فصلنامه رهیافت‌های نوین در مطالعات اسلامی

License Number: 85625 **Article Cod:** SH26R507957 **ISSN-P:** 2676-6442

مرز تفکیک جرم داخلی و جرم بین‌المللی در جنگ‌های سایبری با تکیه بر نظریه‌پردازی کیفری

(تاریخ دریافت ۱۴۰۵/۰۱/۲۵ تاریخ تصویب ۱۴۰۵/۰۳/۰۴)

علی سلیمانی

کارآموز وکالت و عضو مرکز وکلای قوه قضاییه استان کرمانشاه

چکیده

تحولات شتابان فناوری اطلاعات و ارتباطات موجب شکل‌گیری فضای سایبری به‌عنوان یکی از مهم‌ترین عرصه های تعاملات سیاسی، اقتصادی، اجتماعی و امنیتی شده است. در کنار فرصت‌های گسترده ناشی از توسعه این فضا، ظهور اشکال نوین بزهکاری و منازعات سایبری نیز نظام‌های حقوقی داخلی و بین‌المللی را با چالش‌های بی‌سابقه‌ای مواجه ساخته است. جنگ‌های سایبری به‌عنوان یکی از پیچیده‌ترین نمودهای تهدیدات نوین، از مرزهای سنتی حقوق کیفری عبور کرده و پرسش های اساسی درباره صلاحیت کیفری، ماهیت رفتار مجرمانه، مسئولیت دولت‌ها و اشخاص، معیارهای انتساب، قلمرو اجرای قوانین کیفری و مرجع صالح برای رسیدگی ایجاد کرده‌اند. یکی از مهم‌ترین مسائل در این حوزه، تعیین مرز میان جرم داخلی و جرم بین‌المللی در بستر عملیات سایبری است؛ زیرا در بسیاری از موارد، یک حمله سایبری می‌تواند به‌طور هم‌زمان ویژگی‌های هر دو نوع جرم را دارا باشد. مقاله حاضر با رویکردی توصیفی ـ تحلیلی و با بهره‌گیری از نظریه‌های نوین حقوق کیفری، به بررسی معیارهای تمایز میان جرائم داخلی و جرائم بین‌المللی در جنگ‌های سایبری می‌پردازد. یافته‌های پژوهش نشان می‌دهد که معیارهای سنتی مبتنی بر قلمرو سرزمینی، تابعیت و محل

وقوع جرم، پاسخگوی پیچیدگی‌های جنگ‌های سایبری نیستند و لازم است نظریه‌های نوین کیفری مبتنی بر حمایت از ارزش‌های بنیادین جامعه بین‌المللی، اصل مسئولیت مشترک، حمایت از امنیت جهانی و اصل صلاحیت جهانی در کنار قواعد سنتی مورد توجه قرار گیرند. همچنین، توسعه همکاری‌های کیفری بین‌المللی، تدوین قواعد مشترک و ایجاد سازوکارهای تخصصی رسیدگی می‌تواند نقش مؤثری در کاهش خلأهای موجود ایفا کند.

واژگان کلیدی :جنگ سایبری، جرم داخلی، جرم بین‌المللی، نظریه‌پردازی کیفری، صلاحیت کیفری، امنیت سایبری

مقدمه

گسترش فناوری‌های دیجیتال طی دهه‌های اخیر، ساختار روابط میان دولت‌ها، سازمان‌های بین‌المللی، شرکت‌های بزرگ و شهروندان را به‌طور اساسی متحول کرده است. فضای سایبری دیگر صرفاً بستری برای تبادل اطلاعات نیست، بلکه به عرصه‌ای برای رقابت‌های ژئوپلیتیکی، اعمال قدرت، جاسوسی، خرابکاری، عملیات روانی و حتی مخاصمات نظامی تبدیل شده است. در چنین شرایطی، مفهوم امنیت نیز از چارچوب‌های سنتی فاصله گرفته و ابعاد جدیدی یافته است که امنیت سایبری یکی از مهم‌ترین آن‌ها محسوب می‌شود.حملات سایبری امروز قادرند بدون استفاده از تجهیزات نظامی متعارف، زیرساخت‌های حیاتی کشورها را مختل کنند، شبکه‌های برق، آب، حمل‌ونقل، بانکداری، سلامت، ارتباطات و سامانه‌های دفاعی را هدف قرار دهند و خساراتی هم‌سنگ یا حتی فراتر از حملات نظامی کلاسیک ایجاد نمایند. همین ویژگی موجب شده است که بسیاری از اندیشمندان حقوق بین‌الملل، جنگ سایبری را یکی از مهم‌ترین جلوه‌های جنگ‌های نسل پنجم بدانند.در کنار

