فصلنامهٔ پدافند غیرعامل و امنیت (پژوهشی)
سال دوازدهم: شمارهٔ ۴۴- پاییز ۱۴۰۲
صص: ۵۹ - ۸۷

Quarterly of Passive Defense & Security
Vol.12, No.44,Autumn 2023
P-P: 59 - 87

آسیب‌شناسی معاهدات بین‌المللی در ایجاد بازدارندگی سایبری

محمد علمی[۱]
دیدخت صادقی[۲]
محمد شاه‌محمدی[۳]

چکیده

با توجه به اهمیت فضای سایبری و حملات انجام‌گرفته در بستر آن، پژوهش حاضر با روش توصیفی- تحلیلی به این پرسش پرداخته است که چه معاهدات و کنوانسیون‌های بین‌المللی برای ایجاد بازدارندگی علیه حملات تروریستی وجود دارد و آسیب‌شناسی آن‌ها کدام است؟ یافته‌های پژوهش، نشان‌داد که از بازدارندگی حملات سایبری در این کنوانسیون‌ها تحت عناوینی چون تروریسم سایبری، خرابکاری سایبری، حمله یا یورش سایبری، سوءاستفاده از حوزه فنّاوری اطلاعات و ارتباطات و نیز اقدامات مخرب در بستر اینترنت، یاد شده است. از میان کنوانسیون‌های موردبررسی، صرفاً پنج کنوانسیون به‌صورت مستقیم و تخصصی به مقوله اقدامات خرابکارانه سایبری پرداخته‌اند که عبارتند از: قطعنامهٔ ایجاد فرهنگ جهانی امنیت سایبر و حمایت از زیرساخت‌های اطلاعاتی حساس (۲۰۰۴)، قطعنامهٔ مبارزه با سوءاستفادهٔ جنایت‌کارانه از فنّاوری اطلاعات، قطعنامه ایجاد فرهنگ جهانی امنیت سایبری و تلاش‌های ملّی برای حفاظت از زیرساخت‌های اطلاعاتی حساس (۲۰۱۰ و ۲۰۲۰)، کنوانسیون اروپایی مقابله با حملات سایبری و کنوانسیون جرائم سایبری شورای اروپا. سایر کنوانسیون‌ها یا به‌صورت موردی در یکی از مفاد خود از حملات سایبری نام‌برده‌اند یا مجموعه گزاره‌های حقوقی آن‌ها به شکلی است که می‌توان از آن، استنباط بازدارندگی علیه حملات و جرائم سایبری در سطح دولت‌ها داشت؛ بااین‌حال، دشواری در شناسایی عوامل اصلی تهدیدات سایبری و نیز فقدان همه‌شمول بودن یک نظام سیاسی و حقوقی برای شناسایی و مجازات تهدیدکنندگان، سبب شده است تا چالش‌های زیادی در معاهدات و کنوانسیون‌های بین‌المللی در ارتباط با بازدارندگی حملات سایبری باقی بماند.

واژگان کلیدی: حملات سایبری، فضای سایبری، بازدارندگی، کنوانسیون‌های بین‌المللی

---

۱. دانشجوی دکتری روابط بین‌الملل، دانشگاه آزاد اسلامی، واحد تهران مرکزی، تهران، ایران
۲. استادیار دانشکده علوم سیاسی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول) Did.sadeghi_Haqiqi@iauctb.ac.ir
۳. استادیار علوم سیاسی، دانشگاه عالی دفاع ملی، تهران، ایران

مقدمه

رشد فزاینده دستاوردهای علمی درزمینهٔ فنّاوری اطلاعات و ارتباطات و همچنین درگیرشدن هرچه بیشتر جوامع به استفاده از این ابزارها و پیشرفت‌های دیگری که در اثر به‌کارگیری آن‌ها حاصل‌شده، سبب شده است میزان آسیب‌پذیری‌های جوامع افزایش یابد؛ به‌عبارت‌دیگر، فنّاوری اطلاعات و ارتباطات در کنار مزیت‌ها و ظرفیت‌های انکارناپذیری که دارد، همچنین می‌تواند به‌عنوان ابزاری در راستای تهدید علیه امنیت ملی کشورها استفاده شود. نقش مهم رایانه و اینترنت و ترغیب دولت‌ها برای استفاده از آن‌ها به‌عنوان یک ابزار مناسب برای حمله به اهدافشان، انکارناپذیر است. این تغییر در شیوه‌های حمله، از شیوهٔ سنتی به شیوه‌های الکترونیکی، به یکی از بزرگ‌ترین چالش‌های دولت‌های مدرن تبدیل شده است.

از تلاقی کنش‌های تلافی‌جویانه دولتی و فضای سایبر، گونه‌ای نوپا تحت عنوان حملات سایبری[1] پا به عرصه وجود نهاده است. این پدیدهٔ نوظهور عبارت است از: ارتکاب اعمال مجرمانه از طریق سامانه‌های رایانه‌ای و مخابراتی در جهت رسیدن به اهداف عمدتاً سیاسی و بعضاً اقتصادی، نظامی، فرهنگی و ایدئولوژیک (*Van der Meer, 2017: 86*). حملات سایبری به دلیل اتصال جهانی بر بستر اینترنت، امکان‌پذیر شده است. درواقع، اتصال هر چه بیشتر شبکه‌های رایانه‌ای گوناگون در سراسر جهان و قرارگرفتن حجم بیشتری از اطلاعات ارزشمند بر روی این شبکه‌ها، جذابیت رایانه‌ها و شبکه‌های رایانه‌ای را به‌عنوان اهداف حملات سایبری هرچه بیشتر ساخته است؛ بنابراین روزبه‌روز انگیزهٔ مهاجمین احتمالی برای آغاز حمله علیه اهداف سایبری افزوده می‌گردد. انگیزه‌های اقتصادی، صنعتی و نظامی در این میان از همه چشمگیرتر به نظر می‌رسند. بارزترین ویژگی فضای سایبر، دسترس‌پذیر ساختن سریع با حداقل هزینهٔ کلیهٔ اطلاعات آنلاین است که بسیاری از نمونه‌های آن را در تارنماهای شبکه جهانی اینترنت شاهد هستیم. این دسترس‌پذیری، برای همگان فراهم آمده و هیچ‌گونه تبعیضی اعمال نشده است. باوجود این شرایط، به نظر می‌رسد در متزلزل شدن برخی مفاهیم حساس و اساسی؛ به‌ویژه امنیت، تردیدی باقی نمانده باشد. امنیت همانند فضای سایبر، آن‌قدر انعطاف‌پذیر است که در هر سطح و کیفیتی، معنا و کاربرد خود را حفظ می‌کند.

در سطح بین‌الملل، حملات سایبری، معمولاً نقاط حساس و حیاتی جوامع را هدف قرار می‌دهند تا اساسی‌ترین ضربات را به کشور هدف وارد کنند (*Valerino and Maness, 2023*). فنّاوری اطلاعات و ارتباطات، بخش عمده‌ای از فعالیت‌های اقتصادی، اجتماعی و زیست‌محیطی کشورها را بر فضای سایبر مستقر کرده است تا آنجا که حتی سازمان‌های نظامی و دفاعی نیز به تجهیزات و سامانه‌های مدرن سایبری مجهز شده‌اند. ازآنجاکه در این سامانه‌ها، منابع اطلاعاتی حساس و حیاتی وجود دارند، نگرانی از امنیت اطلاعات مبادله شده از موانع توسعه این فنّاوری‌ها و برخورد محتاطانه

1. *Cyber-attack*

با آن شده است؛ ازاین‌رو، چالش‌های اصلی بازدارندگی حملات سایبری در روابط بین‌الملل، هم‌چنان به‌عنوان یک مسئله، باقی مانده است.

بیان مسئله

تأثیرگذاری فضای سایبری به حدی گسترده شده است که اغلب دولت‌ها در سطح بین‌الملل، منطقه‌ای و داخلی درصدد اتخاذ راهکارهایی برای بهبود روش‌های مؤثر بهره‌مندی از این فضای نوین و دفع تهدیدات ناشی از آن هستند. بااین‌حال، نظارت بر فضای سایبر، دشواری‌های خاص خود را دارد و به دلیل تنوع ناشی از حملات سایبری، جرم‌انگاری آن، همواره در حال تغییر و تحول است. یکی از دشواری‌های اساسی در این زمینه، عدم دسترسی و یا دشوار بودن دسترسی به مکانی است که جرم سایبری در آن رخ می‌دهد؛ به‌عنوان‌مثال، یک حمله سایبری که مدعی است از سوی کشور الف انجام می‌شود، ممکن است محل قرارگرفتن حمله‌کنندگان در آن کشور نباشد (*Hearn, 2021*)؛ بنابراین هم پی‌بردن به نقش عوامل اصلی تهدیدات سایبری و هم مدون بودن یک نظام سیاسی و حقوقی برای شناسایی و مجازات تهدیدکنندگان بخش مهمی از دشواری‌های ناشی از بازدارندگی تهدیدات و حملات سایبری هستند؛ چراکه در فضای حملات سایبری، چالش‌های زیادی در ارتباط با بازدارندگی عاملان حملات سایبری وجود دارد.

علاوه بر این، جامعه بین‌المللی در حیطه فضای سایبر، موفق به تدوین قواعد مشخصی که همه جوانب توسل به حملات سایبری را تعیین سازد، نشده است. این در حالی است که حملات طراحی‌شده سایبری، قابلیت ایجاد خسارات گسترده‌تری را نسبت به حملات سنتی دارد. عمدتاً به علت سهولت دسترسی و کم‌هزینه‌تر بودن حملات سایبری، دولت‌ها را برای توسل به این نوع از حملات، جریح می‌سازد. امروزه تهدیدات موجود و بالقوه در فضای امنیتی سایبر در بین جدی‌ترین تعارضات قرن حاضر قراردارند. تأثیرات این تهدیدات، متضمن خطرات بسیاری برای امنیت عمومی، امنیت دولت‌ها و درنهایت بقای جامعه بین‌المللی خواهد بود. ازاین‌رو، ضروری است تا راهکارهایی به‌منظور بازدارندگی حملات سایبری، اندیشیده شود. با توجه به ماهیت و ابزارهای مورداستفاده در حملات سایبری، تلفات و خسارت‌های زیان‌بارتری را نسبت به دیگر انواع تروریسم در بردارد؛ بنابراین گستردگی فضای سایبر و به خدمت گرفتن آن توسط اکثر افراد جامعه و زیرساخت‌های کشور، طیف گسترده‌ای از مباحث را پیرامون چالش‌های بازدارندگی این حملات شکل داده است. در این راستا، مسئله اصلی پژوهش حاضر این است که معاهدات و پیمان‌نامه‌های بین‌المللی برای ایجاد بازدارندگی در حملات سایبری چه ویژگی‌های و کارکردهایی دارند؟

هدف پژوهش

مهم‌ترین هدف پژوهش حاضر، تبیین آسیب‌های معاهدات و قواعد بین‌المللی برای ایجاد بازدارندگی در حملات سایبری است.

سؤال پژوهش

آسیب‌های معاهدات و قواعد بین‌المللی برای ایجاد بازدارندگی در حملات سایبری کدامند؟

فرضیه پژوهش

به نظر می‌رسد عواملی از قبیل انتساب حمله (عاملان)، تعدد عاملان حمله، تکرارپذیری حملات، عدم شفافیت، محاسبه هزینه و فایده[1]، سرعت تغییر رویه‌های حملات، عدم مسئولیت‌پذیری کشورها و نداشتن پشتوانه اجرایی معاهدات، از مهم‌ترین معایب و آسیب‌های معاهدات مرتبط با بازدارندگی علیه حملات سایبری می‌باشند.

پیشینه پژوهش

پژوهش‌های داخلی

در ارتباط با موضوع پژوهش، مجموعه پژوهش‌هایی در سطح داخلی صورت گرفته است؛ اما این پژوهش‌ها عمدتاً از منظر حقوق بین‌الملل به مقوله حملات سایبری پرداخته‌اند. در ادامه به بررسی این پژوهش‌ها پرداخته شده است.

آقابابایان و همکاران (۱۴۰۱) در پژوهشی با عنوان «تبیین وضعیت دولت‌های کنشگر نسبت به حمله سایبری»، به این نتیجه دست‌یافته‌اند که حملات سایبری به‌عنوان یک عمل زیان‌بار، علیرغم تهدیدات گسترده و قدرت تخریبی بالایی دارند، مطابق اسناد بین‌المللی منع نشده‌اند؛ بنابراین عمل زیان‌بار ناشی از تهدیدات سایبری ممنوع نیستند و همین موضوع باعث تهدید تلقی شدن این‌گونه حملات باشند. درواقع، اثرات منفی ناشی از حمله سایبری می‌تواند گریبان‌گیر دولت‌های دیگری غیر از دولتی که حمله سایبری علیه او طراحی‌شده را در بربگیرد. مبارزه با حملات سایبری و خسارات ناشی از آن می‌بایست در حقوق بین‌الملل و در راستای حقوق و منافع کشور خسارت‌دیده سامان داده شود. درنظرگرفتن حملات سایبری خسارت‌بار در زمره حملات جنگی، راهکار حقوقی بین‌المللی برای دفع تهدیدات ناشی از آن است.

