فصلنامه پژوهش های سیاسی و بین المللی
دوره ۱۵، شماره ۶۰، شماره پیاپی (۶۰)، پاییز ۱۴۰۳، ص ۱۴۴ ـ ۱۱۷

مقاله پژوهشی

تحلیل حقوقی کاربرد زور در واکنش به تهدیدات سایبری در عرصه بین الملل

محدثه قوامی پور سرشکه [۱] و امیررضا محمودی* [۲] علی جمشیدی پور [۳]

تاریخ دریافت: ۱۴۰۳/۰۱/۲۸ تاریخ پذیرش: ۱۴۰۳/۰۳/۳۰

چکیده: در دنیای امروز، جنگ سایبری یک واقعیت است و حملات سایبری رو به افزایش می باشند. توانایی حملات سایبری در خاموش کردن سیستم های رایانه ای تأسیسات هسته ای، شبکه های برق و سیستم های کنترل هوایی، این حملات را به تهدیدی جدی برای امنیت ملی تبدیل کرده است. برخی دانشمندان معتقدند حملات سایبری می تواند دلیلی برای شروع جنگ باشد. با این حال، با نگاهی به قوانین سنتی جنگ، تنها بخش کوچکی از حملات سایبری می تواند به عنوان حمله مسلحانه محسوب شود. در حالی که نظام حقوق بین الملل باید خود را با این میدان جدید جنگ تطبیق دهد، در حال حاضر قانون بین المللی پایدار و موثری برای بازدارندگی در برابر حملات سایبری وجود ندارد. در این مقاله، چگونگی اعمال قواعد حقوق بین الملل موجود در خصوص "استفاده از زور" در چارچوب حق استفاده از زور، در قبال حملات سایبری بررسی می شود. تحلیل ها در چهارچوب ماده ۲(۴) منشور ملل متحد مبنی بر ممنوعیت استفاده از زور، فصل هفتم تأمین صلح و امنیت و حق دفاع مشروع مندرج در ماده ۵۱ انجام می گیرد.

واژگان کلیدی: جنگ سایبری، حمله سایبری، حقوق بین الملل، استفاده از زور، دفاع مشروع، حمله مسلحانه.

[۱] دانشجوی دکتری حقوق کیفری و جرم شناسی، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران.
mohadesehghavamipour@gmail.com
[۲] گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران (نویسنده مسئول).
amirreza.mahmodi@gmail.com
[۳] دانشجوی کارشناسی ارشد حقوق جزا و جرم شناسی،، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران.
jamshidipourali@gmail.com

مقدمه

اینترنت و رایانه در تمام کشورهای مدرن از اهمیت حیاتی برخوردار است و همانطور که زیربنای تجارت است، امور استراتژیک دولتی، تولید و توزیع انرژی، مدیریت تأسیسات زیربنایی حیاتی، حمل و نقل عمومی و بسیاری از خدمات عمومی از طریق اینترنت و رایانه ها انجام می شود. هر چه یک کشور توسعه یافته تر باشد، به همان اندازه به فناوری و در نتیجه به اینترنت و رایانه وابسته تر می شود. سیستم های رایانه ای که از طریق شبکه های رایانه ای به یکدیگر متصل هستند، برای جوامع مدرن ضروری شده اند. (The White House" 2003, p.vii)

رایانه و اینترنت، همانند شمشیری دولبه، در حالی که منافع عظیمی برای دولت ها فراهم می کنند، درهای را نیز به روی عوامل متخاصم برای حمله به سیستم های حیاتی اطلاعاتی می گشایند. (Garnett, Clarke, 2004, 456) کشورهایی که بیشترین آسیب را از این حملات متحمل خواهند شد، پیشرفته ترین کشورها از نظر فناوری و بیشترین استفاده کنندگان از اتصالات اینترنتی هستند. (Wilson, 2007, 8) در واقع می توان گفت هیچ کشوری در برابر حملات سایبری ایمن نیست.

یکی از نخستین حوزه هایی که از فناوری نوظهور استفاده شد، محیط نظامی بود که در آن داده و تصمیم گیری سریع اهمیت دارد. در این محیط نیز از فناوری رایانه و ارتباطات استفاده می شود. این مسئله، همانند هر حوزه دیگری،

مشکلاتی را نیز در حوزه نظامی به همراه دارد. گرچه شبکه های ارتباطی نظامی در مواردی برای استفاده غیرنظامی مسدود هستند، اما در برخی موارد استفاده از منابع ارتباطی غیرنظامی اجتناب ناپذیر است و این امر سیستم های نظامی را در معرض حملات سایبری قرار می دهد. رویدادهای رخ داده نشان می دهد که حملات سایبری توانایی ایجاد خرابی های اقتصادی، فیزیکی، جراحات، تلفات و ویرانی های گسترده را دارد. از یک سو، با در نظر گرفتن امکانات فناوری، سناریوهای حمله سایبری تولید می شود و دولت ها در تلاش برای توسعه استراتژی در برابر این حملات هستند؛ از سوی دیگر، مشکلات احتمالی در عرصه حقوق مورد بحث قرار می گیرد.

یکی از مهمترین مشکلاتی که دولت ها یا جوامع بین المللی در محیط سایبری با آن روبرو هستند، این است که آیا قواعد حقوق بین الملل می تواند در مورد حملات سایبری اعمال شود یا خیر. از آنجایی که زمانی که هنجارهای حقوق بین الملل سنتی یا مبتنی بر معاهدات توسعه یافتند، فناوری سایبری تا این حد تهدیدزا نبود، کاربرد قواعد حقوقی موجود برای حملات سایبری قابل بحث است. برخی نویسندگان استدلال می کنند که به جنگ سایبری بیش از حد اهمیت داده می شود، یک حمله سایبری رخ داده نمی تواند دلیلی برای جنگ باشد، یک حمله سایبری سیاسی منبعث از دولت، همان نتیجه یک حمله خرابکارانه، جاسوسی یا تخریبی را خواهد داشت که به اندازه جنگ قدیمی است و نیروی مسلح در معنای سنتی آن مورد استفاده قرار نخواهد گرفت.

