نبرد سایبری و موضوع توسل به زور؛ آیا در فضای سایبر حق دفاع از خود معنا دارد؟

دکتر رحمت حاجی مینه[۱]- فاطمه قربانی[۲]

تاریخ دریافت: ۱۳۹۰/۹/۲۰- تاریخ پذیرش:۱۳۹۰/۱۲/۱۶

چکیده:

نبرد سایبری گونه‌ای جدید از سلاح‌ها را به نمایش گذاشته است که بالقوه می‌تواند جایگزین سایر روش‌های ورود به جنگ توسط دولت‌ها و سایر نقش‌آفرینان غیردولتی شود. ماهیت منحصر به فرد تهدید به جنگ سایبری و موضوع توانایی یا ناتوانایی به کار گیرندگان این شکل از جنگ در ایراد جراحت، قتل یا ایجاد ویرانی‌های فیزیکی از طریق فضای مجازی باعث گسترده‌تر شدن تعریف سنتی توسل به زور گردیده است. به منظور ترسیم صریح و واضح حقوق طرف‌های درگیر در نبرد سایبری ـ مانند حق دفاع از خود ـ جامعهٔ جهانی می‌بایست بر سر تعریف نبرد سایبری بر طبق الگوهای ارائه شده در حقوق جنگ موجود به توافق و اجماع برسد.

کلید واژه: نبرد سایبری، حقوق بین الملل، توسل به زور، حق دفاع از خود

[۱]- استادیار و هیات علمی، دانشگاه آزاد اسلامی، واحد تهران شرق، دانشکده علوم انسانی، تهران ایران.
hajrahmat@gmail.com

[۲]- کاندیدای دریافت درجه کارشناسی ارشد، دانشگاه آزاد اسلامی، دانشکده حقوق و علوم سیاسی، تاکستان، قزوین، ایران
fatemehghorbanii@yahoo.com

مقدمه:

نبرد سایبری گونه‌ای جدید از سلاح‌های مدرن است که شدیداً استعداد ایجاد تغیرات بنیادین در عرصهٔ نبردهای مدرن را دارد. فناوری رایانه امروزه تا جایی پیش رفته است که در آن نیروهای نظامی توانایی وارد کردن جراحت، کشتن و ایجاد خسارت‌های فیزیکی از طریق فضای مجازی را دارند. دامنهٔ نبرد سایبری می‌تواند از خشونت‌های شبکه‌ای بی‌ضرر تا حملات شدید به ساختارهای زیربنایی ملی در نوسان باشد. در حالی که از کار انداختن موقت سایت‌های اینترنتی یک دولت شاید آسیب چندانی به آن دولت وارد نکند، تهدید ارائهٔ اطلاعات نادرست به فرماندهان نظامی در صحنهٔ جنگ‌های فیزیکی، یا یک هجمه سنگین به شبکه‌های الکتریکی، آبرسانی، ارتباطی و ترافیکی یک دولت می‌تواند خطراتی جدی برای سربازان و شهروندان دولت مزبور به بار آورد. نفوذ به شبکه‌های اطلاعاتی دولت‌ها و دست‌اندازی به اطلاعات طبقه‌بندی شده آن‌ها که در اصطلاح با عنوان «جاسوسی کامپیوتری» خوانده می‌شود نیز بخشی از گستره نبرد سایبری به شمار می‌رود. این اعمال امروزه به دلیل وابستگی روزافزون آژانس‌های دولتی به ارتباطات الکترونیکی به مراتب ساده‌تر گردیده است. (ضیایی پرور، ۱۳۸۸: ۲۷) علی‌رغم مرگ‌آوری بالقوهٔ نبرد سایبری، این شکل از جنگ در حال حاضر در محیطی قانونی (فضای مجازی) در حال رخ دادن است. [در اینجا نویسندهٔ در پی بیان این مطلب است که به دلیل قانونی بودن استفاده از فضای مجازی، نبردهایی که به اَشکال مذکور در بالا در این فضا اتفاق می‌افتند نیز وجههٔ قانونی به خود گرفته‌اند.] سناریوهای بسیار مخرب ـ مانند امکان استفاده از تکنیک‌های نبرد سایبری در جنگ‌های نامتقارن ـ باعث افزایش احساس نیاز به یک استاندارد واضح و قابل درک برای رفتار در جنگ‌های سایبری گردیده است که از جانب همه شناسایی و مورد احترام واقع شود. این موضوع که آیا استفاده از جنگ‌های سایبری می‌تواند نوعی توسل به زور به حساب آید تا باعث ایجاد حق دفاع از خود گردد یا خیر، تبدیل به یک سؤال مهم در حقوق بین‌الملل گردیده است.

