فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲
وبگاه مجله: https://cyberlaw.maragheh.iau.ir

The Scope of the Principle of Non-Use of Force in Cyber Attacks in the Framework of the United Nations Charter

Peyman Hakimzade Khoei*
Assistant Professor and Faculty Member, Department of International Law, Faculty of Law, Theology and Political Science, Islamic Azad University, Tabriz Branch, Iran
Reyhane Derogari
PhD in Public International Law, Payame Noor University, Tehran, University Lecturer.
p_hakimzade@iaut.ac.ir
DOI 10.30495/CYBERLAW.2023.701861

Keywords:
Principle of Non-use of Force,
Cyber Attacks, International Law, Self-Defense.

Abstract

The global interconnectedness created through information technology provides a potentially powerful weapon for states and non-state actors to remotely disable or destroy military defense networks. Sending excessive data requests to an internet website, "server or router" can be used as a weapon to destroy major information networks or to infiltrate private networks. The present study, employing descriptive-analytical methods, investigates the possibility of applying the Principle of Non-recourse to Force as an absolute rule of international law in relation to cyber-attacks and existing legal challenges. The questions that arise are: can the cyber attacks be prohibited according to the Principle of Non-recourse to Force in the light of the Article 4 of the Paragraph 4 of the Charter? If so, can the cyber attack allow the use of military in legitimate defence as per the Article 51 of the charter? The findings show that although cyber-attacks may not cause physical damage, and in other words, they do not violate Article 2, Clause 4 of the Charter but, the principle of non-intervention, as a powerful international legal tool, can be used by states to protect and counter cyber-attacks.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

قلمرو اصل عدم توسل به زور در حملات سایبری در چارچوب منشور ملل متحد

پیمان حکیم زاده خوئی*

استادیار و عضو هیات علمی گروه حقوق بین الملل، دانشکده حقوق،الهیات و علوم سیاسی، دانشگاه آزاد اسلامی واحد تبریز، ایران

ریحانه دروگری

دکتری حقوق بین‌الملل عمومی، دانشگاه پیام نور تهران، مدرس دانشگاه.

p_hakimzade@iaut.ac.ir

تاریخ دریافت: ۲۲ آذر ۱۴۰۱ تاریخ پذیرش: ۱۹ فروردین ۱۴۰۲

چکیده

به هم‌پیوستگی جهانی که از طریق فناوری اطلاعات به وجود آمده، سلاح بالقوه قدرتمندی در اختیار دولت‌ها و بازیگران غیردولتی قرار می‌دهد که به‌وسیله آن‌ها می‌توان شبکه‌های دفاع نظامی را از راه دور غیرفعال یا تخریب کرد. ارسال بیش‌ازحد درخواست داده به یک سایت اینترنتی، «سرور یا روتر» می‌تواند به‌عنوان سلاحی جهت از بین بردن شبکه‌های اصلی اطلاعاتی مورداستفاده قرار گیرد یا نفوذ در شبکه‌های خصوصی مورداستفاده قرار گیرد پژوهش حاضر با روش توصیفی – تحلیلی در پی بررسی امکان اعمال اصل عدم توسل به زور به‌عنوان قاعده آمره مسلم حقوق بین‌الملل نسبت به حملات سایبری و چالش‌های حقوقی موجود است. یافته‌ها نشان می‌دهد که هرچند شاید حملات سایبری آسیب فیزیکی ایجاد نکنند و به عبارتی بند ۴ ماده ۲ منشور را نقض نکنند؛ اما اصل عدم‌مداخله به‌عنوان یک ابزار حقوقی بین‌المللی قدرتمند می‌تواند توسط دولت‌ها برای محافظت و مقابله در برابر حملات سایبری مورداستفاده قرار گیرد.

کلید واژگان: اصل ممنوعیت توسل به زور، حملات سایبری، حقوق بین‌الملل، دفاع مشروع.

مقدمه

نامشروع بودن حملات سایبری از ممنوعیت توسل به زور[1] مندرج در بند ۴ ماده ۲ منشور سازمان ملل متحد استنتاج می‌شود و در این‌گونه موارد برای اینکه بتوان به اصل غیرقانونی بودن توسل به زور استناد جست، این مداخلات باید آسیب فیزیکی ایجاد کنند. البته مسئله این است که بسیاری از حملات سایبری آسیب فیزیکی وارد نمی‌کنند و بنابراین به استناد بند ۴ ماده ۲ منشور قابل‌پیگیری نیستند. برخلاف ادعاهای موجود در ادبیات جنگ سایبری، این بدان معنا نیست که این حملات مشروع هستند. تقریباً می‌توان گفت در همه موارد این حملات ماهیت قهری دارند و اصل عدم‌مداخله را به‌عنوان یک اصل پذیرفته شده در حقوق بین‌الملل نقض می‌کنند. به‌عنوان‌مثال از حمله سایبری صورت گرفته علیه استونی در سال ۲۰۰۷ می‌توان به‌عنوان یک حمله سایبری، تحت عنوان مداخله نامشروع نام برد و با توجه به اینکه دولت‌ها از آغاز عصر اطلاعات به‌شدت به کاربرد فناوری رایانه جهت تنظیم مؤثر جوامع خود وابسته شده‌اند، طرف‌های متخاصم این وابستگی را تشخیص داده و به‌شدت به دنبال حمله به سرورهای اطلاعاتی مورداستفاده و تحت اختیار طرف‌های مقابل هستند (Joyner, 2001: 840). و چنین عملیاتی به‌عنوان حملات سایبری شناخته می‌شود. با توجه به خصوصیت ذاتی حملات سایبری و توانایی آن‌ها در ایجاد اثرات مخرب شدید، شاید تعجب‌آور نباشد که حملات سایبری به‌طورکلی از دیدگاه حقوق توسل به زور موردبررسی قرارگرفته و این سؤال مطرح شده است که آیا حملات سایبری بر اساس بند ۴ ماده ۲ منشور سازمان ملل متحد می‌تواند به‌عنوان استفاده غیرقانونی از زور تلقی شود؟ (O'Connell, 2012: 195).

دیدگاه غالب از دیرباز این بوده است که حق دفاع مشروع با استناد به ماده ۵۱ منشور صرفاً در مورد حملات نظامی یا درگیری‌های مسلحانه قابلیت اعمال دارد و معنای واضح و روشن متن منشور، این دیدگاه را مانند سایر جنبه‌های ساختاری منشور ملل متحد تأیید می‌کند. به‌عنوان‌مثال، مواد ۴۱ و ۴۲ منشور به ترتیب به شورای امنیت اجازه می‌دهد تا اقداماتی را انجام دهد که شامل کاربرد نیروی نظامی نیست و تنها درصورتی‌که این اقدامات ناکافی باشد، توسل به نیروی نظامی تجویز می‌شود. البته استدلال‌های متقابلی هم وجود دارد، ازجمله اینکه محدودیت مشخص ماده ۵۱ برای «حملات مسلحانه» نشان می‌دهد که تدوین‌کنندگان، «توسل به زور» ممنوعه را به‌عنوان مقوله‌ای گسترده‌تر پیش‌بینی کرده‌اند که به روش‌های خاصی محدود نمی‌شود، اما بحث در مورد ابزارهای مورداستفاده، در سراسر منشور نشان می‌دهد که قصد تنظیم مقررات در مورد حملات مسلحانه را دارد؛ چراکه توسل به نیروی نظامی شدیدتر از سایر ابزارهای قدرت است و این تعبیر محدود عموماً غالب بوده است (Farer, 1985: 253).