(Rid, 2012, 32 Singel, 2010, Deibert, 2011, 1-8) در مقابل، حملات رخ داده به استونی، گرجستان و ایران جدیت جنگ سایبری را نشان می دهد، موضوع از نظر حقوق بین الملل و حقوق جنگ ارزیابی می شود و استدلال می شود که در صورت یک حمله سایبری از سوی یک دولت دشمن یا گروه های زیرمجموعه دولت، دولت مورد حمله می تواند از "حق دفاع مشروع" مندرج در ماده ۵۱ منشور سازمان ملل متحد استفاده کند.

با این حال، جدا از این بحث، شواهد نشان می دهد که حملات سایبری گسترده قادر به ایجاد آسیب های جدی فیزیکی و تلفات انسانی هستند. بنابراین، نیاز به ایجاد چارچوب حقوقی برای واکنش به چنین حملاتی از اهمیت ویژه ای برخوردار است. اگرچه قواعد سنتی حقوق بین الملل ممکن است کافی نباشد، اما راهکارهای جدیدی همچون اعمال تحریم های سایبری یا حتی پاسخ نظامی در برخی موارد استثنایی، می تواند مورد بررسی قرار گیرد. (Shackelford, 2009, 310-316)

مباحث اصلی در این زمینه عبارتند از: تعریف "حمله مسلحانه" در محیط سایبری؛ سطح آستانه آسیبی که می تواند مصداق استفاده از زور و حمله مسلحانه محسوب شود؛ مشکلات ردیابی و نسبت دادن حملات سایبری به بازیگران دولتی یا غیردولتی؛ و در نهایت اینکه آیا پاسخ نظامی به حمله سایبری مشروع و متناسب خواهد بود. (Hathaway et al., 2012, 821-835) این مباحث نشان می دهد که حقوق بین الملل باید با چالش های ناشی از تکنولوژی

های نوظهور مانند فضای سایبری روبرو شود و قواعد خود را تطبیق دهد. این امر مستلزم گفتگو، بررسی های نظری و علمی، و در نهایت اقدامات عملی در سطح بین المللی است.

پیشرفت های حقوقی، همانند علم، با تخیل و تصور همراه است. زمانی که علم در تعریف پدیده های جدید در جهان دچار مشکل می شود، نظریه های جدیدی در این زمینه ارائه می کند. این موضوع در عرصه حقوق نیز صادق است. حقوقدانان باید تأثیر فناوری مدرن و حملات سایبری را بر درگیری های مسلحانه و حقوق جنگ تصور و در این زمینه کار کنند. در غیر این صورت، حقوق در هدایت دولت ها ساده و بی معنا خواهد ماند. در همین راستا، این مطالعه به دنبال یافتن پاسخ این پرسش است که قواعد حقوق بین الملل موجود در زمینه "استفاده از زور" چگونه می تواند در خصوص حملات سایبری اعمال شود. برای این منظور، ابتدا به بند ۲(۴) منشور ملل متحد پرداخته می شود، سپس استثنائات حق استفاده از زور یعنی استفاده از زور با تصویب شورای امنیت و شرایط حق دفاع مشروع، به همراه قواعد عرفی بین المللی ضرورت و تناسب مورد بررسی قرار می گیرند.

۱: حق استفاده از زور علیه حملات سایبری در حقوق بین الملل

در حقوق بین‌الملل، تفکیک میان حق استفاده از زور و قواعد حاکم بر درگیری‌های مسلحانه وجود دارد. بر این اساس، اعمال قواعد حقوق درگیری‌های مسلحانه کاملاً مستقل از این است که آیا حق استفاده از زور وجود

داشته یا نه، پذیرفته شده است. (Çaycı, 1995, 38) هنگام بررسی حقوق جنگ نیز باید موضوع مشروعیت استفاده از زور از مسئله مشروعیت اهداف، ابزار و روش‌های انتخاب شده در طول درگیری مسلحانه جدا در نظر گرفته و بررسی شود. در مورد حملات سایبری، حق واکنش دولت‌ها ایجاب می‌کند که قواعد مربوط به حق استفاده از زور بررسی شود.

حقوق بین‌الملل در زمینه قابلیت اعمال حق دفاع مشروع علیه حملات سایبری در جامعه بین‌المللی و میان دولت‌ها مورد بحث قرار گرفته است. برخی کشورها همچون ایالات متحده اعلام کرده‌اند در صورت برآورده شدن شرایط، از حق دفاع مشروع ناشی از حقوق بین‌الملل سنتی در برابر حملات سایبری استفاده خواهند کرد. پذیرفته شدن این امر که یک حمله مسلحانه لزوماً از طریق به‌کارگیری نیروهای نظامی متعارف صورت نمی‌گیرد، ریسک‌های بالقوه‌ای را به همراه دارد. این نگرانی وجود دارد که پذیرش حملات سایبری به عنوان حمله مسلحانه، دامنه اعمال ماده ۵۱ منشور ملل متحد را گسترش داده و محیط بین‌المللی را دچار آشفتگی‌های جدیدی کند.

۲: اصول کلی ممنوعیت استفاده از زور و وضعیت حقوقی حملات سایبری

امروزه قاعده اصلی حاکم بر استفاده از زور در حقوق بین‌الملل، منشور سازمان ملل متحد است (Başeren, 2003, 46) این منشور در چارچوب مذاکرات بین‌المللی و کنفرانس‌های سازمان ملل تدوین شده است. همانند سایر معاهدات بین‌المللی، منشور سازمان ملل برای تمامی دولت‌های عضو الزام‌آور است. این

منشور به صراحت استفاده از زور و تهدید به زور در روابط بین‌المللی را ممنوع می‌کند. این ممنوعیت در ماده ۲(۴) منشور چنین بیان شده است: "اعضای سازمان در روابط بین‌المللی خود باید از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشور دیگر یا به هر شکل دیگری که با اهداف ملل متحد سازگار نباشد، خودداری کنند".این ممنوعیت با قاعده سنتی حقوق بین‌الملل مبنی بر عدم مداخله در امور داخلی دیگر کشورها[۱] تکمیل می‌شود. (Manila Declaration, 1982; Friendly Relations Declaration, 1970)

ممنوعیت استفاده از زور مندرج در ماده ۲(۴) منشور، تنها دولت‌های عضو را ملزم می‌کند و مستقیماً تعهدی برای دولت‌های غیرعضو ایجاد نمی‌کند. آنچه موجب می‌شود دولت‌های غیرعضو نیز به این ممنوعیت پایبند باشند، تبدیل شدن آن به یک قاعده عرفی و عادت حقوقی جهانشمول در حقوق بین‌الملل است. (Dinstein,2019.91) بنابراین این ممنوعیت تمامی دولت‌ها، اعم از عضو یا غیرعضو را ملزم می‌کند.