حقوق مدرن در زمینه توسل به زور بر اساس بخش چهارم ماده ۲ منشور ملل متحد شکل گرفته است. البته در منشور ملل متحد تعریف دقیقی از آنچه که توسل به زور به شمار می‌آید ارائه نگردیده است. نه منشور و نه هیچ یک از دیگر ارکان بین‌المللی این اصطلاح را به طور دقیق تعریف ننموده‌اند. تلاش‌ها برای تعریف کردن نبرد سایبری بر اساس مفهوم بخش چهارم ماده ۲ منشور بیشتر باعث دست و پا گیر شدن برداشت‌های سنتی از توسل به زور گردیده است. (حسن‌بیگی،۱۳۸۴: ۲۲-۲۱) آنالیز این موضوع که آیا نبرد سایبری در حقوق جنگ ـ بخشی از حقوق بین‌الملل که بر توسل به زور به عنوان ابزار سیاست داخلی حاکم است ـ قابل پذیرش و بررسی هست یا خیر در منابعی مانند ممنوعیت مطروحه در منشور ملل متحد (بخش۴ ماده۲) در مورد استعمال زور، شمای کلی امنیتی بخش هفتم این منشور، حق ذاتی دفاع از خود که در ماده ۵۱ به آن اشاره شده و حقوق بین‌الملل عرفی که توسط رفتار مستمر دولت‌ها ایجاد شده است قابل قابل جستجو است.(شفیعی، ۱۳۷۵: ۲۵) اگر چه بخش قابل توجهی از حقوق بین‌الملل به توسل به زور توسط دولت‌ها اختصاص دارد، قابلیت اعمال این بخش به فضای مجازی در هاله‌ای ابهام قرار دارد و سؤالات بسیاری حول این مسئله قرار دارد که حقوق بین‌الملل دقیقاً چگونه با نبرد سایبری ارتباط پیدا می‌کند. این مقاله پس از نگاهی کوتاه به تاریخچه نبردهای سایبری به این سؤال اساسی پاسخ خواهد داد که چه چیزی توسل به زور در نبرد سایبری را تشکیل می‌دهد؟ هم‌چنین به سایر سؤالات مرتبط با بحث مانند اینکه حمله مسلحانه در فضای مجازی چیست و آیا اعمال خاصی که از دولت‌ها در نبردهای سایبری سر می‌زند می‌تواند مصداق توسل به زور باشد یا خیر نیز پاسخ داده خواهد شد. پس شناسایی مقررات کلیدی توسل به زور، به مسئله حق توسل به زور برای دفاع از خود و شرایطی که در آن یک دولت می‌تواند به صورت قانونی از این حق استفاده کند پرداخته خواهد شد. قسمت نتیجه‌گیری مقاله شامل بررسی این سؤال است که شیوع نبرد سایبری آیا احتیاج به توسعه اِعمال بخش۴ ماده۲ منشور برای تعریف توسل به زور دارد یا می‌بایست ابزار جدیدی برای برخورد با این تهدید ایجاد شود.

بخش اول: تاریخچه

حملات سایبری گزینه‌ای جذاب برای متخاصمان در درگیری‌های مختلف بوده است. یکی از قربانیان این نبردها ایالات متحده است. این شکل از جنگ به عنوان گونه‌ای از نبردهای چریکی و نامتقارن مورد استفاده قرار می‌گیرد. توهم و ترس از یک حملهٔ غیر منتظره و همه جانبه به ساختارهای زیربنایی حیاتی که باعث از کار افتادن ارکان هسته‌ای و مرکزی کشور می‌شود ـ مانند ارتباطات راه دور، سیستم‌های انرژی برقی، گاز و نفت، بانکداری و سرمایه‌گذاری، حمل‌ونقل، سیستم‌های آبرسانی، خدمات دولتی و خدماتی اورژانسی ـ در گزارش‌های سازمان امنیت ملی و مرکز محافظت از تأسیسات زیربنایی ایالات متحده افزایش یافته است. این مسئله در سایر منابع دولتی نیز مشهود است. (شکرخواه، ۱۳۸۹: ۴۴-۴۱)

در سال ۱۹۹۷، عملیات «الیگیبل ریسیوِر» اولین نبرد اطلاعاتی بود که در ایالات متحده رخ داد و به عنوان نبرد سایبری شناخته شد. در طی ۹ روز نبرد، ۳۵ نفر از جانب یک دولت متخاصم و با استفاده از فناوری‌های تازه اختراع شده و نرم‌افزارهای جدید در جنگ شرکت کردند. سناریو توسط یک دولت متخاصم طراحی شده بود که می‌خواست به جای نبرد فیزیکی با ایالات متحده به سیستم‌های اطلاعاتی آسیب‌پذیر آن حمله کند. یکی از اهداف دولت مزبور این بود که هویت هکرها را پنهان کرده و امکان پاسخ نظامی به این حمله توسط آمریکا را از بین ببرد. چند مورد حمله شبیه‌سازی شده علیه شبکه‌های انرژی و ارتباطی ۹ شهر بزرگ عمده آمریکا صورت گرفت. براساس گزارش-های غیرمحرمانه، سایت‌های اینترنتی دولتی و تجاری در مقابل حمله‌ها نفوذپذیر بودند و تخریب شدند. (سلطانی فر، ۱۳۸۷: ۳۱).

در سال ۲۰۰۱ در یک گزارش که توسط سرویس تحقیقات کنگره آمریکا ارائه شده بود، استفان هیلدرث یکی از متخصصان دفاع ملی از شاخه امور خارجی، دفاع و تجارت ارتش ایالات متحده اظهار داشت که کنگره می‌بایست به سرعت به بازنگری در