فرشاسعید و جلالی (۱۴۰۱) در پژوهشی با نام «مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی»، از منظر حقوق بین‌الملل به میزان تعهد و مسئولیت دولت‌ها در برابر حملات سایبری پرداخته‌اند. نتایج حاصل از این پژوهش، نشان می‌دهد که به علت وابسته شدن گستردهٔ تمامی امورات بشر به فضای سایبر و اینترنت، خطر حملات سایبری صلح و امنیت بین‌المللی را بیش‌ازپیش تهدید می‌کند. گاه‌گاهی اخباری در رسانه‌ها و شبکه‌های مجازی منتشر می‌شود مبنی بر این‌که حملهٔ سایبری علیه دولتی انجام‌گرفته است؛ اما به علت پیچیدگی‌های فضای سایبر مشخص‌نمودن عامل حملهٔ سایبری مشکل است. آنچه می‌تواند در برابر تخلفات دولت‌ها از قواعد و اصول حقوق بین‌الملل همچون سدی استوار عمل کند قواعد مسئولیت بین‌المللی دولت‌ها است. در حال حاضر دو معیار مسئولیت برای دولت‌ها در قبال

1. Cost-benefit calculus

حملات سایبری عوامل غیردولتی وجود دارد که یکی معیار کنترل مؤثر و دیگری معیار کنترل کلی است. در این مقاله به مزایا و معایب این دو معیار برای تعیین مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی پرداخته و نتیجه‌گیری شده است که به علت ویژگی‌های خاص فنّاوری‌های سایبری این دو معیار برای اثبات مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی مناسب نیست و باید معیار مراقبت بایسته مدنظر دولت‌ها قرار گیرد؛ زیرا بر اساس ویژگی‌های این معیار، اثبات مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی ساده‌تر به نظر می‌رسد.

نامدار و قاسمی (۱۳۹۷) در پژوهشی به بررسی مفهوم دفاع مشروع در پرتو حملات سایبری (با تأکید بر حمله استاکس‌نت به تأسیسات هسته‌ای ایران) پرداخته‌اند. به‌زعم نویسندگان این مقاله، یکی از شیوه‌های نوین تخاصم درصحنه بین‌المللی، حملاتی است که در بستر فضای سایبری صورت می‌گیرد، هرچند این حملات توان ایجاد تلفات گسترده و خسارات وسیع را دارند؛ اما سرعت بالای تغییرات در این حوزه موجب گردیده است که حقوق بین‌الملل از وضع قواعد جدید متناسب با فضای سایبری عاجز بماند. توسل به مفهوم دفاع مشروع نیز در خصوص این حملات موردتردید واقع‌شده و امکان اعمال این حق در این فضا به استناد ماده ۵۱ منشور ملل متحد و یا حقوق بین‌الملل عرفی از مهم‌ترین پرسش‌هایی است که بی‌پاسخ مانده است. به نظر می‌رسد درصورتی‌که حملات سایبری به زیرساخت‌های حیاتی یک کشور نفوذ کرده و توان ایجاد تخریب و اضمحلال در حد یک حمله مسلحانه را داشته باشند، مسلحانه فرض شده و دولت قربانی از حق دفاع مشروع برخوردار خواهد بود. در خصوص حمله کرم رایانه‌ای استاکس‌نت در سال ۲۰۱۰ به تأسیسات هسته‌ای ایران، صرف‌نظر از مسئله انتساب آن به‌عنوان یک امر موضوعی، حق دفاع مشروع قابل‌اثبات است.

احمری و همکاران (۱۳۹۵) در مقاله‌ای تحت عنوان «تحلیل سازه‌انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن»، تلاش کرده‌اند که با تبیین اجمالی مفهوم عام تروریسم سایبری به‌عنوان یک پدیدهٔ مجرمانه، راهکارها و خلأهای نظام حقوقی برای مقابله با آن را بررسی کنند. نویسندگان این پژوهش، به این نتیجه دست‌یافته‌اند که تروریسم سایبری از مصادیق مدرن تهدیدهای تروریستی است که به سبب استفاده از فنّاوری‌های نوین و رایانه‌ای در فضای مجازی در آن، توسط بازیگرانی در عرصه بین‌الملل مورداستفاده قرار می‌گیرند و از دانش فنّاورانه بالا برخوردار هستند. ازآنجایی که معمای امنیت بزرگ‌ترین مسئله بشری بوده و تهدیدهای امنیتی تروریسم نوین سایبری آن‌گونه که سازه‌انگاران معتقدند از رهگذر برساخت‌های امنیتی و هویتی باید نگریسته شود، این پژوهش، امنیت سایبری را مبتنی بر ساختارهای هویتی و امنیتی مورد ارزیابی قرار داده که به شکل‌گیری نظام‌های حقوقی در عرصه داخلی و بین‌المللی انجامیده است. درواقع، دولت‌ها بازیگران محوری در عرصه تعاملات بین‌المللی هستند و در کنار دیگر فعالین عرصه بین‌المللی با عنایت به نوع نگاه هویتی خود قواعد حقوقی را تبیین می‌کنند.

پژوهش‌های خارجی

والریانو و منس[1] (۲۰۲۳) در پژوهشی با عنوان «نظریه‌های روابط بین‌الملل و امنیت سایبری»[2]، به این نتیجه دست‌یافته‌اند که تبیین امنیت سایبری بر اساس مکاتب و نظریه‌های مرسوم روابط بین‌الملل تااندازه‌ای با دشواری همراه است؛ چراکه ماهیت حملات سایبری با ماهیت هنجارها و بنیادهای نظریه‌های روابط بین‌الملل تفاوت‌هایی دارد و ازاین‌رو، مقوله امنیت سایبری باید با نظریه‌های سیال‌تر و با تأسی به مفاهیمی متفاوت، بررسی گردد.

هرن[3] (۲۰۲۱) در پژوهشی با نام «روابط بین‌الملل و حملات سایبری: گفتمان رسمی و غیررسمی»[4]، معتقد است که توان جنگ سایبری بسیار زیاد است و برای همه کشورها و دفاع امنیت ملی نگران‌کننده است. به نظر می‌رسد که بسیاری از کشورها فعالانه در تلاش برای محافظت از شبکه‌های رایانه‌ای خود هستند؛ درحالی‌که به دنبال راه‌هایی هستند که ممکن است شبکه‌های سایر کشورها را از بین ببرند، اگرچه این امر به‌طور رسمی تأیید نشده است. ازبین‌بردن شبکه‌های کامپیوتری کشورهای دیگر می‌تواند اطلاعات و کنترل ملی را به مهاجمان بدهد. این نوع تعاملات در حال حاضر بخشی از روشی است که در آن روابط بین‌الملل انجام می‌شود و اینترنت نیز محلی است که در آن روابط بین‌الملل به چالش کشیده می‌شود؛ به‌این‌ترتیب اینترنت نقشی را در تجسم و بیان روابط بین‌الملل به‌صورت رسمی و غیررسمی از طریق اعلامیه‌های رسمی و فعالیت‌های شهروندان خصوصی ایفا می‌کند. آنچه اینترنت را از سایر اشکال رسانه‌ای متمایز می‌کند، این است که اینترنت، فضایی را نشان می‌دهد که در آن روابط بین‌المللی ازنظر حملات سایبری و جنگ اطلاعاتی مورد مناقشه قرارمی‌گیرد. این مقاله گفتمان‌های رسمی و غیررسمی پیرامون نحوه انجام روابط بین‌الملل در رابطه با حملات سایبری از طریق اینترنت را با استفاده از کره شمالی و استاکس‌نت به‌عنوان مطالعات موردی تحلیل کرده است.

واندرمر[5] (۲۰۱۷) در پژوهشی تحت عنوان «چالش‌های بازدارندگی در روابط بین‌الملل: انکار، تلافی و ارسال پیام»[6]، به این نتیجه دست‌یافته است که جلوگیری از حملات سایبری بزرگ برای دولت‌ها، چالش‌های متعددی را به همراه دارد. به‌زعم واندرمر، برای جلوگیری مؤثر از حملات سایبری دولت‌های متخاصم، محاسبات هزینه سود آن‌ها باید تحت‌تأثیر قرار گیرد و آن‌ها را به این نتیجه برساند که هزینه‌های راه‌اندازی یک حمله سایبری ممکن است بیشتر از منافع باشد؛ علاوه بر این، دولت‌ها نباید بر سیاست‌های بازدارندگی کوتاه‌مدت تمرکز کنند؛ بلکه در تلاش‌های دیپلماتیک نیز سرمایه‌گذاری کنند که ممکن است در بلندمدت بازدارندگی مؤثری علیه حملات سایبری ایجاد کند.

---

1. *Brandon Valeriano, Ryan C. Maness*
2. *International Relations Theory and Cyber Security*
3. *Hearn*
4. *International Relations and Cyber Attacks: Official and Unofficial Discourse*
5. *van der Meer*
6. *Deterrence of Cyber-Attacks in International Relations: denial, retaliation and signaling*

همچنان که بررسی پیشینه پژوهش نشان‌داد، پژوهش حاضر به‌عنوان نخستین پژوهشی است که در سطح داخلی به تبیین و بررسی معاهدات و قواعد بین‌المللی برای ایجاد بازدارندگی در حملات سایبری می‌پردازد. درواقع، متغیرهای موردبررسی در این پژوهش، یا به‌صورت موردی در پژوهش‌های پیشین مطالعه شده است و یا نگرشی جامع از دیدگاه حقوق و روابط بین‌الملل به مسئله بازدارندگی حملات سایبری، صورت نگرفته است.

مبانی نظری

در ارتباط با حملات سایبری به‌عنوان استفاده از زور، سه نظریه از سوی نظریه‌پردازان حقوق و روابط بین‌الملل ارائه‌شده است. رویکرد اول، رویکردی ابزارگرا یا مبتنی بر ابزار به موضوع دارد، رویکرد دوم مبتنی بر هدف بوده و اهداف را موردبررسی قرارمی‌دهد و رویکرد سوم رویکرد مبتنی بر پیامدهاست. رویکرد اول یا ابزارگرا تمرکز بر حمله دارد. طرفداران این رویکرد اعتقاددارند اگر حملات سایبری ویژگی‌های فیزیکی را که به‌طور سنتی با یک عملیات نظامی مرتبط است، نشان‌دهند، عملیات سایبری معنای استفاده از زور را خواهد داشت؛ اما قرائت دوم معتقد است هنگامی که زیرساخت‌های ملی حیاتی هدف قرار گیرد، این عملیات به معنای استفاده از زور تلقی می‌شود و رویکرد سوم پیامدهای حمله را به‌عنوان یک نهایتاً کل در نظر می‌گیرد و به دنبال تجزیه‌وتحلیل این است که آیا اثرات عملیات به‌اندازه کافی جدی بوده که آن را به‌عنوان استفاده از زور واجد شرایط ارزیابی کند (رستمی‌فر، ۱۴۰۲: ۵۳)؛ بنابراین با توجه به اهمیت موضوع توصیف و تحلیل هریک از رویکردها ضروری است.

رویکرد ابزارگرایانه

رویکرد ابزارگرا، تفسیر وسیعی از ابزار دارد؛ بنابراین در این راستا ابزاری را در نظر می‌گیرد که توسط آن، یک دولت به استفاده از زور متوسل می‌شود. قرائت طرفداران این رویکرد، این است که یک کشور ممکن است به مدد نیروی اقتصادی، دیپلماتیک/سیاسی یا مسلح، به عملیات نظامی متوسل شود. ازنظر ابزارگراها یک عملیات تنها زمانی به‌عنوان استفاده از زور مشمول بند ۴ ماده ۲ می‌گردد که دارای ویژگی فیزیکی و نظامی باشد. به‌زعم ابزارگرایان، اجبار سیاسی یا اقتصادی را از شمول بند ۴ ماده ۲ منشور مستثنا می‌کنند، این رویکرد بر ابزارهای مورداستفاده متمرکز است و بیشتر به استفاده از سلاح‌های نظامی سنتی توجه دارد (*Lehto, 2022: 13*). گرچه با مجموعه‌ای از پیش‌فرض‌هایی گرچه محدود برخی از عملیات سایبری را به‌عنوان استفاده از زور شناسایی می‌نماید؛ اما هیچ تعریف دقیقی از ماهیت نظامی یک عملیات و به‌خصوص که تکنیک‌های مورداستفاده که به‌سرعت در حال تغییر هستند، اشاره نمی‌کنند. امروزه تحت‌تأثیر تنوع تکنیک‌های نظامی و توسعه فنّاوری‌های نظامی یک تغییر نظری در رویکرد ابزارگرا ایجاد کرده است. برخی از نویسندگان پیشنهاد می‌کنند با توجه به اینکه ماهیت نظامی حملات سایبری

دارای همان تکنیک استفاده از زرادخانه ارتشی دولت بوده؛ بنابراین این موارد بایستی به‌عنوان مصادیق زور فرض شوند. این تغییر نگرش موجب گردیده بسیاری از دولت‌ها واحدهای دفاع سایبری تحت عنوان ارتش سایبری را تحت نظر نیروهای مسلح ایجاد کنند تا در صورت حملات سایبری از طریق ابزارهای سایبری تخصصی از خود دفاع دارند، بنابراین می‌توان گفت که عملیات سایبری می‌تواند جنبه نظامی داشته باشد. باوجود توصیفات فوق، برخی از نویسندگان معیار دوم را اضافه می‌کنند که مربوط به ماهیت فیزیکی عملیات است، ازنظر اینان ویژگی فیزیکی یک عملیات به‌طورکلی به معنای تولید یک موج ضربه‌ای و یک اثر انفجاری است. بر اساس این رویکرد، یک حمله سایبری به‌تنهایی و درصورتی‌که هیچ موج ضربه و اثر انفجاری به دنبال داشته باشد، نمی‌تواند به‌منزله استفاده از زور باشد؛ زیرا فاقد ویژگی فیزیکی مرتبط با اجبار نظامی است. اینان با تفکیک عملیات با ماهیت انفجاری از غیرانفجاری اعتقاددارند، یک حمله سایبری که از طریق استفاده از کدهای رایانه‌ای صورت می‌گیرد که به‌اندازه کافی شبیه سلاح‌های متعارف نبوده و ویژگی فیزیکی مرتبط با اجبار نظامی را ندارند؛ چراکه یک حمله سایبری به‌خودی‌خود باعث آسیب فیزیکی انفجاری نمی‌شود، حتی اگر علت انفجار و با هدف از کار انداختن سامانه‌های رایانه‌ای صورت گرفته باشد (*Al-Turjman and Salama, 2020: 79*).