پیشرفت فناوری و ظهور سلاح‌های سایبری نشان می‌دهد که نه تنها مفهوم "حمله مسلحانه" مندرج در ماده ۵۱ منشور ملل متحد، بلکه مفهوم "استفاده از زور مسلحانه" نیز در حال تحول است. در واقع، آنچه در زمان تدوین منشور

۱. non-intervention

ملل متحد مد نظر بود، بی‌شک استفاده از نیروهای نظامی و سلاح‌های متعارف بود. اما در عصر اطلاعات، مفهوم استفاده از نیروی نظامی متعارف چندان معنایی ندارد. حملات غیرمتعارف به استونی و گرجستان که خسارات قابل توجهی بر جای گذاشتند، گواه این امر هستند.

طبق سیستم سازمان ملل، استفاده از زور غیرقانونی که در خدمت اهداف گسترش مرزهای کشور و تغییر دولت های دیگر باشد، به عنوان "تجاوز" یا "توسعه طلبی" تعریف شده و ممنوع گردیده است. استفاده از زور تنها در شرایط دفاع مشروع یا بر اساس تصمیم شورای امنیت و با هدف حفظ استقلال سیاسی یا تمامیت ارضی مجاز شمرده شده است. (Arend and Beck 1995, 33, 34)سیستم سازمان ملل در خصوص استفاده از زور دارای دو ویژگی اصلی است. نخست اینکه، بر اساس ماده ۲(۴) منشور، تمامی کشورهای عضو باید در روابط بین المللی خود از استفاده یا تهدید به استفاده از زور پرهیز کنند. در این شرایط، استفاده از زور یک عمل غیرقانونی محسوب می شود. دوم اینکه، یک مرجع مرکزی با صلاحیت انحصاری استفاده از زور در برابر نقض این ممنوعیت ایجاد شده است. این موضوع در بخش هفتم منشور، در ماده ۴۲ که به شورای امنیت اجازه استفاده از زور علیه نقض غیرقانونی را می دهد، و مواد بعدی تنظیم گردیده است. (Başeren 1995, 48) بدین ترتیب، از یک سو کشورها از اختیار استفاده از زور صرف نظر کرده اند و استفاده انفرادی از

زور غیرقانونی شده است. از سوی دیگر، یک اختیار جمعی برای استفاده از زور در برابر اعمال غیرقانونی به سازمان ملل واگذار گردیده است.

منشور سازمان ملل معیارهای "استفاده از زور" و "تهدید" را مشخص نکرده است. در متن منشور از واژه "جنگ" پرهیز شده و به جای آن از اصطلاحات "تهدید" یا "استفاده از زور" استفاده گردیده بدون آنکه تعریفی از آنها ارائه شود. این موضوع باعث بروز مناقشاتی در خصوص اینکه آیا ممنوعیت استفاده از زور محدود به استفاده از نیروی نظامی است یا شامل برخی اقدامات اقتصادی و دیپلماتیک اجباری نیز می گردد. (Silver 1999, 80-82; Foltz 2012; Waxman 2011, 44) کشورهای ضعیف و برخی دانشمندان معتقدند ماده ۲(۴) منشور باید شامل فشارهای سیاسی و اقتصادی نیز باشد. اما نظر غالب بر این است که با توجه به استفاده از عبارت "نیروی نظامی" در بخش مقدمه و مواد ۴۱ و ۴۶ منشور، و نیز تأکید بر استفاده از نیروی نظامی در بیانیه روابط دوستانه ۱۹۷۰، این گونه فشارهای سیاسی و اقتصادی مشمول ماده ۲(۴) نمی گردند. (Dinstein 2005, 84)

برای درک اندیشه ممنوعیت استفاده از زور در منشور سازمان ملل، درک جنگ جهانی دوم و نیز ابتکارات و اسناد تاریخی پیشین ضروری است. سال ۱۹۴۵ پس از جنگی ویرانگر ناشی از سیاست های کسب قدرت و سرزمین برخی کشورها رقم خورد. کشورهایی که این تجربه تلخ را پشت سر گذاشته بودند، در

کنفرانس سانفرانسیسکو بر سر جلوگیری از سیاست های مبتنی بر زور به توافق رسیدند تا کاستی های پیمان برایان-کلوگ را جبران نمایند.

امروزه با پیشرفت تکنولوژی و استفاده بیشتر از رایانه و اینترنت توسط کشورهای قدرتمند، بحث های مربوط به استفاده از زور معکوس شده است؛ زیرا این کشورها در برابر حملات سایبری آسیب پذیرتر هستند و این موضوع به کشورهای ضعیف تر امکان حمله را می دهد. به ویژه کشورهایی نظیر ایالات متحده خواستار تفسیر موسع تر از ماده ۲(۴) منشور و شمول حملات سایبری در این ماده شده اند. (Bumiller and Shanker 2012) اما ماده ۲(۴) همچنان استفاده از نیروی نظامی در معنای سنتی را ممنوع می کند.