در خصوص بند ۴ ماده ۲ منشور باید اذعان داشت که توسل به زور مندرج در این بند ناظر به ابزار مورداستفاده نبوده بلکه به هدف و اثر کلی آن می‌پردازد و اجبار را ممنوع می‌کند؛ چراکه نیروی نظامی فقط یکی از ابزارهای اجبار است و اغلب ساده‌ترین نوع آن به شمار می‌رود؛ البته در مقاطع مختلفی، برخی از کشورها (معمولاً کشورهای درحال‌توسعه یا در طول جنگ سرد، «جهان سوم») این مساله را مطرح کرده‌اند که توسل به زور شامل اشکال دیگری از فشار است، مانند اجبار سیاسی و اقتصادی که حاکمیت دولت را تهدید می‌کند (Dinstein, 2001: 153). درواقع بند ۴ ماده ۲ منشور یک ممنوعیت مبتنی بر آثار است. تفسیر عمومی پذیرفته شده این است که فقط آن مداخلاتی که باعث آسیب فیزیکی می‌شوند، به‌عنوان توسل نامشروع به زور تلقی می‌شوند. درنتیجه، طبق قواعد حقوق بین‌الملل، حملات سایبری که آسیب فیزیکی ایجاد نمی‌کنند، نقض بند ۴ ماده ۲ نخواهد بود؛ بنابراین، مفسران حقوقی بر این عقیده هستند که این نوع حملات سایبری خارج از چارچوب مقررات بین‌المللی است و بنابراین به نظر می‌رسد موانع قانونی اندکی برای راه‌اندازی جنگ‌های رایانه‌ای در آینده وجود داشته باشد (Benetar, 2009: 380).

با این تفاسیر به نظر می‌رسد پاسخ به این سؤال که آیا حملات سایبری بر اساس بند ۴ ماده ۲ منشور سازمان ملل متحد می‌تواند به‌عنوان استفاده غیرقانونی از زور تلقی شود؟ برای حقوقدانان بین‌المللی دشوار است، چراکه حملات سایبری می‌توانند پیامدهای مختلفی را در پی داشته باشند. ازیک‌طرف، حملات سایبری می‌توانند آسیب‌های فیزیکی قابل‌مقایسه با حمله با سلاح‌های معمولی ایجاد کنند؛ به‌عنوان‌مثال، یک حمله سایبری می‌تواند یک سیستم کنترل ترافیک هوایی را از کار بیاندازد و باعث سقوط هواپیما شود یا می‌تواند در سیستم‌عامل یک نیروگاه تداخل و خرابی ایجاد کند و باعث ایجاد یک ذوب هسته‌ای شود. از سوی دیگر، حملات سایبری ممکن است

[1] Jus ad bellum

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

هیچ آسیب فیزیکی ایجاد نکنند. به‌عنوان‌مثال می‌توان به حملات سایبری اشاره کرد که باعث ازکارافتادن وب‌سایت‌های کلیدی دولتی یا تخریب یا دست‌کاری اطلاعات مهم واقع در سرورهای اطلاعاتی شوند (Waxman,2011,421).

این استدلال نشان می‌دهد که چون منشور سازمان ملل بلافاصله پس از جنگ جهانی دوم ایجاد شده است یعنی زمانی که صلح و امنیت بین‌المللی توسط ارتش‌های حرفه‌ای تهدید می‌شد که از سلاح‌های متعارف استفاده می‌کردند، بنابراین بند ۴ ماده ۲ به‌منظور رسیدگی به این نوع از توسل به زور ابداع شده است. کاملاً واضح است که بند ۴ ماده ۲ هرگز برای رسیدگی به حملات علیه دستگاه‌های رایانه‌ای یا اطلاعات موجود در آن‌ها نبوده است؛ بنابراین، کاربرد بند ۴ ماده ۲ منشور در اینجا نابجا تلقی شده و در محافظت از دولت‌ها در برابر روش‌های جدید جنگ، مانند حملات سایبری که آسیب فیزیکی آشکار نمی‌کنند، ناتوان خواهد بود.

با توجه به این موضوع و باهدف حفاظت بهتر از امنیت دولت‌ها، محققان جنگ سایبری اصلاحاتی را در چارچوب قواعد حقوق بین‌الملل موجود پیشنهاد می‌کنند و پیشنهاد مرسوم این است که بند ۴ ماده ۲ باید مشمول یک جهت‌یابی مجدد تفسیری شود و دامنه آن برای در برگرفتن حملات سایبری دارای آثار مخرب، گرچه فاقد آسیب فیزیکی هستند، گسترش یابد (Morth, 1998: 120).

۱. قواعد حقوق بین‌الملل و توسل به زور

از زمان آغاز اعمال بند ۴ ماده ۲ منشور بحث‌هایی در مورد اینکه آیا این ممنوعیت فقط کاربرد نیروی نظامی را در برمی‌گیرد یا اینکه این ممنوعیت به‌طور گسترده‌تری به استفاده از اجبار سیاسی و اقتصادی نیز گسترش می‌یابد وجود داشته است (Tunkin, 1985: 236). برای به دست آوردن تفسیر صحیح از بند ۴ ماده ۲ بهتر است کنوانسیون وین ۱۹۶۹ در مورد حقوق معاهدات مدنظر قرار گیرد که قواعدی را در مورد تفسیر معاهده ارائه می‌کند. ماده ۳۱ معاهده مذکور مقرر می‌دارد: یک معاهده با حسن نیت و منطبق بامعنای عادی که باید به اصطلاحات آن در سیاق عبارت و در پرتو موضوع و هدف معاهده داده شود، تفسیر خواهد شد. انطباق اصطلاح توسل به زور به معنای عادی آن نشان می‌دهد که بند ۴ ماده ۲ همه انواع توسل به زور را پوشش می‌دهد.