این رویکرد، گزاره‌های خود را با این واقعیت تقویت می‌کند که ماد هـ ۴۱ منشور سازمان ملل متحد قطع کامل یا جزئی روابط از طریق تلگراف، رادیو و سایر وسایل ارتباطی را از شمول توسل به‌زور مستثنا کرده است، انتقادات وارده به نظریات طرفداران رویکرد ابزارگرا موجب شده، نظریه‌پردازان ابزارگرای جدید با اتکا بر آمیزه‌های رویکرد ابزارگرا و واقع‌گرایی، مفروضات سابق خود را تعدیل کنند و ابراز دارند اگر استفاده از حملات سایبری شبیه به استفاده از سلاح‌های نظامی باشد، هرچند ماهیت فیزیکی آن را نداشته باشد، مانع از تعمیم استناد به‌زور در مفهوم بند ۴ ماد هـ ۲ منشور نخواهد بود؛ اما انتقاد اصلی به قرائت رویکرد ابزارگرا این است که موارد و مصادیق زور را بیش‌ازحد محدود و به‌طور غیرضروری برخی از حملات سایبری را از مصادیق زور مستثنا و آن را مشروط به ماهیت فیزیکی عملیات می‌کند؛ بنابراین با توجه به تحول مفهوم زور نمی‌توان کلیه عملیات سایبری را که با هدف خارج کردن شبکه‌ها و سامانه‌های رایانه‌ای خاص بدون ایجاد آسیب مستقیم می‌گردند و حیات سیاسی، اقتصادی، نظامی و حاکمیتی دولت را مورد تعرض به حملاتی قرار می‌دهند، از زور مستثنا کرد و صرفاً بسنده نمود که می‌تواند به‌طور غیرمستقیم باعث آسیب فیزیکی، مانند انفجار شود. هرچند برخی از عملیات سایبری درواقع به استفاده از تکنیک‌های نظامی شباهت دارند. هرچند برخی دیگر از حملات مشابهت به عملیات نظامی ندارد؛ اما به‌مراتب مخرب‌تر از حملات نظامی بوده و حاکمیت اقتصادی سیاسی دولت‌ها را هدف و تعرض قرار دهند و بایستی با استناد به مفاد منشور به‌عنوان مصادیق زور مورد شناسایی قرار گیرند؛ گرچه به‌سختی می‌تواند شبیه به یک عملیات نظامی باشد (*Makridis, 2024: 69*).

ازآنجایی‌که این رویکرد فقط ماهیت نظامی و فیزیکی یک عملیات را در نظر می‌گیرد و بسیاری از حملاتی را که عواقب جدی ایجاد می‌کنند استثنا می‌کند؛ اما باوجوداین، ایجاد تمایز بر اساس جدیت پیامدها به‌منزله استفاده از رویکرد مبتنی بر پیامد در کلیه موارد قابلیت تعمیم نخواهد داشت. به‌عنوان‌مثال حمله استاکس نت در ایران به‌منزله استفاده از زور است؛ زیرا این عملیات با استفاده از یک ویروس رایانه‌ای و نه با موشک یا سلاح معمولی انجام شده است و موجبات موج انفجاری شده؛ اما اگر رویکرد کلاسیک ابزارگرایی مناط قرار گیرد، چنین حمله سایبری از مصادیق زور محسوب نخواهد شد.

رویکرد هدف‌گرایانه

قرائت رویکرد مبتنی بر هدف یک عملیات سایبری را زمانی که هدف آن نفوذ به سامانه‌های زیرساخت ملی و حیاتی باشد، استفاده از زور تلقی می‌گردد، حتی اگر عملیات آسیب جدی به این سامانه‌ها وارد نکند. برخی از نویسندگان همچنین از رویکرد مسئولیت سخت سخن می‌گویند. قرائت یادشده با این ایده توجیه می‌شود که امروزه عملکرد صحیح این زیرساخت‌ها در جوامع مدرن به‌طور خاص به سامانه‌های رایانه‌ای وابسته بوده و عملیاتی که با ابزارهای غیرنظامی به معنای کلاسیک مانند حملات سایبری انجام می‌گردد، این امکان را فراهم می‌نماید تا آسیب‌های قابل‌توجهی به زیرساخت‌ها وارد گردد؛ زیرا حملات سایبری زیرساخت‌های حیاتی یک کشور را تضعیف کند. برخلاف رویکرد ابزارگرا، رویکرد مبتنی بر هدف صرفاً عملیات بسیار گسترده و محدود را واجد ماهیت زور می‌داند. هرچند برخی از عملیات که زیرساخت‌های حیاتی را هدف قرار دهند و اثراتی در مقیاس بزرگ ایجاد نمی‌کند، مشمول توسل به‌زور خواهند شد (*Lilienthal and Nehaluddin, 2023: 395*).

بنابراین، عملیات سایبری با هدف غیرقابل‌دسترس کردن خدمات دولتی خاص و وب‌سایت‌های یک کشور حتی برای چند دقیقه بایستی به‌عنوان استفاده از زور شناخته شوند. هرچند این وب‌سایت بلافاصله پس‌ازآن دوباره به‌طورمعمول عمل کنند. با توجه به رویه‌های فعلی دولت‌ها در حقوق بین‌الملل و نظر اکثر حقوقدانان، چنین عملیاتی از درجه ثقل کافی برای شمولیت استفاده از زور در معنای بند ۴ ماد ه ۲ برخوردار نبوده، زیرا هیچ تعریفی ازآنچه که زیرساخت ملی حیاتی را تشکیل می‌دهد، در حقوق بین‌الملل وجود ندارد؛ اما زیرساخت‌های حیاتی و ملی به‌طورکلی به زیرساخت‌هایی اطلاق می‌گردند که تخریب آن‌ها می‌تواند تأثیر جدی بر امنیت، اقتصاد ملی یا سلامت عمومی یک کشور داشته باشد؛ به‌ویژه درصورتی که بخشه‌ای انرژی، تأمین آب، بانکداری، حمل‌ونقل و ارتباطات مورد هدف قرار دهند. با اتخاذ رویکرد مبتنی بر هدف، موارد بسیاری از حملات سایبری می‌توانند مشمول استفاده از زور واجد تلقی شوند و دلیل این امر نیز مبتنی بر این است که منطقه هدف توسط دولت قربانی به‌عنوان یک ضرورت حیاتی در نظر گرفته شده است. یکی از انتقادات وارده به رویکرد مبتنی بر هدف این است که دامنه و مفهوم یک عملیات را

به‌عنوان استفاده از زور را بیش‌ازحد توسعه می‌دهد و این امر خطرات تشدید تنش بین روابط بین‌کشورها را به دنبال دارد (*Li and Liu, 2021: 819*).

رویکرد پیامدگرایانه

رویکرد مبتنی بر پیامدها یا اثرات، بر این اصل استوار است که یک حمله سایبری اثراتی معادل استفاده از زور را دارد، زیرا با ابزارهای خاص زمینه تخریب اموال یا تهدید جان انسان‌ها را فراهم می‌کند و در این فرآیند خسارت‌های مالی به اموال و تهدیدات جسمانی، مرگ و آسیب شهروندان یک کشور را به همراه دارد که این امر می‌تواند از مصادیق استفاده از زور قلمداد گردد. در این رویکرد، عملیات سایبری زمانی استفاده از زور تلقی می‌گردد که ابعاد و اثرات آن با عملیات غیر سایبری که به سطح استفاده از زور می‌رسد، قابل‌مقایسه باشد. متخصصان روابط بین‌الملل و حقوق بین‌الملل با توسل به قیاس، استدلال می‌نمایند عملیات سایبری درصورتی‌که اثراتی مشابه عملیات جنگی داشته باشد، استفاده از زور محسوب می‌گردد؛ بنابراین به باور طرفداران رویکرد مبتنی براثر، تحلیل تأثیرات حمله این امکان را فراهم می‌کند که عملیات خاصی را به‌طور نسبی به‌عنوان استفاده از زور قلمداد نمود؛ زیرا این امر به‌ویژه در مورد عملیاتی که باعث تخریب اموال یا مرگ افراد شود صدق می‌نماید؛ ازاین‌رو پیامدهای چنین حملات سایبری در برخی موارد ازجمله حملات سایبری به راکتورهای سایت هسته‌ای، آسیب‌رساندن به سامانه‌های کنترل ترافیک هوایی یا بازکردن در سدها که منجر به سیل شود، اثرات تخریبی آن از جنگ‌های مسلحانه به‌مراتب بیشتر خواهد بود (*Oppenheimer, 2024: 33*). رویکرد پیامدگرا با توجه به اینکه امکان حذف برخی عملیات را که پیامدهای بسیار اندک دارند، به‌عنوان مفهوم استفاده از زور می‌دهد، طرفداران بیشتری نسبت به رویکردهای پیشین دارد. گرچه بر اساس انگاره‌های فوق، یک عملیات روانی و غیر مخرب را که با هدف تضعیف اعتماد عمومی به یک دولت یا یک اقتصاد می‌شود در برخی وضعیت‌ها به‌عنوان مصداق زور در نظر می‌گیرد؛ اما پیامدهای کلیه عملیات سایبری را که با هدف تضعیف دولت و سیستم اتخاذی دولت برای اداره اقتصاد کشور باشد از شمول عملیات سایبری از مصادیق زور مستثنا می‌کند. مفهوم مخالف این امر این است که عملیات یادشده بر اساس قوانین بین‌المللی قانونی فرض می‌شود؛ زیرا به آستانه استفاده از زور نمی‌رسد. به اعتقاد سیمونت[1]، روش مبتنی بر اثرات، مناسب‌ترین روش درزمینهٔ حملات سایبری است و درواقع، عمل تجاوز رایانه‌ای ازاین‌جهت منحصربه‌فرد است که گرانش آن به سازوکار وقوع آن (نفوذ یک ویروس یا یک کرم در یک شبکه رایانه‌ای) نیست، بلکه پیامدهای بالقوه آن را که بر زندگی انسان‌ها یا جمعیت یک کشور تأثیرگذار باشد، در نظر می‌گیرد (*Aravindakshan, 2021: 259*). به‌رغم کثرت طرفداران رویکرد اخیرالذکر؛ اما رویکرد یادشده از ایرادات مصون نمانده است. عمده‌ترین ایراداتی که به این نظریه واردشده این است که به اثراتی که عملیات سایبری ایجاد می‌کند، اهمیت زیادی می‌دهد و این ویژگی

1. Simonet

حملات سایبری را در نظر نمی‌گیرد که می‌تواند آسیب منحصربه‌فردی ایجاد کند که حملات سنتی نمی‌تواند ایجاد نماید؛ ازاین‌رو بر اساس رویکرد مبتنی بر اثرات، چنین حمله‌ای، هرچند می‌تواند هزینه‌های انسانی و مادی زیادی را به همراه داشته باشد؛ اما مشمول استفاده از زور بدان سیاق که در بند ۴ ماده ۲ منشور پیش‌بینی شده است، نخواهد بود. برخی از اندیشمندان با تحلیل اثرات یک حمله اعتقاددارند یک حمله سایبری که نتواند اثرات موردنظر را ایجاد کند، به‌عنوان استفاده از زور تلقی نخواهد شد. یکی از بارزترین انتقاداتی که به نظریه شده این است که این رویکرد فاقد بازدارندگی بوده؛ زیرا پاسخ مناسبی نسبت به اثرات ناخواسته حملات هسته‌ای پیش‌بینی و راهکار مناسب با توجه به شرایط فعلی جهان ارائه نمی‌کند. به همین استناد موردانتقاد بسیاری از متخصصان حوزه امنیت بین‌المللی است؛ اما با توجه به موارد فوق هر یک از رویکردها مزایا و معایبی دارند؛ اما رویکرد مبتنی بر اثرات همان‌طوری که در اعلامیه‌ها، گزارش‌ها بیان می‌گردد، موردتوجه اکثر دکترین‌ها و دولت‌ها بوده است؛ زیرا حداقل ایرادات به آن واردشده و از این منظر به نظر می‌رسد متعادل‌ترین رویکردهای فعلی باشد. اگر حمله سایبری به معنای استفاده از زور تلقی گردد، تاب این تفسیر را دارد که برابر بند ۴ توسط ماده ۲ ممنوع اعلام شود. با این توصیف زمانی که این اثرات برابر با اثرات یک عملیات انتحاری باشد، به‌عنوان استفاده از زور شناخته می‌شود (*Lilienthal and Nehaluddin, 2023: 396*). ازآنجایی که مفهوم زور شامل اجبار ساده سیاسی یا اقتصادی نمی‌شود، حملات سایبری که اثرات آن‌ها محدود به حوزه اقتصادی، سیاسی یا دیپلمات یک است، نباید به‌عنوان استفاده از زور تلقی شود. هرچند این اعمال لزوماً از منظر حقوق و روابط بین‌الملل، قانونی نیستند؛ اما بر اساس قوانین، تلقی نمودن مصادیق فوق به‌عنوان استفاده از زور، طیف وسیعی از گزینه‌ها و واکنش‌های متفاوت را به سهولت در اختیار دولت قربانی می‌گذارد.

