طریق برداشتن گامی اساسی، اجرای جرم را آغاز کند، اما جرم به دلیل اوضاع و احوالی مستقل از اراده او واقع نشود، دارای مسئولیت کیفری می‌باشد. اما، شخصی که از تلاش در جهت ارتکاب جرم دست می‌کشد، یا از تحقق جنایت جلوگیری می‌نماید، در صورتی که به طور کامل و به صورت داوطلبانه این مقاصد جنایی را کنار گذارد، به موجب این اساسنامه مشمول مجازات نخواهد شد.»

[21]. ماده ۲۵(۱) اساسنامه رم مقرر می‌دارد: «دیوان مطابق این اساسنامه نسبت به اشخاص حقیقی صلاحیت رسیدگی دارد.»

۵. مسئولیت فرماندهان و کنترل مؤثر در جنایات جنگی مبتنی بر اینترنت اشیا: ماده ۲۸ اساسنامه رم

ماده ۲۸ اساسنامه رم، مبنایی مستقل برای مسئولیت کیفری فرماندهان نظامی و سایر مافوق‌ها پیش‌بینی می‌کند که از حیث مبنا و شرایط تحقق، با اشکال مسئولیت مقرر در ماده ۲۵ تفاوت دارد. در چارچوب ماده ۲۵، مسئولیت کیفری ناشی از مشارکت مستقیم یا غیرمستقیم شخص در ارتکاب جرم است؛ در حالی‌که ماده ۲۸ ناظر بر مسئولیت ناشی از قصور در اعمال کنترل و نظارت بر زیردستان است. بر این اساس، فرمانده یا مقام مافوق نه به دلیل ارتکاب مستقیم جرم، بلکه به سبب عدم جلوگیری، سرکوب یا ارجاع جرایم ارتکابی زیردستان تحت کنترل مؤثر خود، ممکن است واجد مسئولیت کیفری بین‌المللی شناخته شود.

مطابق بند «الف» ماده ۲۸، فرمانده نظامی یا شخصی که عملاً در مقام فرمانده نظامی عمل می‌کند، در قبال جنایاتی که توسط نیروهای تحت فرماندهی و کنترل مؤثر او ارتکاب می‌یابد، زمانی مسئول است که نخست، آگاه بوده یا با توجه به اوضاع و احوال موجود باید آگاه می‌بود که نیروهای تحت امر وی در حال ارتکاب یا در آستانه ارتکاب جنایت هستند؛ و دوم، تمامی اقدامات لازم و معقول در حدود اختیارات و توانایی خود را برای جلوگیری از ارتکاب جرم، متوقف ساختن آن یا ارجاع موضوع به مراجع صالح جهت تحقیق و تعقیب به عمل نیاورده باشد.

در خصوص مافوق‌های غیرنظامی نیز بند «ب» ماده ۲۸ شرایط خاصی را مقرر کرده است. در این فرض، مافوق زمانی مسئول شناخته می‌شود که از اطلاعاتی که به‌وضوح دلالت بر ارتکاب یا خطر قریب‌الوقوع ارتکاب جرم توسط زیردستان داشته، مطلع بوده یا آگاهانه از توجه به چنین اطلاعاتی خودداری کرده باشد. افزون بر این، جرم باید در حوزه فعالیت‌ها و مسئولیت مؤثر مافوق ارتکاب یافته و وی نیز اقدامات لازم و معقول برای جلوگیری، سرکوب یا ارجاع موضوع به مقامات صلاحیت‌دار را اتخاذ نکرده باشد. (Rome Statute, 1998: art. 28)

در عملیات مبتنی بر اینترنت اشیا، اهمیت ماده ۲۸ اساسنامه رم دوچندان می‌شود؛ زیرا این عملیات معمولاً در ساختارهای پیچیده و سلسله‌مراتبی انجام می‌شوند و کنترل و تصمیم‌گیری میان فرماندهان، پیمانکاران فنی و واحدهای عملیاتی توزیع شده است. ازاین‌رو، هرگاه فرماندهان نظامی یا مافوق‌های غیرنظامی از استفاده مجرمانه سامانه‌های متصل یا زیرساخت‌های دیجیتال آگاه باشند، یا عامدانه از توجه به نشانه‌های خطر خودداری کنند و اقدامات لازم برای جلوگیری یا توقف عملیات را انجام ندهند، امکان انتساب مسئولیت بر مبنای ماده ۲۸ مطرح می‌شود. در این بستر، فرمانده لزوماً شخصی نیست که مستقیماً بدافزار را طراحی یا اجرا کرده باشد، بلکه ممکن است نقش او در هدایت و نظارت بر واحدهای سایبری، اپراتورها یا پیمانکاران فنی تعریف شود. بنابراین، اگر زیردستان تحت کنترل مؤثر وی مرتکب جنایت جنگی شوند و او با وجود آگاهی یا امکان آگاهی و توان مداخله، اقدامات لازم و معقول را برای پیشگیری، توقف یا ارجاع موضوع به مراجع صلاحیت‌دار اتخاذ نکند، امکان انتساب مسئولیت کیفری بر مبنای ماده ۲۸ اساسنامه رم مطرح خواهد بود. (Spadaro, 2023: 1129) ازاین‌رو، مبنای مسئولیت فرمانده در این حوزه نه ارتکاب مستقیم عملیات سایبری، بلکه قصور در اعمال کنترل مؤثر و انجام تکالیف نظارتی نسبت به نیروها و ساختارهای تحت امر است.

کنترل مؤثر، هسته اصلی مسئولیت فرماندهان در ماده ۲۸ اساسنامه رم محسوب می‌شود. منظور از کنترل مؤثر، صرف برخورداری از عنوان رسمی، درجه نظامی یا سمت اداری نیست؛ بلکه مقصود، توان واقعی و عملی فرمانده یا مقام مافوق برای جلوگیری از ارتکاب جرم، متوقف ساختن آن، تنبیه مرتکبان یا ارجاع موضوع به مراجع صلاحیت‌دار است. (تیموری و کاظمی، ۱۴۰۴: ۱۰) ازاین‌رو، احراز مسئولیت فرماندهان مستلزم اثبات وجود رابطه‌ای واقعی از نظارت و اقتدار میان مافوق و زیردستان خواهد بود. در بستر عملیات مبتنی بر اینترنت اشیا، کنترل مؤثر ممکن است از طریق شاخص‌ها و اختیارات متعددی احراز شود؛ از جمله اختیار تصویب یا رد هدف عملیاتی، امکان توقف یا تعلیق عملیات سایبری، تغییر قواعد درگیری، الزام تیم‌های

فنی به رعایت تدابیر حفاظتی، دسترسی به گزارش‌های فنی و ارزیابی‌های ریسک، اختیار جابه‌جایی یا تنبیه اپراتورها، تعلیق ابزارها و سامانه‌های مورد استفاده، و نیز امکان ارجاع موضوع به مراجع ذی‌صلاح برای تحقیق و پیگرد. (Meloni, 2010: 61) بنابراین، در محیط‌های سایبری و سایبر-فیزیکی، کنترل مؤثر بیش از آنکه مبتنی بر حضور فیزیکی یا سلسله‌مراتب سنتی باشد، بر میزان اقتدار عملی و ظرفیت واقعی مداخله در فرایند تصمیم‌گیری و اجرای عملیات استوار است.