در دهه گذشته، حملات سایبری علیه استونی، گرجستان و حمله استاکس نت، نه تنها نقض قاعده ممنوعیت استفاده از زور بلکه نقض اصل عدم مداخله در امور داخلی کشورها را نیز در بر داشته اند. با این حال، کشورها با واگذاری این حملات به بازیگران غیردولتی، خود را پنهان می کنند تا مسئولیتی متوجه آنها نگردد. ضروری است تا در خصوص اینکه آیا حملات سایبری مشمول ممنوعیت استفاده از زور می گردند یا خیر، تعریف روشنی ارائه گردد. همچنین باید مشخص شود که آیا حمله سایبری مشابه با حمله نظامی سنتی ارزیابی می گردد و آیا دولت ها می توانند به آن با حمله سایبری یا نظامی متقابل پاسخ دهند؟ یا به دلیل امکانات فناوری، نمی توان مشخص کرد که حملات از چه منبعی نشأت گرفته است. (Sklerov, 2009, 74-75) در واقع، کشورهایی که

حملات سایبری را انجام می دهند، از ترس نقض قواعد سنتی حقوق بین الملل و اینکه این اعمال در زمره استفاده از نیروی نظامی قرار گیرند، خود را پنهان می کنند یا این حملات را به بازیگران غیردولتی واگذار می نمایند.

ناتو به عنوان یک سازمان بین المللی، مهمترین اقدامات را در زمینه تهدیدات سایبری انجام داده است. در ماده ۴ پیمان ناتو، اگر صلح منطقه ای، امنیت ملی، تمامیت ارضی یا استقلال یک عضو در معرض خطر قرار گیرد، کشورهای عضو موظف به مشورت با یکدیگر شده اند و ناتو اعلام کرده در صورت حمله سایبری در موارد مندرج در این ماده، اقدام خواهد نمود. (EurActiv, 2008) این امر نشان دهنده آن است که ناتو حملات سایبری را نقض قاعده عدم مداخله در امور داخلی می داند. بر اساس برنامه اقدام دفاع سایبری که در اکتبر ۲۰۱۱ توسط وزرا تصویب شد، تهدیدات سایبری به عنوان منشأ بالقوه برای انجام وظیفه دفاع متقابل مندرج در ماده ۵ در راستای مفهوم استراتژیک جدید تعریف گردیده است. در بیانیه نهایی اجلاس شیکاگو ۲۰۱۲ نیز بر لزوم مقابله موثر و هماهنگ با تهدیدات سایبری پیچیده و رو به گسترش تأکید شده است . با وجود پیشرفت های ناتو در زمینه امنیت سایبری، مسأله اصلی این است که آیا ماده ۵ پیمان مربوط به دفاع متقابل، شامل حملات سایبری نیز می گردد یا خیر. به عبارت دیگر، در صورت قرار گرفتن یکی از اعضا در معرض حمله سایبری به جای حمله نظامی، هنوز ابهام وجود دارد که آیا این ماده قابل اجرا است،

چگونه کشور مهاجم در کوتاه مدت شناسایی خواهد شد و چگونه به آن پاسخ داده می شود.

۳: استثناهای ممنوعیت استفاده از زور

امروزه بر اساس منشور سازمان ملل، دو استثنا بر ممنوعیت استفاده از زور وجود دارد: استفاده از زور با تصمیم شورای امنیت و حق دفاع مشروع.

الف: استفاده از زور با تصمیم شورای امنیت

منشور سازمان ملل در ماده ۲۴، مسئولیت اصلی حفظ صلح و امنیت بین المللی را به شورای امنیت واگذار کرده است. مواد ۳۹ تا ۵۱ بخش هفتم منشور تحت عنوان "اقدام در صورت تهدید علیه صلح، نقض صلح و عمل تجاوز" به تدابیری که سازمان می تواند برای حفظ صلح و امنیت بین المللی اتخاذ نماید و نحوه اجرای آنها می پردازد.

بر اساس ماده ۳۹، شورای امنیت صلاحیت تشخیص تهدید یا نقض صلح و ارائه توصیه لازم یا تصمیم گیری در خصوص اقدامات موضوع مواد ۴۱ و ۴۲ را دارد. تشخیص اینکه در چه شرایطی صلح تهدید شده یا نقض گردیده است، بسیار دشوار است. منشور سازمان ملل تعریف روشنی در این زمینه ارائه نکرده و این مسأله در خصوص جنگ یا حملات سایبری پیچیده تر می گردد. تعیین اینکه آیا حملات سایبری با استفاده از سلاح های سایبری می تواند تهدید یا نقض صلح تلقی گردد و در نتیجه اقدامات امنیتی جمعی قابل اتخاذ باشد، یک

مسأله ساده نیست. وقتی شورای امنیت شرایط موضوع ماده ۳۹ را احراز می نماید، اقدامات قابل اتخاذ به دو دسته موقت و اجباری تقسیم می شوند. بر اساس ماده ۴۰، هدف اقدامات موقت جلوگیری از تشدید بیشتر وضعیت است. با وجود اینکه منشور تعریف روشنی از این اقدامات موقت ارائه نکرده، در عمل شورای امنیت اقداماتی نظیر توقف درگیری ها، آتش بس، عقب نشینی نیروهای نظامی، انعقاد توافقنامه و تحریم تسلیحات را در این زمینه اتخاذ نموده است. (Meray, 1975, 444)

منشور سازمان ملل در مواد ۴۱ و ۴۲ دو نوع اقدام اجباری پیش بینی نموده است: اقداماتی که مستلزم استفاده از نیروی نظامی نیستند و اقداماتی که نیازمند استفاده از زور هستند. ماده ۴۱ شامل اقداماتی نظیر قطع روابط دیپلماتیک، اقتصادی، سیاسی و قطع ارتباطات هوایی، دریایی، راه آهن، پست، رادیو و تلویزیون است که استفاده از نیروی نظامی را دربر نمی گیرد. ماده ۴۲ اقدامات اجباری مستلزم استفاده از نیرو از طریق نیروهای هوایی، دریایی و زمینی را در نظر گرفته است.(Meray, 1975, 444)

در نتیجه، در صورت وقوع جنگ یا حمله سایبری، اتخاذ تصمیم شورای امنیت برای استفاده از زور یک فرایند سیاسی دشوار و کند خواهد بود. اما یک بار این موضوع مورد ارزیابی قرار گرفت و نتیجه گیری شد، کشورها موظف به پیروی از این تصمیم خواهند بود و حملات سایبری در این چارچوب، قانونی خواهد بود.