چارچوب تحلیلی: معاهدات و قواعد بین‌المللی مرتبط با حملات سایبری

برای آسیب‌شناسی معاهدات و قواعد بین‌الملل که به‌منظور بازدارندگی و کاهش زمینه‌های ارتکاب حملات سایبری ایجاد شده است، نخست باید مهم‌ترین معاهدات و کنوانسیون‌های مربوطه را بررسی کرد. پس از بررسی مفاد و اهداف این معاهدات و کنوانسیون‌ها، می‌توان به آسیب‌شناسی جامعی از آن‌ها دست‌یافت. از میان معاهدات و پیمان‌نامه‌های مرتبط با حملات سایبری، صرفاً به آن دسته از آن‌ها اشاره خواهد شد که ماهیت حقوقی و رسمی دارند؛ چراکه این معاهدات حاصل توافق عمومی کشورها در روابط بین‌الملل هستند. عمده کنوانسیون‌های یادشده به‌صورت مستقیم به مسئله حملات سایبری نپرداخته‌اند، بلکه یا در یکی از مواد خود به مسئله حمله، خرابکاری یا تروریسم سایبری اشاره کرده‌اند و یا با تفسیر سیاسی و حقوقی از متون آن، می‌توان از آن‌ها گزاره‌هایی برای بازدارندگی علیه حملات سایبری به دست آورد. در ادامه به مهم‌ترین معاهدات و کنوانسیون‌های حقوقی مرتبط با بازدارندگی حملات سایبری، اشاره شده است.

تجزیه‌وتحلیل

حمایت حقوقی و سیاسی از دولت‌های آسیب‌دیده از یورش سایبری در اسناد بین‌المللی، شامل جرم‌انگاری‌های غیرمستقیمی است که با تطبیق قطعنامه‌ها و کنوانسیون‌های بین‌المللی و منطقه‌ای با ارکان تشکیل‌دهندهٔ یورش سایبری، می‌توان مواضع اتخاذشده در آن‌ها را تحت عنوان حمایت کیفری استدلال نمود؛ بنابراین در زیر به تشریح اسناد بین‌المللی و منطقه‌ای در خصوص حمایت‌های حقوقی از دولت‌های آسیب‌دیده پرداخته می‌شود.

کنوانسیون جرائم سایبری شورای اروپا

کنوانسیون جرائم سایبر مصوب سال ۲۰۰۱، تنها سندی است که جرائم سایبری را موردبررسی قرار داده و به جرم‌انگاری‌های متعددی از افعال غیرمجاز در محیط سایبری اقدام نموده است. در خصوص حمایت‌های کیفری از دولت‌های آسیب‌دیده از یورش سایبری در این سند، می‌توان به جرم‌انگاری‌هایی اشاره نمود که افعال غیرقانونی علیه داده‌ها، سامانه‌های رایانه‌ای و مخابراتی به شمار می‌روند. یکی از افعال جرم‌انگاری شده در این سند، ایجاد اختلال عمدی و من غیر حق در داده‌های رایانه‌ای است که خرابکاران سایبری نیز از همین طریق به اختلال و تخریب در زیرساخت‌های حیاتی و اطلاعاتی اقدام می‌کنند. با توجه به طبقه‌بندی صورت‌گرفته در این کنوانسیون، با برخی از جرائم در این سند مواجه می‌شویم که رکن مادی یورش سایبری را تشکیل می‌دهند. ایجاد اختلال در داده یا سامانه‌های رایانه‌ای و دستیابی غیرمجاز، رکن اصلی عملیات تروریستی سایبری علیه زیرساخت‌های اطلاعاتی کشور را تشکیل می‌دهند. کنوانسیون یادشده در خصوص حمایت کیفری از داده‌ها رایانه‌ای که عمده‌ترین آماج حملات تروریستی به شمار می‌روند، به‌عین بیان می‌دارد:

«هر یک از اعضا باید به‌گونه‌ای اقدام به وضع قوانین و دیگر تدابیر کنند که در صورت لزوم بر اساس حقوق داخلی خود، هر نوع صدمه‌زدن، پاک‌کردن، خراب‌کردن، تغییر یا قطع داده‌های رایانه‌ای را که به‌طور عمدی و بدون حق انجام می‌شود جرم‌انگاری کنند. اعضا می‌توانند حق جرم‌انگاری افعال مندرج در بند یک را درجایی که صدمه شدیدی واردشده اعمال کنند» (مادهٔ چهار کنوانسیون جرائم سایبر مصوب کارگروه وزرای شورای اروپا، مصوب ۲۰۰۱).

جرم‌انگاری دیگری که در این کنوانسیون به آن پرداخته شده، حمایت از سامانه‌های رایانه‌ای در مقابل افعال غیرمجازی است که منجر به اختلال در عملکرد آن‌ها یا تخریب خود سامانه‌های رایانه‌ای می‌شود. در این خصوص، یکی از مقررات این کنوانسیون به‌عین اعلام می‌دارد:

«هر یک از اعضا باید به‌گونه‌ای اقدام به وضع قوانین و دیگر تدابیر کنند که در صورت لزوم بر اساس حقوق داخلی خود، هر نوع ایجاد اشکال جدی عمدی و بدون حق را که در عملکرد سیستم رایانه‌ای

در اثر واردکردن، انتقال، صدمه‌زدن، پاک‌کردن، خراب‌کردن، تغییر یا متوقف‌کردن داده‌های رایانه‌ای به وجود می‌آید جرم‌انگاری کنند» (مادهٔ پنج کنوانسیون جرائم سایبر مصوب کارگروه وزرای شورای اروپا، مصوب ۲۰۰۱). در این مقرره، شورای اروپا مجموعه‌ای از افعال غیرقانونی را برای دولت‌های عضو ذکر نموده که ممکن است از این طریق منجر به اختلال در عملکرد سامانه‌های رایانه‌ای شود. اعمال یادشده در مادهٔ پنج به‌طور مصداقی، به ذکر جرائم علیه سامانه‌های رایانه‌ای پرداخته، بنابراین هر عملی که سلامت سامانه‌های یادشده را به خطر بیندازد، بر اساس مادهٔ فوق برای جرم‌انگاری در دولت‌های عضو پیشنهاد شده است. هرچند این کنوانسیون دارای ضمانت اجرای قوی و الزام‌آور نیست؛ اما جرم‌انگاری اعمال یادشده که سامانه‌های رایانه‌ای و داده‌ها را موردحمایت قرارمی‌دهد؛ در تقویت قوانین جزایی کشورها مؤثر واقع می‌شود. دسته‌ای دیگر از افعال جرم‌انگاری شده در راستای حمایت از دولت‌های آسیب‌دیده از یورش سایبری، «سوءاستفاده از وسایل، رمز عبور، کد دستیابی، داده‌ها یا برنامه‌های رایانه‌ای» (مادهٔ شش کنوانسیون جرائم سایبر مصوب کارگروه وزرای شورای اروپا، مصوب ۲۰۰۱) هستند که اغلب خرابکاران سایبری از طریق سوءاستفاده از سامانه‌های رایانه‌ای و مخابراتی یا داده‌ها، به اقدامات خرابکارانهٔ خود دست می‌زنند؛ بنابراین با ذکر مواضع اتخاذشده در مقررات این کنوانسیون که به‌طور غیرمستقیم به افعال تشکیل‌دهندهٔ یورش سایبری پرداخته است، می‌توان به حمایت کیفری از دولت‌های آسیب‌دیده از یورش سایبری استدلال نمود.

کنوانسیون پیشگیری از اقدامات غیرقانونی علیه امنیت هواپیمایی کشوری

با توجه به این‌که امروزه تأسیسات هوانوردی، وابستگی شدیدی به سامانه‌های رایانه‌ای و مخابراتی دارند، این امر جذابیت خاصی را برای خرابکاران سایبری فراهم می‌کند که بدون استفاده از هر سلاح فیزیکی و حضور در محل ارتکاب جرم، به اقدامات تروریستی خود اقدام نمایند. این کنوانسیون درزمینهٔ حمایت کیفری از دولت‌های آسیب‌دیده تروریستی سایبری، به افعال خشونت‌باری اشاره نموده که مرتکب یا مرتکبان از هر طریقی علیه تأسیسات هواپیمایی، اقدام به عملیات خرابکارانه دست می‌زنند (بخش یک مادهٔ یک کنوانسیون درباره جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری، مصوب ۱۹۷۱). هرچند این کنوانسیون به ارکان تشکیل‌دهندهٔ یورش سایبری اشاره‌ای نکرده؛ اما عمومیت مفاد این کنوانسیون و ضد یورش و تروریسم بودن آن، دلالت بر شمول مقررات این کنوانسیون در مورد بزه یادشده است و با حمایت قراردادن تأسیسات هوانوردی، اقدام به حمایت کیفری نسبت به دولت‌های آسیب‌دیده از یورش سایبری نموده است.

کنوانسیون پیشگیری از بدافزارهای سایبری

این کنوانسیون یکی از بارزترین اسناد بین‌المللی ضد یورش و تروریسم است که در سال ۱۹۹۷ تصویب گردید (هاشمی، ۱۳۹۰: ۲۵). کنوانسیون یادشده، همانند دیگر اسناد بین‌المللی در خصوص تروریسم، با ذکر

عبارات مبهم و عام‌الشمول به ذکر جرائم تروریستی پرداخته که منجر به «کشتن، جراحت یا ایراد خسارات عمدهٔ مالی» می‌گردد (مادهٔ یک کنوانسیون جلوگیری از بمب‌گذاری تروریستی، مصوب ۱۹۹۷). ازآنجاکه با استفاده از بدافزارهای رایانه‌ای و یا اقدام اشخاص تروریست در تخریب داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، به‌سادگی می‌توان به ایجاد خسارات جبران‌ناپذیر در تأسیسات و زیرساخت‌های کشور، ازجمله نیروگاه‌های اتمی یا مراکز موشکی گردید، با استناد به برخی قواعد عام ابن کنوانسیون، می‌توان به جرم‌انگاری اعمال تروریستی سایبری استدلال نمود. در خصوص جرم‌انگاری افعال یادشده، یکی از مقررات این کنوانسیون به‌عین بیان می‌دارد:

«مواد منفجرهٔ دیگر یا ابزار انفجاری مهلک؛ به سلاح یا ابزاری انفجاری یا آتش‌زا که به‌منظور کشتن یا وارد ساختن جراحت جدی جسمانی یا خسارات عمدهٔ مالی، طراحی‌شده یا دارای چنین قابلیتی باشد، اطلاق می‌شود» (بخش سهٔ مادهٔ یک کنوانسیون جلوگیری از بمب‌گذاری تروریستی، مصوب ۱۹۹۷).

خرابکاران سایبری، می‌توانند با انجام حملات سایبری علیه تأسیسات ذکرشده در این کنوانسیون، شامل تأسیسات مربوط به مواد شیمیایی سمی، عوامل بیولوژیکی یا تابش مواد رادیواکتیو و توقف در کارکرد عملیات آن‌ها، مرگ‌ومیر، صدمات شدید جسمانی را برای اشخاص حقیقی در مجاورت آن‌ها در پی داشته باشند. بدین منظور تدوین‌کنندگان سند یادشده در خصوص مواد منفجرهٔ دیگر یا ابزارهای انفجاری اعلام می‌دارند:

«سلاح یا ابزاری که به‌منظور کشتن، ورود جراحت جدی جسمانی یا خسارات عمده مالی از طریق آزادکردن، انتشار یا تراکم مواد شیمیایی سمی، عوامل بیولوژیکی یا سموم یا مواد مشابه یا پرتوافکنی و یا مواد رادیواکتیویته طراحی‌شده و یا چنین قابلیتی داشته باشد» (بخش سهٔ مادهٔ یک کنوانسیون جلوگیری از بمب‌گذاری تروریستی، مصوب ۱۹۹۷).

بنابراین با بررسی برخی از مفاد مقررات این کنوانسیون، این‌گونه برداشت می‌شود که رایانه می‌تواند به‌عنوان واسطه و ماشه‌ای برای منفجرکردن بمب یا ابزار مرگباری باشد که اشخاص تروریست از آن برای اقدامات تروریستی استفاده می‌کنند. با توجه به این‌که از رایانه در مراکز حساس و زیرساخت‌هایی همچون رآکتورهای هسته‌ای، آزمایشگاه‌های شیمیایی و پزشکی برای کنترل درجهٔ حرارت دما، رطوبت و اشعه‌های رادیواکتیو استفاده می‌شود، می‌توان به حمایت‌های کیفری این کنوانسیون نسبت به داده‌ها، تأسیسات رایانه‌ای و مخابراتی و اشخاص حقیقی در این کنوانسیون استدلال نمود.