در محیط‌های شبکه‌محور، احراز کنترل مؤثر دشوارتر است؛ زیرا ممکن است ابزار در اختیار پیمانکار، زیرساخت تحت کنترل شرکت ثالث و عملیات در قالب مرکز مشترک انجام شود. با این حال، معیار اصلی همچنان توان واقعی برای هدایت، توقف یا محدودسازی عملیات است. بنابراین، فرماندهی که امکان مداخله یا اعمال محدودیت فنی دارد، نمی‌تواند صرفاً با استناد به پیچیدگی فناوری از مسئولیت رهایی یابد. عنصر روانی مسئولیت فرماندهان نیز شامل علم یا معیار «باید می‌دانست» است که می‌تواند از گزارش‌های فنی، هشدارهای حقوقی، مکاتبات داخلی یا لاگ‌های سامانه استنباط شود. ازاین‌رو، فرماندهانی که از ابزارهای سایبری- فیزیکی پرخطر استفاده می‌کنند، مکلف به ایجاد سازوکارهای نظارتی و ارزیابی هشدارها هستند و بی‌اعتنایی به نشانه‌های آشکار خطر، رافع مسئولیت نخواهد بود. (Jackson & Arnold, 2021: 42)

تدابیر لازم و معقول در عملیات مبتنی بر اینترنت اشیا باید در سه مرحله پیش از عملیات، حین عملیات و پس از آن ارزیابی شود. پیش از عملیات، فرمانده یا مقام مافوق مکلف است مشروعیت هدف، خطر سرایت و آثار احتمالی عملیات را از نظر فنی و حقوقی بررسی کرده و اقداماتی مانند محدودسازی بدافزار، آزمایش سامانه‌ها، پیش‌بینی سازوکارهای توقف اضطراری[۲۲] و تضمین نظارت انسانی مؤثر را اتخاذ کند.

در حین عملیات نیز، هرگاه نشانه‌هایی از گسترش کنترل‌نشده عملیات، سرایت به اهداف غیرمجاز یا خسارات نامتناسب آشکار شود، فرمانده باید عملیات را تعلیق، محدود یا متوقف سازد؛ در غیر این صورت، قصور وی می‌تواند در احراز عدم اعمال کنترل مؤثر مدنظر قرار گیرد.

پس از عملیات نیز، وظایف فرمانده یا مقام مافوق پایان نمی‌یابد و اقداماتی مانند حفظ ادله دیجیتال، تعلیق ابزارهای مورد استفاده، جلوگیری از تداوم رفتار مجرمانه و ارجاع موضوع به مراجع صلاحیت‌دار، می‌تواند از مصادیق تدابیر لازم و معقول موضوع ماده ۲۸ اساسنامه رم محسوب شود. (Spadaro, 2023: 1129-1132)

پرونده دادستان علیه ژان‌پیر بمبا[۲۳] نشان داد که مسئولیت فرماندهان نباید به نوعی مسئولیت مطلق یا صرفِ انتساب سلسله‌مراتبی تبدیل شود.[۲۴] (Bemba Appeals Judgment, 2018) صرف وقوع جرم توسط زیردستان، به‌تنهایی برای احراز مسئولیت کیفری فرمانده کافی نیست؛ بلکه لازم است عناصر اساسی مسئولیت فرماندهان، از جمله وجود کنترل مؤثر، احراز معیار ذهنی مقرر در ماده ۲۸ و نیز قصور در اتخاذ تدابیر لازم و معقول، به‌طور مشخص اثبات شود. این رویکرد در بستر عملیات مبتنی بر اینترنت اشیا نیز اهمیت بنیادین دارد؛ زیرا پیچیدگی فنی و چندلایه بودن ساختارهای سایبری، نه موجب ایجاد مسئولیت مطلق برای فرماندهان و مافوق‌ها می‌شود و نه به‌خودی‌خود مصونیت آنان را توجیه می‌کند. (Jackson, 2022:

---

[22] Kill Switch

[23] Prosecutor v. Jean-Pierre Bemba Gombo

[۲۴]. پرونده دادستان علیه ژان‌پیر بمبا گومبو از مهم‌ترین آرای دیوان کیفری بین‌المللی درباره مسئولیت فرماندهان محسوب می‌شود. ژان‌پیر بمبا، رهبر «جنبش آزادی کنگو»، به سبب جنایات ارتکابی نیروهای تحت فرماندهی خود در جمهوری آفریقای مرکزی، از جمله قتل، تجاوز و غارت، تحت تعقیب قرار گرفت. شعبه بدوی دیوان وی را بر مبنای ماده ۲۸ اساسنامه رم و به دلیل قصور در جلوگیری و سرکوب جرایم زیردستان محکوم کرد؛ اما شعبه تجدیدنظر در سال ۲۰۱۸ این محکومیت را نقض نمود. شعبه تجدیدنظر تأکید کرد که برای احراز مسئولیت فرماندهان، صرف وقوع جرم توسط نیروهای تحت امر کافی نیست، بلکه باید به‌طور دقیق احراز شود که فرمانده دارای کنترل مؤثر بوده، از جرایم آگاه بوده یا باید آگاه می‌بود، و با وجود امکان واقعی مداخله، تدابیر لازم و معقول را اتخاذ نکرده است. این رأی نقش مهمی در تبیین حدود مسئولیت فرماندهان و جلوگیری از تبدیل آن به نوعی مسئولیت مطلق ایفا کرده است.

(437 ازاین‌رو، ارزیابی مسئولیت کیفری در این حوزه مستلزم بررسی دقیق شرایط واقعی عملیات، حدود اختیارات و کنترل مؤثر، میزان اطلاعات در دسترس، قابلیت پیش‌بینی خطرات، و اقدامات عملی انجام‌شده برای پیشگیری، توقف یا سرکوب رفتار مجرمانه خواهد بود.

استفاده از سامانه‌های خودکار و نیمه‌خودکار در عملیات مبتنی بر اینترنت اشیا، موجب زوال یا انتقال مسئولیت کیفری از انسان به ماشین نمی‌شود و اشخاصی که در طراحی، استقرار، فعال‌سازی، نظارت یا توقف این سامانه‌ها نقش دارند، ممکن است در صورت تحقق شرایط قانونی، واجد مسئولیت کیفری شناخته شوند. ازاین‌رو، در ارزیابی مسئولیت کیفری باید زنجیره تصمیم‌گیری و مداخله انسانی به‌دقت شناسایی گردد. در این چارچوب، فرمانده یا مقام مافوق باید بر نقش اشخاص دخیل در چرخه عملیات نظارت کافی داشته باشد؛ از جمله اینکه چه کسانی داده‌ها را تأیید یا سامانه را آزمایش کرده‌اند، چه مرجعی سطح خودکار بودن عملیات را مجاز دانسته و اختیار توقف یا تعلیق عملیات در اختیار چه شخص یا نهادی بوده است. فقدان چنین زنجیره شفاف و قابل‌ردیابی، خطر ایجاد شکاف پاسخگویی را افزایش داده و انتساب مسئولیت کیفری در عملیات سایبری و سایبر- فیزیکی را با دشواری مواجه می‌سازد. (Spadaro, 2023: 1131)

بنابراین ماده ۲۸ در کنار ماده ۲۵ دو مسیر مکمل برای انتساب مسئولیت فراهم می‌کند. ماده ۲۵ نقش‌های فعال را پوشش می‌دهد و ماده ۲۸ قصور فرمانده یا مافوق در کنترل زیردستان را. در هر دو مسیر، معیار نهایی نقش انسانی، کنترل، علم، قصد، سببیت و تدابیر لازم و معقول است.