توسعه تهدیدات سایبری، حقوق کیفری نیز با پرسش‌های جدیدی روبه‌رو شده است. مهم ترین پرسش آن است که آیا تمامی حملات سایبری باید در قلمرو حقوق کیفری داخلی بررسی شوند یا برخی از آن‌ها ماهیت جرم بین‌المللی دارند؟ پاسخ به این پرسش مستلزم بازاندیشی در مبانی نظری جرم، مسئولیت کیفری، صلاحیت قضایی و قلمرو اجرای قوانین کیفری است.در حقوق سنتی، تمایز میان جرم داخلی و جرم بین‌المللی عمدتاً بر پایه محل وقوع جرم، تابعیت مرتکب، تابعیت بزه‌دیده یا منافع دولت‌ها صورت می‌گرفت. اما در فضای سایبری، مرتکب ممکن است در کشوری مستقر باشد، از زیرساخت کشور دیگری استفاده کند، سرورهای کشور سوم را به کار گیرد و آثار رفتار وی در ده‌ها کشور مختلف مشاهده شود. چنین وضعیتی موجب شده است که معیارهای کلاسیک پاسخگوی واقعیت‌های نوین نباشند.از سوی دیگر، پیچیدگی انتساب حملات سایبری به دولت‌ها، گروه‌های سازمان‌یافته یا اشخاص حقیقی، یکی دیگر از چالش‌های مهم نظام عدالت کیفری محسوب می‌شود. بسیاری از عملیات سایبری توسط گروه‌هایی انجام می‌شود که وابستگی رسمی به دولت‌ها ندارند، اما از حمایت یا هدایت غیرمستقیم آن‌ها برخوردارند. این موضوع، مرز میان مسئولیت کیفری فردی و مسئولیت بین‌المللی دولت‌ها را نیز با ابهام مواجه ساخته است.بر همین اساس، نظریه‌پردازی کیفری معاصر تلاش کرده است با ارائه معیارهای جدید، زمینه انطباق حقوق کیفری با تحولات فناوری را فراهم آورد. این نظریه‌ها بر حمایت از منافع بنیادین جامعه جهانی، اصل تناسب، مسئولیت فراملی، عدالت کیفری جهانی و حمایت از ارزش‌های مشترک بشری تأکید دارند.مقاله حاضر درصدد است ضمن بررسی مبانی نظری حقوق کیفری و حقوق بین‌الملل کیفری، معیارهای تفکیک جرم داخلی از جرم بین‌المللی در جنگ‌های سایبری را تحلیل کرده و نقاط ضعف و قوت نظریه‌های موجود را ارزیابی نماید. با توسعه فناوری اطلاعات، بسیاری از جرائم سنتی به فضای سایبری منتقل شده‌اند و در کنار آن، گونه‌های کاملاً جدیدی از رفتارهای مجرمانه نیز شکل گرفته است. در این میان،

جنگ‌های سایبری جایگاهی متفاوت دارند؛ زیرا آثار آن‌ها تنها محدود به خسارت‌های مالی یا نقض حریم خصوصی نیست، بلکه امنیت ملی، ثبات منطقه‌ای و حتی صلح و امنیت بین‌المللی را نیز تحت تأثیر قرار می‌دهند.یکی از مهم‌ترین چالش‌های حقوق کیفری در این حوزه، تعیین ماهیت حقوقی حملات سایبری است. در برخی موارد، حمله علیه سامانه‌های رایانه‌ای یک دولت صرفاً مشمول قوانین کیفری داخلی است؛ اما در موارد دیگر، همان حمله می‌تواند آثار فرامرزی گسترده‌ای ایجاد کند و امنیت جامعه بین‌المللی را به مخاطره اندازد. نبود معیارهای روشن برای تفکیک این دو وضعیت، موجب اختلاف نظر میان حقوقدانان و محاکم شده است.از سوی دیگر، تنوع بازیگران فضای سایبری، دشواری انتساب رفتار مجرمانه، سرعت بالای وقوع حملات، استفاده از زیرساخت‌های چندملیتی و تفاوت قوانین داخلی کشورها، فرآیند تعقیب و مجازات مرتکبان را با مشکلات فراوانی روبه‌رو ساخته است.در چنین شرایطی، این پرسش مطرح می‌شود که چه معیارهایی می‌توانند مرز میان جرم داخلی و جرم بین‌المللی را در جنگ‌های سایبری مشخص کنند و نظریه‌های نوین حقوق کیفری تا چه اندازه قادر به پاسخگویی به این چالش هستند.مطالعات انجام‌شده در حوزه جرائم سایبری عمدتاً بر موضوعاتی مانند صلاحیت کیفری، مسئولیت دولت‌ها، حمایت از زیرساخت‌های حیاتی، جرائم رایانه‌ای و امنیت اطلاعات تمرکز داشته‌اند. بخش قابل توجهی از پژوهش‌ها نیز به تحلیل اسناد بین‌المللی و بررسی قواعد حقوق بشردوستانه در فضای سایبری اختصاص یافته است.در میان پژوهش‌های داخلی، بیشتر آثار به بررسی قانون جرائم رایانه‌ای، صلاحیت کیفری دادگاه‌های ایران، مسئولیت مرتکبان جرائم سایبری و همکاری‌های بین‌المللی پرداخته‌اند. با وجود ارزش علمی این تحقیقات، کمتر پژوهشی به‌صورت مستقل مرز میان جرم داخلی و جرم بین‌المللی را با تکیه بر نظریه‌های کیفری مورد تحلیل قرار داده است.در ادبیات خارجی نیز اگرچه آثار متعددی درباره جنگ سایبری، حقوق بین‌الملل، مسئولیت دولت‌ها و صلاحیت

جهـانی منتشـر شـده اسـت، امـا هنـوز اجمـاع روشـنی دربـاره معیارهـای تفکیـک جـرائم داخلـی و بـین‌المللـی در عملیـات سـایبری وجـود نـدارد. همـین خـلأ، ضـرورت انجـام پژوهش حاضر را آشکار می‌سازد.