کنوانسیون سرکوب حمایت مالی از یورش و تروریسم سایبری

کنوانسیون یادشده، یکی از قطعنامه‌های معروف درزمینهٔ منع حمایت مالی از تروریسم است که در ۹ دسامبر ۱۹۹۹ توسط مجمع عمومی سازمان ملل متحد به تصویب رسید (طیبی فرد، ۱۳۸۴: ۲۷۱). با توجه

به این‌که منابع مالی، نقش اولیه را در شکل‌دهی عملیات تروریستی ایفا می‌کنند، می‌توان از بزه‌دیده شدن اشخاص، به‌طور غیرمستقیم با منع و جرم‌انگاری حمایت‌های مالی، جلوگیری و با تعیین ضمانت اجراهای قوی از آن‌ها حمایت کیفری نمود. در این راستا کنوانسیون یادشده، به جرم‌انگاری تأمین مالی تروریسم در قوانین جزایی پرداخته است و در این خصوص به‌عین بیان می‌دارد:

«هرگاه شخصی منابع مالی را با علم یا قصد این‌که در اعمال تروریستی استفاده گردد، جمع‌آوری یا مهیا نماید درحالی‌که عمل وی غیرقانونی و عامدانه است صرف‌نظر از این‌که وی مستقیماً به این عمل اقدام نماید یا غیرمستقیم، یا همه اموال در حمله مورداستفاده قرار گیرد یا بخشی از آن، آن شخص ازنظر این کنوانسیون مجرم تلقی خواهد شد» (مادهٔ دو کنوانسیون سرکوب حمایت مالی از تروریسم، مصوب ۱۹۹۹).

قطعنامهٔ شورای امنیت سازمان ملل متحد به شمارهٔ ۱۳۷۳، یکی دیگر از اسناد بین‌المللی در رابطه با جرم‌انگاری حمایت مالی از اعمال تروریستی است. در این راستا قطعنامهٔ ۱۳۷۳ به ایجاد سازوکارهای بین‌المللی مبارزه با تأمین مالی تروریسم که شامل جرم‌انگاری تأمین مالی اقدامات تروریستی (ردیف‌های (الف) و (ب) بند یک قطعنامهٔ ۱۳۷۳ شورای امنیت، مصوب ۲۰۰۱) و همچنین به مکلف نمودن دولت‌ها به‌منظور تلاش برای پیشگیری و مقابله با تأمین مالی تروریسم در قالب فعالیت‌های مختلف اقدام نموده است (ردیف (ث) بند دو قطعنامهٔ ۱۳۷۳ شورای امنیت، مصوب ۲۰۰۱).

به‌طورکلی شورای امنیت در ارتباط با تأمین مالی تروریسم، هشت قطعنامه را تصویب نموده است که مهم‌ترین آن‌ها عبارت‌اند از: قطعنامهٔ شمارهٔ ۱۳۷۷ در دسامبر ۲۰۰۱ و قطعنامهٔ ۱۳۹۰ در ۲۸ ژانویهٔ ۲۰۰۲. قطعنامه‌های فوق، ازجمله اسناد بین‌المللی در رابطه با تعهدات حقوقی بین‌المللی دولت‌ها برای منع حمایت مالی و ایمن ساختن سرزمین‌های دولت‌ها از حامیان مالی تروریست‌ها هستند.

قطعنامهٔ شمارهٔ ۱۳۷۳ شورای امنیت

شورای امنیت با تصویب این قطعنامه در سال ۲۰۰۱، اقدامات تروریستی را به‌طورکلی مجرمانه قلمداد نموده و جرم‌انگاری این اقدامات را در بین قوانین داخلی کشورها به‌عنوان تعهدی سازمانی بر تمامی دولت‌های جهان تکلیف و تحمیل می‌کند. این سند بین‌المللی اقدام بی‌سابقهٔ شورای امنیت در مقابله با تروریسم به شمار می‌رود که با تصویب این قطعنامه، قاطعیت خود را در مبارزه با جرائم تروریستی نشان‌داد. درمجموع از مفاد این کنوانسیون، چهار موضوع اساسی استناد می‌شود که عبارت‌اند از: الزام دولت‌ها به همکاری و معاضدت با یکدیگر به‌منظور سرکوب تروریسم، مقابله با تأمین مالی تروریسم، عدم پشتیبانی مستقیم و غیرمستقیم از تروریسم و جرم‌انگاری و تعقیب کیفری تروریسم از عمده نکاتی است که در این قطعنامه مورد تأکید قرار گرفته است (زرنشان، ۱۳۸۶: ۶۹).

دولت‌های خاصی در این کنوانسیون موردحمایت قرار نگرفته‌اند؛ اما از کلیّت اقدامات تروریستی اشاره

شده در این قطعنامه، می‌توان نتیجه گرفت که اگر یورش سایبری منجر به تخریب تأسیسات حیاتی شود، دولت‌های آسیب‌دیده نیز موردحمایت کیفری این قطعنامه قرار خواهند گرفت.

بیانیهٔ یازدهمین نشست پیشگیری از جرائم و بسط عدالت کیفری سازمان ملل متحد

این بیانیه که در سال ۲۰۰۵ در شهر بانکوک صادر شد، دربارهٔ موضوعاتی از قبیل مبارزه با جرم و پی‌جویی عدالت، به‌خصوص درزمینهٔ همکاری بین‌المللی بر ضد یورش و تروریسم و ارتباط تروریسم با دیگر اعمال مجرمانه در چارچوب کاری دفتر مقابله با جرم و مواد مخدر سازمان ملل متحد، مباحث مختلفی را عنوان نموده است (ادارهٔ پژوهش، ۱۳۸۴: ۳۵). در بیانیهٔ یادشده، به جرائمی اشاره کرده که با گسترش استفاده از فضای سایبر، به چالشی بزرگ برای نظام‌های حقوقی دولت‌ها تبدیل شده است. در خصوص جرائم رایانه‌ای، این نشست اقدام به معرفی دسته‌ای از جرائم رایانه‌ای اقدام نموده که عبارتند از: انتشار ویروس‌های رایانه‌ای جهانی و هدف قراردادن فنّاوری‌های اطلاعاتی و ارتباطی، خرابکاری، جعل یا تقلب حرفه‌ای الکترونیکی، سرقت یا کلاه‌برداری (حملات هکری به بانک‌ها یا نظام‌های مالی)، ارسال پیام‌های مزاحم و ایمیل‌های تقلبی، برای به‌دست‌آوردن اطلاعات مالی، خصوصی و کلمات که این اقدامات، نمونه‌ای از تلاش‌های جامعهٔ بین‌المللی در حمایت‌های کیفری از دولت‌های آسیب‌دیده از یورش سایبری؛ یعنی فنّاوری‌های اطلاعاتی و ارتباطی در این سند به شمار می‌رود.

کنوانسیون اروپایی مقابله با حملات سایبری

اتحادیهٔ کشورهای اروپایی، سیاست‌های متعددی را در خصوص حملات علیه شبکه‌های رایانه‌ای، انتشار ویروس‌ها، کرم‌های رایانه‌ای، تروجان‌ها، هرزنامه‌های اینترنتی، حملات فیشینگ و سرقت هویت صادر نموده است. با توجه به این‌که موارد یادشده به‌طور غالب در یورش سایبری مورداستفاده قرار می‌گیرند، بنابراین اتحادیهٔ اروپا یکی از مهم‌ترین سازمان‌هایی است که به‌منظور جرم‌انگاری افعال غیرمجاز در محیط سایبری گام برداشته است (*Dunn&Mauer, 2016: 182-183*). دامنهٔ شمول این کنوانسیون در مقایسه با دیگر اسناد ضد یورش و تروریسم وسیع‌تر است و تقریباً تمامی جرائم یادشده در کنوانسیون‌های بین‌المللی ضد یورش و تروریسم را شامل می‌شود. هرچند این کنوانسیون به جرم‌انگاری صریحی از اقدامات تروریستی اشاره نکرده؛ اما کلیّت مفاد این سند، جا را برای جرم‌انگاری سایر جرائم تروریستی باز گذاشته و با تأکید بر شمول قواعد سایر کنوانسیون‌های بین‌المللی، می‌توان به حمایت از دولت‌های آسیب‌دیده از یورش سایبری ازجمله تأسیسات حیاتی و اشخاص حقیقی استدلال نمود.

در ادامه این کنوانسیون، به اعضاء اجازه داده تا قلمرو جرائم این کنوانسیون را گسترش داده و هر جرمی را که تهدیدی علیه حیات، صدمات جسمانی، آزادی شخص یا اموال باشد را در مقررات این کنوانسیون بگنجانند (مادهٔ دو کنوانسیون اروپایی مقابله با تروریسم، مصوب ۱۹۹۹).

کنوانسیون منطقه‌ای سازمان همکاری‌های منطقه‌ای آسیای جنوبی

کنوانسیون یادشده، یکی دیگر از تلاش‌های منطقه‌ای کشورهای جهان در مبارزه با یورش‌های سایبری است که در سال ۱۹۸۷ در کاتماندو به تصویب رسید (زمانی، ۱۳۹۸: ۱۳۸). بر اساس مقررات این کنوانسیون، جرائم تروریستی قابل پیگرد عبارت‌اند از:

«جرائم یادشده در محدودهٔ کنوانسیون مقابله با اقدامات غیرقانونی علیه امنیت هواپیمایی کشوری مصوب ۱۹۷۱ مونترال» (مادهٔ یک کنوانسیون منطقه‌ای سازمان همکاری‌های منطقه‌ای آسیای جنوبی، مصوب ۱۹۸۷) که در آن تأسیسات هوانوردی موردحمایت کنوانسیون قرار گرفته بودند. دسته‌ای دیگر از جرائم تروریستی، جرائمی هستند که با ماهیت تروریستی، منجر به صدمات شدید جسمی شوند یا برای حیات یا دارایی‌های انسان، خطرات جدی ایجاد نمایند که بر اساس مقررات این کنوانسیون، شامل «قتل (عمد و غیر عمد)، حمله و ضرب و شتمی که منجر به آسیب شدید جسمانی شود یا سلاح‌های انفجاری به‌عنوان یک ابزار، خطرات جدی برای حیات و دارایی‌های اشخاص ایجاد نماید» (مادهٔ یک کنوانسیون منطقه‌ای سازمان همکاری‌های منطقه‌ای آسیای جنوبی، مصوب ۱۹۸۷). دسته‌ای دیگر از جرائمی که در این کنوانسیون منطقه‌ای مورداشاره قرارگرفته‌اند، «شامل جرائم یادشده در محدودهٔ هر کنوانسیون ضد تروریستی که دولت‌های عضو «سارک» با آن ارتباط دارند و عضو آن هستند رخ دهد، اعضاء توافق کنند که مجریان را تعقیب و استرداد نمایند» (مادهٔ یک کنوانسیون منطقه‌ای سازمان همکاری‌های منطقه‌ای آسیای جنوبی، مصوب ۱۹۸۷).

با توجه به بررسی مجموعه‌ای از جرائم اشاره شده در این سند، جرم‌انگاری افعالی که از طریق رایانه یا اینترنت به اقدامات تروریستی منتج می‌شود، دیده نمی‌شود؛ اما با استدلال به قواعد عام ارتکاب جرائم تروریستی که در کنوانسیون‌های متعددی، ازجمله کنوانسیون مقابله با اقدامات غیرقانونی علیه امنیت هواپیمایی کشوری، می‌توان به اشارهٔ غیرمستقیم این کنوانسیون‌ها به افعال تشکیل‌دهندهٔ یورش سایبری و در مقابل به حمایت از دولت‌های آسیب‌دیده این جرم استدلال نمود.

کنوانسیون سازمان اجلاس اسلامی

این کنوانسیون در سال ۱۹۹۹ توسط سازمان اجلاس اسلامی به تصویب و در سال ۱۳۸۰ کشورمان نیز این کنوانسیون را در راستای مبارزه با تروریسم و همکاری‌های بین اعضاء به تصویب رساند (کدخدایی و ساعد، ۱۳۹۶: ۲۵۶). در خصوص حمایت کیفری از دولت‌های آسیب‌دیده از تروریسم و جرم‌انگاری افعال غیرقانونی در این رابطه می‌توان به تعریف سازمان اجلاس اسلامی از تروریسم اشاره نمود که با کلیّت خود، به افعالی اشاره نموده که بدین‌وسیله می‌توان شمول یورش سایبری را نسبت به مفاد این سند منطقه‌ای استدلال نمود. این کنوانسیون، تروریسم را عملی می‌داند که همراه با خشونت یا تهدید به خشونت و با انگیزه‌های سیاسی، مالی، مذهبی، فردی، گروهی در قالب اعمال جنایی (جرائم علیه تمامیت جسمانی،

روانی یا امنیت ملّی) با هدف ایجاد ترس در جامعه یا تهدید به ایراد صدمه به مردم یا اموال عمومی یا خصوصی یا امنیت ملّی، خواه اقدامات یادشده انجام بشود یا این‌که در حالت تهدید باقی بماند، ارتکاب یابد (مادهٔ یک کنوانسیون سازمان اجلاس اسلامی درزمینهٔ مبارزه با تروریسم بین‌المللی، مصوب ۱۹۹۹).

علاوه بر تعریف تروریسم که در بالا به آن اشاره گردید، سازوکارهایی برای مقابله با جرائم تروریستی پیش‌بینی‌شده که در مورد بزه موردبحث و حمایت از دولت‌های آسیب‌دیده صادق است. ازجمله سازوکارهای اشاره شده در این کنوانسیون، می‌توان به ایجاد و تقویت سامانه‌هایی برای تضمین سلامت و حفاظت از اشخاص، تأسیسات حیاتی و وسایل حمل‌ونقل عمومی، اشاره نمود که زیرساخت‌های عمدهٔ یک دولت را تشکیل می‌دهند و به‌طور غالب تروریست‌ها این دسته از آماج را موردتهاجم قرار می‌دهند. این کنوانسیون به حمایت عمده‌ترین دولت‌های آسیب‌دیده از یورش سایبری؛ یعنی تأسیسات حیاتی و زیرساخت‌های حمل‌ونقل اشاره نموده و به‌منظور جبران خسارت زودهنگام از دولت‌های آسیب‌دیده تروریسم که یورش سایبری را نیز شامل می‌شود، کمک‌رسانی فوری به آن‌ها را مورد تأکید قرار داده است (مادهٔ سه کنوانسیون سازمان اجلاس اسلامی درزمینهٔ مبارزه با تروریسم بین‌المللی، مصوب ۱۹۹۹).