ب: حق دفاع مشروع

استثنای دیگر بر ممنوعیت استفاده از زور، "دفاع مشروع" است. حق کشورها برای حفظ امنیت خود همواره یکی از اصول بنیادین حقوق بین الملل بوده و با "حق دفاع مشروع" تضمین گردیده است. این حق در ماده ۵۱ منشور سازمان ملل پیش بینی شده است. طبق این ماده، در صورت وقوع حمله مسلحانه، کشوری که مورد حمله قرار گرفته می تواند تا زمانی که شورای امنیت اقدامات لازم را برای حفظ صلح و امنیت بین المللی انجام دهد، به استناد حق دفاع مشروع فردی یا جمعی، اقدامات ضروری را انجام دهد. (Keskin, 1998, 56-59) برای اعمال حق دفاع مشروع، باید شرایطی همچون وقوع حمله مسلحانه مستقیم یا غیرمستقیم، اطلاع شورای امنیت از اقدامات انجام شده، موقتی بودن این حق تا زمان اقدام شورا و رعایت ضرورت، فوریت و تناسب مطابق حقوق عرفی برقرار باشد.

منشور سازمان ملل در مواد ۴۱ و ۴۲ دو نوع اقدام اجباری پیش بینی نموده است: اقداماتی که مستلزم استفاده از نیروی نظامی نیستند و اقداماتی که نیازمند استفاده از نیرو هستند. ماده ۴۱ شامل اقداماتی نظیر قطع روابط دیپلماتیک، اقتصادی، سیاسی و قطع ارتباطات هوایی، دریایی، راه آهن، پست، رادیو و تلویزیون است که استفاده از نیروی نظامی را دربر نمی گیرد. ماده ۴۲ اقدامات اجباری مستلزم استفاده از نیرو از طریق نیروهای هوایی، دریایی و زمینی را در نظر گرفته است. (Meray 1975, 444)

در نتیجه، در صورت وقوع جنگ یا حمله سایبری، اتخاذ تصمیم شورای امنیت برای استفاده از زور یک فرایند سیاسی دشوار و کند خواهد بود. اما یک بار این موضوع مورد ارزیابی قرار گرفت و نتیجه گیری شد، کشورها موظف به پیروی از این تصمیم خواهند بود و حملات سایبری در این چارچوب، قانونی خواهد بود.

بحث های نظری موجود در خصوص تفسیر متنی از ماده ۵۱ حق دفاع مشروع برای حملات سایبری، با رویدادهای استونی، گرجستان و استاکس نت به اوج خود رسیده است. در واقع، در بسیاری از درگیری های مسلحانه، وضعیتی پیش می آید که هر دو طرف متخاصم ادعا می کنند اقدامات آنها به استناد حق دفاع مشروع قانونی بوده است که این امر مسئله را به بن بست می کشاند. اما پیش از آنکه در این دام گرفتار شویم، مسئله اصلی این است که آیا حملات سایبری می توانند حمله مسلحانه تلقی گردند یا خیر. بسیاری معتقدند که با توجه به تکنولوژی امروز، حملات سایبری می توانند به آستانه حمله مسلحانه برسند. (The White House 2011, 14)

آنچه حل این مسئله را دشوار می سازد، عدم وجود چارچوب تحلیلی مشترک در خصوص پارامترهای حملات سایبری برای اعطای حق استفاده از زور در قالب دفاع مشروع بر مبنای ماده ۵۱ و همچنین اختلاف عمیق نظر کشورها در ارزیابی معیارهای ضرورت، تناسب و فوریت است. با وجود این دشواری، بررسی اینکه در چه شرایطی حملات سایبری حمایت شده از سوی دولت ها یا

انجام شده توسط بازیگران غیردولتی می تواند حمله مسلحانه در چارچوب ماده ۵۱ منشور تلقی گردد، از اهمیت بالایی برخوردار است.

اصطلاح "حمله مسلحانه" بر خلاف سایر اصطلاحات، در منشور سازمان ملل تفسیر محدودی یافته است. (Dinstein 2002, 100) به عنوان مثال، برخی تهدیدات یا استفاده از زور که نقض ماده ۲(۴) منشور را در پی دارد، لزوماً در معنای ماده ۵۱ حمله مسلحانه محسوب نمی گردد. در این صورت، حملات سایبری که نمی توانند حمله مسلحانه تلقی شوند، حق دفاع مشروع را به استناد ماده ۵۱ ایجاد نخواهند کرد.

در ماده ۵۱ منشور سازمان ملل، پیش شرط برای اعمال حق دفاع مشروع، وقوع یک "حمله مسلحانه" و نه صرفاً "حمله" ذکر شده است. اما تعریفی از مفهوم "حمله مسلحانه" نه در این ماده و نه در سایر مواد منشور ارائه نگردیده است. اگرچه مفاهیم "حمله" و "حمله مسلحانه" تا حدودی همپوشانی دارند، اما دقیقاً یکسان نیستند. مهمتر اینکه معانی حقوقی آنها متفاوت بوده و در عمل نتایج متفاوتی را در پی خواهند داشت.

می توان گفت هر حمله مسلحانه ای یک حمله است اما هر حمله ای لزوماً حمله مسلحانه نیست. زیرا مفهوم حمله مسلحانه معنایی محدودتر از حمله دارد. حمله مسلحانه یک زیرمجموعه از حمله تلقی می گردد. علاوه بر این، این دو مفهوم از لحاظ پیامدهایی که به دنبال دارند نیز با یکدیگر متفاوت هستند. حمله مسلحانه به دلیل نامتعارف بودن پیامدهایش، به کشور قربانی این حق را می دهد

تا به استناد دفاع مشروع به صورت انفرادی از زور استفاده نماید. این امر ویژگی و کارکرد متمایز حمله مسلحانه را آشکار می سازد. اما سایر اعمالی که مصداق حمله هستند چنین ویژگی را ندارند؛ بلکه کارکرد دیگری همچون فعال سازی سیستم امنیت جمعی را دارند.

