فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

حمله سایبری و دفاع مشروع در حقوق بین‌الملل: مطالعه موردی تقابل سایبری ایران و رژیم صهیونیستی

علیرضا انصاری مهیاری[۱]،بهنازجهانبازی گوجانی[۲]

چکیده

حملات سایبری به‌عنوان یکی از مهم‌ترین چالش‌های حقوق بین‌الملل معاصر، مبانی سنتی توسل به زور و دفاع مشروع را با دشواری‌های بی‌سابقه‌ای مواجه ساخته است. تقابل سایبری میان جمهوری اسلامی ایران و رژیم صهیونیستی در بازه زمانی ۲۰۱۰ تا ۲۰۲۵، نمونه‌ای بارز از این چالش‌ها را به تصویر کشیده است. این مقاله با رویکردی تحلیلی–حقوقی به بررسی این پرسش اساسی می‌پردازد که حملات سایبری در چه شرایطی می‌توانند مصداق «توسل به زور» یا «حمله مسلحانه» محسوب شوند و دولت قربانی تا چه حد می‌تواند به دفاع مشروع متوسل شود. رشد فزاینده تکنولوژی در حوزه اطلاعات و ارتباطات، تهدیدهایی نیز به دنبال داشته است که حمله سایبری نمونه بارز چنین تهدیدی محسوب می‌گردد. بدافزار استاکس‌نت که در سال ۲۰۱۰ تأسیسات هسته‌ای ایران را هدف قرار داد، نقطه عطفی در این بحث محسوب می‌شود و بسیاری از حقوقدانان آن را با یک حمله مسلحانه قابل مقایسه دانسته‌اند. یافته‌های پژوهش نشان می‌دهد که با وجود خلأ هنجاری موجود و عدم اجماع بر سر تعریف حمله سایبری، حملات سایبری با آثار مخرب فیزیکی می‌توانند در چارچوب ماده ۲ بند ٤ و ماده ۵۱ منشور ملل متحد تحلیل شوند و دولت قربانی در صورت احراز شرایط ضرورت و تناسب، حق دفاع مشروع دارد. با این حال، چالش‌های انتساب و فقدان رویه قضایی مشخص، کاربست این قواعد را با دشواری مواجه ساخته است.

واژگان کلیدی: حمله سایبری، دفاع مشروع، توسل به زور، استاکس‌نت، مسئولیت بین‌المللی دولت‌ها.

[۱] استادیارگروه حقوق،واحدنجف آباد،دانشگاه آزاد اسلامی،نجف آباد،ایران.
[۲] دانشجوی دکتری حقوق بین الملل، واحد نجف آباد، دانشگاه ازاد اسلامی، نجف آباد، ایران. behnaz.jahanbazi@iau.ac.ir

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

مقدمه

فضای سایبر در دهه‌های اخیر به عرصه‌ای حیاتی برای رقابت‌های ژئوپلیتیکی و منازعات بین‌المللی تبدیل شده است. حمله سایبری، مصداق سلاح جدیدی است که می‌تواند روش هدایت جنگ مدرن توسط بازیگران دولتی و غیر دولتی را دگرگون سازد. سرشت بی‌مانند این تهدید و توانمندی مرتکبان جنگ‌های سایبری در آسیب‌رساندن، کشتار و تخریب فیزیکی از طریق فضای سایبر، تعاریف سنتی توسل به زور را متحول ساخته است (بشیری، ۱۳۹٤: ۱). حملات سایبری از معضلات نوین حقوق بین‌الملل محسوب می‌شود که نسبت به آن‌ها هیچ گونه قاعده‌ای در سطح بین‌المللی وضع نگردیده است، اما با بررسی این حملات بر اساس چهارچوب‌های سنتی حقوق بین‌الملل می‌توان این گونه نتیجه گرفت که سطح قابل‌توجهی از این حملات موجب نقض اصل عدم توسل به زور، اصل عدم مداخله و اصل برابری دولت‌ها بوده است (بشیری، ۱۳۹٤: ۱).

مهم‌ترین چالش فراروی این موضوع، مسئله مفهوم‌شناسی و تعریف حمله سایبری و لزوم تبیین و تعیین دایره مفهومی این پدیده است که در میان رویه رسمی کشورها و سازمان‌های بین‌المللی به شدت اختلافی است، به طوری که تاکنون هیچ‌گونه اجماعی در خصوص تعریف حمله سایبری حاصل نشده است (اصلانی و رنجبریان، ۱۳۹٤: ۲۵۸). جنگ‌های سایبری چالش‌ها و راهکارهای تعامل در پرتو مقررات توسل به زور را با دشواری مواجه ساخته است؛ به‌گونه‌ای که اصول سنتی منشور ملل متحد در مواجهه و تطبیق با تحولات معاصر جامعه بین‌الملل از جمله پیدایش پدیده نوظهور فضای سایبری ناتوان است (امیری و حیدری‌فرد، ۱۳۹۷: ۱۵۵). فضای سایبر شبکه‌ای به هم پیوسته از زیرساخت‌های فن‌آوری اطلاعات، اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای، کنترل‌کننده‌ها، پردازشگرها، کابل‌های فیبر نوری و مسیریاب‌ها است که عملکرد اکثر سازوکارهای اقتصادی جوامع امروزی را به خود متکی ساخته و از طرف دیگر، امکان مورد هدف قرار گرفتن آنها در قالب حملات و عملیات سایبری هشداربرانگیز است (امیری و حیدری‌فرد، ۱۳۹۷: ۱۵٦).

یکی از مهم‌ترین نمونه‌های تقابل سایبری در عرصه بین‌الملل، رویارویی میان جمهوری اسلامی ایران و رژیم صهیونیستی است. این تقابل که با حملات سایبری به تأسیسات هسته‌ای ایران از طریق بدافزار استاکس‌نت در سال ۲۰۱۰ آغاز شد، تاکنون با شدت‌های مختلف ادامه یافته است. دامنه یک جنگ سایبری می‌تواند از خشونت‌های شبکه‌ای ظاهرا بی‌ضرر تا حملات شدید به زیرساخت‌های زیربنایی در نوسان باشد (امیری و حیدری‌فرد، ۱۳۹۷: ۱۵۷). با این حال، در حالی که بیشتر نگرانی کشورها در برخورد با این پدیده بعد حفاظتی امنیتی داشته و تاکید آنها حفاظت از زیرساخت‌های رایانه‌ای در برابر فیلترینگ، ایجاد اختلال و آسیب به آنها بوده، چالش‌های حقوقی این حوزه و نحوه اعمال و تفسیر قواعد حقوق جنگ به ویژه مقررات توسل به زور با توجه به ویژگی‌های ذاتی

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

فضای سایبری کمتر بدان پرداخته شده و قابلیت اعمال مقررات مذکور در فضای مجازی در هاله‌ای از ابهام قرار دارد (امیری و حیدری‌فرد، ۱۳۹۷: ۱۵۸).

افزایش روزافزون سطح اتکای عملکرد بسیاری از زیرساخت‌های شهری به فضای مجازی، هشدارها نسبت به آسیب‌پذیری آنها را به دنبال داشته است (حیدری‌فرد، ۱٤۰۰: ۱٥٦). بخصوص وقتی که بدانیم ترتیبات قراردادی این حوزه حقوقی (کنوانسیون‌های چهارگانه ژنو و پروتکل‌های الحاقی اول و دوم ۱۹۷۷) بر مبنای شرایط عینی بروز جنگ‌های کلاسیک تدوین شده‌اند و تفاوت‌های ماهوی آن با نبرد سایبری، همچنین پیوندهای درون شبکه‌ای فضای سایبری، طبیعتاً چالش‌های اساسی در اعمال قواعد هدایت مخاصمات در این عرصه را باعث می‌گردد (حیدری‌فرد، ۱٤۰۰: ۱۵۷).