بخش اول: مبانی نظری جرم داخلی و جرم بین‌المللی در فضای سایبری

بند اول: مفهوم جرم بین‌المللی و ویژگی‌های آن

جرم بین‌المللی به رفتاری اطلاق می‌شود که به دلیل شدت، گستره آثار و تعرض به ارزش‌هـای بنیادین جامعه جهانی، صرفاً نقض قوانین داخلی یک کشـور محسـوب نمـی‌شـود، بلکـه نقـض قواعد آمره یا هنجارهای اساسی حقوق بین‌الملل نیز به شمار می‌آید. این دسته از جرائم، امنیت و منافع مشترک جامعه بـین‌المللـی را مـورد تهدیـد قـرار داده و از ایـن رو، تعقیـب و مجـازات مرتکبان آن‌ها تنها در صلاحیت یک دولت خاص قـرار نـدارد، بلکـه امکـان اعمـال صـلاحیت توسط جامعه بین‌المللی یا دولت‌های دیگر نیز در شرایط معین وجود دارد.در نظام سنتی حقوق بین‌الملل کیفری، جرائمی مانند نسل کشـی، جنایـت علیـه بشـریت، جنایـات جنگـی و تجـاوز، مهم‌ترین مصادیق جرائم بین‌المللی محسوب می‌شوند. با ایـن حـال، توسـعه فنـاوری‌هـای نـوین سبب شده است که برخی عملیات سایبری نیز در صورت تحقـق شـرایط خـاص، قابلیـت قـرار گرفتن در زمره رفتارهای واجد وصف بـین‌المللـی را پیـدا کننـد. بـرای نمونـه، حملـه سـایبری گسترده به شبکه برق، سامانه‌های درمانی یا تأسیسات هسـته‌ای یـک کشـور در زمـان مخاصـمه مسلحانه، ممکن است آثار انسانی و امنیتی به اندازه یک حمله نظامی کلاسیک داشته باشد و از منظر حقوق بین‌الملل کیفری قابل ارزیابی باشد.ویژگی مهـم جـرائم بـین‌المللـی آن اسـت کـه عنصر زیان‌بار آن‌ها تنها متوجه یک دولت نیست، بلکه امنیت منطقه‌ای، ثبات بین‌المللی، حقوق بنیادین انسان‌ها و نظم عمومی جهانی را نیز تحت تأثیر قرار می‌دهد. به همـین دلیـل، بسـیاری از نظریه‌های نوین کیفری معتقدند که معیار اصلی تشخیص جـرم بـین‌المللـی، صـرفاً محـل وقـوع

رفتار نیست، بلکه میزان تعرض به ارزش‌های بنیادین جامعه جهانی نیز باید مورد توجه قرار گیرد.

بند دوم: مفهوم جنگ سایبری و جایگاه آن در حقوق کیفری

جنگ سایبری به مجموعه عملیات برنامه‌ریزی‌شده‌ای اطلاق می‌شود که با استفاده از ابزارهای دیجیتال، شبکه‌های رایانه‌ای و سامانه‌های ارتباطی، با هدف ایجاد اختلال، تخریب، جاسوسی، سرقت اطلاعات، فلج کردن زیرساخت‌های حیاتی یا تضعیف توان دفاعی و اقتصادی یک دولت انجام می‌شود. تفاوت اساسی جنگ سایبری با بسیاری از جرائم رایانه‌ای در آن است که هدف اصلی آن صرفاً کسب منفعت مالی یا ارتکاب بزه علیه اشخاص نیست، بلکه تحقق اهداف راهبردی، نظامی، امنیتی یا سیاسی است.در بسیاری از موارد، عملیات سایبری بخشی از یک راهبرد کلان نظامی یا امنیتی محسوب می‌شود و هم‌زمان با اقدامات سیاسی، اقتصادی یا نظامی اجرا می‌گردد. این ویژگی سبب شده است که تحلیل حقوقی جنگ سایبری تنها در چارچوب حقوق کیفری داخلی امکان‌پذیر نباشد و نیازمند بهره‌گیری از قواعد حقوق بین‌الملل عمومی، حقوق بشردوستانه و حقوق بین‌الملل کیفری باشد.از منظر حقوق کیفری، جنگ سایبری به دلیل فقدان مرزهای جغرافیایی مشخص، ناشناس بودن بسیاری از عاملان، استفاده از ابزارهای غیرمتمرکز و امکان انجام عملیات از فاصله هزاران کیلومتری، چالش‌های متعددی در زمینه احراز عنصر مادی، انتساب رفتار مجرمانه، اثبات سوءنیت و اجرای مجازات ایجاد کرده است. همین ویژگی‌ها موجب شده‌اند که نظریه‌های کلاسیک حقوق کیفری به تنهایی پاسخگوی این پدیده نباشند.

بند سوم: مبانی نظریه‌پردازی کیفری در مواجهه با جنگ‌های سایبری

نظریه‌پردازی کیفری همواره متناسب با تحولات اجتماعی، اقتصادی و فناوری دستخوش تغییر شده است. ظهور فضای سایبری نیز ضرورت بازنگری در بسیاری از مفاهیم بنیادین حقوق

کیفری را آشکار ساخته است. امروزه اندیشمندان حقوق کیفری بر این باورند که قواعد سنتی مبتنی بر قلمرو سرزمینی، دیگر برای مقابله با جرائم فراملی کافی نیست و باید رویکردهای نوینی در سیاست جنایی اتخاذ شود.یکی از مهم‌ترین رویکردهای جدید، نظریه حمایت از منافع بنیادین جامعه جهانی است. بر اساس این دیدگاه، هر رفتاری که امنیت جمعی، زیرساخت‌های حیاتی، جان انسان‌ها یا ثبات بین‌المللی را به مخاطره اندازد، صرف‌نظر از محل وقوع آن، می‌تواند واجد آثار بین‌المللی باشد. این نظریه تلاش می‌کند فاصله میان حقوق کیفری داخلی و حقوق بین‌الملل کیفری را کاهش دهد و سازوکارهای مشترکی برای مقابله با تهدیدات نوین ایجاد کند.دیدگاه دیگر بر اصل مسئولیت مشترک دولت‌ها در حفاظت از امنیت سایبری تأکید دارد. مطابق این نظریه، امنیت فضای سایبری یک منفعت مشترک جهانی است و همه دولت‌ها وظیفه دارند از تبدیل قلمرو خود به بستری برای حملات سایبری علیه سایر کشورها جلوگیری کنند. این برداشت، زمینه گسترش همکاری‌های قضایی، استرداد مجرمان، تبادل ادله الکترونیکی و هماهنگی قوانین کیفری را فراهم می‌سازد.