پیش شرط استفاده از زور در برابر حملات سایبری، پذیرفته شدن آنها به عنوان "حمله مسلحانه" در چارچوب ماده ۵۱ است. بنابراین برای قانونی بودن یک عملیات نظامی، ضروری است حمله به مرحله حمله مسلحانه ارتقا یافته باشد. با توجه به عدم تعریف مفهوم حمله مسلحانه در منشور، سه دیدگاه علمی در خصوص اینکه چه زمانی یک حمله سایبری می تواند حمله مسلحانه محسوب شده و حق دفاع مشروع نظامی را ایجاد نماید، وجود دارد: "رویکرد مبتنی بر ابزار"، "رویکرد مبتنی بر هدف" و "رویکرد مبتنی بر اثر" (Hathaway et al. 2012, 845)

۱: رویکرد ابزار محور

رویکرد "ابزار محور" بر این باور است که حملات سایبری نمی‌توانند در چارچوب حملات مسلحانه ماده ۵۱ منشور ملل متحد در نظر گرفته شوند. زیرا حملات سایبری هرگز در معنای کلاسیک، سلاح‌های نظامی نیستند. حملات سایبری تنها در صورتی که همراه با استفاده از سلاح نظامی کلاسیک یا از طریق یک حمله سایبری باشند، می‌توانند حمله مسلحانه محسوب شوند. به عنوان مثال، اگر بمبی که توسط یک حمله سایبری هدایت می‌شود، به یک مرکز

پشتیبانی رایانه‌ای یا کابل‌های اینترنتی برخورد کند و این حمله مسلحانه به "وزن کافی "برسد، نمونه‌ای از چنین موردی است. (Stahn, 2003, 40)

در واقع، به نظر می‌رسد که متن منشور ملل متحد رویکرد "ابزار محور" را تأیید می‌کند. ماده ۴۱ می‌گوید: "شورای امنیت می‌تواند تصمیم بگیرد که چه اقداماتی باید انجام شود که شامل استفاده از نیروی مسلح نباشد و از اعضای ملل متحد بخواهد که این اقدامات را اجرا کنند. این اقدامات می‌تواند شامل قطع کامل یا جزئی روابط اقتصادی و ریلی، دریایی، هوایی، پستی، تلگرافی، رادیویی و سایر وسایل ارتباطی و حمل و نقل، و قطع روابط دیپلماتیک باشد". (Schmitt, 1999, 21-22)با این تفسیر که "تلگراف، رادیو و سایر وسایل ارتباطی و حمل و نقل" اشاره به ابزارهای سایبری دارد، می‌توان گفت که حملات سایبری نمی‌توانند در چارچوب منشور به عنوان حمله مسلحانه در نظر گرفته شوند با این نتیجه می‌توان با استناد به قطعنامه "تعریف تجاوز" مورخ ۱۴ دسامبر ۱۹۷۴ با شماره ۳۳۱۴/۲۹ مجمع عمومی سازمان ملل متحد نیز رسید (Gündüz, 1998, 91) در ماده ۳ قطعنامه تعریف تجاوز، هفت نوع تجاوز برشمرده شده که همه آنها مربوط به سلاح یا نیروی نظامی در معنای کلاسیک است (Taşdemir, 2006, 143-144).

در تعریف تجاوز، "تهدید به استفاده از زور" لحاظ نشده است. حذف تهدید به استفاده از زور از تعریف، به این معنی است که تجاوز تنها زمانی وجود خواهد داشت که از نیروی مسلح واقعی استفاده شود و فشارهای سیاسی، اقتصادی،

فرهنگی یا ایدئولوژیکی یا مداخلات غیرنظامی "تجاوز" محسوب نمی‌شوند. (Schmitt, 1999, 21-22)

تأکید بر اینکه تجاوز به معنای "استفاده از نیروی مسلح" است و شکل جدی‌ترین و خطرناک‌ترین استفاده غیرقانونی از زور در مقدمه قطعنامه تعریف تجاوز، نشان می‌دهد که هر استفاده از زور مغایر با منشور سازمان ملل نمی‌تواند تجاوز محسوب شود. این مسئله رویکرد "ابزار محور" منشور را تأیید می‌کند و حملات سایبری نمی‌توانند حمله مسلحانه تلقی شوند. ویژگی مهم رویکرد "ابزار محور"، سادگی اجرایی آن است. زیرا تعریف نیروی نظامی یا سلاح در معنای سنتی آسان است. با این حال، از آنجا که حملات سایبری قادر به ایجاد خسارات به اندازه سلاح‌های متعارف هستند، بسیاری از دانشمندان معتقدند که رویکرد "ابزار محور" دیگر قابل استفاده نیست.

۲: رویکرد هدف محور

با در نظر گرفتن توانایی‌ها و خسارات بالقوه حملات سایبری، "رویکرد هدف محور" مطرح شده است. در این رویکرد، حمله مسلحانه به معنای هدف قرار دادن یک سیستم رایانه‌ای بحرانی در یک حمله سایبری است. در این رویکرد، برای دفاع مشروع پیشگیرانه، حمله سایبری باید نشانه‌ای از خسارت قابل توجه و احتمال کافی باشد.(Hollis, 1997) مزیت مهم رویکرد هدف محور این است که به کشورها امکان محافظت از زیرساخت‌های بحرانی ملی را می‌دهد. اما ریسک آن این است که با کاهش آستانه حق دفاع مشروع با استفاده از زور،

می‌تواند محیط بین‌المللی را به سمت درگیری‌های مسلحانه سنتی ویرانگر سوق دهد. زیرا اگر این رویکرد پذیرفته شود، حملات سایبری به سیستم‌های زیرساختی بحرانی، راه را برای حملات متقابل فیزیکی و سینتیک در چارچوب دفاع مشروع باز خواهد کرد.

۳: رویکرد اثرمحور

بر اساس "رویکرد اثرمحور"، یک حمله سایبری بر اساس شدت اثر آن به عنوان حمله مسلحانه تلقی می‌شود. در مقایسه با سایر رویکردها، اکنون "رویکرد اثرمحور" در محیط بین‌المللی، به ویژه بین کشورهای پیشرفته فناوری مانند ایالات متحده که بیشترین آسیب را از حملات متحمل می‌شوند، پذیرفته‌ترین رویکرد است. با این حال، در مورد اندازه‌گیری اثر یک حمله سایبری برای ایجاد حق دفاع مشروع، ایده‌های مختلفی مطرح شده و این مهمترین مسئله برای دانشمندان است. به عنوان مثال، باید مشخص شود که حمله سایبری به سیستم کنترل فرودگاه، حمله‌ای که منجر به قطعی برق منطقه‌ای می‌شود، حمله‌ای که سیستم بورس یا مالی را از کار می‌اندازد یا حمله استونی در سال ۲۰۰۷، کدام یک به حد کافی از شدت برای استفاده از زور دفاعی رسیده است. این حملات می‌توانند خسارات کوچک یا بزرگ ایجاد کنند، حتی برخی از آنها منجر به مرگ یا سقوط سیستم اقتصادی شوند، اما آثار حمله را به راحتی نمی‌توان نشان داد یا درک کرد.