ساختار مقاله بدین گونه است که در بخش نخست به بررسی اصل ممنوعیت توسل به زور و جایگاه حملات سایبری در این چارچوب پرداخته می‌شود و چالش تعریف حمله سایبری و ضرورت ارائه معیارهای روشن مورد تحلیل قرار می‌گیرد. در بخش دوم، مفهوم دفاع مشروع در برابر حملات سایبری و شرایط تحقق آن با تأکید بر معیارهای «حمله مسلحانه»، «ضرورت» و «تناسب» تحلیل می‌گردد و نقش رویه قضایی بین‌المللی در این زمینه بررسی می‌شود. در بخش سوم، چالش‌های انتساب و مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری با تأکید بر معیارهای کنترل مؤثر و کنترل کلی و نیز اصل مراقبت بایسته مورد بررسی قرار می‌گیرد و در بخش چهارم، مطالعه موردی استاکس‌نت و تقابل سایبری ایران و رژیم صهیونیستی به‌عنوان نقطه عطف این رویارویی تحلیل می‌شود.

۱- اصل ممنوعیت توسل به زور و جایگاه حملات سایبری

۱-۱.ماده ۲ بند ٤ منشور ملل متحد و حملات سایبری

اصل ممنوعیت توسل به زور که در ماده ۲ بند ٤ منشور ملل متحد تجلی یافته است، به‌عنوان یکی از بنیادین‌ترین قواعد آمره حقوق بین‌الملل شناخته می‌شود. این ماده مقرر می‌دارد که «کلیه اعضا در روابط بین‌المللی خود از تهدید به زور یا استفاده از زور، علیه تمامیت ارضی یا استقلال سیاسی هر کشوری خودداری می‌نمایند.» منشور سازمان ملل متحد تمامی اعضای جامعه بین‌المللی را از تهدید یا توسل به زور علیه تمامیت ارضی یا استقلال اقتصادی سایر کشورها، یا هر اقدامی که در تعارض با اهداف ملل متحد باشد، نهی نموده است (امیری و حیدری‌فرد، ۱۳۹۷: ۱۵۵). با این حال، اصولی مثل اصل توسل به دفاع مشروع و یا توسل کشورها به مکانیزم تامین امنیت دسته جمعی در مقابل کشور خاطی، به عنوان استثنای این اصل، در قالب ماده حقوقی دیگری در منشور مورد تاکید قرار گرفته است (امیری و حیدری‌فرد، ۱۳۹۷: ۱۵۵).

پرسش اساسی آن است که آیا حملات سایبری نیز در شمول این قاعده قرار می‌گیرند؟ پاسخ به این پرسش، مستلزم بررسی این موضوع است که آیا حملات سایبری می‌توانند مصداق «توسل به زور» محسوب شوند. با توجه

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

به اینکه منشور ملل متحد در سال ۱۹٤٥ و پیش از ظهور فضای سایبر تدوین شده است، تفسیر این ماده در مورد حملات سایبری همواره محل اختلاف بوده است. به‌نظر می‌رسد که حملات سایبری می‌تواند مصداق توسل به زور در قالب ماده ۲ بند ٤ منشور ملل متحد باشند و بر اساس آن دولت‌های قربانی این حملات حق خواهند داشت که به اقدام‌هایی چون دفاع مشروع، دفاع پیش‌دستانه و اقدام متقابل متوسل شوند (بشیری، ۱۳۹٤: ۱).

چالش اصلی در این زمینه، تعیین معیارهای تشخیص یک حمله سایبری به‌عنوان «توسل به زور» است. مهم‌ترین چالش فراروی این موضوع، مسئله مفهوم‌شناسی و تعریف حمله سایبری و لزوم تبیین و تعیین دایره مفهومی این پدیده است که در میان رویه رسمی کشورها و سازمان‌های بین‌المللی به شدت اختلافی است (اصلانی و رنجبریان، ۱۳۹٤: ۲۵۸). فقدان چنین اجماع حقوقی در حقوق بین‌الملل به عنوان یک چالش جدی قلمداد شده است (اصلانی و رنجبریان، ۱۳۹٤: ۲۷۸). برخی از کشورها، حمله سایبری را در چارچوب عملیات اطلاعاتی و برخی دیگر به‌عنوان یک اقدام نظامی تلقی می‌کنند و این اختلاف نظر، کاربست قواعد حقوق بین‌الملل را با دشواری مواجه ساخته است.

۱-۲.چالش تعریف و ضرورت ارائه معیارهای روشن

همان‌گونه که اشاره شد، یکی از موانع اساسی در کاربست قواعد حقوق بین‌الملل بر حملات سایبری، عدم اجماع بر سر تعریف این پدیده است. اصلانی و رنجبریان در پژوهش تطبیقی خود به این نکته اشاره کرده‌اند که تعاریف ارائه‌شده از حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل، تفاوت‌های قابل‌توجهی با یکدیگر دارند و این امر، فرآیند تشخیص مصداق حمله سایبری را با دشواری مواجه می‌سازد (اصلانی و رنجبریان، ۱۳۹٤: ۲٦۰). به‌عنوان مثال، برخی از تعاریف بر جنبه «تخریب فیزیکی» تأکید دارند، در حالی که برخی دیگر «اخلال در عملکرد سیستم‌ها» را نیز در شمول تعریف قرار می‌دهند.

با توجه به این خلأ هنجاری، ضرورت ارائه معیارهای روشن برای تشخیص حمله سایبری به‌عنوان «توسل به زور» بیش از پیش احساس می‌شود. دیوان بین‌المللی دادگستری در قضیه سکوهای نفتی (۲۰۰۳)، بر این نکته تأکید کرد که برای احراز «حمله مسلحانه»، باید شدت و آثار حمله به سطحی برسد که آن را از سایر اشکال توسل به زور متمایز سازد .(ICJ, ۲۰۰۳: para. ٥١) همچنین، در دستورالعمل تالین تلاش شده است تا با ارائه معیارهایی مانند «شدت»، «آثار فوری»، «نفوذ نظامی» و «ماهیت ابزارهای به‌کاررفته»، به این ابهام پاسخ داده شود (Schmitt, ۲۰۱۳: ٤٥). با این حال، این دستورالعمل از اعتبار حقوقی الزام‌آور برخوردار نیست و صرفاً به‌عنوان یک منبع دکترینال قابل استناد است.

افزایش روزافزون سطح اتکای عملکرد بسیاری از زیرساخت‌های شهری به فضای مجازی، هشدارها نسبت به آسیب‌پذیری آنها را به دنبال داشته است (حیدری‌فرد، ۱٤۰۰: ۱٥٦). بخصوص وقتی که بدانیم ترتیبات قراردادی این حوزه حقوقی بر مبنای شرایط عینی بروز جنگ‌های کلاسیک تدوین شده‌اند و تفاوت‌های ماهوی آن با نبرد

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

سایبری، طبیعتاً چالش‌های اساسی در اعمال قواعد هدایت مخاصمات در این عرصه را باعث می‌گردد (حیدری‌فرد، ۱٤۰۰: ۱۵۷). با توجه به گسترش جنگ ترکیبی در منازعات معاصر، ضرورت تدوین قواعد روشن‌تر در این زمینه بیش از پیش احساس می‌شود تا «منطقه خاکستری» حقوقی به حداقل ممکن کاهش یابد.