صراحتاً، بند ۴ ماده ۲ هرگونه صلاحیتی را برای توسل به زور منع می‌کند. علاوه بر این، مطمئناً قابل‌توجه است که در سایر بخش های منشور سازمان ملل متحد از واژه نیروی نظامی به‌صراحت استفاده شده است. به‌عنوان‌مثال، مقدمه منشور ملل متحد توضیح می‌دهد که «نیروی مسلح نباید استفاده شود، مگر در جهت منافع مشترک»، مضافاً اینکه مواد ۴۱ تا ۴۶ منشور مقرر می‌دارند که شورای امنیت می‌تواند «اقداماتی را که مستلزم استفاده از نیروی مسلح نیست» یا در صورت ناکافی بودن این اقدامات، «نیروی مسلحانه» را به کار گیرد؛ بنابراین، این واقعیت که تدوین‌کنندگان منشور سازمان ملل متحد قصد داشتند به‌صراحت نیروی مسلح را در مواد خاصی بیان کنند، نشان می‌دهد که استفاده از واژه نیرو، بدون قید و شرط در بند ۴ ماده ۲ به این معنی است که این ممنوعیت فراتر از نیروی مسلح اعمال شده و شامل نیروی اقتصادی و سیاسی نیز گردد.

به نظر می‌رسد که این تفسیر قطعاً شایستگی لازم را دارد؛ بااین‌حال، مهم است که به رسمیت شناخته شود. همان‌طور که توسط بند ۱ ماده ۳۱ عهدنامه ۶۹ وین الزامی شده است، قبل از اینکه اصطلاح معاهده بتواند معنای معمولی خود را بدهد، این معنی باید در برابر اهداف و اصول گسترده‌تر معاهده تأیید شود. در اصل، درصورتی‌که یک اصطلاح معاهده مبنا و هدف گسترده‌تر معاهده را نقض یا تضعیف کند، نمی‌تواند معنای عادی خود را به آن بدهد؛ زیرا منشور ملل متحد کاملاً روشن می‌سازد که هدف اصلی سازمان ملل حفظ صلح و امنیت بین‌المللی از طریق محدود کردن حق کشورهای عضو برای استفاده از نیروی مسلح و در عوض حفاظت از آن‌ها در قالب یک سیستم امنیت جمعی است. به‌عنوان‌مثال، مقدمه منشور (که زمینه مناسبی برای تشخیص اهداف و مقاصد یک معاهده تلقی می‌شود) به‌وضوح بیان می‌کند که سازمان ملل متحد سازمانی است که مصمم به جلوگیری از جنگ است و نیروی مسلح نباید استفاده شود. درنتیجه، اگر هدف سازمان ملل متحد محدود کردن توانایی کشورهای عضو آن برای استفاده از نیروی مسلح باشد، این نشان می‌دهد که واژه نیرو در بند ۴ ماده ۲ باید به معنای نیروی مسلح تفسیر شود.

همچنین ماده ۳۲ عهدنامه ۶۹ وین مقرر می‌دارد که اگر پس از اعمال ماده ۳۱ همچنان معنای اصطلاح یا حکم مبهم باشد، می‌توان به مواد مقدماتی معاهده مراجعه کرد. این موضوع در چارچوب بند ۴ ماده ۲ حائز اهمیت است؛ زیرا مواد مقدماتی نشان می‌دهد که پیشنهاد شده بود که بند ۴ ماده ۲ صراحتاً تهدید یا استفاده از زور و تهدید یا استفاده از اقدامات اقتصادی را به هر شکلی که مغایر با اهداف

دانشگاه آزاد اسلامی واحد مراغه

سازمان را شامل گردد. همان‌طور که مشخص است، این پیشنهاد توسط کمیته پیش‌نویس وتو شد. درنتیجه، اقدامات نشان می‌دهد که طراحان قصد نداشتند ممنوعیت را به‌اجبار اقتصادی و فشارهای سیاسی گسترش دهند (Roscini, 2010: 96).

بااین‌حال، هنوز باید در مورد معنای نیروی مسلح تحقیق صورت می‌گرفت و واضح است که اصطلاح «مسلح» مستلزم استفاده از یک سلاح است. فرهنگ لغت بلک لا[2]، «مسلح» را به معنای «مجهز به سلاح» یا «شامل استفاده از سلاح» تعریف می‌کند (Garner, 2009: 125). اما این سؤال نیز مطرح می‌شود که چگونه باید از این سلاح استفاده کرد تا نقض بند ۴ ماده ۲ رخ دهد؟

در ابتدا، به‌طورکلی پذیرفته شده بود که نیروهای مسلح نیاز به استفاده از سلاحی دارند که نیروی جنبشی تولید کند، یعنی استفاده از سلاحی که «اثر انفجاری به همراه امواج ضربه و گرما» داشته باشد (Brownlie, 1963: 184). ولی این رویکرد بعداً موردانتقاد قرار گرفت، چراکه این برداشت استفاده از سلاح‌های شیمیایی، بیولوژیکی و هسته‌ای را در برنمی‌گیرد و واضح است که چنین سلاح‌هایی لزوماً منجر به وقوع انفجار نمی‌شوند که نتیجتاً امواج شوک‌آور یا گرما ایجاد کنند؛ بنابراین به‌منظور حصول اطمینان از اینکه چنین سلاح‌هایی نیز در محدوده ممنوعیت توسل به زور قرار می‌گیرند، تعریف بند ۴ ماده ۲ منشور از الزام نیروی جنبشی و اثراتی که سلاح ایجاد می‌کند فاصله گرفت. به‌عنوان‌مثال، مرگ یا آسیب شخصی به افراد و تخریب اموال فیزیکی به‌عنوان معیاری برای تعریف استفاده از زور معرفی می‌شوند و به همچنین بیان شده است که حملات سایبری باید آسیب فیزیکی داشته باشند تا به‌عنوان توسل غیرقانونی به زور تلقی شوند و در اینجا مهم نیست که از چه ابزار خاصی (جنبشی یا الکترونیکی) برای واردکردن استفاده می‌شود؛ اما نتیجه نهایی باید این باشد که خشونت رخ دهد یا تهدیدی انجام گیرد .(Dinstein,2001,164)

بر اساس شرایط بند ۴ ماده ۲، تمایز بین جنگ و سایر اشکال اعمال زور از بین رفته است. این ممنوعیت، هر تهدید یا توسل غیرقانونی به زور را تحت هر عنوانی پوشش می‌دهد و ما می‌دانیم که توسل به زور به‌طورکلی ممنوع است، نه‌فقط جنگ. تعیین اینکه آیا توسل به زور وجود دارد یا خیر، مهم است؛ زیرا کشور قربانی ممکن است تحت تأثیر گستره وسیع‌تری از گزینه‌ها قرار داشته باشد تا اینکه حمله صورت گرفته، به‌منزله توسل به زور تلقی نشود (Simma at al, 2002: 216).

دیوان بین‌المللی دادگستری در نظر مشورتی خود در مورد مشروع بودن استفاده از سلاح‌های هسته‌ای اعلام کرد که مواد ۲(۴)، ۵۱ و ۴۱ به سلاح‌های خاصی اشاره نمی‌کنند. آن‌ها برای هرگونه استفاده از زور، صرف‌نظر از سلاح‌های به‌کاررفته، اعمال می‌شوند (I.C.J, 1996: 39).