پروفسور مایکل اشمیت[۱] در این زمینه در رویکرد "اثرمحور" پذیرفته شده در دکترین، به عنوان بهترین تعیین کننده معیارها شناخته می‌شود. از نظر او، اثرات یک حمله سایبری باید بر اساس شش معیار زیر ارزیابی شود: (Schmitt, 1999, pp.18-19)

- شدت[۲] : نوع و میزان خسارت
- فوریت[۳] : زمانی که خسارت پس از حمله ظاهر می‌شود
- پیوند علیت[۴] : ارتباط علیت بین حمله و خسارت
- تهاجمی بودن : [۵]میزان ورود حمله به قلمرو کشور قربانی
- قابلیت اندازه‌گیری[۶] : میزان قابل اندازه‌گیری بودن خسارت ناشی از حمله
- مشروعیت فرضی[۷] : اینکه در نظر گرفتن یک حمله مسلحانه به عنوان حمله سایبری باید استثنا و نه قاعده باشد.

۱ Schmitt

۲ severity

۳ immediacy

۴ directness

۵ invasiveness

۶ measurability

۷ presumptive legitimacy

اگرچه این معیارها برای تصمیم‌گیرندگان روشنگر است، اما کافی نیست. به عبارت دیگر، معیارهای جدیدی می‌تواند به رویکرد اثرمحور اضافه شود یا مورد انتقاد قرار گیرد. (Silver, 89, Barkham, 2001, 57) در تمام رویکردهای فوق، مهم این است که حمله سایبری باید با هدف تهدید سیاسی یا امنیت ملی انجام شود تا بتوان از مفهوم حمله سایبری یا جنگ سایبری صحبت کرد، در غیر این صورت، حمله سایبری فراتر از یک رویداد نظم عمومی نخواهد بود.

۴: معیارهای ضرورت و تناسب

دولتی که قصد استفاده از نیروی مسلحانه در برابر حمله سایبری را دارد، باید علاوه بر قواعد ذکر شده، از قواعد سنتی حقوق بین‌الملل در زمینه استفاده از زور یعنی "ضرورت" و "تناسب" نیز پیروی کند. امروزه تمام کشورها موافق هستند که معیارهای ضرورت و تناسب، پارامترهای حق دفاع مشروع قانونی را در چارچوب ماده ۵۱ منشور ملل متحد تشکیل می‌دهند. این شرایط امروزه به عنوان محدودیت‌هایی ناشی از حقوق عرفی بین‌المللی، اعتبار خود را در استفاده از حق دفاع مشروع حفظ کرده‌اند.(Gray, 2000, 105)

اگرچه این معیارها در ماده ۵۱ منشور ذکر نشده است، اما به عنوان بخشی از حقوق عرفی، کشورها را ملزم می‌کند. رعایت این اصول در زمان استفاده از زور توسط کشورها بر مبنای دفاع مشروع در برابر حملات سایبری، بسیار مهم است.

در غیر این صورت، خطر تبدیل شدن پاسخ‌های مبتنی بر دفاع مشروع به حملات سایبری به خسارات غیرقانونی وجود دارد. ایالات متحده اعلام کرده است که از این معیارها در برابر حملات سایبری استفاده خواهد کرد (International Strategy for Cyberspace, 2011, 14).

ارزیابی ضرورت در زمان تصمیم‌گیری برای استفاده از زور انجام می‌شود و معیار ضرورت پس از تصمیم‌گیری، کارکرد خود را تکمیل می‌کند. اما، وقوع یک حمله سایبری که به عنوان حمله مسلحانه محسوب می‌شود، به معنای "ضرورت" دفاع مشروع نیست. بنابراین، کشور قربانی یک حمله مسلحانه باید ثابت کند که هیچ گزینه دیگری به جز دفاع مسلحانه ندارد. در این چارچوب، شرایط ضرورت زمانی مصداق پیدا می‌کند که در یک "تهدید داغ" هیچ گزینه رفتار جایگزین دیگری وجود نداشته باشد. (Aral, 1999, 26) برای اینکه پاسخ مسلحانه فوری، مطابق با حقوق بین‌الملل به عنوان حق دفاع مشروع شناخته شود، باید هیچ گزینه رفتاری جایگزین دیگری برای جبران خسارت طرف قربانی وجود نداشته باشد. اگر بین طرفین در ارتباط با اقدام تهاجمی مذاکراتی آغاز شده باشد، پاسخ مسلحانه در صحنه دیگر دفاع مشروع محسوب نمی‌شود.(Dinstein, 202)

اصل تناسب به این معنا نیست که خسارت ناشی از اقدامات دفاعی باید متناسب با خسارات مادی و جانی ناشی از حمله مسلحانه اولیه باشد یا اینکه کشور دفاع کننده باید از همان سلاح‌ها و تعداد نیروهای مسلح مشابه کشور مهاجم استفاده

کند. در این چارچوب، این اصل با ایجاد محدودیت‌هایی برای نیروی متقابل قابل استفاده برای برطرف کردن یک حمله مسلحانه، از تشدید درگیری‌های مسلحانه نیز جلوگیری می‌کند.(Aral, 29)

اگرچه اصول ضرورت و تناسب روشن هستند، اما مشکل این است که چگونه این اصول باید در برابر حملات سایبری اعمال شوند. درحالی که چگونگی اعمال این اصول حتی در موارد حمله مسلحانه کلاسیک هنوز موضوع بحث است، نحوه اندازه‌گیری آثار یا خسارات حملات سایبری و ارائه پاسخی مناسب نیز یکی از مسائل حل نشده در عرصه بین‌المللی است.