۱-۳.حملات سایبری به‌عنوان نقض اصل عدم مداخله

علاوه بر اصل ممنوعیت توسل به زور، حملات سایبری می‌توانند ناقض اصل عدم مداخله در امور داخلی دولت‌ها نیز باشند. اصل عدم مداخله که در ماده ۲ بند ۷ منشور ملل متحد و نیز قطعنامه ۲٦۲۵ مجمع عمومی سازمان ملل به رسمیت شناخته شده است، دولت‌ها را از دخالت در امور داخلی یکدیگر منع می‌کند (ضیایی بیگدلی، ۱۳۸٤: ۲۲۰). حملات سایبری که با هدف نفوذ در سیستم‌های اطلاعاتی، اختلال در فرآیندهای انتخاباتی یا تأثیرگذاری بر افکار عمومی انجام می‌شوند، می‌توانند مصداق مداخله در امور داخلی دولت‌ها محسوب گردند.

در مورد حملات سایبری، تعیین اینکه یک حمله در چه سطحی از «مداخله» فراتر رفته و به «توسل به زور» تبدیل می‌شود، همواره محل اختلاف بوده است. برخی از صاحبنظران بر این باورند که حملات سایبری با آثار مخرب فیزیکی مانند استاکس‌نت، به‌وضوح مصداق توسل به زور هستند، در حالی که حملات سایبری با هدف جاسوسی یا اختلال موقت در خدمات، ممکن است در سطح مداخله باقی بمانند. این تمایز، هرچند از منظر نظری قابل توجیه است، اما در عمل با دشواری‌های فراوانی مواجه است، زیرا تشخیص دقیق مرز میان مداخله و توسل به زور در فضای سایبر، به دلیل پیچیدگی و ناملموس بودن آثار حملات، بسیار دشوار است.

همچنین، حملات سایبری می‌توانند ناقض اصل برابری دولت‌ها نیز باشند، به‌ویژه در مواردی که دولت‌های قدرتمند از قابلیت‌های سایبری پیشرفته خود برای اعمال فشار بر دولت‌های ضعیف‌تر استفاده می‌کنند. این موضوع، به‌ویژه در تقابل سایبری ایران و رژیم صهیونیستی که با عدم تقارن قابل‌توجهی در قابلیت‌های سایبری همراه است، از اهمیت ویژه‌ای برخوردار است. اصل برابری دولت‌ها که در ماده ۲ بند ۱ منشور ملل متحد به رسمیت شناخته شده است، دولت‌ها را از بهره‌گیری از برتری‌های فنی یا اقتصادی خود برای اعمال نفوذ بر دولت‌های دیگر منع می‌کند (ضیایی بیگدلی، ۱۳۸٤: ۱۵۰).

۲- دفاع مشروع در برابر حملات سایبری

۱.۲-ماده ۵۱ منشور ملل متحد و حملات سایبری

ماده ۵۱ منشور ملل متحد، «حق ذاتی دفاع مشروع فردی یا جمعی را در صورت وقوع حمله مسلحانه» به رسمیت می‌شناسد. بر اساس این ماده، دولت‌ها می‌توانند در برابر حملات مسلحانه، به اقدامات دفاعی متوسل شوند، مشروط بر اینکه این اقدامات فوری، ضروری و متناسب باشند و بلافاصله به شورای امنیت گزارش داده شوند. پرسش کلیدی آن است که آیا حملات سایبری نیز می‌توانند «حمله مسلحانه» محسوب شوند و در نتیجه، دولت قربانی از حق دفاع مشروع برخوردار باشد (حلمی، ۱۳۸۷: ۱۸۰)؟

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

پاسخ به این پرسش، مستلزم تفسیر مفهوم «حمله مسلحانه» در پرتو تحولات فناورانه معاصر است. دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه (۱۹۸٦)، «حمله مسلحانه» را به «شدیدترین شکل توسل به زور» محدود کرده است و آن را از سایر اشکال توسل به زور که ممکن است مصداق «مداخله» یا «تجاوز» باشند، متمایز ساخته است (ICJ, ۱۹۸٦: para. ۱۹۵).دیوان در این پرونده اعلام داشت که کمک‌رسانی به شورشیان، حتی اگر شامل تأمین سلاح و تجهیزات باشد، به‌تنهایی مصداق «حمله مسلحانه» محسوب نمی‌شود، مگر اینکه به سطحی از شدت برسد که با یک حمله نظامی سنتی قابل مقایسه باشد (راعی، ۱۳۸۸: ۱۵٤). با این حال، دیوان در آن زمان، حملات سایبری را مورد بررسی قرار نداده است و لذا، تعیین اینکه یک حمله سایبری در چه سطحی به «حمله مسلحانه» تبدیل می‌شود، همچنان محل اختلاف است.

برخی از حقوقدانان بر این باورند که حملات سایبری در صورتی که منجر به تلفات جانی، خسارات فیزیکی گسترده یا اختلال جدی در عملکرد دولت شوند، می‌توانند مصداق «حمله مسلحانه» تلقی شوند. این دیدگاه با معیارهای ارائه‌شده در دستورالعمل تالین نیز همخوانی دارد که بر «شدت» و «آثار» حملات سایبری تأکید می‌کند (Schmitt, ۲۰۱۳: ۵۸).در مقابل، گروهی دیگر معتقدند که برای احراز «حمله مسلحانه»، حمله باید دارای آثار قابل‌مقایسه با حملات نظامی سنتی باشد و صرف اختلال در عملکرد سیستم‌ها، کافی نیست. دیوان بین‌المللی دادگستری در قضیه سکوهای نفتی (۲۰۰۳)، بر این نکته تأکید کرد که برای احراز «حمله مسلحانه»، باید شدت و آثار حمله به سطحی برسد که آن را از سایر اشکال توسل به زور متمایز سازد.(ICJ, ۲۰۰۳: para. ۵۱)

با توجه به عدم اجماع بر سر این موضوع، دولت‌ها در عمل، رویکردهای متفاوتی را در پیش گرفته‌اند. برخی از دولت‌ها مانند ایالات متحده، با اتخاذ موضعی گسترده‌تر، حملات سایبری با آثار مخرب قابل‌توجه را مشمول حق دفاع مشروع دانسته‌اند، در حالی که برخی دیگر مانند روسیه و چین، رویکردی محدودتر را اتخاذ کرده و بر لزوم احراز آثار قابل‌مقایسه با حملات نظامی سنتی تأکید کرده‌اند. این اختلاف نظر، نشان‌دهنده خلأ هنجاری در حقوق بین‌الملل و ضرورت تدوین قواعد روشن‌تر در این زمینه است.

۲-۲.شرایط تحقق دفاع مشروع در برابر حملات سایبری

برای تحقق دفاع مشروع در برابر حملات سایبری، احراز سه شرط اساسی ضروری است: «وقوع حمله مسلحانه»، «ضرورت» و «تناسب». شرط نخست، همان‌گونه که در بخش پیشین بررسی شد، به تعیین اینکه آیا یک حمله سایبری مصداق «حمله مسلحانه» است یا خیر، مربوط می‌شود. این شرط، پیش‌شرط اساسی برای توسل به دفاع مشروع محسوب می‌شود و در صورت عدم احراز آن، توسل به زور فاقد مشروعیت خواهد بود. دیوان بین‌المللی دادگستری در قضیه فعالیت‌های نظامی و شبه‌نظامی در نیکاراگوئه، بر این نکته تأکید کرد که برای تحقق دفاع مشروع، ابتدا باید وقوع «حمله مسلحانه» احراز شود و صرف «تهدید» یا «خطر قریب‌الوقوع» کافی نیست (ICJ, ۱۹۸٦: □□□□. ۱۹۵).