این امر منجر به این نتیجه می‌شود که اگر یک عملیات سایبری به معنای استفاده از زور باشد، طبقه‌بندی این امر که آیا این نیرو از طریق ابزارهای سایبری انجام شده است یا خیر، بی‌فایده خواهد بود؛ بنابراین، بر اساس اظهارات دیوان، هیچ دلیلی وجود ندارد که سلاح‌ها لزوماً اثرات انفجاری داشته باشند یا فقط برای اهداف انفجاری ایجاد شوند. استفاده از سلاح‌های بیولوژیکی و شیمیایی، به‌عنوان سلاح‌های غیر جنبشی با کاربرد دوگانه، بدون شک به معنای استفاده از زور علیه دولت قربانی تلقی می‌شوند. علاوه بر این، دیوان بین‌المللی دادگستری تلویحاً تشخیص داد که استفاده از نیروی غیر جنبشی می‌تواند منجر به نقض بند ۴ ماده ۲ شود، زمانی که مسلح ساختن و آموزش نیروهای مخالف توسط ایالات‌متحده را به‌عنوان تهدید یا توسل به زور علیه نیکاراگوئه شناخت (I.C.J, 1986: 228).

۲. حمله سایبری به‌عنوان یک حمله مسلحانه

زمانی که بین دولت‌ها درگیری وجود دارد، منشور ملل متحد از اعضا می‌خواهد که «اختلافات بین‌المللی خود را با روش‌های مسالمت‌آمیز حل‌وفصل کنند، به‌گونه‌ای که صلح و امنیت بین‌المللی و عدالت به خطر نیافتد» (بند ۳ ماده ۲ منشور ملل متحد)؛ بنابراین اختیار توسل به زور توسط یک دولت یا از شورای امنیت سازمان ملل متحد یا از حق دولت برای اقدام جهت دفاع مشروع فردی یا جمعی ناشی می‌شود. حال سؤال این است که آیا حمله سایبری یا مجموعه حملات سایبری مستمر می‌تواند به آستانه «حمله مسلحانه» برسد که بر اساس ماده ۵۱ منشور حق دفاع مشروع را ایجاد کند؟ آیا بین «حمله مسلحانه» طبق ماده ۵۱ و «توسل به زور» طبق بند ۴ ماده ۲ منشور ملل متحد تفاوتی وجود دارد؟ پاسخ به این سؤال‌ها آسان نیست، زیرا اصطلاح حمله مسلحانه به‌طور خاص توسط معاهده یا هر شکل دیگری از توافق بین‌المللی تعریف نشده است. بااین‌حال، چارچوب بین‌المللی برای تجزیه‌وتحلیل اینکه آیا برخی اقدامات دولت‌ها حملات مسلحانه را تشکیل می‌دهند در طول زمان تکامل‌یافته و این اصول حقوقی هستند که باید در ارزیابی ماهیت حملات

[2] Black's Law Dictionary

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

سایبری اعمال شوند. به‌طورکلی، جامعه بین‌المللی بر روی این موضوع توافق دارد که معیارهای ارائه شده در کنوانسیون‌های ۱۹۴۹ ژنو باید به‌عنوان معیار برای تشخیص وجود یک درگیری مسلحانه بین‌المللی به‌عنوان راهنما مورداستفاده قرار گیرد (کنوانسیون ژنو، ۱۹۴۹). بر اساس این معیار، توسل به زور زمانی حمله مسلحانه تلقی می‌شود که نیرو از «وسعت، مدت و شدت کافی» برخوردار باشد.

بااین‌حال، ابزارهای بین‌المللی خاصی در طول سال‌ها تکامل‌یافته‌اند که تشخیص معیارهای ارائه شده را تسهیل کرده‌اند. به‌ویژه قطعنامه «تعریف تجاوز» مجمع عمومی سازمان ملل متحد که در آن تجاوز به‌عنوان «استفاده از نیروی مسلح توسط یک دولت علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی یک کشور دیگر، یا به هر روش دیگری که با منشور ملل متحد مغایرت داشته باشد، تعریف شده است.» (U. N. Gen Ass Res. 3314 (XXIX), 1974) درحالی‌که این قطعنامه حمله مسلحانه را تعریف نمی‌کند، نمونه‌هایی از اقدامات دولتی را ارائه می‌دهد که به نظر می‌رسد واجد شرایط هستند و این اقدامات موردپذیرش گسترده بین‌المللی قرارگرفته است.

اگرچه، این اعلامیه‌ها در اسناد بین‌المللی و تصمیمات دیوان‌های بین‌المللی درزمینه ارزیابی استفاده‌های متعارف از زور (نیکاراگوئه علیه ایالات‌متحده آمریکا) مفید است، اما در تعیین اینکه حملات سایبری چه زمانی حملات مسلحانه را تشکیل می‌دهند، دارای حداقل ارزش هستند. به این دلیل است که سلاح‌های سایبری همه‌کاره هستند و می‌تواند بازیگر نقش مکمل درگیری‌ها یا رویدادهای اصلی را بازی کنند. آن‌ها سلاح‌های یکپارچه‌ای نیستند که استفاده از آن‌ها منجر به پاسخ‌های صریح شود در مورد اینکه آیا ممنوعیت زور را نقض می‌کنند یا خیر؟ در عوض، اثرات مضر بی‌شمار ناشی از حملات سایبری، طبقه‌بندی آن‌ها را پیچیده‌تر و ضروری‌تر می‌کند. اثرات یک حمله سایبری می‌تواند از یک درگیری ساده (مانند حمله محروم‌سازی از سرویس[3] که به‌طور موقت ترافیک وب را مختل می‌کند) تا تخریب فیزیکی (مانند تغییر دستورات به یک ژنراتور برق که باعث انفجار آن می‌شود) و حتی تا مرگ متغیر باشد؛ مانند ایجاد اختلال در خطوط اورژانس به‌طوری‌که امکان تماس با پلیس یا خدمات آمبولانس وجود نداشته باشد؛ اما تلقی همه اشکال حمله سایبری به‌عنوان توسل به زور مستلزم تفسیر موسع غیرقابل قبولی از بند ۴ ماده ۲ است که شامل آسیب‌های غیر فیزیکی می‌شود (Gervais, 2012: 529).

علاوه بر این، شدت و دامنه زمانی یک حمله سایبری می‌تواند یک رویداد را از یک اقدام تهاجمی سطح پایین به یک توسل به زور ممنوعه تبدیل کند. دیوان بین‌المللی دادگستری در قضیه فعالیت‌های مسلحانه در قلمرو کنگو، (I.C.J, 2005: 165) تشخیص داد که نقض بند ۴ ماده ۲ ناشی از «وسعت و مدت» اقدامات اوگاندا است؛ بنابراین، بزرگی و مدت حمله، عوامل مناسبی برای در نظر گرفته شدن در هر مدلی هستند که تاکتیک‌های اجباری به کار گرفته شده توسط یک دولت را تحلیل می‌کند. مضافاً اینکه، اخیراً سه مدل تحلیلی متمایز ارائه شده است تا کاربرد معیارهای نیرو، دامنه، مدت‌زمان و شدت را برای نیروی غیرمتعارف، ازجمله حملات سایبری، تسهیل کند.