سیاست‌ها، سازمان‌ها و چهارچوب‌های قانونی‌ای بپردازد که قوهٔ مجریه را درتصمیم‌سازی در زمینهٔ نبردهای سایبری هدایت می‌کنند. گزارش هیلدرث موضوعات وسیعی در حیطهٔ نبرد سایبری و سؤالات اساسی آن را مورد بررسی قرار داده بود. گزارش مذکور بر جدی و خطرناک بودن این تهدید تأکید کرده بود و اظهار می‌داشت که خطر نبرد سایبری به عنوان یک عرصهٔ قابل تأمل ملی قابل طرح است. (www.mosnews.com) تأثیر حملات سایبری در زندگی واقعی در سال ۲۰۰۷ بر همگان آشکار شد. در این سال هکرهای روسی با به راه انداختن یک هجوم سایبری بین‌المللی باعث شدند که کامپیوترهای دولتی کشور استونی به طور موقت از کار بیفتند. این کار به دلیل حرکت توهین‌آمیز کشور استونی در نبش قبر یک سرباز روسی جنگ دوم جهانی بود. برخی از تحلیل‌گران این هجمه را اولین تهاجم مستقیم روسیه به یکی از اعضای سازمان اتحاد آتلانتیک شمالی (ناتو) دانستند. در سال ۲۰۰۸روسیه دوباره از حملات سایبری برای تکمیل نبرد فیزیکی علیه گرجستان استفاده نمود که این‌بار تعداد زیادی از وب سایت‌های دولتی این کشور را از کار انداخت. یکی از این وب سایت‌های دولتی مربوط به وزارت امور خارجهٔ گرجستان بود. (https://rt.com/usa/news)

روسیه تنها کشوری نیست که از تکنیک‌های نبرد سایبری استفاده می‌کند. آنگونه که گزارش‌های اخیر اشاره کرده‌اند، هکرهای چینی که با ارتش این کشور ارتباط دارند توانسته‌اند با موفقیت وارد پایگاه‌های اطلاعاتی پنتاگون شده و به برخی اطلاعات دسترسی پیدا کنند. مقامات رسمی پنتاگون اعلام کرده‌اند که این مزاحمان اینترنتی از این طریق به جاسوسی پرداخته و اطلاعات زیادی را دانلود کرده‌اند. برخی ادعا نموده‌اند که حمله‌ها مستقیماً از جانب ارتش آزادی بخش خلق ترتیب داده شده‌اند. دولت آلمان نیز به حاکمان چینی اعتراضاتی نموده است که دلیل آن ادعای مورد حمله قرار گرفتن توسط ارتش آزادی بخش خلق بود. نظر به نقاط آسیب‌پذیر ایالات متحده آمریکا، استفاده از زمان برای پیشگیری از مواجهه با یک حمله سایبری حمایت شده از جانب تروریست‌ها که خساراتی برابر با حمله تروریستی ۱۱ سپتامبر دارد حرف نهایی را خواهد

زد. یک گزارش رسمی پنتاگون در سال ۲۰۰۸ که در مورد نیروهای نظامی چین تنظیم شده بود اشاره می‌کند که این کشور در حال آماده‌سازی تاکتیک‌هایی برای به دست آوردن سلطه الکترومغناطیسی بر آمریکا و پس از یک جنگ سایبری است. این گزارش اضافه می‌کند در حالیکه چین هنوز یک دکترین رسمی برای نبرد الکترونیکی ندارد، شروع به استفاده از حملات سایبری در تمرینات عملیاتی خود نموده و به شدت در حال حرکت به سمت وارد کردن جنگ سایبری به واژه‌نامه نظامی، نهادهای مربوطه، تمرینات نظامی و دکترین جنگی خویش است. (www.guardian.co.uk) این حقیقت که حاکمان ملی چنین نفوذ فاجعه‌باری به تمامیت خود را بدون پاسخی که فراتر از یک اعتراض دیپلماتیک باشد نخواهند گذاشت، مشخص خواهد نمود که چه پاسخ‌های حقوقی‌ای برای مقابله با نبرد سایبری وجود دارد.

بخش دوم: بحث اصلی

الف: نبرد سایبری، حقوق معاهدات و عرف‌های بین‌المللی

در سال ۱۹۹۹ وزارت دفاع ایالات متحده آمریکا سندی ارائه کرد که در آن گستره معاهدات بین‌المللی و بخشی از حقوق بین‌الملل که می‌تواند که در مورد به کارگیری نبرد سایبری بر علیه کشورهای دیگر قابل اعمال است را مشخص نموده بود و از آن به عنوان مکملی برای قوانین مختلف آمریکا که هدایتگر این کشور در مورد جنگ‌ها به معنای اعم هستند و هم‌چنین رفتار دولت این کشور در حوزهٔ فضای مجازی به طور خاص استفاده کرد. ارزیابی مذکور در ابتدا نتیجه گرفت که، جامعه بین‌المللی علاقه‌ای به ایجاد فوری بدنه قدرتمندی از قوانین در زمینهٔ موضوع مدنظر ندارد. دومین نکته مطروحه در سند آن بود که هیچ محدودیت یا حوزه حقوقی‌ای وجود ندارد که شکل خاص نبرد سایبری مورد نظر ایالات متحده را مخاطب قرار دهد. سند مذکور به عنوان نکته سوم پیشنهاد کرده بود که اِلمان‌های متنوع و شرایط مختلف هر نوع عملیات یا فعالیت برنامه‌ریزی شده خاص مورد تحلیل قرار گیرد تا مشخص شود که آیا قواعد