۶. چالش‌های انتساب در جنایات جنگی مبتنی بر اینترنت اشیا

چالش محوری این بحث را باید در مسئله انتساب مسئولیت کیفری جست‌وجو کرد. مقصود از انتساب در این حوزه، صرف شناسایی منشأ فنی حمله، نظیر آدرس آی پی[۲۵]، بدافزار یا زیرساخت دیجیتال مورد استفاده نیست؛ بلکه انتساب زمانی از منظر حقوق کیفری بین‌المللی معنا پیدا می‌کند که در نهایت بتوان مشخص کرد کدام شخص حقیقی، با چه رفتار و نقشی، در چه سطحی از کنترل یا مشارکت، و با برخورداری از چه عنصر روانی، مسئول ارتکاب جنایت جنگی است.

پیچیدگی عملیات مبتنی بر اینترنت اشیا، انتساب مسئولیت کیفری را دشوارتر می‌سازد؛ زیرا نتیجه زیان‌بار غالباً حاصل تعامل هم‌زمان عناصر انسانی و فنی متعدد است. در این عملیات، بازیگرانی مانند فرماندهان، اپراتورها، پیمانکاران، گروه‌های نیابتی و سامانه‌های نیمه‌خودکار ممکن است هر یک بخشی از زنجیره ارتکاب را تشکیل دهند. ازاین‌رو، انتساب مسئولیت مستلزم بازسازی زنجیره تصمیم‌گیری و احراز نقش، کنترل، رابطه سببیت و عنصر روانی هر یک از اشخاص دخیل است.

نخستین لایه از فرایند انتساب، انتساب فنی است که به شناسایی زیرساخت‌ها و عناصر دیجیتال دخیل در عملیات، مانند سرورها، حساب‌های کاربری، بدافزارها، داده‌ها و مسیرهای ارتباطی مربوط می‌شود. با این حال، انتساب فنی به‌تنهایی برای احراز مسئولیت کیفری کافی نیست؛ زیرا مسیر ترافیک دیجیتال الزاماً بیانگر هویت مرتکب واقعی نیست و ممکن است دستگاه‌ها یا خدمات دیجیتال بدون اطلاع مالک یا ارائه‌دهنده، در عملیات مورد استفاده قرار گرفته باشند. (Davis, 2022: 15) ازاین‌رو، انتساب کیفری مستلزم تکمیل انتساب فنی با ادله‌ای درباره نقش انسانی، میزان کنترل، نحوه مشارکت و عنصر روانی اشخاص دخیل است.

دومین چالش در فرایند انتساب، ناشناسی دیجیتال و عملیات «پرچم دروغین[۲۶]» است. در فضای سایبری، مهاجم می‌تواند با استفاده از ابزارها و روش‌هایی نظیر شبکه‌های خصوصی مجازی (وی پی ان[۲۷])، سرورهای واسط، حساب‌های کاربری

[25] Internet Protocol (IP)
[26] False flag operations
[27] Virtual private network (VPN)

سرقت‌شده یا دستگاه‌های آلوده، منشأ واقعی عملیات را پنهان یا آن را به بازیگر دیگری منتسب جلوه دهد. ازاین‌رو، شناسایی منشأ فنی حمله به‌تنهایی برای اثبات مسئولیت کیفری کافی نیست و شاخص‌های فنی باید در کنار ادله انسانی، سازمانی و سایر قرائن مورد ارزیابی قرار گیرند؛ زیرا معیار اثبات در حقوق کیفری بین‌المللی فراتر از سطح اطمینان تحلیل‌های اطلاعاتی و امنیتی است. (Berkeley Protocol, 2022: 41)

سومین چالش، تفکیک میان انتساب دولتی و انتساب کیفری فردی است. در حقوق بین‌الملل عمومی، قواعد مسئولیت دولت بر این پرسش متمرکزند که آیا رفتار ارتکابی قابل‌انتساب به دولت است و آیا از رهگذر آن، تعهدات بین‌المللی دولت نقض شده است یا خیر. در مقابل، حقوق بین‌الملل کیفری بر مسئولیت اشخاص حقیقی تمرکز دارد و می‌کوشد مشخص کند کدام فرد، با چه میزان مشارکت و برخورداری از عنصر روانی لازم، مسئول ارتکاب جرم بین‌المللی است. (دلخوش، ۱۳۹۰: ۲۵۶) بر این اساس، حتی اگر یک عملیات مبتنی بر اینترنت اشیا از منظر حقوق بین‌الملل عمومی به دولت خاصی منتسب شود، این امر به‌تنهایی برای احراز مسئولیت کیفری افراد کافی نیست و نقش، میزان مشارکت و عنصر روانی اشخاص دخیل باید به‌طور مستقل اثبات شود. همچنین، ممکن است مسئولیت کیفری فردی احراز گردد، بی‌آنکه انتساب رسمی عملیات به دولت مشخصی ثابت شده باشد؛ بنابراین، انتساب دولتی و انتساب کیفری دو نظام متمایز با معیارهای متفاوت‌اند. (International Law Commission, 2001: Arts. 4, 8, 58; Rome Statute, 1998: art. 25)

چهارمین چالش، احراز رابطه سببیت است. در عملیات مبتنی بر اینترنت اشیا، نتیجه زیان‌بار معمولاً حاصل تعامل عوامل متعدد فنی و انسانی، از جمله بدافزار، آسیب‌پذیری‌های امنیتی، خطاهای طراحی، واکنش سامانه‌های خودکار و تصمیمات انسانی است. ازاین‌رو، صرف اثبات نفوذ یا وجود بدافزار برای انتساب مسئولیت کیفری کافی نیست و باید احراز شود که رفتار منتسب به متهم، به‌طور مؤثر و قابل‌انتساب، به نتیجه مجرمانه منتهی شده است. (Chaumette, 2018: 17)

پنجمین چالش، آثار آبشاری و مسئله پیش‌بینی‌پذیری نتایج است. ماهیت به‌هم‌پیوسته سامانه‌های مبتنی بر اینترنت اشیا موجب می‌شود که اختلال در یک جزء، به سایر زیرساخت‌ها و خدمات غیرنظامی نیز سرایت کرده و پیامدهایی فراتر از هدف اولیه ایجاد کند. (Greer, et al. 2019: 5) ازاین‌رو، در ارزیابی عناوینی همچون حمله نامتناسب، قتل عمدی، ایراد آسیب شدید یا مسئولیت فرماندهان، باید بررسی شود که آیا این پیامدهای تبعی و زنجیره‌ای در زمان اتخاذ تصمیم، به‌طور متعارف قابل پیش‌بینی بوده‌اند یا خیر و نیز آیا مرتکب نسبت به احتمال وقوع آن‌ها علم داشته یا با توجه به اوضاع و احوال، می‌بایست از آن آگاه می‌بود. در این زمینه، عواملی مانند گزارش‌های فنی، هشدارهای امنیتی، نتایج شبیه‌سازی‌ها، سوابق آزمایش ابزار و ارزیابی‌های ریسک، از مهم‌ترین قرائن برای احراز آگاهی، پیش‌بینی‌پذیری و حدود مسئولیت کیفری به شمار می‌روند.