بخش دوم: معیارهای تفکیک جرم داخلی و جرم بین‌المللی در جنگ‌های سایبری

بند اول: معیار سرزمینی و محدودیت‌های آن

اصل سرزمینی یکی از قدیمی‌ترین مبانی اعمال صلاحیت کیفری است. بر اساس این اصل، هر دولتی نسبت به جرائمی که در قلمرو آن واقع می‌شوند، صلاحیت انحصاری رسیدگی دارد. این اصل در اغلب نظام‌های حقوقی پذیرفته شده و همچنان مبنای اصلی اعمال قوانین کیفری داخلی محسوب می‌شود.با وجود این، در فضای سایبری تعیین محل وقوع جرم همواره امکان‌پذیر نیست. ممکن است مرتکب در یک کشور حضور داشته باشد، بدافزار از طریق سرورهای کشور دوم منتقل شود، سامانه آسیب‌دیده در کشور سوم قرار گیرد و خسارت نهایی در چندین کشور مختلف ایجاد شود. در چنین وضعیتی، تعیین اینکه جرم دقیقاً در کدام قلمرو

واقع شده، با دشواری فراوان همراه است.علاوه بر این، برخی عملیات سایبری به صورت هم‌زمان چندین کشور را هدف قرار می‌دهند و آثار آن‌ها به یک قلمرو محدود نمی‌شود. در نتیجه، اصل سرزمینی به تنهایی نمی‌تواند پاسخگوی همه اختلافات صلاحیتی باشد و ناگزیر باید در کنار سایر اصول مورد استفاده قرار گیرد.

بند دوم: معیار آثار و نتایج جرم

یکی از معیارهای مهم در تشخیص ماهیت حملات سایبری، بررسی دامنه آثار و نتایج آن‌ها است. هرچه آثار رفتار از مرزهای داخلی فراتر رود و امنیت یا منافع چند کشور را به طور هم‌زمان تهدید کند، احتمال بین‌المللی تلقی شدن آن افزایش می‌یابد.برای مثال، اگر یک حمله سایبری موجب اختلال گسترده در شبکه بانکی جهانی، سامانه‌های ناوبری بین‌المللی، خطوط هوایی یا شبکه های ارتباطی چند کشور شود، آثار آن دیگر صرفاً داخلی نیست. همچنین حملاتی که منجر به از کار افتادن بیمارستان‌ها، تأسیسات انرژی، شبکه‌های آب‌رسانی یا سامانه‌های هشدار اضطراری شوند، در صورت ایجاد خسارات انسانی گسترده، ممکن است واجد ویژگی‌های جرائم بین‌المللی تلقی شوند.بنابراین، ارزیابی گستره آثار جرم یکی از مهم‌ترین شاخص‌های تفکیک میان جرائم داخلی و بین‌المللی در فضای سایبری است. هرچه منافع بیشتری از جامعه جهانی در معرض آسیب قرار گیرد، ضرورت اعمال قواعد حقوق بین‌الملل کیفری نیز افزایش خواهد یافت.

بند سوم: معیار ماهیت هدف حمله سایبری

هدف عملیات سایبری نیز نقش تعیین‌کننده‌ای در تشخیص ماهیت حقوقی آن دارد. حمله به یک حساب کاربری شخصی، یک شرکت خصوصی یا یک سامانه تجاری، معمولاً در قلمرو جرائم داخلی قرار می‌گیرد؛ اما حمله به زیرساخت‌های حیاتی، مراکز کنترل نیروگاه‌ها، سامانه‌های دفاع موشکی، تأسیسات هسته‌ای، مراکز درمانی یا شبکه‌های حیاتی ملی، از حیث

آثار و اهمیت، وضعیت متفاوتی دارد.در نظریه‌های نوین کیفری، هرچه هدف حمله با امنیت عمومی، حاکمیت دولت، سلامت عمومی یا صلح و امنیت بین‌المللی ارتباط بیشتری داشته باشد، امکان تحلیل آن در چارچوب جرائم بین‌المللی نیز افزایش می‌یابد. به بیان دیگر، صرف ابزار سایبری تعیین‌کننده نیست، بلکه موضوع و هدف حمله نیز در تعیین ماهیت جرم نقش اساسی ایفا می‌کند.این معیار به ویژه در شرایط مخاصمات مسلحانه اهمیت بیشتری پیدا می‌کند؛ زیرا بسیاری از عملیات سایبری در زمان جنگ با هدف تضعیف توان دفاعی یا ایجاد رعب عمومی انجام می‌شوند و آثار آن‌ها از حدود یک جرم رایانه‌ای معمولی فراتر می‌رود.

بخش سوم: معیارهای تفکیک جرم داخلی و جرم بین‌المللی در جنگ‌های سایبری

بند اول: معیار شدت خسارت و میزان تهدید علیه امنیت عمومی

یکی از مهم‌ترین شاخص‌های تمایز میان جرم داخلی و جرم بین‌المللی در جنگ‌های سایبری، میزان خسارت واردشده و گستره تهدید علیه امنیت عمومی است. در حقوق کیفری کلاسیک، شدت زیان وارده یکی از عوامل مؤثر در تعیین درجه جرم و نوع واکنش کیفری محسوب می‌شود؛ اما در فضای سایبری، این معیار ابعاد گسترده‌تری یافته است. ممکن است یک حمله سایبری بدون تخریب فیزیکی، خسارات اقتصادی، اجتماعی و امنیتی بسیار گسترده‌ای ایجاد کند و عملکرد بخش‌های حیاتی یک یا چند کشور را برای مدت طولانی مختل سازد.هرچه پیامدهای یک حمله از حوزه منافع خصوصی فراتر رفته و نظم عمومی، سلامت شهروندان، امنیت اقتصادی یا ثبات سیاسی را تهدید کند، احتمال آنکه رفتار ارتکابی در زمره جرائم بین‌المللی قرار گیرد افزایش می‌یابد. برای نمونه، حمله به سامانه کنترل یک سد، نیروگاه برق، شبکه گاز، سیستم کنترل ترافیک هوایی یا سامانه‌های درمانی در صورتی که موجب تلفات انسانی گسترده یا اخلال جدی در زندگی عمومی شود، صرفاً یک جرم رایانه‌ای عادی تلقی نمی‌شود، بلکه می‌تواند از منظر امنیت بین‌المللی نیز مورد ارزیابی قرار گیرد.در مقابل، حملاتی