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

شرط دوم، «ضرورت» است که به معنای آن است که دولت قربانی باید قبل از توسل به زور، راه‌های مسالمت‌آمیز حل‌وفصل اختلاف را امتحان کرده باشد و هیچ راه دیگری برای دفع حمله وجود نداشته باشد. در حملات سایبری، احراز این شرط با دشواری مواجه است، زیرا دولت قربانی ممکن است نتواند به‌سرعت مبدأ حمله را شناسایی کند و یا ممکن است راه‌های مسالمت‌آمیز مانند شکایت به شورای امنیت، کارایی لازم را نداشته باشند. با این حال، دولت قربانی موظف است قبل از توسل به دفاع مشروع، تمامی راه‌های مسالمت‌آمیز را امتحان کند و صرفاً در صورت عدم موفقیت، به زور متوسل شود. دیوان بین‌المللی دادگستری در قضیه قانونی بودن تهدید یا استفاده از سلاح‌های هسته‌ای (۱۹۹٦)، بر لزوم رعایت شرط ضرورت در اقدامات دفاعی تأکید کرد و اعلام داشت که اقدام دفاعی تنها در صورتی مشروع است که هیچ راه دیگری برای دفع حمله وجود نداشته باشد (ICJ, ۱۹۹٦: para. ٤٢).

شرط سوم، «تناسب» است که به معنای آن است که اقدام دفاعی باید متناسب با حمله باشد و از آن فراتر نرود. تعیین تناسب در حملات سایبری، به دلیل پیچیدگی و ناملموس بودن خسارت‌های سایبری، بسیار دشوار است. دیوان بین‌المللی دادگستری در قضیه سکوهای نفتی، بر لزوم رعایت تناسب در اقدامات دفاعی تأکید کرد و اعلام داشت که اقدام دفاعی نباید از آنچه برای دفع حمله ضروری است، فراتر رود (ICJ, ۲۰۰۳: para. ۷۷). در مورد حملات سایبری، تعیین تناسب مستلزم ارزیابی دقیق از شدت حمله و خسارت‌های واردشده است و این ارزیابی، به دلیل ماهیت ناملموس بسیاری از خسارت‌های سایبری، با دشواری‌های فراوانی مواجه است.

۲-۳.نقش رویه قضایی بین‌المللی

رویه قضایی بین‌المللی، نقش مهمی در شکل‌دهی به معیارهای دفاع مشروع در برابر حملات سایبری ایفا کرده است. دیوان بین‌المللی دادگستری به‌عنوان عالی‌ترین مرجع قضایی سازمان ملل، در موارد متعددی به بررسی ابعاد مختلف دفاع مشروع پرداخته و معیارهای روشنی را برای احراز شرایط آن ارائه کرده است. با این حال، تاکنون هیچ پرونده‌ای به دیوان ارائه نشده است که در آن، حملات سایبری به‌عنوان موضوع اصلی مورد بررسی قرار گرفته باشند و این امر، خلأ قابل‌توجهی در رویه قضایی بین‌المللی ایجاد کرده است.

با وجود این خلأ، می‌توان از اصول کلی مستخرج از رویه دیوان در سایر پرونده‌ها برای تحلیل حملات سایبری بهره گرفت. به‌عنوان مثال، رأی دیوان در پرونده نیکاراگوئه، معیارهای روشنی برای تشخیص «حمله مسلحانه» از سایر اشکال توسل به زور ارائه کرده است که می‌تواند در مورد حملات سایبری نیز قابل اعمال باشد (ICJ, ۱۹۸٦: □□□□. ۱۹۵). همچنین، رأی دیوان در قضیه دیوار حائل (۲۰۰٤) بر لزوم رعایت شرایط ضرورت و تناسب در اقدامات دفاعی تأکید کرده است که این اصول در مورد حملات سایبری نیز کاربرد دارند (ICJ, ۲۰۰٤: para. ۱٤۱). در قضیه سکوهای نفتی نیز، دیوان به بررسی حدود و ثغور دفاع مشروع در شرایطی پرداخت که حمله مسلحانه به‌وضوح قابل تشخیص نبود و این رأی می‌تواند برای حملات سایبری که تشخیص آنها به‌عنوان حمله مسلحانه دشوار است، راهگشا باشد.(ICJ, ۲۰۰۳: para. ٥١)

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

علاوه بر دیوان بین‌المللی دادگستری، سایر مراجع قضایی و داوری بین‌المللی نیز به‌نوعی به موضوع حملات سایبری و دفاع مشروع پرداخته‌اند. دادگاه کیفری بین‌المللی برای یوگسلاوی سابق در پرونده تادیچ، معیار «کنترل کلی» را برای انتساب رفتار گروه‌های غیردولتی به دولت‌ها ارائه کرد که این معیار می‌تواند در حملات سایبری توسط گروه‌های نیابتی نیز قابل استناد باشد (راعی، ۱۳۸۸: ۱۵۸). با این حال، این معیار با انتقاد دیوان بین‌المللی دادگستری مواجه شده است و لذا، اعتبار حقوقی آن با تردید مواجه است .(ICJ, ۲۰۰۷: para. ٤٠٣) این اختلاف رویه، نشان‌دهنده عدم اجماع در جامعه بین‌الملل بر سر معیارهای انتساب است و این ابهام، یکی از چالش‌های اساسی در حوزه حملات سایبری محسوب می‌شود.

۳- چالش‌های انتساب و مسئولیت بین‌المللی دولت‌ها

۳-۱.انتساب حملات سایبری به دولت‌ها

یکی از مهم‌ترین چالش‌های حقوقی در زمینه حملات سایبری، مسئله «انتساب» است. برای تحقق مسئولیت بین‌المللی یک دولت در قبال یک حمله سایبری، باید اثبات شود که آن حمله قابل انتساب به آن دولت است. با این حال، ویژگی‌های خاص فضای سایبر مانند ناشناس بودن، قابلیت جعل و سرعت و پیچیدگی حملات، فرآیند انتساب را با دشواری‌های بی‌سابقه‌ای مواجه ساخته است (قرشی سروندانی، ۱۳۹۱: ٤٥). مهاجمان سایبری می‌توانند با استفاده از ابزارهایی مانند پروکسی، شبکه‌های Tor و سرورهای زنجیره‌ای، هویت واقعی خود را پنهان کنند و یا آثاری از خود بر جای بگذارند که به دولت دیگری نسبت داده شود.

طرح مواد راجع به مسئولیت دولت‌ها (ARSIWA) که توسط کمیسیون حقوق بین‌الملل تدوین شده است، معیارهای اصلی انتساب رفتار به دولت را تعیین می‌کند. ماده ۸ این طرح مقرر می‌دارد که رفتار یک شخص یا گروه از اشخاص، در صورتی به‌عنوان رفتار یک دولت تلقی می‌شود که آن شخص یا گروه در واقع بر اساس دستورات یا به هدایت یا تحت کنترل آن دولت عمل کند .(ILC, ۲۰۰۱: Art. ۸) ماده ۱۱ نیز به موضوع پذیرش و تأیید رفتار توسط دولت می‌پردازد و مقرر می‌دارد که رفتاری که به موجب مواد ٤ تا ۱۰ قابل انتساب نیست، در صورتی به دولت قابل انتساب خواهد بود که آن دولت، آن رفتار را به‌عنوان رفتار خود تأیید و پذیرش کند (ILC, ۲۰۰۱: □□□. ۱۱). این ماده می‌تولند در مواردی که دولتی پس از وقوع یک حمله سایبری توسط یک گروه غیردولتی، از آن حمایت یا آن را تأیید کند، مبنای مسئولیت قرار گیرد، هرچند اثبات این تأیید نیز در عمل با دشواری‌هایی مواجه است (نصیری محلاتی، ۱۳۸۹: ٦٠).