معاهدهٔ همکاری میان دولت‌های عضو کشورهای مستقل مشترک‌المنافع در مبارزه یا تروریسم

معاهدهٔ یادشده، توسط کشورهای مستقل مشترک‌المنافع در سال ۱۹۹۹، تصویب شده است (کدخدایی و ساعد، ۱۳۹۰: ۳۹۰). در خصوص حمایت کیفری از دولت‌های آسیب‌دیده از تروریسم، افعال مجرمانه‌ای جرم‌انگاری شده‌اند که آماج خرابکاران سایبری نیز محسوب می‌شوند. دسته‌ای از جرائم یادشده، «خشونت یا تهدید به خشونت علیه اشخاص حقیقی یا حقوقی» (مادهٔ یک کنوانسیون همکاری میان دولت‌های عضو کشورهای مستقل مشترک‌المنافع در مبارزه یا تروریسم، مصوب ۱۹۹۹) هستند که خرابکاران سایبری نیز از این طریق درصدد دستیابی به اهداف خود هستند. خرابکاران سایبری، با استفاده از فضای سایبر، می‌توانند به اعمال خشونت‌آمیز علیه اشخاص حقوقی؛ یعنی زیرساخت‌های حیاتی کشور یا تارنماهای دولتی یا تهدید به خشونت علیه اشخاص حقیقی، از طریق تخریب در سامانه‌های رایانه‌ای متعلق به امور اجرایی کشور یا تأسیسات حمل‌ونقل عمومی و یا تهدید به چنین اعمالی اقدام نمایند.

علاوه بر موارد فوق، دسته‌ای دیگر از جرائم مورداشاره در این معاهده، «جرائمی هستند که منجر به تخریب یا تهدید به تخریب و وارد آوردن خسارت به دارایی یا سایر اشیاء مادی می‌شوند؛ به‌نحوی که زندگی افراد را به مخاطره اندازند. خرابکاران سایبری نیز با استفاده از همین راهکارها؛ یعنی تهدید به تخریب یا تخریب دارایی‌هایی مانند اختلال در سامانه‌های اورژانس یا آتش‌نشانی که به‌واسطهٔ تخریب این تأسیسات، زندگی بسیاری از افراد به مخاطره می‌افتد به عملیات تروریستی اقدام می‌کنند» (مادهٔ یک کنوانسیون همکاری میان دولت‌های عضو کشورهای مستقل مشترک‌المنافع در مبارزه یا تروریسم، مصوب ۱۹۹۹).

تروریسم فنّاورانه، نیز از جرائمی است که در این معاهده به آن اشاره گردیده است. با توجه به این‌که یورش

سایبری با استفاده از فنّاوری جدید اقدام به عملیات تروریستی می‌شود، می‌توان به جرم‌انگاری غیرمستقیم این بزه در این سند استدلال نمود (مادهٔ یک کنوانسیون همکاری میان دولت‌های عضو کشورهای مستقل مشترک‌المنافع در مبارزه با تروریسم، مصوب ۱۹۹۹).

کنوانسیون سازمان وحدت آفریقا و پروتکل الحاقی سال ۲۰۰۴

این کنوانسیون در سال ۱۹۹۹، توسط سازمان وحدت آفریقا در راستای مبارزه با تروریسم به تصویب رسید (کدخدایی و ساعد، ۱۳۹۰: ۳۹۰). در تطبیق مفاد این کنوانسیون منطقه‌ای، با افعال تشکیل‌دهندهٔ یورش تروریستی و بررسی حمایت‌های کیفری از دولت‌های آسیب‌دیده آن، می‌توان به یکی از مقررات این سند اشاره نمود که به جرم‌انگاری عملی که منجر به «آسیب به حیات، تمامیت جسمانی و آزادی فردی یا گروهی شود یا موجب خسارت به دارایی خصوصی و عمومی افراد، منابع طبیعی، محیط‌زیست، میراث فرهنگی بشود یا قصد ارتکاب چنین عملی را داشته باشد، اشاره نمود»(بند سهٔ مادهٔ یک کنوانسیون سازمان وحدت آفریقا دربارهٔ پیشگیری و مبارزه با تروریسم، مصوب ۱۹۹۹). در این مقرره، از برخی دولت‌های آسیب‌دیده یعنی، تمامیت جسمانی افراد و دارایی‌های آن‌ها حمایت کیفری شده است. در ادامه همین ماده، به اقداماتی اشاره می‌کند که کسی به‌واسطهٔ عملی «ایجاد وحشت نماید و حالت ترس یا وحشت را تحریک کند یا بر روی دولت یا نهاد، جمعیت و گروهی متوسل به اعمال فشار و تهدید شود» (بند سهٔ مادهٔ یک کنوانسیون سازمان وحدت آفریقا دربارهٔ پیشگیری و مبارزه با تروریسم، مصوب ۱۹۹۹). همچنان که از ماهیت جرائم تروریستی پیداست، عنصر ترس و وحشت، رکن اصلی چنین بزه‌هایی به شمار می‌رود. این امر نیز در یورش سایبری قطعاً به‌مراتب مشهودتر است و اشخاص بزهکار با استفاده از محیط سایبر بیشتر می‌توانند به چنین اقداماتی دامن بزنند.

در ادامه همین مقرره، به عمده‌ترین دولت‌های آسیب‌دیده از یورش سایبری یعنی، «زیرساخت‌های عمومی و حیاتی کشور که به‌منظور ارائهٔ خدمات عمومی و همچنین خدمات مالی عمومی استفاده می‌شوند و درنتیجه چنین عملی، منجر به اختلال در عملکرد این خدمات بشود اشاره نموده است» (بند سهٔ مادهٔ یک کنوانسیون سازمان وحدت آفریقا دربارهٔ پیشگیری و مبارزه با تروریسم، مصوب ۱۹۹۹).

بنابراین در این کنوانسیون، دو دسته از اعمالی را که بتوانیم آن‌ها را با ارکان یورش سایبری تطبیق دهیم و حمایت از دولت‌های آسیب‌دیده آن را نتیجه بگیریم، اشاره شده که یکی، تهدید و ایجاد ترس در افراد یک گروه یا جامعه و دیگری، اقدام به اخلال در تأسیساتی است که ارائهٔ خدمات عمومی و خدمات مالی را به عهده دارند. با توجه به این‌که این دو دسته از افعال غیرقانونی، ارکان اصلی بزه یورش سایبری را تشکیل می‌دهند و به حمایت کیفری از عمده‌ترین آماج خرابکاران سایبری پرداخته است، با استناد به مفاد عام این کنوانسیون، می‌توان به حمایت کیفری از دولت‌های آسیب‌دیده بزه یادشده استدلال نمود.

کنوانسیون عربی مقابله با تروریسم

کنوانسیون عربی مقابله با تروریسم، یکی از اسناد منطقه‌ای در مبارزه یا تروریسم است که در سال ۱۹۹۸ تصویب گردید. این سند همانند برخی دیگر اسناد مبارزه با تروریسم، در راستای حمایت کیفری از دولت‌های آسیب‌دیده از یورش تروریستی، مجموعه افعالی را که با اهداف تروریستی ارتکاب می‌یابند، جرم‌انگاری نموده و از ذکر مصادیق جرائم تروریستی خودداری نموده است؛ بنابراین در این کنوانسیون فقط از تعریف ارائه‌شده از تروریسم می‌توان به جرم‌انگاری غیرمستقیم افعال مربوط به یورش سایبری پی برد. از عام بودن حوزهٔ ارتکاب مفاد این کنوانسیون، این‌چنین استدلال می‌شود که در صورتی عملی تروریستی، از طریق رایانه ارتکاب یابد و تأسیسات رایانه‌ای و مخابراتی را مورد اختلال یا تخریب قرار دهد، بر اساس این کنوانسیون قابل پیگرد است؛ زیرا بر اساس مفاد این کنوانسیون، تروریسم عبارت است از:

«هرگونه ارتکاب جرم یا شروع به جرمی که به‌قصد اجرای یک هدف تروریستی در هر یک از کشورهای هم‌پیمان یا علیه هر یک از اتباع یا مصالح آن دولت‌ها که طبق قوانین داخلی آن‌ها موجب پیگرد یا کیفر باشد» (مادهٔ یک کنوانسیون عربی مقابله با تروریسم، مصوب ۱۹۹۸).

کنوانسیون سازمان کشورهای آمریکایی برای پیشگیری و مجازات اعمال تروریستی

کنوانسیون منطقه‌ای سازمان کشورهای آمریکایی، در تاریخ دو فوریهٔ ۱۹۷۱ توسط ۳۵ عضو این سازمان در واشنگتن تصویب گردید. کنوانسیون سازمان کشورهای آمریکایی، همانند دیگر اسناد منطقه‌ای یا بین‌المللی، به‌طور صریح و روشن به پیشگیری از جرائم رایانه‌ای، به‌خصوص یورش سایبری اشاره‌ای نکرده است؛ بلکه با عناوین کلی سعی داشته جرائمی را که منجر به تضییع حقوق عامهٔ مردم شود و بازتاب بین‌المللی داشته باشد را موردتوجه قرار دهد. کنوانسیون مزبور در این رابطه مقرر می‌دارد: «هر یک از دولت‌های عضو مکلف هستند نسبت به جرائمی که حقوق عامهٔ مردم را مورد تعرض قرار می‌دهند و خصیصهٔ بین‌المللی داشته باشند و همچنین شامل جرائمی از قبیل ناامنی، آدم‌ربایی و قتل بشوند، حمایت‌های خود را بر اساس حقوق بین‌المللی از اشخاص بزه‌دیده به عمل آورند» (مادهٔ دو کنوانسیون پیشگیری و سرکوب اعمال تروریستی سازمان کشورهای آمریکایی، مصوب ۱۹۷۱).

بنابراین به نظر می‌رسد جرائمی مانند یورش سایبری که اغلب دارای خصیصهٔ فراملی هستند و منجر به تعرض مستقیم و غیرمستقیم حقوق شهروندان می‌شود، بر اساس این سند منطقه‌ای قابل پیگرد باشد.

قطعنامه ایجاد فرهنگ جهانی امنیت سایبری و تلاش‌های ملّی برای حفاظت از زیرساخت‌های اطلاعاتی حساس[1]

مجمع عمومی در طی این قطعنامه به شمارهٔ ٦٤/٢١١ که در مارس سال ۲۰۱۰ به تصویب رسیده است، به تشویق کشورهای عضو و سازمان‌های بین‌المللی و منطقه‌ای در شناخت شکاف‌ها در دسترسی و

1. *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*

استفاده از فنّاوری اطلاعات و به اشتراک گذاشتن سازوکارهای امنیتی و حفاظت از زیرساخت‌های اطلاعاتی حساس به‌منظور جلوگیری از افزایش رو به رشد جرائم مربوط به فنّاوری اطلاعات پرداخته است (See: A/RES/64/211, 2010).

قطعنامهٔ مبارزه با سوءاستفادهٔ جنایت‌کارانه از فنّاوری اطلاعات[1]

قطعنامه‌های ۵۵/۶۳ و ۵۶/۱۲۱، به مسائل کیفری مرتبط به فنّاوری اطلاعات و به ابراز نگرانی از پیشرفت فنّاوری‌های جدید که به‌موازات آن، فعالیت‌های مجرمانهٔ جدید را به وجود آورده‌اند و سوءاستفادهٔ بزهکارانی که از فنّاوری‌های اطلاعاتی برای ارتکاب اعمال مجرمانه استفاده می‌کنند، پرداخته‌اند. عمده‌ترین دولت‌های آسیب‌دیده موردحمایت در این دو قطعنامه، حمایت از محرمانه‌بودن و تمامیت داده‌ها و سامانه‌های رایانه‌ای از اختلال و دسترسی غیرمجاز و به‌طورکلی مجموعهٔ فنّاوری اطلاعات است که امروزه با تهدیدات نوینی ازجمله یورش سایبری مواجه هستند (See: A/RES/56/121, 2002).

هرچند این قطعنامه‌ها در مورد دولت‌های آسیب‌دیده از یورش سایبری، عنوانی به میان نیاورده‌اند؛ اما نکات ارائه‌شده در این قطعنامه‌ها، به‌صورت است که مفاد آن مشمول یورش سایبری و حمایت از دولت‌های آسیب‌دیده آن (داده‌ها و سامانه‌های رایانه‌ای) خواهد شد.

قطعنامهٔ ایجاد فرهنگ جهانی امنیت سایبر و حمایت از زیرساخت‌های اطلاعاتی حساس[2]

قطعنامهٔ فوق با شمارهٔ ۵۸/۱۹۹ در ژانویهٔ سال ۲۰۰۴ توسط مجمع عمومی سازمان ملل متحد به تصویب رسید. دولت‌های آسیب‌دیده موردحمایت در این قطعنامه، زیرساخت‌های اطلاعاتی حساس هستند که بر اساس مقررات این قطعنامه، به تلاش دولت‌ها برای حفاظت از زیرساخت‌های حساس با توجه به قوانین داخلی و ملّی با رعایت حفظ حریم خصوصی اشاره شده است (See:A/RES/58/199, 2004).