که آثار آن‌ها محدود به خسارت مالی اشخاص، سرقت اطلاعات یا اختلال در فعالیت یک مؤسسه خصوصی باشد، هرچند از منظر حقوق داخلی واجد وصف کیفری هستند، اما معمولاً فاقد ویژگی‌های لازم برای بین‌المللی شدن جرم محسوب می‌شوند. بنابراین، شدت خسارت و کیفیت منافع آسیب‌دیده از مهم‌ترین معیارهای تشخیص ماهیت حقوقی عملیات سایبری به شمار می‌رود.

بند دوم: معیار انتساب عملیات سایبری به دولت‌ها

یکی از پیچیده‌ترین موضوعات در حقوق کیفری بین‌المللی، مسئله انتساب عملیات سایبری است. برخلاف جرائم سنتی که مرتکب غالباً قابل شناسایی است، در بسیاری از حملات سایبری، عامل یا عوامل واقعی با استفاده از ابزارهای فنی پیشرفته، هویت خود را پنهان می‌کنند یا عملیات را از طریق شبکه‌ای از سرورها و سامانه‌های واسطه انجام می‌دهند.از منظر حقوق بین‌الملل، زمانی که حمله سایبری مستقیماً توسط نهادهای رسمی یک دولت انجام شود یا گروه‌های غیردولتی تحت هدایت، کنترل مؤثر یا حمایت سازمان‌یافته آن دولت اقدام کنند، امکان انتساب رفتار به دولت افزایش می‌یابد. در چنین شرایطی، موضوع از حوزه صرف مسئولیت کیفری فردی فراتر رفته و مسئولیت بین‌المللی دولت نیز مطرح می‌شود.با این حال، اثبات چنین انتسابی همواره دشوار است. بسیاری از دولت‌ها از گروه‌های غیررسمی یا پیمانکاران سایبری استفاده می‌کنند تا امکان انتساب مستقیم عملیات به آن‌ها کاهش یابد. همین موضوع سبب شده است که نظریه‌پردازان حقوق کیفری بر ضرورت توسعه قواعد اثبات، استانداردهای ادله دیجیتال و همکاری‌های بین‌المللی در زمینه کشف منشأ حملات تأکید کنند.

بند سوم: نقش صلاحیت جهانی در تعقیب جرائم سایبری

اصل صلاحیت جهانی یکی از مهم‌ترین ابزارهای حقوق بین‌الملل کیفری برای مقابله با جرائمی است که آثار آن‌ها کل جامعه جهانی را متأثر می‌سازد. بر اساس این اصل، برخی جرائم به اندازه‌ای مهم هستند که هر دولت، صرف‌نظر از محل وقوع جرم یا تابعیت مرتکب و بزه‌دیده، می‌تواند نسبت به تعقیب و محاکمه مرتکبان اقدام کند.اگرچه تاکنون همه حملات سایبری مشمول اصل صلاحیت جهانی شناخته نشده‌اند، اما بسیاری از حقوقدانان معتقدند که حملات گسترده علیه زیرساخت‌های حیاتی، در صورتی که آثار انسانی و امنیتی وسیعی ایجاد کنند، می‌توانند در آینده مشمول این اصل قرار گیرند. چنین رویکردی به ویژه در مواردی اهمیت پیدا می‌کند که دولت محل وقوع جرم توانایی یا اراده لازم برای تعقیب مرتکبان را نداشته باشد.اعمال صلاحیت جهانی در حوزه فضای سایبری علاوه بر مزایا، با چالش‌هایی نیز همراه است. تفاوت نظام‌های حقوقی، اختلاف در تعریف جرائم سایبری، تعارض صلاحیت‌ها و ملاحظات سیاسی از جمله عواملی هستند که اجرای این اصل را با دشواری روبه‌رو می‌کنند. با وجود این، گسترش تهدیدات سایبری ضرورت بازنگری در قلمرو صلاحیت جهانی را بیش از گذشته آشکار ساخته است.

بند چهارم: چالش‌های اثبات جرم در جنگ‌های سایبری

یکی از اساسی‌ترین موانع اجرای عدالت کیفری در حوزه جنگ‌های سایبری، دشواری اثبات عناصر جرم است. در بسیاری از پرونده‌ها، داده‌های دیجیتال به سرعت حذف یا تغییر می‌یابند، مسیر انتقال اطلاعات از چندین کشور عبور می‌کند و ابزارهای ناشناس‌ساز، شناسایی مرتکبان را بسیار پیچیده می‌کنند.عنصر مادی جرم در فضای سایبری معمولاً در قالب داده‌های الکترونیکی، لاگ‌های شبکه، اطلاعات سرورها و شواهد دیجیتال قابل احراز است. این ادله، برخلاف ادله سنتی، ماهیتی شکننده دارند و در صورت عدم جمع‌آوری صحیح، ارزش اثباتی خود را از دست می‌دهند. از سوی دیگر، اثبات عنصر روانی نیز با دشواری‌هایی همراه است؛

زیرا در بسیاری از عملیات سایبری، تشخیص قصد واقعی مرتکب، انگیزه سیاسی یا اقتصادی و میزان آگاهی وی از آثار رفتار، نیازمند تحلیل‌های فنی و اطلاعاتی گسترده است.به همین دلیل، نظریه‌های نوین کیفری بر ایجاد سازوکارهای تخصصی برای حفظ، جمع‌آوری و ارزیابی ادله الکترونیکی تأکید دارند. تشکیل تیم‌های مشترک تحقیق، توسعه آزمایشگاه‌های جرم‌شناسی دیجیتال و تدوین استانداردهای واحد برای اعتبارسنجی ادله، از جمله راهکارهایی است که می‌تواند فرآیند اثبات جرائم سایبری را تسهیل کند.