در تقابل سایبری ایران و رژیم صهیونیستی، هر دو طرف متهم به استفاده از گروه‌های نیابتی برای انجام عملیات‌های سایبری هستند. ایران به حمایت از گروه‌های هکری مانند APT۳٥ و Black Shadow متهم است، در حالی که رژیم صهیونیستی به همکاری با شرکت‌های امنیتی خصوصی برای انجام عملیات‌های سایبری متهم شده است. این موضوع، چالش‌های حقوقی قابل‌توجهی را در زمینه انتساب و اثبات مسئولیت دولت‌ها ایجاد کرده است.

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

اثبات انتساب در فضای سایبر با دشواری‌های متعددی مواجه است که از جمله آنها می‌توان به ناشناس بودن فضای سایبر، قابلیت جعل و سرعت و پیچیدگی حملات اشاره کرد (کولین، ۲۰۱۳: ٦٥). با توجه به این موانع، برخی از صاحبنظران بر این باورند که قواعد سنتی انتساب برای فضای سایبر کارایی لازم را ندارند و ضرورت تدوین قواعد جدید در این زمینه احساس می‌شود (کولین، ۲۰۱۳: ۷۰).

۳-۲.ضابطه کنترل در نظام مسئولیت بین‌المللی

در خصوص انتساب رفتار گروه‌های غیردولتی به دولت‌ها، دو معیار اصلی در رویه قضایی بین‌المللی ارائه شده است که هر یک با چالش‌های خاص خود مواجه هستند. معیار «کنترل مؤثر» که توسط دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه ارائه شد، مستلزم اثبات کنترل دولت بر تک‌تک اعمال گروه است .(ICJ, ۱۹۸٦: para. ۱۱۵)دیوان در این پرونده اعلام کرد که صرف تأمین مالی، سازماندهی، آموزش و تجهیزات گروه، برای انتساب اعمال آن‌ها به دولت کافی نیست و باید اثبات شود که دولت کنترل مؤثر بر عملیات خاص داشته است. این معیار در پرونده نسل‌کشی بوسنی (۲۰۰۷) نیز مورد تأکید مجدد قرار گرفت و دیوان، معیار «کنترل کلی» را که توسط دادگاه کیفری بین‌المللی برای یوگسلاوی سابق ارائه شده بود، رد کرد.(ICJ, ۲۰۰۷: para. ٤۰۳)

بررسی رویه دیوان بین‌المللی دادگستری نشان می‌دهد دیوان در خصوص ضابطه کنترل در قضایای مختلف رویه‌ای واحد پیموده و در رویارویی با چالش‌های رویه خود توسط سایر مراجع حل‌وفصل اختلاف، بر رویه خود تاکید کرده است (ملکی‌زاده، ۱۳۹۲: ۱٦۰). با این حال، برخی از صاحبنظران بر این باورند که رویه دیوان در این زمینه چندان شفاف نیست و ابهامات زیادی در مورد نحوه احراز کنترل مؤثر وجود دارد (راعی، ۱۳۸۸: ۱٥٦). اتخاذ رویه‌های گوناگون از سوی مراجع قضایی بین‌المللی در زمینه ضابطه کنترل، نشان از تعارض رویه قضایی بین‌المللی در این موضوع است و دیوان در قضیه نیکاراگوا و نسل‌زدایی، معیارهای مربوط به کنترل را مورد بررسی قرار داد، در حالی که دادگاه کیفری بین‌المللی یوگسلاوی سابق به شیوه‌ای متفاوت به ضابطه کنترل توجه کرد (ملکی‌زاده، ۱۳۹۲: ۱٦۲). ضابطه کنترل مؤثر در زمینه مسئولیت بین‌المللی قابل طرح است، اما ضابطه کنترل کلی در موضوع رسیدگی به مسئولیت کیفری افراد موضوعیت پیدا می‌کند (ملکی‌زاده، ۱۳۹۲: ۱٦۳).

با این حال، در فضای سایبر، اثبات کنترل مؤثر بر گروه‌های هکری که ماهیتی پراکنده و غیرمتمرکز دارند، تقریباً ناممکن است. به‌ویژه اینکه گروه‌های هکری معمولاً فاقد ساختار سلسله‌مراتبی هستند و اعضای آنها ممکن است در کشورهای مختلف زندگی کنند و به‌صورت مستقل و خودجوش عمل کنند. در چنین شرایطی، اثبات اینکه یک دولت خاص، کنترل مؤثر بر عملیات خاص یک گروه هکری داشته است، کاری بس دشوار و گاه غیرممکن خواهد بود (قرشی سروندانی، ۱۳۹۱: ۷۸). لذا، برخی از صاحبنظران بر این باورند که برای فضای سایبر، باید از معیار «کنترل کلی» استفاده کرد که سطح اثباتی پایین‌تری دارد و اثبات آن آسان‌تر است (کولین، ۲۰۱۳: ۷۵). با این

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

حال، این معیار نیز با انتقادهایی مواجه است و در عالی‌ترین مرجع قضایی بین‌المللی به رسمیت شناخته نشده است.

۳-۳.اصل مراقبت بایسته در فضای سایبر

علاوه بر معیارهای کنترل مؤثر و کنترل کلی، قاعده دیگری نیز در حقوق بین‌الملل وجود دارد که می‌تواند مبنای مسئولیت دولت‌ها در قبال حملات سایبری قرار گیرد. اصل مراقبت بایسته(Due Diligence) ، دولت‌ها را ملزم می‌کند که از اقدامات مخربی که از قلمرو آن دولت سرچشمه می‌گیرد و به حقوق دولت‌های دیگر آسیب می‌رساند، جلوگیری کنند (حدادی و مرادیان، ۱۳۹۸: ۱٦۸). بر اساس این اصل، دولت موظف است با استفاده از ابزارهای مناسب، از وقوع اعمال متخلفانه توسط اشخاص خصوصی در قلمرو خود جلوگیری کند (حدادی و مرادیان، ۱۳۹۸: ۱۷۰). این اصل در قضیه تنگه کورفو (۱۹٤۹) توسط دیوان بین‌المللی دادگستری به رسمیت شناخته شد و دیوان اعلام داشت که هر دولتی موظف است اجازه ندهد قلمرو آن برای اقدامات خلاف حقوق دولت‌های دیگر مورد استفاده قرار گیرد.(ICJ, ۱۹٤۹: ۲۲)

مراقبت بایسته به معنای هوشیاری لازم در انجام تعهد حقوقی، یکی از اصول حقوق بین‌الملل است که بارها در دیوان‌های بین‌المللی تایید شده است (حدادی و مرادیان، ۱۳۹۸: ۱٦٦). علاوه بر زمینه‌های عرفی الزامات این اصل، کشورها آن را در معاهدات بسیاری وارد نموده و در چارچوب تعهدات قراردادی نیز سامان داده‌اند (حدادی و مرادیان، ۱۳۹۸: ۱۷۵). یکی از نمونه‌های بارز این اصل در حوزه مبارزه با تأمین مالی تروریسم، الزامات گروه ویژه اقدام مالی (FATF) است که دولت‌ها را به اعمال نظارت بر سیستم‌های مالی و جلوگیری از سوءاستفاده آنها توسط تروریست‌ها ملزم می‌کند (حدادی و مرادیان، ۱۳۹۸: ۱۸۰).