ششمین چالش، مسئله ادله دیجیتال است. در عملیات مبتنی بر اینترنت اشیا، داده‌هایی مانند لاگ‌های سامانه، اطلاعات حسگرها، گزارش‌های خطا، داده‌های سنجش و پایش از راه دور[۲۸]، داده‌های ذخیره‌شده در فضای ابری و مکاتبات داخلی، نقش مهمی در اثبات یا رد مسئولیت کیفری دارند. با این حال، این ادله به‌دلیل ماهیت دیجیتال، در معرض حذف، جعل و دستکاری قرار دارند؛ ازاین‌رو، اعتبار آن‌ها مستلزم رعایت معیارهای دقیق فنی و حقوقی است. در همین راستا، پروتکل برکلی بر ضرورت گردآوری، تحلیل و نگهداری حرفه‌ای ادله دیجیتال در تحقیقات بین‌المللی تأکید می‌کند. در پرونده‌های مرتبط با اینترنت اشیا نیز حفظ زنجیره اصالت ادله، ثبت دقیق زمان و منشأ داده‌ها، نگهداری مقادیر هش[۲۹]، مشخص بودن نسخه نرم‌افزارها و فراهم بودن امکان ارزیابی و اعتراض مؤثر برای دفاع، از الزامات اساسی دادرسی عادلانه و انتساب معتبر مسئولیت کیفری محسوب می‌شود. (Berkeley Protocol, 2022: 59)

---

[28] telemetry
[29] hash

هفتمین چالش، پیچیدگی زنجیره تأمین در سامانه‌های اینترنت اشیا است. دستگاه‌های متصل معمولاً از مؤلفه‌ها و خدمات متعددی مانند تراشه، سفت‌افزار، سیستم‌عامل و زیرساخت ابری تشکیل می‌شوند که توسط بازیگران مختلف فراهم شده‌اند. این تعدد بازیگران، شناسایی منشأ رفتار مجرمانه و انتساب مسئولیت را دشوار می‌کند. با این حال، صرف وجود آسیب‌پذیری امنیتی یا نقص فنی، برای تحقق مسئولیت کیفری بین‌المللی کافی نیست. مسئولیت زمانی مطرح می‌شود که شخص، با علم یا قصد تسهیل جنایت، اقدام به تعبیه سازوکارهای پنهان دسترسی[30]، طراحی سفت‌افزار مخرب یا ارائه ابزار نفوذ اختصاصی[31] برای حمله به اهداف حمایت‌شده‌ای همچون بیمارستان‌ها، شبکه‌های آب‌رسانی یا سایر اموال غیرنظامی کرده باشد. در چنین وضعیتی، رفتار مزبور می‌تواند در چارچوب اشکال مختلف مشارکت کیفری مورد ارزیابی قرار گیرد. (ENISA, 2020: 19)

هشتمین چالش، نقش بازیگران خصوصی و شرکت‌های فناوری در عملیات مبتنی بر اینترنت اشیا است. این بازیگران ممکن است در طراحی، پشتیبانی یا اجرای عملیات، از طریق تولید تجهیزات، توسعه نرم‌افزار، خدمات ابری یا پیمانکاری نظامی مشارکت داشته باشند. با این حال، اساسنامه رم مسئولیت کیفری مستقیم اشخاص حقوقی را پیش‌بینی نکرده و صلاحیت دیوان عمدتاً ناظر بر اشخاص حقیقی است. بنابراین، مسئولیت کیفری تنها زمانی متوجه افراد فعال در این ساختارها خواهد بود که علم، قصد و مشارکت مؤثر آنان در ارتکاب یا تسهیل جنایت احراز شود. در نتیجه، صرف ارائه خدمات یا فناوری‌های دوگانه‌کاربرد، بدون آگاهی از استفاده مجرمانه یا قصد تسهیل جرم، برای تحقق مسئولیت کیفری بین‌المللی کافی نیست. (Rome Statute, 1998: arts. 25-26)

نهمین چالش، نقش گروه‌های نیابتی و هکرهای داوطلب در عملیات مبتنی بر اینترنت اشیا است. این گروه‌ها ممکن است تحت حمایت یا هدایت دولت‌ها و گروه‌های مسلح فعالیت کنند، یا به‌صورت مستقل اما همسو با یکی از طرف‌های مخاصمه عمل نمایند. (ICRC, 2025: 3) در چنین وضعیتی، انتساب مسئولیت کیفری با دشواری روبه‌رو می‌شود. برای مسئول شناختن اعضای این گروه‌ها، باید وجود مخاصمه مسلحانه، ارتباط رفتار با مخاصمه، انطباق آن با عناوین ماده ۸ اساسنامه رم و عنصر روانی لازم احراز شود. همچنین، صرف حمایت سیاسی یا بهره‌برداری از نتایج عملیات، برای مسئولیت فرماندهان یا مقامات دولتی کافی نیست؛ بلکه وجود کنترل مؤثر، علم و قصور در جلوگیری یا سرکوب رفتار مجرمانه، مطابق ماده ۲۸ اساسنامه رم، باید اثبات گردد. (Rome Statute, 1998: arts. 8, 28)

دهمین چالش، احراز عنصر روانی در جنایات جنگی مبتنی بر اینترنت اشیا است. مرتکب ممکن است ادعا کند هدف او صرفاً نفوذ به سامانه یا ایجاد اختلال محدود بوده و قصدی برای ایراد مرگ یا آسیب به غیرنظامیان نداشته است. ازاین‌رو، احراز قصد و علم وی نیازمند بررسی قرائن فنی و رفتاری مانند نحوه انتخاب هدف، نوع ابزار مورد استفاده، هشدارهای فنی، غیرفعال‌سازی سازوکارهای حفاظتی، تداوم عملیات با وجود آثار زیان‌بار و مکاتبات داخلی است. با این حال، عنصر روانی نباید صرفاً از وقوع نتیجه مجرمانه استنتاج شود، بلکه باید در پرتو مجموع قرائن فنی، عملیاتی و سازمانی ارزیابی گردد. (Trahan, 2021: 1150)

یازدهمین چالش، نقش هوش مصنوعی و سامانه‌های خودکار در فرایند ارتکاب جنایت است. در این سامانه‌ها، الگوریتم ممکن است داده‌های دریافتی از حسگرها را تحلیل کرده، هدف را شناسایی یا پیشنهاد کند و یا سامانه متصل، به‌صورت خودکار واکنش عملیاتی نشان دهد. با وجود این، سامانه هوشمند یا الگوریتم به‌خودی‌خود واجد مسئولیت کیفری نیست و برای احراز مسئولیت کیفری، لازم است زنجیره مداخله و تصمیم‌گیری انسانی در مراحل طراحی، تولید داده‌های آموزشی، اعتبارسنجی، استقرار، نظارت، تعیین حدود عملکرد سامانه و اختیار توقف یا مداخله انسانی، به‌دقت بازسازی و بررسی شود. (پیری، ۱۴۰۴: ۱۶۵) همچنین باید میان خطاهای غیرقابل‌پیش‌بینی الگوریتمی و مواردی که اشخاص، آگاهانه از سامانه‌ای فاقد کنترل مؤثر یا نظارت کافی استفاده کرده‌اند، تفکیک قائل شد. (Coco, 2023:1079)

---

[30] Backdoor
[31] exploit

بنابراین انتساب مسئولیت در عملیات مبتنی بر اینترنت اشیا باید به‌صورت لایه‌مند و چندمرحله‌ای تحلیل شود. انتساب فنی، هرچند نقطه آغاز بررسی است، به‌تنهایی برای احراز مسئولیت کیفری کفایت نمی‌کند. در این فرایند، لازم است از داده‌ها و شواهد فنی به ساختار عملیاتی و سپس به نقش سازمانی و انسانی بازیگران مرتبط رسید و در نهایت، مسئولیت کیفری شخص حقیقی بر مبنای عناصر لازم، از جمله قصد، علم، میزان کنترل و ادله معتبر احراز گردد. ازاین‌رو، پیچیدگی‌های فنی و فناورانه نباید به ابزاری برای ایجاد مصونیت کیفری تبدیل شود.