بخش چهارم: تحلیل نظریه‌های کیفری در تفکیک جرم داخلی و جرم بین‌المللی

بند اول: نظریه حمایت از ارزش‌های بنیادین جامعه بین‌المللی

این نظریه بر این مبنا استوار است که حقوق کیفری نباید صرفاً حافظ منافع دولت‌ها باشد، بلکه باید از ارزش هایی حمایت کند که متعلق به کل جامعه جهانی هستند. امنیت جمعی، جان انسان‌ها، زیرساخت‌های حیاتی، صلح بین‌المللی و کرامت انسانی از جمله این ارزش‌ها محسوب می‌شوند.بر اساس این دیدگاه، هرگاه عملیات سایبری این ارزش‌های بنیادین را به طور گسترده تهدید کند، صرف‌نظر از محل وقوع حمله یا تابعیت مرتکب، رفتار ارتکابی می‌تواند واجد وصف بین‌المللی باشد. این نظریه تلاش می‌کند مرزهای سنتی حقوق کیفری را با واقعیت‌های عصر دیجیتال هماهنگ سازد و از محدود شدن واکنش کیفری به قلمرو یک دولت جلوگیری کند.با وجود مزایای این رویکرد، برخی منتقدان معتقدند که نبود معیارهای دقیق برای تشخیص ارزش های بنیادین ممکن است موجب تفسیرهای متفاوت و گسترش بی‌ضابطه قلمرو جرائم بین‌المللی شود. ازاین‌رو، لازم است شاخص‌های مشخصی برای ارزیابی میزان تهدید علیه جامعه جهانی تدوین گردد.

بند دوم: نظریه مسئولیت فراملی

نظریه مسئولیت فراملی بر این اصل استوار است که در جهان به‌هم‌پیوسته امروز، بسیاری از تهدیدها از مرزهای ملی عبور می‌کنند و مقابله با آن‌ها مستلزم همکاری مشترک دولت‌ها است. در این چارچوب، جنگ‌های سایبری نمونه بارزی از تهدیدات فراملی محسوب می‌شوند؛ زیرا آثار آن‌ها معمولاً محدود به یک کشور نیست و امنیت شبکه‌های بین‌المللی را نیز تحت تأثیر قرار می‌دهد.این نظریه پیشنهاد می‌کند که در کنار مسئولیت کیفری مرتکبان، مسئولیت دولت‌ها نیز در زمینه پیشگیری، همکاری قضایی، تبادل اطلاعات، استرداد مجرمان و جلوگیری از سوءاستفاده از قلمرو ملی مورد توجه قرار گیرد. به بیان دیگر، اگر دولتی آگاهانه اجازه دهد از زیرساخت‌های آن برای انجام حملات گسترده علیه سایر کشورها استفاده شود و اقدامات لازم برای جلوگیری از آن را انجام ندهد، ممکن است از منظر حقوق بین‌الملل با مسئولیت مواجه شود.مزیت اصلی این نظریه آن است که بر همکاری و همگرایی میان نظام‌های حقوقی تأکید دارد و از نگاه صرفاً سرزمینی فاصله می‌گیرد. البته اجرای مؤثر آن مستلزم وجود اعتماد متقابل میان دولت‌ها، استانداردهای مشترک در زمینه تبادل ادله و سازوکارهای شفاف همکاری قضایی است.

بند سوم: نظریه عدالت کیفری جهانی و تأثیر آن بر جرائم سایبری

نظریه عدالت کیفری جهانی بر این باور است که برخی رفتارها به اندازه‌ای خطرناک هستند که تعقیب آن‌ها نباید وابسته به اراده یا توانایی یک دولت خاص باشد. این دیدگاه که ابتدا در خصوص شدیدترین جرائم بین‌المللی مطرح شد، به تدریج در حوزه تهدیدات نوظهور از جمله حملات سایبری گسترده نیز مورد توجه قرار گرفته است.بر اساس این نظریه، اگر عملیات سایبری موجب خسارات وسیع انسانی، اقتصادی یا زیست‌محیطی شود و آثار آن امنیت بین‌المللی را به طور جدی تهدید کند، جامعه جهانی باید سازوکارهای مؤثری برای تعقیب مرتکبان ایجاد کند. چنین رویکردی می‌تواند از ایجاد مناطق امن برای مجرمان سایبری

جلوگیری کرده و سطح بازدارندگی حقوق کیفری را افزایش دهد.با وجود این، تحقق کامل عدالت کیفری جهانی در حوزه سایبری همچنان با موانع حقوقی، سیاسی و فنی روبه‌رو است. اختلاف دولت‌ها درباره حدود حاکمیت ملی، تفاوت در سیاست‌های کیفری و نبود معاهده جامع جهانی درباره جنگ‌های سایبری از جمله مهم‌ترین این چالش‌ها به شمار می‌رود.