به‌کارگیری این اصل در فضای سایبر، می‌تواند راهگشا باشد، زیرا اثبات نقض تعهد مراقبت بایسته، نیازمند اثبات استاندارد بالای کنترل نیست و دولت‌ها را ملزم می‌کند که حداقل اقدامات معقول را برای جلوگیری از حملات سایبری از قلمرو خود انجام دهند. با این حال، اجرای این اصل نیز با چالش‌هایی از جمله دشواری تعیین مصادیق عینی اقدامات معقول، تفاوت در توانایی‌های فنی و مالی دولت‌ها و نبود رویه قضایی مشخص مواجه است (لیو، ۲۰۱۷: ۲۰۰). سنجه سنجش مراقبت بایسته، یک سنجه عرفی و متغیر است که به توانایی‌های فنی و مالی دولت و همچنین جدیت تهدید بستگی دارد و از یک دولت توسعه‌یافته انتظار بیشتری نسبت به یک دولت درحال‌توسعه می‌رود (لیو، ۲۰۱۷: ۲۰۵).

٤-مطالعه موردی استاکس‌نت و تقابل سایبری ایران و رژیم صهیونیستی

٤-۱.بدافزار استاکس‌نت: نقطه عطف جنگ سایبری مدرن

بدافزار استاکس‌نت که در سال ۲۰۱۰ شناسایی شد، یکی از پیچیده‌ترین و پیشرفته‌ترین حملات سایبری تاریخ محسوب می‌شود. این بدافزار با هدف تخریب تجهیزات غنی‌سازی اورانیوم در تأسیسات هسته‌ای ایران، به‌ویژه

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

تأسیسات نطنز، طراحی شده بود و با حمله به سیستم‌های کنترلی صنعتی(SCADA) ، موجب اختلال در عملکرد سانتریفیوژها و تأخیر در برنامه هسته‌ای ایران شد. آنچه استاکس‌نت را از سایر حملات سایبری متمایز می‌ساخت، سطح بالای پیچیدگی فنی، استفاده از چندین آسیب‌پذیری روز صفر و هدف‌گیری دقیق و محدود بود که نشان می‌داد حملات با آگاهی کامل از جزئیات تأسیسات هدف طراحی شده‌اند.

از منظر حقوقی، استاکس‌نت این پرسش اساسی را مطرح کرد که آیا یک حمله سایبری که منجر به خسارت فیزیکی می‌شود، مصداق «توسل به زور» یا «حمله مسلحانه» است یا خیر. اهداف و آثار این بدافزار به‌گونه‌ای بود که بسیاری آن را با یک حمله مسلحانه مقایسه کردند. در تحلیل این موضوع، باید به چند عامل توجه کرد: شدت حمله (که در استاکس‌نت، با تخریب تجهیزات گران‌قیمت، قابل‌توجه بود)، آثار فوری (که هرچند فوری نبود، اما در کوتاه‌مدت اختلال جدی در برنامه هسته‌ای ایران ایجاد کرد)، نفوذ نظامی (که در این مورد، هدف‌گیری تأسیسات هسته‌ای را شامل می‌شد) و ماهیت ابزارهای به‌کاررفته (که به‌عنوان یک سلاح سایبری پیشرفته طراحی شده بود). دیوان بین‌المللی دادگستری در قضیه سکوهای نفتی، بر این نکته تأکید کرد که برای احراز «حمله مسلحانه»، باید شدت و آثار حمله به سطحی برسد که آن را از سایر اشکال توسل به زور متمایز سازد (ICJ, ۲۰۰۳: □□□□. ۵۱).

برخی از حقوقدانان بر این باورند که استاکس‌نت به دلیل آثار مخرب فیزیکی، می‌تواند مصداق «توسل به زور» تلقی شود و در نتیجه، ایران از حق دفاع مشروع برخوردار بوده است (نامدار و قاسمی، ۱۳۹۷: ۲۱۰). با این حال، گروهی دیگر معتقدند که برای احراز «توسل به زور»، باید حمله به سطحی از شدت برسد که با حملات نظامی سنتی قابل‌مقایسه باشد و از آنجا که استاکس‌نت منجر به تلفات جانی نشد، نمی‌توان آن را مصداق توسل به زور دانست (محمدعلی‌پور، ۱۳۹۷: ۲٤٥). این اختلاف نظر، نشان‌دهنده خلأ هنجاری در حقوق بین‌الملل و ضرورت تدوین قواعد روشن‌تر در این زمینه است. رژیم صهیونیستی به‌عنوان یکی از پیشگامان توسعه قابلیت‌های تهاجمی سایبری، با تکیه بر برتری فنی و همکاری نزدیک با ایالات متحده، استراتژی «جنگ سایبری تهاجمی» را در پیش گرفته است که استاکس‌نت نمونه بارز آن محسوب می‌شود (نامدار و قاسمی، ۱۳۹۷: ۲۱۲).

٤-۲.چالش‌های حقوقی تقابل سایبری ایران و رژیم صهیونیستی

تقابل سایبری ایران و رژیم صهیونیستی، ابعاد حقوقی پیچیده‌ای را به همراه داشته است که از جمله مهم‌ترین آنها می‌توان به «مشروعیت توسل به زور در فضای سایبر»، «مسئولیت دولت‌ها در قبال حملات سایبری گروه‌های غیردولتی» و «حقوق بشردوستانه در جنگ‌های سایبری» اشاره کرد (امیری و حیدری‌فرد، ۱۳۹۷: ۱٦۰). در خصوص مشروعیت توسل به زور، یکی از چالش‌برانگیزترین مسائل، تعیین معیارهای تشخیص یک حمله سایبری به‌عنوان «توسل به زور» یا «حمله مسلحانه» است که به‌نوبه خود، تعیین کننده حق دفاع مشروع دولت قربانی خواهد بود (بشیری، ۱۳۹٤: ۵). در مورد حملات سایبری ایران و رژیم صهیونیستی، هر دو طرف از اعلام رسمی حمله و استناد به حق دفاع مشروع خودداری کرده‌اند و ترجیح داده‌اند که حملات خود را محرمانه نگه دارند تا از

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

مناقشات حقوقی پیچیده جلوگیری کنند. این رویکرد، هرچند از منظر عملیاتی قابل توجیه است، اما به تضعیف هنجارهای حقوقی و ایجاد ابهام در قواعد حاکم بر فضای سایبر دامن زده است (قرشی سروندانی، ۱۳۹۱: ۹۵).

در خصوص مسئولیت دولت‌ها در قبال حملات سایبری گروه‌های غیردولتی، هر دو طرف متهم به استفاده از گروه‌های نیابتی برای انجام عملیات‌های سایبری شده‌اند. ایران به حمایت از گروه‌های هکری مانند APT۳۵ و Black Shadowمتهم است، در حالی که رژیم صهیونیستی به همکاری با شرکت‌های امنیتی خصوصی مانند NSO Groupبرای انجام عملیات‌های سایبری متهم شده است (نامدار و قاسمی، ۱۳۹۷: ۲۱۵). این موضوع، چالش‌های حقوقی قابل‌توجهی را در زمینه انتساب و اثبات مسئولیت دولت‌ها ایجاد کرده است و کاربرد قواعد سنتی مسئولیت دولت‌ها را در فضای سایبر با دشواری مواجه می‌سازد. اثبات انتساب در فضای سایبر با دشواری‌های متعددی مواجه است و معیارهای کنترل مؤثر و کنترل کلی که در رویه قضایی بین‌المللی به رسمیت شناخته شده‌اند، برای فضای سایبر کارایی لازم را ندارند (کولین، ۲۰۱۳: ۷۰). اصل مراقبت بایسته نیز هرچند می‌تولند راهکاری عملی‌تر ارائه دهد، اما اجرای آن با چالش‌هایی مانند دشواری تعیین مصادیق عینی اقدامات معقول و تفاوت در توانایی‌های فنی و مالی دولت‌ها مواجه است (لیو، ۲۰۱۷: ۲۰۵).