یکی از این رویکردها، رویکرد مبتنی بر ابزار است. تحت این مدل، ارزیابی می‌شود که آیا آسیب ناشی از یک حمله سایبری قبلاً فقط با یک حمله جنبشی به دست می‌آمد یا خیر. به‌عنوان‌مثال، با استفاده از این مدل، یک حمله سایبری که به‌منظور خاموش کردن شبکه برق انجام می‌شود، یک حمله مسلحانه تلقی می‌شود. چراکه قبل از توسعه قابلیت‌های سایبری، تخریب یک شبکه برق معمولاً مستلزم بمباران یک نیروگاه یا استفاده از شکل دیگری از نیروی جنبشی برای دستیابی به چنین نتیجه‌ای بود. علاوه بر این، اگر مهاجم به دنبال ایجاد تخریب فیزیکی مستقیم، جراحت یا مرگ باشد، حمله سایبری توسل به زور تلقی خواهد شد. این رویکرد به جامعه بین‌المللی اجازه می‌دهد تا منشور را با فناوری در حال تکامل تطبیق دهد و درعین‌حال تفاوت‌های ظریف، درشدت حمله سایبری را در نظر بگیرد (Brownlie, 2012: 362).

رویکرد دیگر «رویکرد مبتنی بر اثرات» است که اغلب به‌عنوان مدل مبتنی بر پیامد از آن یاد می‌شود. طبق این رویکرد، هیچ تلاشی برای ارزیابی اینکه آیا آسیب ناشی از یک حمله سایبری قبلاً فقط از طریق استفاده جنبشی از زور به دست می‌آمد یا خیر، انجام نمی‌شود. در اینجا توجه به تأثیر کلی حمله سایبری بر دولت قربانی خواهد بود.

رویکرد سوم «رویکرد مسئولیت دقیق» است که به‌طور خودکار هرگونه حمله سایبری علیه زیرساخت‌های حیاتی ملی را حمله مسلحانه تلقی می‌کند. این رویکرد مبتنی بر پیامدهای شدیدی است که ممکن است از هرگونه حمله به چنین سیستم‌های زیربنایی ناشی شود؛ بنابراین، از بحث‌هایی که تاکنون انجام شده، مشخص می‌شود که حملات سایبری، حملات مسلحانه است. به‌این‌ترتیب، یک دولت ممکن است در پاسخ به یک حمله سایبری به‌عنوان اعمال حق دفاع مشروع از زور استفاده کند.

[3] Denial Of Service Attack (DdoS)

۳. رویکردهای پیشرو در توسل به زور

اگر ما بخواهیم به این سؤال پاسخ دهیم که آیا عملیات سایبری در محدوده بند ۴ ماده ۲ قرار می‌گیرد یا خیر؟ درنهایت به چگونگی درک ماهیت یک حمله سایبری بستگی دارد. در این خصوص سه رویکرد اصلی توسعه‌یافته و یک گفتمانی در مورد در پیش گرفتن این رویکردها وجود دارد که در درک سنتی از توسل به زور نیز قابل‌مشاهده بوده و در بحث حمله مسلحانه نیز قابل‌اجرا هستند.

رویکرد مبتنی بر ابزار یعنی تمرکز بر ابزاری خاص برای انجام یک عمل، چیزی است که به‌طور سنتی، توسل به نیروی مسلح را از اجبار اقتصادی و سیاسی متمایز می‌کند. این رویکرد به دلیل تمرکز بر ابزارهای فیزیکی، سازگاری ضعیفی با عملیات سایبری دارد و تحت این رویکرد، یک کد مخرب هرگز و صرف‌نظر از پیامدهایی که ایجاد می‌کند، توسل به زور نخواهد بود. از فحوای متن منشور سازمان ملل نتیجه گرفته می‌شود که هرچه یک سلاح جدید، مشابه سلاح‌های متعارف باشد، احتمال بیشتری وجود دارد که عملیات آن به‌منزله توسل به زور یا حمله مسلحانه در نظر گرفته شود (Nguyen, 2013: 101).

رویکرد مبتنی بر هدف استدلال می‌کند که حمله سایبری باید زیرساخت‌های حیاتی یک کشور را هدف قرار دهد تا این امر توسل به زور تلقی شود. به نظر می‌رسد تا زمانی حمله سایبری علیه زیرساخت‌های حیاتی کشور نباشد، حمله تلقی نخواهد شد. بااین‌حال دو مشکل وجود دارد. اول اینکه، این رویکرد بسیار گسترده است و این نتیجه را در پی دارد که یک عملیات سایبری درصورتی‌که فقط باعث ایجاد ناراحتی شده یا صرفاً هدفش جمع‌آوری اطلاعات باشد، به‌عنوان توسل به زور واجد شرایط نمی‌شود. دوم اینکه، تعریف عمومی پذیرفته‌شده‌ای از زیرساخت‌های ملی حیاتی وجود ندارد و این مساله ممکن است بسته به مفهوم در کشورهای مختلف منجر به عملکرد متفاوتی شود. هر دو رویکرد مبتنی بر ابزار و هدف دارای این مزیت واضح هستند که یک حادثه به‌راحتی طبقه‌بندی می‌شود؛ اما آن‌ها برای درک پیچیدگی عملیات سایبری بسیار ظریف بوده و از سوی دیگر فراگیر نیز می‌باشند. رویکرد مبتنی بر پیامد یا اثر، بیشتر از دو رویکرد دیگر موردحمایت و پذیرش قرارگرفته است و واضح است که دولت‌ها بیشتر، نگران پیامدهای یک عملیات سایبری هستند تا سلاح یا ماهیت هدف. ایالات‌متحده اشاره‌کرده است که جوامع بین‌المللی به‌احتمال‌زیاد بر پیامدهای یک حمله سایبری تمرکز خواهند کرد تا مکانیسم آن. درواقع هدف این رویکرد شناسایی عملیات سایبری است که مشابه سایر اقدامات غیر جنبشی یا جنبشی است که جامعه بین‌المللی آن را به‌عنوان توسل به زور توصیف می‌کند. بااین‌حال، این دیدگاه این مساله را در نظر نمی‌گیرد که وابستگی جوامع مدرن به رایانه‌ها، دستگاه‌های رایانه‌ای و شبکه‌ها امکان ناتوانی زیرساخت‌های فیزیکی را بدون تخریب آن‌ها فراهم کرده است. به‌علاوه، ارزیابی عواقب حمله به‌طور عینی دشوار است و مسائل مربوط به ناحیه خاکستری بیشتری رخ خواهد داد (US Department of Defense, 1999).