بخش پنجم: ارزیابی نظریه‌ها و ارائه الگوی پیشنهادی برای تفکیک جرم داخلی و جرم بین‌المللی در جنگ‌های سایبری

بند اول: نقد رویکردهای موجود در تفکیک جرائم سایبری

بررسی نظریه‌های مطرح‌شده نشان می‌دهد که هیچ‌یک از رویکردهای موجود به‌تنهایی قادر به پاسخگویی کامل به پیچیدگی‌های جنگ‌های سایبری نیستند. معیارهای سنتی حقوق کیفری، مانند اصل سرزمینی، تابعیت مرتکب یا محل وقوع نتیجه، در بسیاری از پرونده‌های سایبری با دشواری‌های عملی مواجه می‌شوند؛ زیرا در این نوع حملات، عناصر مختلف جرم ممکن است در کشورهای متعدد تحقق یابند و تعیین محل دقیق ارتکاب رفتار یا نتیجه، عملاً امکان‌پذیر نباشد.از سوی دیگر، نظریه‌هایی که صرفاً بر آثار فرامرزی یا شدت خسارت تأکید می‌کنند نیز با محدودیت‌هایی روبه‌رو هستند. بسیاری از حملات سایبری اگرچه خسارت اقتصادی قابل توجهی ایجاد می‌کنند، اما لزوماً امنیت یا صلح بین‌المللی را تهدید نمی‌کنند. بنابراین، نمی‌توان هر حمله فرامرزی را به‌عنوان جرم بین‌المللی تلقی کرد؛ زیرا چنین تفسیری موجب گسترش بی‌رویه قلمرو حقوق بین‌الملل کیفری خواهد شد.همچنین، رویکرد مبتنی بر انتساب عملیات به دولت‌ها نیز همواره کارآمد نیست. در عمل، بخش قابل توجهی از حملات توسط گروه‌های مستقل، شبکه‌های مجرمانه سازمان‌یافته یا بازیگران غیردولتی انجام می‌شود که وابستگی رسمی آنان به دولت‌ها قابل اثبات نیست. در نتیجه، محدود کردن مفهوم جرم بین‌المللی به حملاتی که مستقیماً به دولت‌ها منتسب هستند، بسیاری از تهدیدات جدی فضای سایبری را از قلمرو این مفهوم خارج می‌کند.بر این اساس، ضروری است معیارهای حقوق کیفری داخلی، حقوق

بین‌الملل کیفری و ملاحظات فنی فضای سایبری در قالب یک الگوی تلفیقی مورد استفاده قرار گیرند تا امکان تفکیک دقیق‌تر میان جرائم داخلی و بین‌المللی فراهم شود.

بند دوم: الگوی پیشنهادی برای تفکیک جرم داخلی و جرم بین‌المللی

با توجه به تحولات فناوری و ناکارآمدی برخی معیارهای سنتی، می‌توان الگویی چندمعیاره برای تشخیص ماهیت جرائم سایبری ارائه کرد. در این الگو، تصمیم‌گیری نباید صرفاً بر پایه یک معیار انجام شود، بلکه مجموعه‌ای از شاخص‌ها باید به صورت هم‌زمان مورد ارزیابی قرار گیرد.نخستین شاخص، گستره جغرافیایی آثار حمله است. هرچه پیامدهای عملیات از قلمرو یک کشور فراتر رفته و چند دولت یا جامعه بین‌المللی را متأثر سازد، احتمال بین‌المللی بودن جرم افزایش می‌یابد.دومین شاخص، نوع هدف مورد حمله است. حمله به زیرساخت‌های حیاتی، مراکز درمانی، شبکه‌های انرژی، سامانه‌های دفاعی، تأسیسات هسته‌ای یا سایر مراکز مرتبط با امنیت عمومی، از اهمیت بیشتری نسبت به حمله به سامانه‌های خصوصی برخوردار است.سومین شاخص، میزان خسارت و آثار انسانی عملیات است. چنانچه حمله سایبری موجب مرگ، جراحت، خسارت گسترده اقتصادی، اختلال طولانی‌مدت در خدمات عمومی یا تهدید امنیت جمعی شود، باید در ارزیابی بین‌المللی بودن آن نقش تعیین‌کننده داشته باشد.چهارمین شاخص، ماهیت و سازمان‌یافتگی مرتکبان است. عملیات برنامه‌ریزی‌شده توسط گروه‌های سازمان‌یافته، شبکه‌های فراملی یا بازیگرانی که از حمایت مستقیم یا غیرمستقیم دولت‌ها برخوردارند، نسبت به حملات فردی از اهمیت بیشتری برخوردار است.پنجمین شاخص، قابلیت تهدید صلح و امنیت بین‌المللی است. هرگاه آثار حمله از اختلافات داخلی فراتر رود و احتمال بروز تنش‌های منطقه‌ای یا بین‌المللی را افزایش دهد، ضرورت اعمال قواعد حقوق بین‌الملل کیفری نیز بیشتر خواهد بود.به‌کارگیری هم‌زمان این شاخص‌ها می‌تواند از برداشت‌های سلیقه‌ای جلوگیری کرده و چارچوبی منطقی برای تشخیص مرز میان جرائم داخلی و بین‌المللی ایجاد کند.