ابعاد حقوقی دیگری نیز در این تقابل قابل بررسی است، از جمله «نقض حاکمیت دولت‌ها» از طریق عملیات سایبری و «تأثیر حملات سایبری بر حقوق شهروندان غیرنظامی». حملات سایبری که زیرساخت‌های حیاتی مانند بیمارستان‌ها، سیستم‌های آب و برق، یا سامانه‌های حمل و نقل را هدف قرار می‌دهند، می‌توانند تأثیرات شدیدی بر زندگی روزمره شهروندان غیرنظامی داشته باشند و حقوق بشردوستانه را نقض کنند (حیدری‌فرد، ۱٤۰۰: ۱٦۵). با این حال، به دلیل نبود یک نهاد نظارتی مؤثر و نیز دشواری در اثبات انتساب، دولت‌ها می‌توانند با کم‌ترین هزینه حقوقی و سیاسی به چنین حملاتی دست بزنند و بدین‌ترتیب، خلأ نظارتی قابل‌توجهی در این عرصه وجود دارد که به تداوم چرخه حملات سایبری دامن می‌زند (محمدعلی‌پور، ۱۳۹۷: ۲۵۰).

٤-۳.چشم‌انداز آینده و ضرورت تدوین قواعد جدید

بررسی‌های انجام‌شده نشان می‌دهد که حقوق بین‌الملل موجود، پاسخ‌گوی تمامی چالش‌های ناشی از حملات سایبری نیست و خلأ هنجاری قابل‌توجهی در این زمینه وجود دارد. تلاش‌های برخی کشورها و مجامع بین‌المللی برای نظام‌مندسازی ابزارها، شیوه‌ها و اثرات این سبک از حمله و مخاصمه، هنوز با توجه به عدم اجماع و وفاق جامعه جهانی منتهی به یک سند بین‌المللی نشده است (امیری و حیدری‌فرد، ۱۳۹۷: ۱۷۵). این خلأ هنجاری، به دولت‌ها امکان می‌دهد تا با بهره‌گیری از ابهامات حقوقی، به اعمال راهبردهای خصمانه در فضای سایبر بپردازند و از مسئولیت بین‌المللی فرار کنند.

با توجه به افزایش روزافزون حملات سایبری و پیچیدگی‌های آنها، ضرورت تدوین قواعد روشن‌تر و متناسب‌تری در این زمینه بیش از پیش احساس می‌شود. این قواعد باید شامل معیارهای شفاف برای تشخیص «حمله سایبری» به‌عنوان «توسل به زور» یا «حمله مسلحانه»، چارچوب مشخص برای اعمال دفاع مشروع در برابر حملات سایبری،

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

و سازوکارهای کارآمد برای انتساب حملات سایبری به دولت‌ها باشد. همچنین، ایجاد یک نهاد تخصصی بین‌المللی با وظیفه بررسی فنی حملات سایبری و ارائه گزارش‌های کارشناسی، می‌تواند به تسهیل فرآیند انتساب و کاهش سیاسی‌شدن آن کمک کند (نامدار و قاسمی، ۱۳۹۷: ۲۱۸). با این حال، به دلیل اختلافات عمیق میان قدرت‌های بزرگ بر سر نحوه تنظیم فضای سایبر، پیشرفت در این زمینه بسیار کند بوده است و انتظار نمی‌رود که در کوتاه‌مدت، توافقات جامعی در این زمینه حاصل شود (امیری و حیدری‌فرد، ۱۳۹۷: ۱۷۸). از سوی دیگر، قواعد عرفی موجود نیز هرچند قابل اعمال هستند، اما به دلیل عدم شفافیت کافی، نمی‌توانند پاسخگوی تمامی چالش‌های حوزه حملات سایبری باشند (اصلانی و رنجبریان، ۱۳۹٤: ۲۷۵).

در نهایت، با توجه به اهمیت روزافزون فضای سایبر در زندگی بشر و افزایش تهدیدات ناشی از حملات سایبری توسط گروه‌های غیردولتی و دولتی، ضروری است که حقوق بین‌الملل با تحولات این حوزه همگام شود و چارچوب‌های هنجاری مناسبی برای پاسخگویی به چالش‌های نوین فراهم آورد. اگرچه در حال حاضر جامعه بین‌الملل در مورد معیارهای انتساب و نحوه اعمال قواعد مسئولیت دولت‌ها در فضای سایبر به اجماع کامل نرسیده است، اما روند رو به رشد حملات سایبری و افزایش آگاهی دولت‌ها از خطرات این حوزه، می‌تواند زمینه‌ساز تحولات مثبتی در آینده نزدیک باشد (محمدعلی‌پور، ۱۳۹۷: ۲۵۵). انتظار می‌رود که رویه قضایی دولت‌ها، تلاش‌های نهادهای بین‌المللی و نیز همکاری‌های دوجانبه و چندجانبه در زمینه امنیت سایبری، گام‌های مؤثری در جهت پر کردن خلأهای موجود و ایجاد نظم حقوقی کارآمدتر در این عرصه بردارد (نامدار و قاسمی، ۱۳۹۷: ۲۲۰).

نتیجه‌گیری

بررسی مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری به زیرساخت‌های حیاتی، ابعاد مختلف چالش‌های حقوقی ناشی از این نوع حملات را به تصویر کشیده است. یافته‌های پژوهش نشان می‌دهد که با وجود خلأ هنجاری موجود و عدم اجماع بر سر تعریف حمله سایبری و معیارهای انتساب، قواعد عمومی مسئولیت دولت‌ها و اصل مراقبت بایسته می‌توانند مبنایی برای مسئولیت دولت‌ها در قبال حملات سایبری از قلمرو خود فراهم آورند. با این حال، چالش‌های اثباتی، دشواری انتساب حملات به دولت‌ها و فقدان رویه قضایی مشخص، کاربست این قواعد را با دشواری مواجه ساخته است.

معیارهای کنترل مؤثر و کنترل کلی که در رویه قضایی بین‌المللی به رسمیت شناخته شده‌اند، برای فضای سایبر کارایی لازم را ندارند و اثبات انتساب حملات سایبری به دولت‌ها را با دشواری‌های بی‌سابقه‌ای مواجه می‌سازند. اصل مراقبت بایسته، هرچند می‌تواند راهکاری عملی‌تر ارائه دهد، اما اجرای آن با چالش‌هایی مانند دشواری تعیین مصادیق عینی اقدامات معقول و تفاوت در توانایی‌های فنی و مالی دولت‌ها مواجه است. همچنین، بررسی رویه دولت‌ها در مواردی مانند استاکس‌نت و حملات به زیرساخت‌های اوکراین و ایران نشان می‌دهد که دولت‌ها اغلب

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

از پذیرش مسئولیت خودداری کرده و راهبرد انکار را در پیش می‌گیرند که این امر، پاسخ‌گویی در برابر حملات سایبری را با دشواری مواجه می‌سازد.

با توجه به یافته‌های این پژوهش، چند پیشنهاد برای ارتقای نظام حقوقی حاکم بر حملات سایبری به زیرساخت‌های حیاتی قابل ارائه است. نخست، ضرورت تدوین یک معاهده بین‌المللی خاص در زمینه حمایت از زیرساخت‌های حیاتی در برابر حملات سایبری که به‌صراحت، معیارهای انتساب را متناسب با ویژگی‌های فضای سایبر تعیین کند و تعهدات دولت‌ها را در زمینه مراقبت بایسته به‌صورت روشن‌تر تبیین نماید. دوم، ایجاد یک نهاد تخصصی بین‌المللی با وظیفه بررسی فنی حملات سایبری و ارائه گزارش‌های کارشناسی به دولت‌ها و مراجع قضایی، تا فرآیند انتساب فنی را تسهیل نماید و از سیاسی‌شدن آن جلوگیری کند. سوم، تدوین استانداردهای اثباتی یکسان و قابل‌قبول در جامعه بین‌الملل که معیارهای روشنی برای تشخیص حمله سایبری و تعیین سطح ادله مورد نیاز برای اثبات انتساب ارائه دهد. چهارم، توسعه همکاری‌های بین‌المللی در زمینه تبادل اطلاعات و تجارب در مورد نحوه مدیریت ریسک‌های سایبری و همچنین تدوین استانداردهای بین‌المللی برای اقدامات پیشگیرانه در فضای سایبر.