حقوقی بین‌المللی کنونی قابلیت اِعمال در این شرایط را دارند یا خیر. (نورمحمدی، ۱۳۹۰: ۷۱) در حال حاضر تعدادی معاهده بین‌المللی وجود دارند که می‌توانند تشکیل دهنده یک عرف بین‌المللی باشند که نهایتاً بتواند در تنظیم نبرد سایبری مورد استفاده قرار گیرد. به عنوان مثال، معاهده روابط از راه دور بین‌المللی (ITC) هرگونه مداخله زیان‌بار با استفاده از ارتباطات از راه دور را ممنوع می‌کند. گرچه تأثیر معاهده می‌تواند به خاطر استثنائاتی که دولت‌ها بر آن وارد می‌کنند محدود شود، اما تشبیه کردن فضای مجازی به فضای جو باعث پدیدار شدن نیاز حیاتی به وجود قوانین بین‌المللی در مورد فضای اینترنت می‌شود. البته تخطی از معاهده (ICT) توسل به زور را آن‌طوری که مد نظر بخش ۴ ماده ۲ منشور ملل متحد است تشکیل نمی‌دهد و بنابراین باعث ایجاد موضع‌گیری مشابهی در میان جامعه بین‌المللی نمی‌شود. (Gordon,1997,p.12) یک سند حقوقی بین‌المللی دیگر که استعداد مرتبط شدن با موضوع را دارد موافقتنامه اجتناب از فعالیت‌های خطرناک نظامی است که در سال ۱۹۸۹بین ایالات متحده آمریکا و شوروی سابق به امضا رسیده بود. این موافقتنامه هرگونه مداخله زیان‌بار در سیستم‌های فرماندهی و کنترلی دشمن را ممنوع کرده بود که می‌توانست به عنوان امکان ایجاد عرفی شناخته شود که حملات واقع شده در فضای مجازی را نوعی توسل به زور به شمار می‌آورد. (Kelsey,2008)

در دهه نهم قرن بیستم با افزایش توجه رسانه‌ها به مفهوم نوظهور نبرد سایبری، در جامعه بین‌المللی تلاش‌هایی برای مذاکراتی برای انعقاد معاهده‌ای در این باب صورت گرفت. روسیه در اکتبر سال ۱۹۹۸ متولی تصویب قطعنامه‌ای در کمیته اول شورای امنیت سازمان ملل گردید که به عنوان تلاشی آشکار برای جلب نظر سازمان ملل به این موضوع شناخته می‌شود. این قطعنامه شامل فراخوانی برای دولت بود که از نظرات آن‌ها در مورد ایجاد نظام‌های حقوقی بین‌المللی به منظور تحدید گسترش، ساخت و استفاده از سلاح‌های اطلاعاتی خاص حمایت کند. این تلاش با استقبال اندکی در جامعه

بین‌المللی مواجه شد و هرگز برای رأی‌گیری عمومی وارد مجمع عمومی سازمان ملل متحد نگردید. (Rid and Mcburney,2012,p.17)

در نتیجه ناکامی جامعه بین‌المللی در تدوین یک موافقتنامه لازم‌الاجرای بین‌المللی، موضوعات حقوقی کلیدی در مورد نبرد سایبری هنوز حل نشده باقی مانده است. موارد مذکور به عنوان مثال شامل نیاز به تعریف استانداردهایی برای تعقیب قطعی ناقضان حقوق، احتیاجات قانونی در مورد نظارت الکترونیکی بر رفتار کشورهایی که از حملات سایبری استفاده می‌کنند و ایجاد قوانین شفاف و مناسب برای درگیری در زمان دفاع سایبری می‌شوند.(همان: ۱۸)

ب: نبرد سایبری، حقوق بین‌الملل و توسل به زور

هر تعداد از مقاصدی که ممکن است یک کشور را تحریک به استفاده از نبرد سایبری کند و بدون در نظر گرفتن هدف، ارزیابی عرفی جامعه بین‌المللی در این زمینه بر این مسئله متمرکز خواهد بود که آیا نبرد سایبری، چه در مقام حمله و چه در قالب اقدام تلافی‌جویانه می‌تواند نوعی توسل به زور غیر قانونی یا تهدید به آن که مخالف با حقوق بین‌الملل باشد تلقی شود یا خیر؟ به منظور ارائه تعریف مؤثری برای نبرد سایبری، جامعه بین‌المللی باید در چارچوب منشور ملل متحد و به خصوص بند۴ ماده۲ منشور که توسل به زور را تنظیم می‌کند و ماده ۵۱ که به حق دفاع از خود اشاره دارد. (محمدعلی پور، ۱۳۸۹: ۴۵-۴۳). بند۴ ماده۲ منشور حاوی قواعد کلیدی حقوق بین‌الملل در زمینه توسل به زور است. این مقررات بیان می‌دارد که «تمام اعضا در روابط بین‌المللی خود از تهدید یا توسل به زور علیه تمامیت ارضی یا استقلال اقتصادی هر کشوری، یا هرگونه اقدامی دیگری که در تعارض با اهداف ملل متحد باشد اجتناب خواهد نمود.» با در نظر گرفتن این چارچوب تحلیلی، سؤال اصلی این خواهد بود که در چه حالتی یک عمل توسل به زور خواهد بود؟ منشور به‌طور آشکاری توسل به زور را غیر قانونی اعلام می‌کند در حالیکه در حق ذاتی دولت برای دفاع از خود جمعی و فردی را