بند سوم: راهکارهای تقویت نظام کیفری در مقابله با جنگ‌های سایبری

کارآمدی نظام عدالت کیفری در برابر جنگ‌های سایبری مستلزم اصلاح قوانین داخلی و توسعه همکاری‌های بین‌المللی است. نخستین اقدام، به‌روزرسانی قوانین کیفری با توجه به فناوری‌های نوین و پیش‌بینی مقررات اختصاصی درباره حملات علیه زیرساخت‌های حیاتی است.راهکار دوم، توسعه همکاری میان دولت‌ها در زمینه تبادل اطلاعات، استرداد مجرمان، انتقال ادله الکترونیکی و اجرای نیابت‌های قضایی است. بدون چنین همکاری‌هایی، تعقیب بسیاری از مجرمان سایبری با دشواری جدی روبه‌رو خواهد بود.راهکار سوم، ایجاد بانک‌های اطلاعاتی مشترک درباره تهدیدات سایبری و ارتقای ظرفیت فنی نهادهای قضایی و انتظامی است. آموزش مستمر قضات، دادستان‌ها، ضابطان و کارشناسان ادله دیجیتال نیز نقش مهمی در افزایش کیفیت رسیدگی به این پرونده‌ها خواهد داشت.همچنین، تقویت همکاری میان دانشگاه‌ها، مراکز پژوهشی و نهادهای سیاست‌گذار می‌تواند زمینه تولید نظریه‌های بومی و ارائه راهکارهای حقوقی متناسب با شرایط جدید را فراهم کند. توسعه دیپلماسی سایبری و مشارکت فعال در تدوین اسناد بین‌المللی نیز از دیگر اقداماتی است که می‌تواند به کاهش خلأهای موجود کمک کند.

نتیجه‌گیری

جنگ‌های سایبری یکی از مهم‌ترین جلوه‌های تحول در ماهیت تهدیدات امنیتی و کیفری در عصر دیجیتال هستند. ویژگی‌های خاص این پدیده، از جمله فرامرزی بودن، دشواری انتساب، ناشناس ماندن مرتکبان، سرعت بالای وقوع و آثار گسترده اقتصادی، اجتماعی و امنیتی، موجب شده است که معیارهای سنتی حقوق کیفری برای تعیین مرز میان جرم داخلی و جرم بین‌المللی با چالش‌های جدی مواجه شوند.تحلیل مبانی نظری نشان داد که هیچ معیار واحدی برای تشخیص این مرز کفایت نمی‌کند. اصل سرزمینی، تابعیت، محل وقوع نتیجه، شدت خسارت، نوع هدف، آثار فرامرزی، میزان تهدید علیه امنیت عمومی و نقش دولت‌ها، هر یک

بخشی از واقعیت پیچیده جنگ‌های سایبری را تبیین می‌کنند. از این‌رو، اتخاذ رویکردی تلفیقی که مجموعه این شاخص‌ها را به صورت هم‌زمان مورد ارزیابی قرار دهد، منطقی‌ترین راهکار برای تفکیک میان جرائم داخلی و جرائم بین‌المللی است.همچنین، بررسی نظریه‌های نوین حقوق کیفری نشان داد که گرایش به حمایت از ارزش‌های بنیادین جامعه جهانی، مسئولیت فراملی و عدالت کیفری جهانی، ظرفیت مناسبی برای پاسخگویی به تهدیدات نوظهور فضای سایبری دارد. با وجود این، تحقق کامل این اهداف مستلزم توسعه همکاری‌های بین‌المللی، هماهنگ سازی قوانین داخلی، ارتقای توان فنی مراجع قضایی و تدوین اسناد الزام‌آور بین‌المللی در حوزه جنگ‌های سایبری است.در نهایت، می‌توان نتیجه گرفت که آینده حقوق کیفری در مواجهه با جنگ‌های سایبری، در گرو فاصله گرفتن از نگرش صرفاً سرزمینی و حرکت به سوی نظامی انعطاف‌پذیر، چندسطحی و مبتنی بر همکاری جهانی است؛ نظامی که ضمن احترام به حاکمیت دولت‌ها، توانایی حمایت مؤثر از امنیت و منافع مشترک جامعه بین‌المللی را نیز داشته باشد.

منابع و مآخذ

الف: منابع فارسی

- اردبیلی، محمدعلی. حقوق جزای عمومی. جلد اول. تهران: میزان، چاپ سی و نهم، ۱۴۰۲.
- آشوری، محمد. آیین دادرسی کیفری. جلد اول. تهران: سمت، چاپ بیست وچهارم، ۱۴۰۱.
- حبیب‌زاده، محمدجعفر. حقوق کیفری بین‌المللی. تهران: میزان، چاپ هشتم، ۱۴۰۰.
- خالقی، علی. آیین دادرسی کیفری. تهران: شهر دانش، چاپ سی و دوم، ۱۴۰۲.
- گلدوزیان، ایرج. بایسته های حقوق جزای عمومی. تهران: میزان، چاپ بیست و هشتم، ۱۴۰۱.
- میرمحمدصادقی، حسین. جرائم علیه امنیت و آسایش عمومی. تهران: میزان، چاپ دوازدهم، ۱۴۰۰.
- نجفی ابرندآبادی، علی‌حسین. سیاست جنایی. تهران: میزان، چاپ ششم، ۱۳۹۹.
- ولیدی، محمدصالح. حقوق جزای عمومی. تهران: امیرکبیر، چاپ هجدهم، ۱۴۰۰.

ب: منابع لاتین

- Cassese, Antonio. *International Criminal Law*. ۳rd Edition. Oxford University Press, ۲۰۱۳.
- Dinstein, Yoram. *War, Aggression and Self-Defence*. ۷th Edition. Cambridge University Press, ۲۰۲۱.
- Goodman, Ryan. *Cyber Operations and International Law*. Oxford University Press, ۲۰۲۰.

- Hathaway, Oona A., et al. *The Law of Cyber-Attack*. Harvard National Security Journal, Vol. ۴, ۲۰۱۲.
- Schmitt, Michael N. *Tallinn Manual ۲.۰ on the International Law Applicable to Cyber Operations*. Cambridge University Press, ۲۰۱۷.
- Shaw, Malcolm N. *International Law*. ۹th Edition. Cambridge University Press, ۲۰۲۱.
- Tsagourias, Nicholas & Buchan, Russell. *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing, ۲۰۲۱.
- Werle, Gerhard & Jeßberger, Florian. *Principles of International Criminal Law*. Oxford University Press, ۲۰۲۰.