در نهایت، با توجه به اهمیت روزافزون فضای سایبر و افزایش تهدیدات متوجه زیرساخت‌های حیاتی، ضروری است که حقوق بین‌الملل با تحولات این حوزه همگام شود و چارچوب‌های هنجاری مناسبی برای پاسخگویی به چالش‌های نوین فراهم آورد. اگرچه در حال حاضر جامعه بین‌الملل در مورد معیارهای انتساب و نحوه اعمال قواعد مسئولیت دولت‌ها در فضای سایبر به اجماع کامل نرسیده است، اما روند رو به رشد حملات سایبری و افزایش آگاهی دولت‌ها از خطرات این حوزه، می‌تولند زمینه‌ساز تحولات مثبتی در آینده نزدیک باشد. انتظار می‌رود که رویه قضایی دولت‌ها، تلاش‌های نهادهای بین‌المللی و نیز همکاری‌های دوجانبه و چندجانبه در زمینه امنیت سایبری، گام‌های مؤثری در جهت پر کردن خلأهای موجود و ایجاد نظم حقوقی کارآمدتر در این عرصه بردارد. در غیر این صورت، ادامه وضعیت موجود، نه‌تنها به بی‌ثباتی در فضای سایبر دامن خواهد زد، بلکه می‌تواند به تشدید تنش‌های بین‌المللی و حتی رویارویی نظامی منجر شود که هزینه‌های جبران‌ناپذیری برای جامعه بین‌الملل به همراه خواهد داشت.

فهرست منابع

منابع فارسی

اصلانی، جبار و رنجبریان، امیرحسین. (۱۳۹٤). «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل». تحقیقات حقوقی، دوره ۱۸، شماره ۷۱، صص ۲۷۸-۲۵۷.

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

امیری، علی و حیدری‌فرد، مهدی. (۱۳۹۷). «جنگ‌های سایبری: چالش‌ها و راهکارهای تعامل در پرتو مقررات توسل به زور». سیاست خارجی، سال ۳۲، شماره ۳، صص ۱۸۲-۱۵۳.

بشیری، سپیده. (۱۳۹٤). «بررسی جایگاه حملات سایبری در حقوق بین‌الملل». پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.

حلمی، نصرت‌الله (مترجم). (۱۳۸۷). مسئولیت بین‌المللی دولت و حمایت سیاسی. تهران: نشر میزان، چاپ اول.

حدادی، مهدی و مرادیان، بهرام. (۱۳۹۸). «مفهوم مراقبت بایسته در حقوق بین‌الملل و مقررات گروه ویژه اقدام مالی». مجله حقوق بین‌المللی، سال ۳٦، شماره ٦۱، صص ۲۰۲-۱٦۵.

حیدری‌فرد، مهدی. (۱٤۰۰). «اعمال مقررات حقوق بین‌الملل بشردوستانه در عرصه جنگ‌های سایبری: چالش‌ها و راهکارها». سیاست خارجی، سال ۳۵، شماره ٤، صص ۱۷٤-۱۵۵.

راعی، مسعود. (۱۳۸۸). «کنترل کلی یا مؤثر عاملی برای تحقق مسئولیت بین‌المللی دولت‌ها؟». مطالعات حقوق خصوصی، سال ۳۹، شماره ۳، صص ۱٦٤-۱۵۱.

ضیایی بیگدلی، محمدرضا. (۱۳۸٤). حقوق بین‌الملل عمومی. تهران: انتشارات گنج دانش، چاپ بیست‌ویکم.

قرشی سروندانی، سید هنرگس. (۱۳۹۱). مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری. پایان‌نامه کارشناسی ارشد، دانشکده حقوق دانشگاه شهید بهشتی.

ملکی‌زاده، امیرحسین. (۱۳۹۲). «ضابطه کنترل در نظام مسئولیت بین‌المللی؛ وحدت یا تعارض رویه قضایی بین‌المللی». مجله حقوقی دادگستری، سال ۷۷، شماره ۸۲، صص ۱۹۱-۱٦۰.

محمدعلی‌پور، فریده. (۱۳۹۷). «حملات سایبری و چالش‌های جدید برای اصل منع توسل به زور در روابط بین‌الملل». مطالعات حقوقی، سال ٦، شماره ۳، صص ۲۵۷-۲۳۳.

نامدار، ساسان و قاسمی، غلامعلی. (۱۳۹۷). «تحلیل مفهوم دفاع مشروع در پرتو حملات سایبری (با تأکید بر حمله استاکس‌نت به تأسیسات هسته‌ای ایران)». مطالعات حقوق عمومی، سال ٤۸، شماره ٤، صص ۱۹۹- ۲۳۵.

نصیری محلاتی، ژوبین. (۱۳۸۹). بررسی انطباق تصمیمات محاکم آمریکا در انتساب اعمال افراد و گروه‌ها به دولت ایران. پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.

فصلنامه طلوع نگارندگان عدالت
www.journaltne.ir

منابع خارجی

Collin, S. A. (۲۰۱۳). Attribution issues in cyberspace. Chicago-Kent Journal of International and Comparative Law, ۱۳(۲), ۸۲-۵۷.
International Court of Justice. (۱۹٤۹). The Corfu Channel Case (United Kingdom v. Albania) (Merits). Judgment of ۹ April ۱۹٤۹. I.C.J. Reports ۱۹٤۹.
International Court of Justice. (۱۹۸٦). Military and para-military activities in and against Nicaragua (Nicaragua v. United States of America) (Merits). Judgment of ۲۷ June ۱۹۸٦. I.C.J. Reports ۱۹۸٦.
International Court of Justice. (۱۹۹٦). Legality of the threat or use of nuclear weapons. Advisory Opinion of ۸ July ۱۹۹٦. I.C.J. Reports ۱۹۹٦.
International Court of Justice. (۲۰۰۳). Oil platforms (Islamic Republic of Iran v. United States of America). Judgment of ٦ November ۲۰۰۳. I.C.J. Reports ۲۰۰۳.
International Court of Justice. (۲۰۰٤). Legal consequences of the construction of a wall in the occupied Palestinian territory. Advisory Opinion of ۹ July ۲۰۰٤. I.C.J. Reports ۲۰۰٤.
International Court of Justice. (۲۰۰۷). Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro). Judgment of ۲٦ February ۲۰۰۷. I.C.J. Reports ۲۰۰۷.
International Law Commission. (۲۰۰۱). Draft Articles on Responsibility of States for Internationally Wrongful Acts. UN Doc. A/۱۰/٥٦.
Kulesza, J. (۲۰۰۹). State Responsibility for Cyberattacks on International Peace and Security. Polish Yearbook of International Law, (۲۹), ۱٥۲-۱۳۹.
Liu, I. Y. (۲۰۱۷). State Responsibility and Cyberattacks: Defining Due Diligence Obligations. The Indonesian Journal of International and Comparative Law, ٤, ۲۲۰-۱۹۱.
Schmitt, M. N. (Ed.). (۲۰۱۳). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press.