در ماده ۵۱ به رسمیت می‌شناسد. بنابراین، اگر فعالیت‌های یک دولت با توجه به معنای بند۴ ماده۲ تشکیل دهنده نهاد توسل به زور باشد، غیر قانونی خواهد بود مگر آنکه در راستای اعمال حق ذاتی دفاع از خود توسط یک دولت باشد. (همان: ۵۲) در حالیکه تعریف دقیق آنچه که توسل به زور به شمار می‌رود صورت نگرفته است، برخی پارامترهای سازنده این جرم به خوبی تعریف شده‌اند. به عنوان مثال، حمله با استفاده از سلاح‌های متعارف در تعریف موجود در بند۴ ماده۲ گنجانده شده است. از این گذشته، آن دسته از حملات سایبری که به قصد ایجاد مستقیم خسارت فیزیکی به دارائی‌های قابل لمس یا ایراد جراحت به افراد یا کشتن انسان‌ها به راه انداخته می‌شوند ضرورتاً به عنوان استفاده از نیروی نظامی شناخته خواهند شد و متعاقباً مشمول ممنوعیت مدنظر منشور می‌گردند. برعکس، با وجود تلاش‌های کشورهای در حال توسعه برای وارد کردن اجبارها و تهدیدات اقتصادی به عناوین مجرمانه مطرح در بند۴ ماده۲ منشور، این اقدامات صریحاً از این محدوه خارج شده‌اند. بنابراین، تحلیلی که بخواهد بر پایه متن بند۴ ماده۲ یا پیش‌زمینه تاریخی تدوین آن بنا شود نیاز به تفسیری دارد که اجبار یا تهدید اقتصادی و سیاسی را از حیطه دیدگاه این ماده خارج کند. (مدنی، ۱۳۷۳: ۱۱۸) امکان اعمال احتمالی بند۴ ماده۲ منشور در مورد نبرد سایبری مشکلات تفسیری زیادی ایجاد خواهد کرد که دلیل آن هم تمایز موجود میان «زور»و«اجبار یا تهدید» است. وارد کردن تمام فعالیت‌های مرتبط با نبرد سایبری ذیل تعریف توسل به زور نیازمند گسترش عمده دامنه شمول بند۴ ماده۲ است. چنین تعریفی از توسل به زور مانع خارج کردن اجبار یا تهدید از دامنهٔ شمول بند۴ ماده۲ می‌شود زیرا حقوق بین‌الملل می‌بایست میان آن دسته از حملات سایبری که خسارات فیزیکی به جا نمی‌گذارند مانند دزدی الکترونیکی یا محاصره الکترونیکی با فعالیت‌هایی مانند اجبار یا تهدید اقتصادی و سیاسی مانند تحریم اقتصادی که به شکل سنتی از شمول این ماده خارج شده‌اند اما ممکن است تأثیر مشابهی داشته باشند تمایز قائل شود. دو راه ریشه در، طبقه‌بندی حملات سایبری منجر به خسارت فیزیکی و حملاتی که خسارات فیزیکی ندارند در برابر ممنوعیت توسل به زور دارد. (کازنوو، ۱۳۸۷: ۹۱)

مایکل اشمیت در تلاش برای حل مشکل طبقه‌بندی، مرز اجبار و تهدید اقتصادی و سیاسی را با استفاده از ۶ معیار مشخص می‌کند: ۱) شدت،۲) مستقیم و بی‌واسطه بودن، ۳) صراحت،۴) حالت تهاجمی داشتن،۵) قابلیت اندازه‌گیری داشتن،۶) مشروعیت مفروض. بر اساس این مشخصات، عواقب عمل نبرد سایبری با این معیارها سنجیده می‌شوند تا مشخص شود که این عواقب بیشتر شبیه به نتایج نبردهای مسلحانه هستند یا بهتر است که خارج از محدوده ممنوعیت توسل به زور قرار گیرند. به نظر اشمیت، این تکنیک اجازه می‌دهد که محدوده تعریف «زور» گسترش یابد تا خلاءهایی را پر کند که در نتیجه ظهور توان اجبار یک دولت توسط دولت دیگر که ریشه در پیشرفت‌های تکنولوژیکی دارد ایجاد شده بدون اینکه وزن موجود در چهارچوب فعلی را بر هم بزند. (Thomas,2002,p.31-35) با استفاده از تکنیک اشمیت در تعیین اینکه آیا یک حمله سایبری در تعریف اثر محور و انعطاف‌پذیرتر «زور» قابل گنجاندن است یا خیر، ماهیت آن دسته از عواقب عمل که عقلاً قابل پیش‌بینی هستند مورد ارزیابی قرار می‌گیرند تا مشخص شود که آیا به عواقب حملات مسلحانه شباهت دارند یا شباهتی میان این دو وجود ندارد. اگر این عواقب شبیه به نتایج حملات مسلحانه باشد، توسعه گسترده ممنوعیت توسل به زور قابل توجیه است. اما اگر امکان این تشبیه وجود نداشته باشد، نامشروعیت اقدام به حمله سایبری در حقوق بین‌الملل باید با توسل به مقرراتی غیر از آن‌ها که حاوی ممنوعیت توسل به زور هستند تعیین شود. یک روش ساده‌تر که می‌تواند چارچوبی برای تعیین این مسئله باشد، که آیا برخی اعمال خاص صورت گرفته در نبرد سایبری توسل به زور هستند یا خیر روش نتیجه محور است. بر اساس رویکرد نتیجه محوری مطلق، هیچ تفاوتی میان مهاجمی که از راه دور موشکی به یک هدف شلیک می‌کند با فردی که از کامپیوتر برای ایجاد خسارت فیزیکی از راه دور استفاده می‌کند وجود ندارد. اگر یک تهاجم سایبری به همان اهداف دست پیدا کند که استفاده از بمب و گلوله می‌تواند به آن‌ها برسد، بر اساس حقوق بین‌الملل با آن‌ها به صورت یکسان و با استفاده از قوانین حاکم بر توسل به زور برخورد خواهد شد. مشکلی که در مورد رویکرد نتیجه محور وجود دارد آن است این رویکرد، مرزهای میان طبقه‌بندی