۴. قابلیت اجرای حقوق بر جنگ[4] و حقوق بشردوستانه در مخاصمه سایبری

این سؤال که چگونه می‌توان حقوق بین‌الملل بشردوستانه را در جنگ سایبری به کار برد، تنها پس‌ازاینکه برای اولین بار مشخص شد که یک دولت ممکن است به‌طور مشروع از زور برای پاسخ دادن به آنچه «حملات سایبری» تصور می‌کند استفاده کند، قابل‌بررسی است. تعیین این امر باید در چارچوب حقوق بر جنگ صورت بگیرد، یعنی آن دسته از هنجارها و رویه‌هایی که تعیین می‌کنند چه زمانی یک دولت می‌تواند یا نمی‌تواند به‌طور مشروع از زور به‌عنوان ابزار حل اختلاف استفاده کند.

حقوق بر جنگ بر اساس منشور ملل متحد، متضمن تفاسیر منشور و حقوق بین‌الملل عرفی است. اصطلاحات «استفاده از زور»، «تهدید زور» یا «حمله مسلحانه» در منشور سازمان ملل تعریف نشده است. بااین‌حال، دولت‌ها می‌دانند که برخی از اقدامات غیردوستانه، ازجمله تصمیم‌های تجاری نامطلوب، تحریم، قطع روابط دیپلماتیک، انکار ارتباطات، جاسوسی، رقابت یا تحریم‌های اقتصادی و اجبار اقتصادی و سیاسی صرف‌نظر از مقیاس تأثیرات آن‌ها، به سطح یک توسل به زور افزایش نمی‌یابد. حمله مسلحانه ممکن است شامل جنگ اعلام شده، اشغال قلمرو، محاصره دریایی و استفاده از نیروی مسلح علیه قلمرو، نیروهای نظامی یا غیرنظامیان خارج از کشور باشد. بااین‌حال، هیچ سابقه‌ای مبنی بر اینکه چگونه یک عملیات سایبری یک حمله تهاجمی در نظر گرفته شود، وجود ندارد (Lin, 2010: 63).

[4] Jus ad bellum

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال دوم | شماره اول | بهار ۱۴۰۲

گرچه نظر حقوقدانان و به‌ویژه حقوقدانان بین‌المللی در مورد معنای واقعی بند ۴ ماده ۲ منشور سازمان ملل متحد موجود هست و این ماده یک دولت را از تهدید یا استفاده از «زور» علیه دولت دیگر در جامعه بین‌المللی منع می‌کند اما در مواد ۳۹ و ۴۲، منشور دو استثنا در خصوص این ممنوعیت توسل به زور وجود دارد: ۱- اقدامات مجاز توسط شورای امنیت و ۲- اقدامات دفاع مشروع طبق ماده ۵۱ منشور ملل متحد.

۱،۴. اختیارات شورای امنیت

شورای امنیت این صلاحیت را دارد که به اعضای ملل متحد اجازه دهد که در زمان استفاده از هر اقدامی علیه کشوری دیگر که درصدد تهدید و توسل زور علیه یک عضو دیگر ملل متحد است شرکت کنند (منشور ملل متحد، مواد ۴۱ و ۴۲). بااین‌حال، شورا تنها در صورتی می‌تواند این کار را انجام دهد که طبق ماده ۳۹ به این نتیجه رسیده باشد که اقدامات یک دولت «تهدیدی برای صلح، نقض صلح یا اقدام تجاوزکارانه» است. تجربه نشان داده است که دستیابی به تصمیمات اتخاذی وفق ماده ۳۹ و انجام توصیه‌ها جهت متوقف کردن توسل به زور بسیار دشوار است.

اکثر چنین تصمیماتی تنها پس از بررسی‌های دقیق و وقت‌گیر اتخاذ می‌شوند و حتی در آن صورت نیز چنین تصمیماتی مشمول حق وتوی اعضای دائم شورای امنیت است (ماده ۲۷ منشور سازمان ملل). بر این اساس، با توجه به ماهیت مبهم حملات سایبری و عدم اطمینان در مورد اینکه آیا شورای امنیت به چنین حملاتی به‌موقع پاسخ خواهد داد یا خیر، به نظر می‌رسد این فرض درست‌تر باشد که یک دولت با استناد به حق دفاع مشروع در مقابل حملات سایبری از خود دفاع کند.

۲،۴. دفاع مشروع

حق یک دولت برای انجام اقدامات دفاعی، حقی نیست که توسط ماده ۵۱ منشور ملل متحد ایجاد شده باشد. منشور صرفاً بر این حق ذاتی حقوق بین‌الملل عرفی برای بقای دولت‌ها در جامعه بین‌المللی تأکید کرده است[۵]. درحالی‌که در تحلیل حق دفاع مشروع باید به مفاد ماده ۵۱ و حقوق بین‌الملل عرفی توجه شود، اجماع بین‌المللی گسترده‌ای در مورد این موضوع بسیار اساسی وجود دارد. اگرچه همیشه چندین نظریه در مورد انواع اقدامات دولتی که «حملات مسلحانه» را تشکیل می‌دهند وجود داشته است، بی‌تردید یک دولت دارای حق ذاتی در پاسخ دفاعی «مناسب» به چنین حمله‌ای است.

ولی سؤال اصلی اینجاست که دفاع مشروع مناسب چیست؟ دفاع زمانی مشروع است که با دو اصل اساسی «ضرورت» و «تناسب» مطابقت داشته باشد. زمانی که مشخص شود در شرایط حاکم، دولت نمی‌تواند از راه‌های مسالمت‌آمیز به یک حل‌وفصل معقول اختلاف دست یابد، شرط ضرورت برآورده می‌شود و شرط «تناسب» هم مستلزم آن است که دولت اقدامات دفاعی از خود را به میزان نیروی موردنیاز برای پس راندن یک حمله در حال انجام یا جلوگیری از حمله آینده محدود کند. بدیهی است رعایت این اصل بستگی به شرایط خاص آن وضعیت دارد (Wingfield, 2000: 136).

حملات سایبری پیچیده به‌گونه‌ای طراحی شده‌اند که سیستم‌های رایانه‌ای یک دولت هدف را به‌طور آنی تحت تأثیر قرار دهند. البته حملات سایبری وجود دارد که ممکن است یک دولت پیش‌بینی کند و با آن‌ها مقابله کند. ممکن است یک دولت شواهدی از تلاش مهاجمان سایبری برای نفوذ به شبکه پیدا کند، ممیزی سیستم‌های رایانه‌ای ممکن است بدافزارهای غیرمجاز را آشکار کنند، یا دولت‌های هدف ممکن است یک گروه آنلاین را کشف کنند که به‌عنوان محل تجمع هکرها برای تجارت اطلاعات و ابزارها، قبل از حمله هماهنگ عمل می‌کند. در چنین مواردی، دولت هدف قبلاً از یک حمله سایبری برنامه‌ریزی شده آگاه بوده و ممکن است در صورت برآورده شدن معیارهای اصل کارولین، از حق خود برای پاسخ‌گویی در قالب دفاع مشروع پیش‌بینی شده استفاده کند (Gervais, 2012: 530). در صورت مواجهه، یک دولت ممکن است به‌طور قانونی سرورهای میزبان گروه آنلاین را که در آن مهاجمان سایبری در آن جمع می‌شوند غیرفعال کند، با این فرض که دولت هیچ وسیله دیگری برای جلوگیری از حمله‌های قریب‌الوقوع ندارد.