۷. مدل پیشنهادی چندلایه برای انتساب مسئولیت کیفری در جنایات جنگی مبتنی بر اینترنت اشیا

مدل پیشنهادی مقاله برای پاسخ به چالش‌های فوق، مدل چندلایه انتساب کیفری در جنایات جنگی مبتنی بر اینترنت اشیا است. این مدل جرم جدیدی ایجاد نمی‌کند و جایگزین اساسنامه رم نیست؛ بلکه روش تحلیل را سامان می‌دهد تا پژوهشگر، دادستان یا قاضی بداند از کجا آغاز کند، چه پرسش‌هایی بپرسد و چگونه از یافته فنی به مسئولیت کیفری شخص حقیقی برسد.

مبنای نخست این مدل، فناوری‌خنثی بودن عنوان جنایت جنگی است. بر این اساس، هرگاه عناصر یکی از مصادیق مقرر در ماده ۸ اساسنامه رم محقق شود، تفاوتی ندارد که رفتار مجرمانه از طریق ابزارهای متعارف نظامی ارتکاب یافته باشد یا از طریق ابزارهای سایبری و سامانه‌های سایبری ـ فیزیکی. مبنای دوم، تفکیک میان نقض حقوق بشردوستانه و جنایت جنگی است؛ زیرا هر نقض حقوق بشردوستانه لزوماً واجد وصف جنایت جنگی نیست و تنها نقض‌های شدید و واجد شرایط مقرر می‌توانند در قلمرو مسئولیت کیفری بین‌المللی قرار گیرند. مبنای سوم، اصل شخصی بودن مسئولیت کیفری است. بر این اساس، سامانه‌های هوشمند، الگوریتم‌ها یا شرکت‌ها، در نظام دیوان کیفری بین‌المللی واجد مسئولیت کیفری نیستند و مسئولیت صرفاً متوجه اشخاص حقیقی خواهد بود. مبنای چهارم، ضرورت تفکیک میان انتساب فنی، عملیاتی، سازمانی و کیفری است؛ زیرا شناسایی منشأ فنی عملیات، به‌تنهایی برای احراز مسئولیت کیفری کفایت نمی‌کند و باید نقش انسانی و سازمانی اشخاص نیز به‌طور مستقل احراز شود. سرانجام، مبنای پنجم، ضرورت اتکا به ادله دیجیتال معتبر و قابل‌ارزیابی قضایی است؛ ادله‌ای که بتواند در فرایند دادرسی، از حیث صحت، تمامیت و قابلیت‌استناد، مورد ارزیابی و آزمون قرار گیرد.

لایه نخست این مدل، احراز وجود مخاصمه مسلحانه و بررسی پیوند رفتار ارتکابی با مخاصمه است. در این مرحله، باید وجود مخاصمه مسلحانه بین‌المللی یا غیربین‌المللی احراز شده و همچنین ثابت شود که عملیات مبتنی بر اینترنت اشیا دارای ارتباط واقعی و مؤثر با آن مخاصمه بوده است. صرف هم‌زمانی رفتار با وقوع مخاصمه برای تحقق این شرط کافی نیست؛ بلکه لازم است عملیات مزبور از حیث هدف، بستر وقوع، طرف‌های درگیر، نوع قربانیان، آثار و پیامدها یا کارکرد عملیاتی، با مخاصمه مسلحانه مرتبط باشد. ازاین‌رو، احراز این پیوند، شرط اساسی برای ورود رفتار به قلمرو حقوق بین‌الملل کیفری و بررسی آن در قالب جنایت جنگی محسوب می‌شود. (ICC, 2013: 9)

لایه دوم، شناسایی و تعیین عنوان دقیق جنایت جنگی است. در این مرحله، باید مشخص شود که رفتار ارتکابی با کدام یک از مصادیق پیش‌بینی شده در ماده ۸ اساسنامه رم قابل‌انطباق است؛ از جمله حمله علیه غیرنظامیان، حمله به اموال غیرنظامی، حمله نامتناسب، حمله به بیمارستان‌ها و مراکز درمانی، قتل عمدی، تخریب گسترده اموال یا محروم‌سازی جمعیت غیرنظامی از اشیای ضروری برای بقا یا عنوان دیگر. این مرحله ارتباط مستقیم با اصل قانونی بودن جرایم و مجازات‌ها دارد و تضمین می‌کند که مسئولیت کیفری صرفاً بر پایه عناوین مصرح و شناخته‌شده در حقوق بین‌الملل کیفری احراز شود. (Rome Statute, 1998: arts. 8)

لایه سوم، بازسازی فنی عملیات مبتنی بر اینترنت اشیا است. در این مرحله، باید نحوه اجرای عملیات به‌صورت دقیق و مرحله به مرحله تبیین شود؛ بدین معنا که مشخص گردد عملیات از چه طریقی آغاز شده و چه فرایندی را طی کرده است، از جمله

شناسایی هدف، کشف و بهره‌برداری از آسیب‌پذیری، نفوذ به سامانه، تثبیت دسترسی، دستکاری داده‌ها یا سفت‌افزار، فعال‌سازی اثر بر حسگرها یا عملگرها، پایش نتایج عملیات و پنهان‌سازی آثار دیجیتال. (Greer, et al. 2019: 27) اهمیت این لایه در آن است که بدون بازسازی فنی دقیق و بدون اتکا به تحلیل‌های تخصصی معتبر، امکان درک صحیح سازوکار عملیات و ارزیابی نقش اشخاص دخیل در آن وجود نخواهد داشت. ازاین‌رو، این مرحله مبنای ضروری برای بررسی رابطه سببیت، انتساب رفتار و احراز مسئولیت کیفری به شمار می‌آید.

لایه چهارم، احراز رابطه سببیت و تبیین فرایند تبدیل اثر دیجیتال به نتیجه کیفری است. در این مرحله، باید مشخص شود که فرمان، کد یا ابزار مخرب وارد سامانه شده و در نتیجه، عملکرد دستگاه یا زیرساخت هدف را تغییر داده است و این تغییر، نهایتاً به وقوع نتیجه‌ای مجرمانه، از قبیل مرگ، صدمه بدنی، تخریب اموال یا محرومیت از خدمات حیاتی، منتهی شده است. افزون بر این، لازم است احراز شود که نتیجه حاصل، از منظر حقوقی، قابل‌انتساب به رفتار متهم بوده و میان رفتار ارتکابی و نتیجه زیان‌بار، رابطه سببیت وجود دارد. (Trahan, 2021: 1135) در این چارچوب، بررسی عواملی نظیر دخالت عامل مستقل، تعدد اسباب و عوامل مؤثر در وقوع نتیجه، و نیز آثار آبشاری و زنجیره‌ای ناشی از اختلال در سامانه‌های متصل، اهمیت اساسی دارد؛ زیرا در محیط‌های مبتنی بر اینترنت اشیا، یک تغییر محدود در یک سامانه می‌تواند پیامدهایی گسترده و چندلایه در سایر زیرساخت‌ها و خدمات وابسته ایجاد کند. ازاین‌رو، احراز رابطه سببیت در این حوزه، مستلزم تحلیل دقیق فنی و حقوقی به‌صورت توأمان است.

لایه پنجم، انتساب عملیاتی و سازمانی است. در این مرحله، باید عملیات ارتکابی به ساختار انسانی و سازمانی مرتبط شود و مشخص گردد که کدام واحد، تیم، گروه سازمان‌یافته، پیمانکار، شرکت، دولت یا شبکه، در طراحی، هدایت، پشتیبانی یا اجرای عملیات نقش داشته است. هدف این لایه، شناسایی پیوند میان عملیات فنی و کنشگران انسانی و سازمانی دخیل در آن است. با این حال، این سطح از انتساب، صرفاً نقش واسطه میان داده‌ها و شواهد فنی با مسئولیت کیفری فردی را ایفا می‌کند و به‌تنهایی برای احراز مسئولیت کیفری کافی نیست.