سنتی توسل به زور که به عنوان حمله مسلحانه شناخته می‌شود با اجبار و تهدید اقتصادی را کدر و غیر شفاف می‌نماید زیرا اجبار اقتصادی نیز می‌تواند همراه با آثار تخریبی و خسارت‌های فیزیکی باشد. (ضیایی پرور، ۱۳۸۸: ۵۷)

ج: نبرد سایبری و استثناء دفاع از خود

بر اساس منشور ملل متحد، دو استثاء بر اصل ممنوعیت توسل به زور وجود دارد: اقدام شورای امنیت سازمان ملل در راستای ماده۴۲ منشور و دفاع از خود فردی یا جمعی بر اساس ماده۵۱. دانشمندان علم حقوق با وضعیت فعلی حقوق بین‌الملل عرفی در مورد نحوه ارتباطش با توسل به زور و مسئله تفسیر صحیح ماده۵۱ اختلاف نظر دارند. ماده۵۱ منشور بیان می‌دارد:

هیچ چیز در منشور حاضر ناقض حق ذاتی بر دفاع از خود به صورت فردی یا جمعی و در صورت مورد تهاجم مسلحانه قرار گرفتن برای یکی از اعضای ملل متحد نیست، تا زمانی که شورای امنیت اقدامات لازم برای برقراری صلح و امنیت بین‌المللی را اتخاذ کند. اقدامات صورت گرفته در راستای اعمال این حق به سرعت به شورای امنیت گزارش خواهد شد و این اقدامات به هیچ عنوان بر صلاحیت و مسئولیت شورای امنیت بر اساس این منشور و در هر زمان برای اتخاذ هر اقدام لازم که برای حفظ یا بازگرداندن صلح و امنیت ضروری به نظر می‌رسد تأثیری نخواهد گذاشت. (محمدعلی پور، ۱۳۸۹: ۱۱۲) قلمروی ماده۵۱ یکی از موضوعات مشاجره برانگیز میان دانشمندان حقوق بین‌الملل است. برخی دانشمندان این ماده را به صورت مضیق تفسیر کرده و اظهار می‌کنند که هیچ کشوری امکان استفاده از حق دفاع از خود را ندارد مگر آنکه به صورت مسلحانه مورد تهاجم قرار گرفته باشد. بر اساس این برداشت، یک دولت نمی‌تواند به بهانه پیش‌بینی یک حملهٔ مسلحانه اقدام به دفاع از خود کند (دست به اقدام پیشگیرانه بزند). در مقابل، عدهٔ زیادی جانب نظریه مخالفان تفسیر مضیق را گرفته‌اند و از این اعتقاد طرفداری می‌نمایند که در شرایطی خاص می‌توان در عین مشروعیت پیش از

وقوع هرگونه اقدام عملی موسل به زور شد. آن دسته از دانشمندان حقوقی که موافق با نظر دوم هستند اعتقاد دارند که ماده۵۱ منشور حاوی برخی اصول حقوق بین‌الملل عرفی می‌باشد که توسط استاندارد کارولین ایجاد شده است و دفاع پیش‌دستانه را مجاز می‌داند. آنگونه که وزیر کشور دانیل وبستر در پروندهٔ کارولین تعریف کرده است، دفاع پیش‌دستانه زمانی می‌تواند رخ دهد که «ضرورت آن محرز باشد، برجسته باشد و هیچ ابزار دیگری برای انتخاب به جای نگذاشته باشد و هم‌چنین زمان کافی برای ارزیابی وجود نداشته باشد. (ضیایی بیگدلی،۱۳۸۰: ۱۱۱-۱۰۲) براساس الگوی طراحی شده توسط حقوق جنگ، پاسخ یک دولت به حمله مسلحانه دولت دیگر باید سه شرط داشته باشد تا به عنوان دفاع از خود شناخته شود: ضرورت، تناسب و فوریت. برای احراز شرط ضرورت، یک دولت می‌بایست حمله را به یک منبع خاص ارتباط دهد، قصد مهاجم از حمله مشخص و برجسته باشد. اصل تناسب می‌گوید که زور استفاده شده در پاسخ به یک حمله باید با هجوم اولیه تناسب داشته باشد. اصل فوریت، پاسخ به یک حمله پس از گذشت مدت زمان طولانی را ممنوع می‌کند. بر اساس ضابطهٔ فوریت، برای اقدام تدافعی بلافاصله پس حمله مسلحانه مقرره دیگری وجود ندارد. (سلطانی‌فر: ۱۳۸۵) در حوزه نبرد سایبری، برقراری ارتباط میان حمله با یک منبع خاص و تشخیص قصد طرف از این حمله اهمیت بسیار زیادی دارد. عموماً حقوق بین‌الملل به دفاع از خود در مورد اقدام به دفاع فعال در مرزهای بین‌المللی قضاوت نمی‌کند مگر آنکه بتواند انگیزه‌ای را به یک ارگان یا نهاد دولت مورد نظر نسبت دهد. با در نظر گرفتن امکاناتی که فضای مجازی برای اقدام به حمله از راه دور و ناشناس ماندن فراهم می‌نماید، عاملان حملات سایبری علاقه به ناشناس ماندن دارند. «برقراری ارتباط میان حمله و یک منبع خاص این امکان را فراهم می‌آورد که یک دولت به شخص یا مکان بی‌تقصیر حمله نکند. علاوه بر این، یک دولت می‌بایست میان حمله و منبع ارتباط برقرار کند زیرا قوانینی که بر پاسخ مشروع به یک تهاجم حکومت می‌کنند بر اساس دولت بودن یا دولت نبودن مهاجم متفاوت هستند. ممنوعیت موضوع بند۴ ماده۲ منشور در زمینه توسل به زور فقط در مورد دولت‌ها قابل اعمال و استناد است نه دربارهٔ اشخاص. این بدان معناست که