کنوانسیون بین‌المللی حقوق مدنی و سیاسی

کنوانسیون یادشده، به‌طورکلی قربانیان تخلف از حقوق بشر را موردحمایت و توجه قرار داده است. با توجه به این‌که حملات تروریستی نیز یکی از جرائمی است که به‌شدت حقوق بشر را نقض می‌کند، می‌توان قواعد این کنوانسیون را دربارهٔ دولت‌های آسیب‌دیده از یورش تروریستی مشمول دانست. در این راستا این سند بین‌المللی با درنظرگرفتن ضوابط و هنجارهای حقوق بشر، تضمین کرده است که قربانیان تخلف از حقوق بشر، از حق جبران و چاره‌جویی مؤثر، شامل حق داشتن چنین جبرانی که توسط مقامات قضایی، اجرایی و قانونی ذی‌صلاح تعیین‌شده و از حق اجراشدن این جبران در زمان اعطا برخوردار باشند (پاراگراف سهٔ مادهٔ دو کنوانسیون بین‌المللی حقوق مدنی و سیاسی، مصوب ۱۹۶۶).

قطعنامهٔ حمایت از قربانیان تخلفات فاحش بین‌المللی

این قطعنامه به شمارهٔ ۶۰/۱۴۷ در دسامبر سال ۲۰۰۵ توسط مجمع عمومی سازمان ملل متحد به

1. *Combating the criminal misuse of information technologies*
2. *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*

تصویب رسید. این سند، دستاورد تلاش سازمان‌های بین‌المللی و دولت‌ها درزمینهٔ شناسایی حق‌های دولت‌های آسیب‌دیده‌ای است که در اثر جرائم خشونت‌بار و اعمال مخالفِ جدیِ حقوق بشردوستانهٔ بین‌المللی صدمه و آسیب‌دیده‌اند. این قطعنامه حق‌های جبران را برای بزه‌دیده ازجمله: «جبران خسارت، پرداخت غرامت، توان‌بخشی و اعادهٔ حیثیت، اقناع‌سازی بزه‌دیده و تضمین‌های تکرارنکردن بزه‌دیدگی دوباره به رسمیت شناخته است که قواعدی همچون اعادهٔ حیثیت و پرداخت غرامت در قالب حمایت‌های کیفری از دولت‌های آسیب‌دیده موردبحث قابل‌اعمال است» (رایجیان اصلی، ۱۳۹۸: ۲۶۲).

نشست هفتم سازمان ملل متحد

این نشست در سال ۱۹۸۵ به حقوق افراد و دولت‌های آسیب‌دیده از جرائم رایانه‌ای در رابطه با دریافت غرامت و اختیار حذف یا اصلاح برخی داده‌های شخصی بزه‌دیده و اقدامات هماهنگ بین‌المللی درزمینهٔ مقابله با جرائم سایبری اشاره‌کرده است که از عمومیت آن می‌توان به حمایت‌های مختلف از دولت‌های آسیب‌دیده از یورش تروریستی (و نه سایبری) به‌خصوص حمایت کیفری استناد کرد (زندی، ۱۳۹۷: ۲۷).

نشست هشتم سازمان ملل متحد

این نشست که در ۲۷ اوت تا ۷ دسامبر ۱۹۹۰ برگزار شد، به صدور قطعنامه‌ای انجامید که مجمع عمومی سازمان ملل متحد نیز همراه با قطعنامهٔ ۴۵/۱۲۱ اسناد نشست هشتم را مورد تصویب قرارداد. در این نشست از کشورهای عضو خواسته‌شده که به مدرنیزه‌کردن قوانین و دادرسی‌های کیفری خود تلاش نمایند. منظور از مدرنیزه‌کردن قوانین در این نشست شامل «ارتقای ضوابط مربوط به آیین دادرسی جرائم سایبری و تقویت سازوکارهای پیشگیرانه از این جرائم، افزایش آگاهی مردم درزمینهٔ وقوع جرائم رایانه‌ای و پیشگیری از آن‌ها، آموزش مجریان قضایی درزمینهٔ برخورد با جرائم رایانه‌ای، حمایت از دولت‌های آسیب‌دیده بر اساس اعلامیهٔ اصول بنیادی عدالت برای دولت‌های آسیب‌دیده و قربانیان سوءاستفاده از قدرت از عمده نکات مورداشاره در این نشست به شمار می‌روند» (زندی، ۱۳۸۷: ۲۸). با توجه به مورد خطاب دادن همهٔ دولت‌های آسیب‌دیده سایبری، از قواعد این نشست می‌توان به حمایت کیفری از دولت‌های آسیب‌دیده از یورش تروریستی (و نه لزوماً سایبری) پرداخت.

نشست دهم سازمان ملل متحد

نشست دهم سازمان ملل متحد در سال ۲۰۰۰، دربارهٔ جرائم شبکه‌های رایانه‌ای به شمارهٔ ۱۸۷/۱۰ در وین برگزار شد. درزمینهٔ افعال غیرقانونی و مشابه با یورش تروریستی، این نشت به چند دسته از جرائم رایانه‌ای اشاره‌کرده است که عبارت‌اند از: جرائم ارتکابی علیه فنّاوری‌ها و کاربران آن‌ها که شامل پنج گونه از جرائم تحت عنوان دستیابی غیرمجاز به رایانه و سامانه‌های رایانه‌ای، استفاده غیرمجاز از سامانه‌های رایانه‌ای، خواندن، کپی کردن یا کپی گرفتن دادهٔ بدون مجوز، ایجاد برنامه‌های مهاجم،

تخریب داده‌ها یا سامانه‌های رایانه‌ای مورداستفادهٔ عموم و خرابکاری رایانه‌ای هستند. در نشست یازدهم نیز نکاتی دربارهٔ مبارزه با جرائم رایانه‌ای مورداشاره قرار گرفته که شامل تلاش‌های صورت‌گرفته در مبارزه با جرائم رایانه‌ای در کشورها و به اقدامات سازمان‌های بین‌المللی درزمینهٔ مبارزه با جرائم رایانه‌ای اشاره شده است (زندی، ۱۳۹۷: ۲۹).

پیش‌نویس کنوانسیون سازمان ملل متحد دربارهٔ عدالت و پشتیبانی از قربانیان سوءاستفاده از قدرت

این سند که مصوب هشتم فوریهٔ ۲۰۱۰ توسط مجمع عمومی سازمان ملل متحد است، یکی دیگر از اسناد بین‌المللی در رابطه با حمایت از دولت‌های آسیب‌دیده ناشی از حملات تروریستی به شمار می‌رود. با استناد این کنوانسیون، اشخاص حقیقی تحت حمایت این سند، کسانی هستند که «قوانین جزایی دولت‌های عضو را نقض می‌کنند، یا در اثر سوءاستفاده از قدرت یا اعمال مرتبط با تروریسم، منجر به صدمه‌های شدید بدنی یا مرگ شهروندان و غیرنظامیان می‌شوند» (مادهٔ دو پیش‌نویس کنوانسیون سازمان ملل متحد دربارهٔ عدالت و پشتیبانی برای دولت‌ها و قربانیان سوءاستفاده از قدرت، مصوب ۲۰۱۰)؛ بنابراین با توجه به مادهٔ فوق، می‌توان به تحت شمول قراردادن یورش سایبری در خصوص قواعد این کنوانسیون استناد کرد. کنوانسیون یادشده به‌طور گسترده با مخاطب قراردادن دولت‌ها به انواع حمایت از دولت‌های آسیب‌دیده از هر نوع تروریسم، ازجمله حمایت‌های کیفری، شکلی، روانی، اجتماعی پرداخته است. از دیگر تلاش‌های سازمان ملل متحد در مبارزهٔ کیفری با افعال یورش سایبری، می‌توان به قطعنامه‌های ۵۳/۷۰ در دسامبر ۱۹۹۸، ۵٤/٤۹ در دسامبر ۱۹۹۹، ۵۵/۲۸ و ۵۵/۶۳ در سال ۲۰۰۰، ۵۶/۱۹ در نوامبر ۲۰۰۱، ۵۵/۷۳ در نوامبر ۲۰۰۲، ۵۸/۳۲ در دسامبر ۲۰۰۳ در رابطه با «تحولات در حوزهٔ اطلاعات و ارتباطات درزمینهٔ امنیت بین‌الملل»[1] و قطعنامه‌ای با شمارهٔ ۲۳/۲۱ در سال ۲۰۰۸ که بر افزایش آگاهی عمومی دربارهٔ یورش تروریستی و فراخوان دولت‌ها برای جرم‌انگاری مجازات استاندارد درزمینهٔ مقابله با یورش تروریسم فنّاورانه تأکید کرده است (*Teodoro et al.* 2021:3). روی‌هم‌رفته، با توجه به مادهٔ فوق، نمی‌توان به تحت شمول قرارگرفتن دولت‌های آسیب‌دیده از یورش سایبری در خصوص قواعد این کنوانسیون استناد کرد.

بحث و نتیجه‌گیری

هنگامی که تبعات یورش‌های سایبری کاملاً واضح و عیان باشد، ارزیابی تأثیرات آن با واقعیت سنجیده می‌شود. در این صورت، دولت‌ها حملات سایبری را به‌عنوان اقدام علیه امنیت ملی خود قلمداد می‌کنند. بااین‌حال، کاربست این معیار در فضای سایبر با چالش‌هایی همراه است. درواقع، اگر پیامدهای یورش‌های سایبری، محسوس، عینی، قابل‌اندازه‌گیری و شناسایی باشد، این احتمال تقویت می‌یابد که دولت آسیب‌دیده برای جبران از کنش‌های سخت‌افزاری و حملات نظامی استفاده کند. چنین روندی، در صورتی است که دولتی بتواند پیامدهای حملات سایبری، تخریب داده‌ها، فایل‌های استخراج‌شده، تعداد

1. *Developments in the Field of Information and Telecommunications in the Context of International Security*

سرورهای آسیب‌دیده و حجم ویروس و تروژان را تعیین کند. در این راستا، حمله سایبری به معنای استفاده از زور است و ماهیت نظامی- سخت‌افزاری دارد؛ چراکه در چنین صورتی، حمله سایبری همانند یک حمله نظامی و به‌منزله استفاده از زور است. هنگامی که عملیاتی توسط ارتش یک کشور انجام شود، ویژگی نظامی خواهد داشت؛ چراکه شماری از ویژگی برخی از جنگ‌های سایبری این‌که تخریب‌هایی که به دنبال دارد، لزوماً همراه با کشتار نیست، بلکه با پیامدهای جدی برای زیرساخت‌های حیاتی یک کشور همراه است. در این راستا، تخریب زیرساخت‌های یک کشور با استفاده از ویروس‌ها یا بدافزارها، عینیت زیادی با حمله مستقیم نظامی دارد. بااین‌حال، هم‌چنان که گفته شد، شناسایی دولت متخاصم در این زمینه، امر دشواری است. علاوه بر این، فقدان مکان رخداد واقعی نیز چالش دیگری است که بازدارندگی حملات سایبری را با چالش مواجه می‌کند. بدین‌معنا که با استفاده از فنّاوری‌های پیشرفته از هر نقطه‌ای از جهان و نه لزوماً در محیط جغرافیایی کشور متخاصم، می‌توان دست به حمله سایبری زد. چنین چالش‌هایی باعث شده است تا کارایی و ضمانت اجرایی معاهدات مرتبط با بازدارندگی حملات سایبری، تقلیل یابد.

در این رابطه، مجموعه کنوانسیون‌ها و پیمان‌نامه‌های حقوقی که با هدف ایجاد بازدارندگی علیه حملات سایبری به تصویب رسیده است، نگرشی کلی و غیرشمول به این مقوله دارند. اقدامات سایبری در این کنوانسیون‌ها تحت عناوینی چون تروریسم سایبری، خرابکاری سایبری، حمله یا یورش سایبری، سوءاستفاده از حوزه فنّاوری اطلاعات و ارتباطات و نیز اقدامات مخرب در بستر اینترنت، یاد شده است. از میان کنوانسیون‌های موردبررسی، صرفاً پنج کنوانسیون به‌صورت مستقیم و تخصصی به مقوله اقدامات خرابکارانه سایبری پرداخته‌اند که عبارتند از: قطعنامهٔ ایجاد فرهنگ جهانی امنیت سایبر و حمایت از زیرساخت‌های اطلاعاتی حساس (۲۰۰٤)، قطعنامهٔ مبارزه با سوءاستفادهٔ جنایت‌کارانه از فنّاوری اطلاعات، قطعنامه ایجاد فرهنگ جهانی امنیت سایبری و تلاش‌های ملّی برای حفاظت از زیرساخت‌های اطلاعاتی حساس (۲۰۱۰ و ۲۰۲۰)، کنوانسیون اروپایی مقابله با حملات سایبری و کنوانسیون جرائم سایبری شورای اروپا. سایر کنوانسیون‌ها یا به‌صورت موردی در یکی از مفاد خود از حملات سایبری نام‌برده‌اند یا مجموعه گزاره‌های حقوقی آن‌ها به شکلی است که می‌توان از آن، استنباط بازدارندگی علیه حملات و جرائم سایبری در سطح دولت‌ها داشت. بااین‌حال، مجموعه کنوانسیون‌ها و پیمان‌نامه‌های یادشده، باآنکه احکام حقوقی مشخصی علیه دولت‌های مجری حملات سایبری و دولت‌های آسیب‌دیده از این حملات مشخص کرده است؛ اما از پیش‌بینی و تخصیص پیچیدگی‌های این نوع از حملات ناتوان مانده است. بااین‌حال، نظارت بر فضای سایبر، دشواری‌های خاص خود را دارد و به دلیل تنوع ناشی از حملات سایبری، جرم‌انگاری آن، همواره در حال تغییر و تحول است. یکی از دشواری‌های اساسی در این زمینه، عدم دسترسی و یا دشوار بودن دسترسی به مکانی است که جرم سایبری در آن رخ می‌دهد.