۵. قرارگیری عملیات سایبری بر اساس بند ۴ ماده ۲ در سطح توسل به زور

ازآنجایی‌که رویکرد پیامدها به‌خودی‌خود راهنمایی چندانی در مورد نحوه در نظر گرفتن عملیات سایبری ارائه نمی‌دهد، پیشنهاد شده است که دولت‌ها عوامل مختلفی را در نظر گرفته و در هنگام تصمیم‌گیری در مورد اینکه آیا یک عملیات سایبری معادل توسل به زور

[۵] ماده ۳۸ اساسنامه دیوان بین‌المللی دادگستری

است دقت زیادی داشته باشند. این عوامل عبارت‌اند از: شدت، فوریت، مستقیم بودن، تهاجمی بودن، قابل‌سنجش بودن اثرات، ویژگی نظامی و دخالت دولت. این عوامل جامع نبوده و معیار دقیق حقوقی نیستند، بلکه بسته به شرایط، دولت ممکن است به سایر عوامل نیز توجه نماید؛ مانند محیط سیاسی حاکم، هویت هکر، هرگونه سابقه عملیات سایبری توسط هکر و ماهیت هدف. درواقع این عوامل مؤثر به‌طور هماهنگ عمل می‌کنند؛ به این معنی که چندین عامل با درجه اهمیت متفاوت و بسته به نوع حمله می‌توانند وجود داشته باشند. این معیارها برای تجزیه بسیاری از ویژگی‌هایی که نیروی مسلح را شناسایی می‌کنند مفید هستند و به این معنا که هرچه شدت، فوریت و مستقیم بودن بیشتر باشد، احتمال اینکه این عملکرد منتسب به یک نیروی مسلح باشد، بیشتر است (Schmitt, 2017: 49). فوری بودن حمله راهی برای توصیف مدت‌زمان نیرو است. اگر حمله در عرض چند ثانیه تا چند دقیقه محقق شود و دولت را غافلگیر کند و به آن فرصتی برای جلوگیری یا خنثی کردن آن ندهد، احتمال بیشتری وجود دارد که عملیات سایبری به‌عنوان توسل به زور توصیف شود و این حمله ممکن است هفته‌ها یا ماه‌ها طول بکشد. از سوی دیگر، بدافزار ایجادکننده این اثرات می‌تواند پیچیده باشد و بسته به اینکه خود را بازتولید کرده و رایانه‌ها یا دستگاه‌های دیگر را آلوده کرده باشد، در طول زمان اثرات متفاوتی ایجاد کند. محدوده کلی چنین بدافزاری به‌سختی قابل‌شناسایی است و بنابراین تعیین اثرات ناشی از آن ممکن است دشوار باشد. در حقیقت بی‌واسطگی و مستقیم بودن ارتباط نزدیکی باهم دارند و هرچه یک عملیات سایبری بیشتر به سمت هدف هدایت شود، حمله به هدف فوری‌تر خواهد بود. مستقیم بودن حمله به رابطه میان عمل اولیه و پیامدهای ناشی از آن اشاره دارد. درواقع هرچه مستقیم‌تر باشد، احتمال توسل به زور بیشتر است (Harold, 2012: 96).

بااین‌حال، غیرمستقیم بودن یکی از مشخصه‌های معمول حملات شبکه رایانه‌ای است. نمونه‌هایی از این حملات غیرمستقیم عبارت‌اند از: دست‌کاری سیستم‌های ماهواره‌ای موقعیت‌یابی جهانی[6]، غیرفعال کردن سیستم‌های کنترل ترافیک هوایی و یا دست‌کاری در داده‌های گروه خونی بیمارستان‌ها که درنتیجه گروه خونی اشتباه به سرباز داده می‌شود. با اشاره به اثرات ثانویه و فرعی، همه این موارد اقداماتی هستند که برای دستیابی به نتیجه مطلوب نیاز به اقدام بیشتر توسط بازیگر یا هدف دوم دارند. این ویژگی‌های غیرمستقیم در قضیه نیکاراگوئه نیز بررسی شده است، جایی که آموزش چریک‌ها به معنای توسل به زور تلقی گردید.

اگر تصور کلاسیک از زور به‌عنوان نیرویی که منجر به آسیب، جراحت یا از دست دادن جان می‌شود به‌عنوان یک اثر اولیه (مانند موارد مربوط به یک سلاح جنبشی) باشد، حمله سایبری هرگز تحت بند ۴ ماده ۲ قرار نخواهد گرفت. بر اساس دانش موجود در مورد اثراتی که یک حمله سایبری ممکن است ایجاد کند، این تفسیر رضایت‌بخش نیست. اتکای شدید جامعه مدرن به سیستم‌های اطلاعاتی به‌هم‌پیوسته به این معنی است که اثرات غیرمستقیم و ثانویه حملات سایبری ممکن است بسیار بیشتر از حملات مستقیم و فوری باشد.

نتیجه‌گیری

کاملاً قابل‌تصور است که یک حمله سایبری آسیب فیزیکی ایجاد نکرده و درنتیجه بند ۴ ماده ۲ را نقض نکند. برخلاف ادعاهای موجود این بدان معنا نیست که چنین حملاتی لزوماً قانونی هستند. هدف نشان دادن این است که حملات سایبری که آسیب فیزیکی ایجاد نمی‌کنند، اما اثرات مخربی دارند، ممکن است همچنان با اصل عدم‌مداخله مغایرت داشته باشند. حمله سایبری بر اساس حقوق بین‌الملل عرفی، یک مداخله غیرقانونی است که می‌تواند به‌عنوان اعمال عمدی اجبار علیه یک دولت در رابطه با موضوعی تلقی شود که آزادانه حق تعیین آن را دارد. حملات سایبری علیه استونی در سال ۲۰۰۷ نمونه خوبی از حملات سایبری است که به‌منزله مداخله غیرقانونی است؛ بنابراین آشکار است که اصل عدم‌مداخله نشان‌دهنده یک ابزار حقوقی بین‌المللی قدرتمند است که می‌تواند توسط دولت‌ها برای محافظت از آن‌ها در برابر حملات سایبری اجباری استفاده شود.