بر اساس حقوق بین‌الملل دولت‌ها از تهدید یا استفاده زور علیه یکدیگر منع شده‌اند در حالیکه اعمال مشابهی که از اشخاص سر می‌زند در حیطه حقوق کیفری داخلی قابل بررسی و قضاوت است. (کاستلز،۱۳۸۰: ۸۸-۸۵) در جائیکه کشف هویت مهاجم کار دشواری است، یافتن قصد و انگیزه او برای اتخاذ اقدامات پیشگیرانه به مراتب مشکل‌تر و پرچالش‌تر است. برای اینکه یک دولت بتواند به اقدام دولت دیگر با استفاده از زور پاسخ دهد، می‌بایست قصد متخاصمانه دولت مهاجم را احراز کند. برخلاف نبردهای فیزیکی متعارف، ماهیت سریع و آنی حملات سایبری باعث می‌شود که قربانی حمله از امکان پاسخ مناسب به هجمه محروم شود. والترگری شارپ در مقام یافتن راه حل برای این مشکل پیشنهاد نمود که تمام کشورها می‌بایست قانونی وضع کنند که به آن‌ها اجازه می‌دهد در راستای اقدام پیش‌دستانه، علیه هر کشور شناسایی شده‌ای که مقاصد خصمانه خود را با استفاده از نفوذ سیستم‌های کامپیوتری حساس و حیاتی کشور نشان می‌دهد متوسل به زور بشوند. (Koepsel,2000,p.65)

بخش سوم: تحلیل و بررسی

تلاش‌های صورت گرفته در راستای ارائه تعریفی از نبرد سایبری در چارچوب الگوهای حقوق جنگ، در راه پیشنهاد سپرهای حفاظتی در مقابل حملات سایبری ناکام مانده‌اند. فناوری ذاتی موجود در نبرد سایبری امکان ایجاد ارتباط میان حمله و یک منبع خاص و یا شناسایی قصد و انگیزه مهاجم را تقریباً غیر ممکن می‌سازد. علاوه بر این، اقدام به حملات سایبری معمولاً به شکل هم‌زمان صورت می‌پذیرد. نظام حقوقی‌ای که احتیاج به شناسایی منبع حمله و هم‌چنین احراز قصد و نیت آن دارد، با این مشخصات دنیای دیجیتال همگونی و تناسب ندارد. الگوی فعلی بین‌المللی گزینه‌های پیش روی کشورها را محدود و امکان عکس‌العمل مناسب در برابر حمله‌های سایبری بدون خطر تخطی از حقوق بین‌الملل را مشکل ساخته است. محدود ساختن توانایی یک کشور به حمله سایبری باعث تشویق شدن دولت‌های متخاصم، گروه‌های تروریست و برخی افراد به استفاده از این ابزار می‌شود. (تومی، ۱۳۸۳: ۱۳۵)

در رویکرد اثر محور چارچوب مایکل اشمیت برای تحلیل نبرد سایبری تحت مفاد بند ۴ ماده۲ منشور، نقایص جدی وجود دارد. با استفاده از فاکتور «مشروعیت مفروض» که در نظریهٔ اشمیت ارائه شده است، برای اثبات مشروعیت یک حمله در حقوق بین‌الملل باید بپرسیم آیا حمله مشروع بوده است؟! (در واقع در اینجا یک دور و تسلسل وجود دارد) در عمل، این یک رویکرد رو به عقب است. علاوه بر این، بر خلاف سایر گونه‌های جنگ، مثال‌های نبرد مسلحانه به سرعت و به شکل آنی در زمان حمله قابل استحصال نیستند تا بتوان بزرگی و عکس‌العمل قانونی نسبت به آن‌ها را مشخص نمود. این مشکل در مورد سایر رویکردهایی که ذکر آن‌ها رفت (رویکرد نتیجه محور) نیز صادق است. (سلطانی فر و هاشمی، ۱۳۸۲) برای مخاطب قرار دادن ماهیت منحصر به فرد نبرد سایبری، حقوق بین‌الملل می‌بایست در تلاش برآید تا از دولت‌هایی که در پاسخ به یک حمله سایبری با حسن نیت عمل می‌کنند حمایت نماید تا بتوانند بدون نیاز به برقراری ارتباط میان حمله و منبع و شناسایی قصد مهاجم اقدام به دفاع از خود در فضای سایبری نمایند. ممکن است نجات یک کشور وابسته به پاسخی سریع، شدید و خشن باشد. بنابراین حقوق بین‌الملل نباید دولت‌ها را در راه دفاع از تأسیسات و نهادهای حیاتی خود وادار به ارائه ملزومات انعطاف‌ناپذیر مانند احراز ضرورت به شکل سنتی کند. (سلطانی فر، ۱۳۸۵: ۷۴) قانون باید به گونه‌ای رشد کند که حق ذاتی دولت‌ها برای دفاع از خود که شامل دفاع پیش‌دستانه در پاسخ به حمله سایبری مخصوصاً حمله‌ای که تأسیسات زیربنایی حیاتی ملی را هدف قرار داده است را به رسمیت بشناسد.