لایه ششم، انتساب مسئولیت کیفری فردی است. در این مرحله، باید مشخص شود که کدام شخص حقیقی بر اساس مواد ۲۵ یا ۲۸ اساسنامه رم واجد مسئولیت کیفری است. مسیر مقرر در ماده ۲۵ ناظر بر اشکال مختلف مشارکت فعال در ارتکاب جرم است؛ از جمله مباشرت، صدور دستور، معاونت یا مشارکت در قالب فعالیت گروهی و سازمان‌یافته. در مقابل، ماده ۲۸ به مسئولیت فرماندهان و مافوق‌ها در قبال قصور در اعمال کنترل مؤثر بر زیردستان اختصاص دارد؛ بدین معنا که شخص مافوق، علی‌رغم آگاهی یا امکان آگاهی از ارتکاب جرم، در پیشگیری یا جلوگیری از آن یا ارجاع موضوع به مراجع صالح کوتاهی کرده باشد. (Rome Statute, 1998: arts. 25, 28) هر یک از این دو مسیر، دارای ارکان و شرایط اختصاصی خود است. ازاین‌رو، انتساب مسئولیت کیفری فردی مستلزم بررسی و اثبات مستقل عناصر مربوط، از جمله نقش شخص، میزان کنترل، علم، قصد و نحوه مشارکت وی در ارتکاب جنایت است.

لایه هفتم، ناظر بر عنصر روانی و کفایت ادله است. ماده ۳۰ اساسنامه رم، اصل کلی قصد و علم را به‌عنوان معیار عنصر روانی مقرر کرده است، مگر در مواردی که اساسنامه به‌طور خاص ترتیب دیگری پیش‌بینی کرده باشد. (Rome Statute, 1998: arts. 30) در عملیات مبتنی بر اینترنت اشیا، احراز عنصر روانی مستلزم بررسی ابعاد مختلفی است؛ از جمله علم مرتکب به وجود مخاصمه مسلحانه، آگاهی از وضعیت و ماهیت هدف، قصد نسبت به رفتار ارتکابی، قصد و علم نسبت به نتیجه مجرمانه، آگاهی از خسارات تبعی احتمالی و همچنین عنصر روانی لازم در مسئولیت فرماندهان و مافوق‌ها.

علاوه بر این، ادله مورد استناد باید از ویژگی‌هایی نظیر اعتبار، اصالت، تمامیت و قابلیت‌ارزیابی و آزمون قضایی برخوردار باشد؛ به‌گونه‌ای که امکان بررسی صحت و قابلیت‌استناد آن‌ها در فرایند دادرسی فراهم شود.

مزیت اصلی مدل پیشنهادی آن است که از دو رویکرد افراطی و متقابل پرهیز می‌کند؛ از یک‌سو، پیچیدگی‌های فنی و فناورانه را به ابزاری برای ایجاد مصونیت کیفری تبدیل نمی‌کند و از سوی دیگر، هرگونه اختلال یا حمله دیجیتال را بدون ضابطه و صرفاً به‌دلیل ماهیت فناورانه آن، در قالب جنایت جنگی تفسیر نمی‌نماید. این مدل، احراز مسئولیت کیفری را بر پایه نقش انسانی، عنوان قانونی جرم، رابطه سببیت، قصد، علم، کنترل مؤثر و وجود ادله معتبر استوار می‌سازد.

برای مثال در حمله به یک بیمارستان متصل، مدل پیشنهادی ابتدا وجود مخاصمه مسلحانه و پیوند عملیات با مخاصمه را بررسی می‌کند. سپس عنوان احتمالی جنایت، از قبیل حمله به بیمارستان یا قتل عمدی، شناسایی می‌شود. در مرحله بعد، فرایند فنی نفوذ به تجهیزات و سامانه‌های پزشکی بازسازی شده و رابطه میان اختلال ایجادشده در دستگاه‌ها و مرگ یا آسیب واردشده به بیماران ارزیابی می‌گردد. پس از آن، واحد، تیم یا ساختار عملیاتی دخیل در حمله شناسایی می‌شود و نقش اشخاصی همچون اپراتور، فرمانده، مهندس یا پیمانکار، در چارچوب مواد ۲۵ یا ۲۸ اساسنامه رم، مورد تحلیل قرار می‌گیرد. در نهایت، علم مرتکب به ماهیت غیرنظامی و درمانی هدف، قصد ایجاد اختلال در فرایند درمان یا آگاهی وی نسبت به احتمال وقوع مرگ یا آسیب در جریان عادی امور، بر اساس ادله معتبر و قابل‌استناد بررسی می‌شود.

در حمله به شبکه هوشمند آب‌رسانی نیز، مدل می‌کوشد مشخص کند که آیا هدف عملیات، محروم‌سازی جمعیت غیرنظامی از آب آشامیدنی بوده است یا حمله به یک هدف نظامی مشخص. همچنین بررسی می‌شود که آیا اختلال ایجادشده در شبکه، عملاً به قطع آب آشامیدنی منتهی شده و آیا آثار و پیامدهای آن بر بیمارستان‌ها، مراکز درمانی و سایر خدمات عمومی، قابل پیش‌بینی بوده است یا خیر. افزون بر این، نقش اشخاص یا نهادهای دخیل در طراحی، توسعه یا اجرای ابزار حمله مورد ارزیابی قرار می‌گیرد و آگاهی فرماندهان، پیمانکاران یا سایر اشخاص مسئول نسبت به خطرات و پیامدهای عملیات بررسی می‌شود.

مدل هفت‌لایه انتساب مسئولیت کیفری در جنایات جنگی مبتنی بر اینترنت اشیا

لایه	عنوان	پرسش محوری
لایه اول	زمینه مخاصمه	آیا عملیات در مخاصمه مسلحانه و مرتبط با آن انجام شده است؟
لایه دوم	عنوان جنایت جنگی	کدام مصداق ماده ۸ قابل تطبیق است؟
لایه سوم	بازسازی فنی	عملیات از مسیر داده، دستگاه، شبکه، حسگر یا عملگر چگونه انجام شده است؟
لایه چهارم	سببیت	اثر دیجیتال چگونه به نتیجه فیزیکی یا انسانی منتهی شده است؟
لایه پنجم	انتساب عملیاتی	کدام ساختار انسانی عملیات را طراحی، هدایت یا اجرا کرده است؟
لایه ششم	انتساب فردی	کدام شخص حقیقی ذیل ماده ۲۵ یا ۲۸ مسئول است؟
لایه هفتم	عنصر روانی و ادله	آیا قصد، علم یا معیار فرماندهی با ادله معتبر ثابت شده است؟

نتیجه‌گیری

گسترش فناوری‌های مبتنی بر اینترنت اشیا و ادغام روزافزون سامانه‌های دیجیتال با زیرساخت‌های فیزیکی، ماهیت عملیات نظامی و مخاطرات ناشی از مخاصمات مسلحانه را دگرگون ساخته است. در این میان، هرچند اینترنت اشیا به‌خودی‌خود موجب ظهور دسته‌ای مستقل از جنایات بین‌المللی نشده، اما ظرفیت آن برای ارتکاب، تسهیل یا تشدید نقض‌های شدید حقوق بشردوستانه بین‌المللی، چالش‌های نوینی را در حوزه حقوق بین‌الملل کیفری پدید آورده است. حمله به زیرساخت‌های متصل، سامانه‌های درمانی، شبکه‌های انرژی، تجهیزات صنعتی و سایر محیط‌های سایبر- فیزیکی می‌تواند بدون استفاده از ابزارهای