در این پژوهش بررسی شد که تا چه حد می‌توان حملات سایبری را تحت رژیم موجود حقوق مخاصمات مسلحانه تنظیم کرد. چارچوب این حقوق هم از بعد توسل به زور و هم از بعد حق بر جنگ برای دولت‌هایی که به دنبال تعیین دامنه حملات سایبری تهاجمی و تدافعی مجاز هستند، راهنمایی‌هایی هرچند ناقص، ارائه می‌کند، ولی اکثریت قریب به‌اتفاق حملات سایبری را تنظیم نمی‌کند. بیشتر حملات سایبری به سطح حمله مسلحانه نمی‌رسد یا اینکه در چارچوب یک درگیری مسلحانه صورت نمی‌گیرد. درنتیجه، آن‌ها مشمول قواعد موجود مخاصمات مسلحانه نیستند. این بدان معنا نیست که این حملات سایبری غیرقابل‌کنترل هستند. چارچوب‌های حقوقی متعدد

[6] Global Positioning System (GSP)

دیگری مانند قواعد بین‌المللی، اقدامات متقابل، قوانین داخلی و غیره وجود دارد که شکاف‌های باقی‌مانده توسط حقوق مخاصمات مسلحانه را پر می‌کند. حملات سایبری ماهیت جهانی دارند و تغییرات در قوانین داخلی و سیاست جرم‌انگاری حملات سایبری، نمی‌تواند به‌اندازه کافی و مؤثر اقدامی را که واقعاً یک مفهوم بین‌المللی است، مهار کند. این تهدید جهانی ممکن است تنها با یک راه‌حل جهانی توسط جامعه بین‌المللی که با یکدیگر همکاری می‌کنند تا قواعد جدیدی برای حملات سایبری طراحی کنند، به‌طور مؤثر می‌تواند پاسخ داده شود. چنین امری باید با توافق نسبت به تعریف اصطلاحاتی چون حمله سایبری، جنگ سایبری، خسارت، توسل به زور، درگیری مسلحانه و همچنین تمایز و تناسب آغاز شود.

در ارزیابی کاربرد حقوق مخاصمات مسلحانه برای تهدیدات سایبری، ابتدا باید به اصول مربوط به توسل به زور توجه کرد که در حال حاضر مشروعیت توسل به زور توسط یک دولت را تعیین می‌کند. بررسی اجمالی این هنجارها نشان می‌دهد که یک دولت ممکن است به‌طور قانونی در هنگام اقدام برای دفاع مشروع در برابر حمله مسلحانه به زور متوسل شود، مشروط بر اینکه با مفاهیم حقوق بین‌الملل عرفی در مورد ضرورت و تناسب مطابقت داشته باشد. در بررسی سه مدل تحلیلی که برای تسهیل تعیین اینکه آیا استفاده خاص از زور به سطح یک حمله مسلحانه ارتقا یافته است یا خیر، می‌توان نتیجه گرفت که برخی از حملات سایبری را می‌توان حملات مسلحانه تلقی کرد. همان‌طور که نشان داده شد تا آنجا که به حقوق بین‌الملل مربوط می‌شود، عملیات سایبری تابع اصول و قواعد مسلم حقوق بین‌الملل هستند. بااین‌حال، انتقال این قواعد به یک دامنه جدید برخی پرسش‌های دشوار را ایجاد می‌کند و همان‌طور که بررسی شد یک عملیات سایبری می‌تواند به‌منزله توسل به زور و حمله مسلحانه تلقی شود، زیرا مقیاس و اثرات حمله باعث مرگ یا جراحت افراد یا آسیب رساندن به اموال می‌شود و در مواردی با خساراتی که توسط سلاح‌های جنبشی ایجاد می‌شود قابل‌مقایسه است. مقایسه مداوم با سلاح‌ها و عملیات‌های جنبشی می‌تواند مفید باشد، اما منحصربه‌فرد بودن عملیات سایبری را کاملاً نشان نمی‌دهد و انطباق با مفاهیم کلاسیک شواهد، دفاع مشروع و اقدامات متقابل را دشوار می‌سازد.

منابع

- Benetar, Marco. (2009). "The Use of Cyber Force: Need for Legal Justification?" Goettingen Journal of International Law, Vol 1, No 3.
- Brownlie, Ian. (1963). *International Law and the Use of Force by States*, Published online by Cambridge University Press.
- Brownlie, Ian. (2012). *International Law and the Use of Force by States*. Oxford: Oxford University Press.
- Dinstein, Yoram. (2001). *War Aggression and Self-Defence*, Cambridge: Cambridge University Press.
- Farer, Tom J. (1985). "Political and Economic Coercion in Contemporary International Law", The American Journal OF International Law, Vol 79, No 2.
- Garner, Bryan A. Ed. (2009). *Black's Law Dictionary*, 9th Ed, Minesota: Publisher West Group.
- Gervais, Michael. (2012). "Cyber-Attacks and the Laws of War. Berkeley", Journal of International Law, Vol 30, No 1.
- Harold. Hongju Koh. (2012). "International Law in Cyberspace", Harvard International Law Journal, Vol 54, No 1.
- I.C.J. (1986). Military and Paramilitary Activities in and against Nicaragua (Nicar V. US). 14 (June 27).
- I.C.J. (1986). Nicaragua Judgment: Military and Paramilitary Activities in and against Nicaragua (Nicar. V. US), 1986 I.C.J. 14 (27 June), para 228. (hereinafter: Nicaragua) The facts in the judgment will be presented below.
- I.C.J. (1996). Advisory Opinion on the Legality of Nuclear Weapons, ICJ Reports 1996, para 39. (hereinafter Advisory Opinion).
- I.C.J. (2005). Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda) 116, 165 (Dec. 19).
- Joyner, Catherine. (2001). "Information Warfare as International Coercion: Elements of a Legal Framework", European Journal of International Law, Vol 12, No 5.
- Lin, Herbert S. (2010). "Offensive Cyber Operations and the Use of Force", Journal of National Security Law & Policy, Vol 4, No 1.
- Morth, Todd A. (1998). "Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter", Journal of International Law, Vol 30, No 2.
- Nguyen, Reese. (2013). "Navigating Jus ad Bellum in the Age of Cyber Warfare", California Law Review Journal, Vol 101, No 4.
- O'Connell, Mary Ellen. (2012). "Cyber Security Without Cyber War", Journal of Conflict & Security Law, Vol 17, No 2.
- Roscini, Marco. (2010). *World Wide Warfare: Jus ad bellum and the Use of Force* Publisher Martinus Nijhoff.
- Schmitt, Michael. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*, New York: Cambridge University Press.
- Simma, Bruno, Mosler, Hermann, Paulus, Andreas and Chaitidou, Eleni. (2002). *The Charter of the United Nations*, 2th ed, Oxford: Oxford University Press.
- Tunkin, Grigory. (1985). *Law and Force in the Interstate System*, Delhi: Progress Publishers.
- U. N. Gen Ass Res. 3314 (XXIX), (1974), https://legal.un.org/avl/ha/da/da.html
- US Department of Defense. (1999). An Assessment of International Legal Issues in Information Operations.

- Waxman, Matthew C. (2011). "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", The Yale Journal of International Law, Vol 36, No 1.
- Wingfield, Thomas C. (2000). *The Law of Information Conflict: National Security Law in Cyberspace*, Publisher by Aegis Research Corp.