نتیجه

دولت‌ها مجبورند مرزهای خود، امنیت ملی و محیط صلح‌آمیز را حفظ کنند. امروزه امنیت سایبری برای همه کشورها، کوچک یا بزرگ، توسعه یافته یا کمتر توسعه یافته، مهم است و همتراز با امنیت ملی در نظر گرفته می‌شود. فضای سایبری یک حوزه با مرزهای مشخص تحت حاکمیت یک کشور نیست، بلکه امکانات فناوری در حال پیشرفت و ماهیت فرامرزی حملات سایبری، یکی از بزرگترین تهدیدات علیه صلح و امنیت بین‌المللی شده است. اگرچه ایجاد یک محیط سایبری کاملاً امن یک آرمان‌شهر تلقی می‌شود، اما نیاز به همکاری جهانی برای جلوگیری از حملات سایبری آشکار است. کشورهای عضو سازمان ملل متحد هنوز در مورد تعریف، استراتژی یا راه‌حل واحد به توافق نرسیده‌اند. به

دلیل تفاوت در رویکرد و استراتژی کشورها در برابر تهدیدات سایبری و تفسیر حقوقی آن‌ها، یافتن راه‌حل جمعی دشوارتر می‌شود.

جامعه بین‌المللی که هنوز نتوانسته زبان مشترکی در مورد حمله سایبری و جنگ سایبری ایجاد کند، و در مورد اینکه کدام حمله سایبری در زمره تجاوز نظامی قرار می‌گیرد و آیا می‌توان در چارچوب حقوق جنگ در برابر حملات سایبری از زور استفاده کرد، به توافق نرسیده است؛ ارزیابی می‌شود که ورود به یک تلاش مشترک و آمادگی حقوقی لازم در مورد حملات سایبری پیچیده‌تر و پیامدهای جدی‌تر در آینده نزدیک، اجتناب‌ناپذیر است. علاوه بر این، تصور می‌شود که مناسب است حقوقدانان در مورد تأثیرات جنگ و حملات سایبری که تهدیدی برای امنیت ملی، صلح ملی و بین‌المللی محسوب می‌شوند، قابلیت اعمال قوانین موجود و مقررات مورد نیاز، مطالعه کنند.

منابع و ماخذ:

1. Aslan Gündüz (1998). Milletlerarası Hukuk Temel Belgeler Örnek Kararlar (3. Baskı). Beta Yayınları.
2. Berdal Aral (1999). Uluslararası Hukukta Meşru Müdafaa Hakkı. Siyasal Kitabevi.
3. Christine Gray (2000). International Law and Use of Force. Oxford University Press.
4. Clay Wilson (2007). Boot nets, Cybercrime, and Cyber terrorism: Vulner abilities and Policy Issues for Congress. http://www.fas.org/sgp/crs/terror/RL32114.pdf
5. Daniel B. Silver (1999). Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter. Computer Network Attack and International Law, 73-98.
6. Declaration on Principles of International Law Concerning Friendly Relations and Cooperation Among States in Accordance with the Charter of the United Nation, G.A.Res. http://www.unhcr.org/refworld/topic,459d17822,459d17a82,3dda1f104,0.html
7. Duncan B. Hollis (1997). Why States Need an International Law for Information Operations. Lewis & Clark Law Review, 11, 1023-1061.
8. Elisabeth Bumiller ve Thom Shanker, 2012, Panetta Warns of Dire Threat of Cyber attack on U.S. The New York Times. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewan ted=all&_r=0
9. EurActiv (2008, 4 Nisan). NATO Agrees on Common Approach to Cyber Defense. http://www.euractiv.com/en/infosociety/nato-agrees-common-approachcyber-defence/article-171377
10. Fatma Taşdemir (2006). Uluslararası Terörizme Karşı Devletlerin Kuvvete Başvurma Yetkisi (1.Baskı). Siyasal Basın Yayın Dağıtım.

11. Funda Keskin (1998). Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler. Mülkiyeliler Birliği Vakfı Yayınları Tezler Dizisi: 4.
12. Jason Barkham (2001). Information Warfare and International Law on the Use of Force. New York University Journal of International Law & Policy, 34, 57-113.
13. Michael N. Schmitt (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Research Publication 1 Information Series. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993
14. Matthew J. Sklerov (2009). Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect their Duty to Prevent. Military Law Review, 201, 1-85. http://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/201-fall-2009.pdf.
15. Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, & Julia Spiegel 2012, The Law of Cyber Attack. California Law Review, 100, 817-886.
16. Richard Garnett ve Paul Clarke (2004). Cyberterrorism: A New Challange for InternationalLaw. A. Bianchi (Ed.), Enforcing International Law Norms against Terrorosim, 465-487.
17. Ronald Deibert (2011). Tracking the Emerging Arms Race in Cyberspace. Bulletin of the Atomic Scientists, 1-8.
18. Ryan Singel (2010, 3 Nisan). White House Cyber Czar: There is no Cyber War. Wired. http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/
19. Sadi Çaycı (1995). Silahlı Kuvvetlerin Kullanılması. Genelkurmay Basımevi.
20. Seha L. Meray (1975). Devletler Hukukuna Giriş (İkinci Cilt), Yeniden Gözden Geçirilmiş Dördüncü Bası.

21. Sertaç H. Başeren (2003). Uluslararası Hukukta Devletlerin Münferiden Kuvvet Kullanmasının Sınırları. Ankara Üniversitesi Basımevi.
22. The White House (2003). The National Strategy to Secure Cyberspace. http://www.us-cert.gov/reading
23. The White House (2011, May). International Strategy for Cyberspace. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
24. Thomas Rid (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5-32.
25. Yoram Dinstein (2002). Computer Network Attack and Self-Defense. In Computer Network Attack and International Law (Vol. 76, pp. 99-120). Naval War College International Law Studies, William S. Hein & Co., Inc. https://www.usnwc.edu/getattachment/95012329-e379-4341-bd1d-a4764c84dd4c/Vol--76----ComputerNetwork-Attack-and-Internation.aspx

Yoram Dinstein (2001). War, Aggression And Self-Defence. Grotius Publications