سنتی خشونت، آثار انسانی و مادی گسترده‌ای ایجاد کند و در شرایط معین، مشمول عناوین موجود جنایات جنگی قرار گیرد. یافته‌های این پژوهش نشان می‌دهد که چالش اصلی در این حوزه، دشواری انتساب مسئولیت کیفری در محیط‌های پیچیده و چندلایه دیجیتال است. عملیات مبتنی بر اینترنت اشیا غالباً حاصل تعامل مجموعه‌ای از بازیگران انسانی و فنی، شامل فرماندهان، اپراتورها، برنامه‌نویسان، پیمانکاران خصوصی، سامانه‌های نیمه‌خودکار و زیرساخت‌های متصل است. در چنین فضایی، انتساب مسئولیت کیفری صرفاً از طریق شناسایی منشأ فنی حمله ممکن نیست و مستلزم بازسازی دقیق زنجیره تصمیم‌گیری، کنترل، مشارکت و عنصر روانی اشخاص دخیل در عملیات خواهد بود. به همین دلیل، تفکیک میان انتساب فنی، انتساب دولتی و انتساب کیفری فردی اهمیت بنیادین دارد و نباید این سطوح مختلف انتساب با یکدیگر خلط شوند. بررسی مقررات اساسنامه رم نیز نشان می‌دهد که چارچوب موجود حقوق بین‌الملل کیفری، به‌ویژه از رهگذر مواد ۲۵ و ۲۸، همچنان ظرفیت مواجهه با بسیاری از رفتارهای مجرمانه در بستر اینترنت اشیا را داراست. اشکال مختلف مشارکت کیفری، مسئولیت فرماندهان، معیارهای علم و قصد، و تعهد به اتخاذ تدابیر لازم و معقول، قابلیت انطباق با عملیات سایبری و سایبر ـ فیزیکی را دارند؛ مشروط بر آنکه تفسیر این قواعد با درک دقیق ویژگی‌های فنی محیط‌های متصل همراه باشد. در نهایت، می‌توان گفت که تحول فناوری، شیوه ارتکاب و سازمان‌دهی عملیات نظامی را تغییر داده است و پاسخ حقوقی مناسب در توسعه تفسیرهای تخصصی، تقویت سازوکارهای انتساب، ارتقای استانداردهای ادله دیجیتال و حفظ زنجیره انسانی تصمیم‌گیری در عملیات مبتنی بر اینترنت اشیا نهفته است.

نخستین پیشنهاد آن است که نهادهای قضایی، تقنینی و پژوهشی، رویکردی «فناوری‌خنثی» اما در عین حال «فناوری‌حساس» اتخاذ کنند. فناوری‌خنثی بودن به این معناست که تحقق جنایات جنگی به استفاده از ابزار یا فناوری خاصی محدود نمی‌شود و قواعد موجود حقوق بین‌الملل کیفری قابلیت اعمال بر ابزارهای نوین را نیز دارند. در مقابل، فناوری‌حساس بودن اقتضا می‌کند که ویژگی‌های فنی عملیات مبتنی بر اینترنت اشیا، در تحلیل عناصر حقوقی جرم، از جمله سببیت، پیش‌بینی‌پذیری، قصد، علم، کنترل و ارزیابی ادله، مورد توجه ویژه قرار گیرد.

پیشنهاد دوم، تدوین و توسعه دستورالعمل‌های تفسیری درباره عملیات سایبری- فیزیکی و عملیات مبتنی بر اینترنت اشیا است. این دستورالعمل‌ها باید مفاهیمی همچون «حمله»، «ازکارافتادگی عملکردی»، «داده‌های حیاتی»، «زیرساخت‌های دوگانه»، «آثار آبشاری» و معیارهای احتیاط در حمله را متناسب با محیط‌های متصل و دیجیتال تبیین کنند، بی‌آنکه اصل قانونی بودن جرایم و مجازات‌ها مخدوش شود.

پیشنهاد سوم، تقویت فرایند بررسی حقوقی سلاح‌ها، وسایل و روش‌های نوین جنگی است. دولت‌ها باید ابزارهای سایبری ـ فیزیکی، سامانه‌های نظامی مبتنی بر اینترنت اشیا، بدافزارهای عملیاتی، سامانه‌های نیمه‌خودکار و ابزارهای نفوذ به زیرساخت‌های متصل را در فرایند ارزیابی حقوقی قرار دهند و معیارهایی نظیر قابلیت تمایز، امکان کنترل آثار، خطر سرایت، وجود سازوکار توقف اضطراری، میزان نظارت انسانی و قابلیت ثبت و مستندسازی تصمیم‌ها را مورد بررسی قرار دهند.

پیشنهاد چهارم، ایجاد استانداردهای تخصصی برای ادله دیجیتال در پرونده‌های مرتبط با اینترنت اشیا است. در این حوزه، داده‌هایی نظیر لاگ‌های سامانه، اطلاعات حسگرها، سفت‌افزارها، داده‌های سنجش از راه دور، داده‌های ابری، مکاتبات داخلی و گزارش‌های ارزیابی ریسک، باید با رعایت اصول حفظ زنجیره نگهداری ادله[۳۲]، ثبت هش دیجیتال، نسخه نرم‌افزار، منشأ داده و امکان بررسی و ارزیابی توسط دفاع، گردآوری و نگهداری شوند. همچنین، تحقیقات کیفری در این حوزه مستلزم رویکردی چندرشته‌ای است و همکاری حقوق‌دانان، متخصصان ادله دیجیتال، مهندسان شبکه، کارشناسان زیرساخت و متخصصان فنی را ضروری می‌سازد.

---

[32] Chain of Custody

پیشنهاد پنجم، لزوم حفظ و مستندسازی زنجیره انسانی تصمیم‌گیری در عملیات مبتنی بر اینترنت اشیا است. نیروهای مسلح، نهادهای امنیتی و پیمانکاران فنی باید به‌گونه‌ای عمل کنند که در هر مرحله از عملیات، نقش و مسئولیت اشخاص دخیل به‌طور روشن و قابل‌ردیابی مشخص باشد. در این چارچوب، باید معلوم شود چه شخص یا مرجعی هدف عملیاتی را تأیید کرده، چه افرادی ارزیابی فنی و حقوقی انجام داده‌اند، چه کسانی ابزار یا سامانه را طراحی و آزمایش کرده‌اند، چه مقامی مجوز اجرای عملیات را صادر کرده، چه اشخاصی بر روند اجرا نظارت داشته‌اند، اختیار توقف یا تعلیق عملیات در اختیار چه فرد یا نهادی بوده و مسئول ثبت و گزارش نتایج عملیات چه کسی است. شفاف بودن این زنجیره تصمیم‌گیری، از یک‌سو می‌تواند با افزایش نظارت، دقت و پاسخگویی، از ارتکاب رفتارهای غیرقانونی پیشگیری کند و از سوی دیگر، در صورت وقوع جنایت، امکان انتساب دقیق و عادلانه مسئولیت کیفری را فراهم سازد.