به‌عنوان‌مثال، یک حمله سایبری که مدعی است از سوی کشور الف انجام می‌شود، ممکن است محل قرارگرفتن حمله‌کنندگان در آن کشور نباشد؛ بنابراین هم پی‌بردن به نقش عوامل اصلی تهدیدات سایبری و هم مدون بودن یک نظام سیاسی و حقوقی برای شناسایی و مجازات تهدیدکنندگان بخش مهمی از دشواری‌های ناشی از بازدارندگی تهدیدات و حملات سایبری هستند؛ ازاین‌رو، چالش‌های زیادی در ارتباط با بازدارندگی حملات سایبری باقی مانده است.

جدول زیر (جدول ۱)، مجموعه کنوانسیون‌های موردمطالعه و آسیب‌شناسی آن‌ها در ارتباط با موضوع بازدارندگی حملات سایبری را خلاصه کرده است.

جدول ۱) آسیب‌شناسی کنوانسیون‌های مرتبط با بازدارندگی حملات سایبری

کنوانسیون	مفاد مرتبط با بازدارندگی حملات سایبری	آسیب‌شناسی
کنوانسیون جرائم سایبری شورای اروپا	ممنوعیت ایجاد اختلال در سامانه‌های رایانه‌ای و دستیابی غیرمجاز به زیرساخت‌های اطلاعاتی کشورها	در مقررات این کنوانسیون، به‌طور غیرمستقیم به موارد یورش سایبری پرداخته است و ضمانت اجرایی قوی و الزام‌آوری ندارد
کنوانسیون پیشگیری از اقدامات غیرقانونی علیه امنیت هواپیمایی کشوری	حمایت کیفری نسبت به دولت‌های آسیب‌دیده از یورش‌های تروریستی	این کنوانسیون به یورش سایبری اشاره نکرده است
کنوانسیون پیشگیری از بدافزارهای سایبری	ممنوعیت استفاده از بدافزارهای رایانه‌ای در تخریب داده‌ها و سامانه‌های رایانه‌ای و مخابراتی	با عبارات مبهم و عام‌الشمول به توصیف یورش سایبری پرداخته
کنوانسیون سرکوب حمایت مالی از یورش و تروریسم سایبری	مکلف کردن دولت‌ها برای پیشگیری و مقابله با تأمین مالی تروریسم در قالب فعالیت‌های مختلف	عدم احراز پیچیدگی‌های مرتبط با یورش‌های سایبری
قطعنامهٔ شماره ۱۳۷۳ شورای امنیت	الزام دولت‌ها به همکاری با یکدیگر برای سرکوب تروریسم، مقابله با تأمین مالی تروریسم	عدم اشاره صریح به یورش‌های سایبری و در نظر نگرفتن لایه‌های متعدد آن
یازدهمین نشست پیشگیری از جرائم و بسط عدالت کیفری سازمان ملل متحد	ممنوعیت انتشار ویروس‌های رایانه‌ای و هدف قراردادن فنّاوری‌های اطلاعاتی و ارتباطی	تمرکز روی سوءاستفاده‌های شخصی از فضای سایبر و عدم‌جامعیت حقوقی و سیاسی
کنوانسیون اروپایی مقابله با حملات سایبری	ممنوعیت انتشار ویروس‌ها، کرم‌ها، تروجان‌ها، هرزنامه‌های اینترنتی، حملات فیشینگ	عدم جرم‌انگاری صریح از اقدامات مرتبط با یورش‌های سایبری
کنوانسیون منطقه‌ای سازمان همکاری‌های منطقه‌ای آسیای جنوبی	همکاری منطقه‌ای برای مبارزه با یورش‌های تروریستی سایبری	جرم‌انگاری کنش‌های خرابکارانه‌ای که از طریق فضای سایبر صورت می‌گیرد، دیده نمی‌شود
کنوانسیون سازمان اجلاس اسلامی	حمایت کیفری از دولت‌های آسیب‌دیده از تروریسم و جرم‌انگاری افعال غیرقانونی	خلط مفهومی و مصداقی یورش تروریستی و یورش سایبری
معاهدهٔ همکاری میان دولت‌های عضو کشورهای مستقل مشترک‌المنافع در مبارزه با تروریسم	ممنوعیت و جرم‌انگاری علیه تروریسم فنّاورانه	عدم اشاره مستقیم به یورش سایبری و در نظر نگرفتن پیچیدگی‌های حقوقی-سیاسی آن
کنوانسیون سازمان وحدت آفریقا و پروتکل الحاقی سال ۲۰۰۴	مبارزه با افعال تشکیل‌دهندهٔ یورش تروریستی	عدم ذکر صریح حملات سایبری و فقدان ضمانت حقوقی و اجرایی

کنوانسیون	مفاد مرتبط با بازدارندگی حملات سایبری	آسیب‌شناسی
کنوانسیون عربی مقابله با تروریسم	حمایت کیفری از دولت‌های آسیب‌دیده از یورش تروریستی	فقدان واژه یورش سایبری، نپرداختن به مصادیق یورش تروریستی، ضعف حقوقی-اجرایی
کنوانسیون سازمان کشورهای آمریکایی برای پیشگیری و مجازات اعمال تروریستی	همکاری منطقه‌ای برای کاهش و ممنوعیت حملات تروریستی	به‌طور صریح و روشن به پیشگیری از جرائم رایانه‌ای، به‌خصوص یورش سایبری اشاره‌ای نکرده است
قطعنامه ایجاد فرهنگ جهانی امنیت سایبری و تلاش‌های ملّی برای حفاظت از زیرساخت‌های اطلاعاتی حساس	جلوگیری از افزایش رو به رشد جرائم مربوط به فنّاوری اطلاعات	تمرکز خاص روی تروریسم و فقدان اشاره به یورش سایبری
قطعنامهٔ مبارزه با سوءاستفادهٔ جنایت‌کارانه از فنّاوری اطلاعات	ابراز نگرانی از پیشرفت فنّاوری‌های جدید و فعالیت‌های مجرمانهٔ جدید	این قطعنامه درباره دولت‌های آسیب‌دیده از یورش سایبری، عنوانی به میان نیاورده است
قطعنامهٔ ایجاد فرهنگ جهانی امنیت سایبر و حمایت از زیرساخت‌های اطلاعاتی حساس	حفاظت از زیرساخت‌های حساس با توجه به قوانین ملّی و بین‌المللی	فقدان ذکر جزئیات و مصادیق، فقدان ضمانت حقوقی و اجرایی
کنوانسیون بین‌المللی حقوق مدنی و سیاسی	حمایت از قربانیان تخلف از حقوق بشر	عدم اشاره به مصادیق و جزئیات حملات سایبری
قطعنامهٔ حمایت از قربانیان تخلفات فاحش بین‌المللی	شناسایی حقوق دولت‌های آسیب‌دیده	فقدان حمایت از دولت‌های آسیب‌دیده از حملات سایبری
نشست هفتم سازمان ملل متحد	حمایت از حقوق افراد و دولت‌های آسیب‌دیده از جرائم رایانه‌ای	به رسمیت نشناختن حقوق افراد و حقوق دولت‌های آسیب‌دیده از حملات سایبری
نشست هشتم سازمان ملل متحد	حمایت از دولت‌های آسیب‌دیده بر اساس اعلامیهٔ اصول بنیادی عدالت	حمایت کیفری از دولت‌های آسیب‌دیده از یورش تروریستی (و نه لزوماً سایبری)
نشست دهم سازمان ملل متحد	محکومیت افعال غیرقانونی، مانند یورش تروریستی	گزارش توصیفی محض از تلاش‌های صورت گرفته در مبارزه با جرائم رایانه‌ای در کشورها و سازمان‌های بین‌المللی
کنوانسیون سازمان ملل متحد درباره عدالت و پشتیبانی از قربانیان سوءاستفاده از قدرت	حمایت از دولت‌های آسیب‌دیده ناشی از حملات تروریستی	نمی‌توان به شمولیت دولت‌های آسیب‌دیده از یورش سایبری در این کنوانسیون استناد کرد

در راستای افزایش بازدارندگی حملات سایبری، موارد زیر پیشنهاد می‌شود:

– افزایش الزام حقوقی و ضمانت اجرایی در معاهدات و کنوانسیون‌های مربوطه

– قراردادن موضوع بازدارندگی حملات سایبری در سازوکار سازمان‌ها و ائتلاف‌های منطقه‌ای و به‌ویژه در حوزه امنیت جمعی

– افزایش ضریب آزادی نقل‌وانتقال اطلاعات میان کشورهای عضو پیمان‌های منطقه‌ای به‌منظور ایجاد شفافیت اطلاعات و پیشگیری از حملات سایبری در حوزه اطلاعات راهبردی

– بالابردن هزینه‌های ناشی از حملات سایبری با تعیین مجازات و تحریم‌های دارای پشتوانه شورای امنیت سازمان ملل

– حمایت مادی و لجستیکی از کشورهای آسیب‌دیده در حملات سایبری و تقویت زیرساخت‌های دفع و مقابله با این حملات

منابع

- احمری، حسین، کحلکی، غلامرضا، رحیم‌پور اصفهانی، حامد (۱۳۹۵)، **تحلیل سازه‌انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن**، پژوهش‌های روابط بین‌الملل، سال نوزدهم، شماره ۶، صص ۳۳-۳۰۵.
- اسکندری، حمید (۱۳۹۳)، **دفاع سایبری: کلیات امنیت در فنّاوری اطلاعات**، تهران: بوستان حمید.
- آقابابایان، حمیدرضا، مرادی، مریم، میرعباسی، سیدباقر (۱۴۰۱)، **تبیین وضعیت دولت‌های کنشگر نسبت به حمله سایبری**، فصلنامه مطالعات فقه اقتصادی، سال نهم، شماره ۳، صص ۳۲۵-۳۴۳.
- باستانی، برومند (۱۳۹۷). **جرائم کامپیوتری و سایبری جلوه‌ای نوین از بزهکاری**. تهران: بهنامی.
- جلالی فراهانی، امیرحسین (۱۳۹۸)، **کنوانسیون جرائم سایبر و پروتکل الحاقی آن (به همراه گزارش‌های توجیهی آن‌ها)**، تهران: خرسندی
- حسن‌بیگی، ابراهیم (۱۳۹۴)، **حقوق و امنیت در فضای سایبر**، تهران: مؤسسه فرهنگی مطالعات و پژوهش‌های بین‌المللی ابرار معاصر تهران.
- رستمی‌فر، علی (۱۴۰۲)، **فضای مجازی و چالش‌های حقوق بین‌الملل در مواجهه با حملات سایبری**، فصلنامه سیاست و روابط بین‌الملل، دوره ۶، شماره ۱۱، صص ۷۴-۵۵.
- فرشاسعید، پرویز، جلالی محمود (۱۴۰۱)، **مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری عوامل غیردولتی**، فصلنامه حقوق فنّاوری‌های نوین، سال ششم، شماره ۳، صص ۱۸۴-۱۷۳.
- کلاریک، اندرو. ام و یانچوسکی، لخ (۱۳۹۸)، **مقدمه‌ای بر جنگ سایبر و تروریسم سایبر**، ترجمه ابراهیم نژاد سلمانی، تهران: بوستان حمید
- ماه‌پیشانیان، مهسا (۱۳۹۰)، **فضای سایبر و شیوه‌های نوین درگیری ایالات‌متحدهٔ آمریکا با جمهوری اسلامی ایران**، پژوهش‌نامه فرهنگی، سال ۱۲، شمارهٔ ۱۳، صص ۱۲۱-۹۶.
- نامدار، سعید، قاسمی، غلامعلی (۱۳۹۷)، **بررسی مفهوم دفاع مشروع در پرتو حملات سایبری (با تأکید بر حمله استاکس‌نت به تأسیسات هسته‌ای ایران)**، فصلنامه مطالعات حقوقی، سال دهم، شماره ۱، صص ۲۳۵-۱۹۹.
- *Al-Turjman, F. and Salama, R. (2020). "An Overview about the Cyberattacks in Grid and Like Systems". Smart Grid in IoT-Enabled Spaces. CRC Press.*
- *Aravindakshan, S. (2021). "Cyberattacks: a look at evidentiary thresholds in International Law". Indian Journal of International Law. 59 (1–4): 285–299*
- *Colarik, A.M. (2016). Cyber terrorism political and economic implication, Massachusetts, United States: Idea Group Pub.*
- *Hearn, K (2021). International Relations and Cyber Attacks: Official and Unofficial Discourse, School of Computer and Information Science, Edith Cowan University,*

Perth, Western Australia.

- *Lehto, M. (2022). "Cyber-Attacks Against Critical Infrastructure". Cyber Security: Critical Infrastructure Protection. Springer International Publishing.*
- *Li, Y. and Liu, Q. (2021). "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments". Energy Reports. 7(4): 817–826*
- *Lilienthal, G. and Nehaluddin, A. (2023). "Cyber-attack as inevitable kinetic war". Computer Law & Security Review. 31(3): 390–400*
- *Makridis, C.A. (2021). "Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018". Journal of Cybersecurity. 7(1): 69-79.*
- *Oppenheimer, H. (2024). "How the process of discovering cyberattacks biases our understanding of cybersecurity". Journal of Peace Research. 61(1): 28–43.*
- *Valeriano, B. and Maness, R.C. (2023). International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain, The Oxford Handbook of International Political Theory, 259–272.*
- *Van der Meer, S. (2017). Deterrence of Cyber-Attacks in International Relations: denial, retaliation and signaling, International Affairs Forum, 6(3): 85-90.*