پیشنهاد ششم، توسعه مفهوم «مراقبت مقتضی»[33] در حوزه حقوق بشردوستانه برای شرکت‌های فناوری و پیمانکاران خصوصی است. شرکت‌هایی که تجهیزات اینترنت اشیا، خدمات ابری، سامانه‌های هدف‌گیری، تجهیزات پزشکی متصل یا ابزارهای امنیت سایبری ارائه می‌کنند، باید خطر استفاده از محصولات و خدمات خود در مخاصمات مسلحانه را ارزیابی کرده و در صورت مشاهده خطر آشکار استفاده مجرمانه، سازوکارهای مناسب برای توقف خدمات، گزارش‌دهی یا کاهش خطر را پیش‌بینی کنند. البته این امر به معنای شناسایی مسئولیت کیفری خودکار برای شرکت‌ها نیست، بلکه ناظر بر تقویت مدیریت ریسک، پیشگیری و رعایت الزامات احتیاطی در محیط‌های مخاصمه‌آمیز است.

جمع‌بندی نهایی این است که پاسخ حقوقی به جنایات جنگی مبتنی بر اینترنت اشیا باید میان دو افراط حرکت کند: نه فناوری‌هراسی و جرم‌انگاری بی‌ضابطه، و نه مصونیت فناورانه. معیار نهایی باید رفتار مشخص، عنوان قانونی، رابطه سببیت، نقش انسانی، قصد یا علم، کنترل مؤثر و ادله معتبر باشد. مدل چندلایه پیشنهادی مقاله می‌تواند چارچوبی برای تحقق این هدف فراهم کند.

منابع

- ابوذری، مهرنوش، برزگر، محمدرضا، نادری، زهرا. (۱۴۰۲). «امکان‌سنجی مسئولیت کیفری سلاح‌های جنگی مبتنی بر هوش مصنوعی و مسئله بی‌کیفرمانی در دادگاه کیفری بین‌المللی»، فصلنامه حقوق فناوری‌های نوین، ۴(۸)، ۱۱۹-۱۳۵.
- پیری، حیدر. (۱۴۰۴). «مسئولیت کیفری سیستم‌های مبتنی‌بر هوش مصنوعی برای ارتکاب جرائم بین‌المللی و اعطای وضعیت رزمنده یا شخصیت الکترونیکی به آن‌ها؛ ضرورت‌ها، موانع و راه‌حل‌ها»، فصلنامه پژوهش حقوق کیفری، ۱۴(۵۲)، ۱۵۱-۱۹۶.
- تیموری، مهرداد، کاظمی، سید سجاد. (۱۴۰۴). «مسئولیت کیفری ناشی از نقض فاحش حقوق بین‌الملل بشردوستانه توسط سیستم‌های تسلیحاتی خودمختار هوشمند به‌مثابه جنایت جنگی»، فصلنامه حقوق جزای بین‌الملل، ۳(۲)، ۱-۱۵.
- دلخوش، علیرضا. (۱۳۹۰). «جنبه‌های گوناگون مسئولیت در حقوق بین‌الملل کیفری»، مجله حقوقی بین‌المللی، ۲۸(۴۴)، ۲۲-۲۲۳.
- رنجبریان، امیرحسین، بذّار، وحید. (۱۳۹۷). «رعایت حقوق بین الملل بشردوستانه از سوی ربات‌های نظامی خود فرمان و مسئولیت ناشی از اقدامات آن‌ها»، مجله حقوقی بین‌المللی، ۳۵(۵۹)، ۶۳-۸۴.
- ساعد، نادر. (۱۳۹۳). *حقوق بشردوستانه و مسائل نوظهور (جنگ‌های پسانوین)*، چاپ ۲، تهران: انتشارات خرسندی.
- شریفی طرازکوهی، حسین، صیادنژاد، محمدحسین. (۱۳۹۹). «اِعمال اصول بنیادین حقوق بین‌الملل بشردوستانه بر تسلیحات کاملاً خودکار به‌عنوان ابزار نوین جنگی»، فصلنامه مطالعات حقوق عمومی، ۵۰(۲)، ۵۵۱-۵۷۵.

[33] Due Diligence

- ممتاز، جمشید، رنجبریان، امیرحسین. (۱۳۹۵). *حقوق بین‌الملل بشردوستانه مخاصمات مسلحانه داخلی*، چاپ ۵، تهران: انتشارات میزان.
- ممتاز، جمشید، شایگان، فریده. (۱۳۹۷). *حقوق بین‌الملل بشردوستانه در برابر چالش‌های مخاصمات مسلحانه عصر حاضر*، چاپ ۲، تهران: انتشارات شهر دانش.

- Additional Protocol to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977.
- Chaumette, A.-L. (2018). International Criminal Responsibility of Individuals in Case of Cyberattacks. International Criminal Law Review, 18(1), 1–35.
- Coco, A. (2023). Exploring the Impact of Automation Bias and Complacency on Individual Criminal Responsibility for War Crimes. Journal of International Criminal Justice, 21(5), 1077–1096.
- Davis, J. K. (2022). Developing Applicable Standards of Proof for Peacetime Cyber Attribution (Tallinn Paper No. 13). NATO Cooperative Cyber Defence Centre of Excellence.
- European Union Agency for Cybersecurity. (2020). Guidelines for Securing the Internet of Things: Secure Supply Chain for IoT.
- Greer, C., Burns, M., Wollman, D., & Griffor, E. (2019). Cyber-physical Systems and Internet of Things (NIST Special Publication 1900-202). National Institute of Standards and Technology.
- Greipl, A. R. (2023). Data-driven Learning Systems and the Commission of International Crimes: Concerns for Criminal Responsibility? Journal of International Criminal Justice, 21(5), 1097–1118.
- Henckaerts, J.-M., & Doswald-Beck, L. (2005). Customary International Humanitarian Law: Volume I: Rules. Cambridge University Press.
- International Committee of the Red Cross (ICRC). (2024). International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Building a Culture of Compliance for IHL to Protect Humanity in Todays and Future Conflicts.
- International Committee of the Red Cross (ICRC). (2025). International Humanitarian Law and the Growing Involvement of Civilians in Cyber Operations and Other Digital Activities Related to Armed Conflict.
- International Criminal Court (ICC). (2013). Elements of Crimes.
- International Criminal Court. (1998). Rome Statute of the International Criminal Court. United Nations.
- International Law Commission. (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries. United Nations.
- Jackson, M. (2022). Causation and the Legal Character of Command Responsibility after Bemba at the International Criminal Court. Journal of International Criminal Justice, 20(2), 437–459.
- Jackson, M., & Arnold, R. (2021). Responsibility of Commanders and other Superiors. In K. Ambos (Ed.), The Rome Statute of the International Criminal Court: Article-by-Article Commentary (4th ed.).
- McKenzie, S. (2021). Cyber Operations against Civilian Data: Revisiting War Crimes against Protected Objects and Property in the Rome Statute. Journal of International Criminal Justice, 19(5), 1165–1192.
- Meloni, C. (2010). Command Responsibility in International Criminal Law. T. M. C. Asser Press.
- Prosecutor v. Bemba Gombo, ICC-01/05-01/08 A, Judgment on the Appeal of Mr. Jean-Pierre Bemba Gombo against Trial Chamber III's Judgment Pursuant to Article 74 of the Statute. International Criminal Court Appeals Chamber, June 8, 2018.
- Schmitt, M. N. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
- Spadaro, A. (2023). A Weapon is no Subordinate: Autonomous Weapon Systems and the Scope of Superior Responsibility. Journal of International Criminal Justice, 21(5), 1119–1136.
- Trahan, J. (2021). The Criminalization of Cyber-operations under the Rome Statute. Journal of International Criminal Justice, 19(5), 1133–1164.

- United Nations Human Rights Office of the High Commissioner, & Human Rights Center, University of California, Berkeley. (2022). Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law.