ارائه مجوز به دولت‌ها برای اقدام به دفاع فعال در پاسخ به حمله یک کشور دیگر به تأسیسات زیربنایی حساس بدون اینکه مسئولیتی به کشور تحمیل کند می‌تواند چهارچوب مناسبی برای حکومت بر حوزه نبرد سایبری تحت الگوهای فعلی حقوق جنگ باشد. برای ترسیم این استثناء بر قوانین عادی حاکم بر توسل به زور (توسل به زور در قالب دفاع از خود و در پاسخ به حمله سایبری یک کشور)، جامعهٔ جهانی می‌بایست لیستی از تأسیسات زیربنایی حساس را صادر کند که یک کشور می‌تواند برای دفاع از

آن‌ها به اقدامات دفاعی فعال متوسل شود. اگر تأسیسات زیربنایی حساسی که در لیست شناسایی شده‌اند مورد تهاجم سایبری قرار گیرند، کشور هدف می‌تواند با حسن نیت مفروض (بدون نیاز به اثبات) در پاسخ اقدام به دفاع از خود نماید بدون اینکه پیش از دفاع مجبور به برقراری ارتباط میان حمله و منبع و شناسایی قصد به شکلی باشد که در نظام سنتی مطرح شده است. چنین استثنائی چارچوب حقوق جنگ را به صورت بنیادین تغییر نمی‌دهد اما در عوض به کشور اجازه می‌دهد که در پاسخ به یک تهدید نوین از حق ذاتی خویش که همان دفاع از خود می‌باشد را به کار گیرد.

نتیجه‌گیری:

در منشور ملل متحد پیش از وجود اینترنت نوشته شده است و به همین دلیل نبرد سایبری چالشی جدید برای تعاریف سنتی آنچه که توسل به زور به شمار می‌رود ایجاد نموده است. با وجود دشواری موضوع، به دلیل فراگیر و جدی شدن این تهدید جامعه بین‌المللی می‌بایست بر سر تعریف نبرد سایبری در چارچوب الگوی فعلی حقوق جنگ و ارائه گزینه‌های در دسترس برای دولت‌هایی که هدف چنین تهاجمی قرار گرفته‌اند به اجماع برسد. اگر دولت‌ها توان دفاع از خود در پاسخ به حملات سایبری را بدون محدود شدن توسط تفاسیر تاریخ گذشته از حقوق بین‌الملل حاکم بر توسل به زور نداشته باشند، تهدیداتی بسیار جدی به بار خواهد آمد.

منابع:

- تومی، ایلکا،(۱۳۸۳)، **جامعه دانایی و پرسش های پژوهشی آینده**، ترجمه اسماعیل یزدان پور، تهران: مرکز پژوهش های ارتباطات.
- حسن بیگی، ابراهیم،(۱۳۸۴)، **حقوق و امنیت در فضای سایبر**، تهران: موسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار تهران.
- سلطانی فر، محمد، (۱۳۸۵)، **حقوق بین‌الملل؛ رسانه‌ها؛ صلح و امنیت بین المللی، مطالعات سایبر ژورنالیسم**، تهران: انتشارات دانشگاه آزاد اسلامی.
- .....، (۱۳۸۷)، **اصول جنگ روانی در طراحی سناریوهای خبری**، مجموعه مقالات قدرت سایبر، زیر نظر دکتر سید رضا صالحی امیری، مرکز تحقیقات استراتژیک مجمع.
- شکرخواه، یونس،(۱۳۸۹)، **تکنولوژی‌های ارتباطی و جامعه اطلاعاتی**، تهران: انتشارات انوشه.
- ضیایی پرور، حمید، (۱۳۸۸)، **جنگ نرم۲ ویژه جنگ رسانه‌ای**، تهران: موسسه ابرار معاصر.
- کازنوو، ژان، (۱۳۸۷)، **جامعه شناسی وسایل ارتباط جمعی**، ترجمه باقر ساروخانی و منوچهر محسنی، تهران: نشر اطلاعات.
- کاستلز، مانوئل،(۱۳۸۰)، **عصر اطلاعات - قدرت و هویت**، ترجمه حسین چاوشیان، تهران: انتشارات طرح نو.
- محمد سلطانی فر و شهناز هاشمی، (۱۳۸۲)، **پوشش خبری**، تهران: انتشارات سیمای شرق.
- محمدعلی پور، فریده، (۱۳۸۹)، **دفاع مشروع در حقوق بین الملل**، چاپ اول، تهران: دفتر مطالعات سیاسی و بین‌المللی.
- مدنی، سید جلال الدین، (۱۳۷۳)، **حقوق بین‌الملل عمومی و اصول روابط بین‌دول**، چاپ اول، تهران: نشر پایدار.

- نورمحمدی، مرتضی، (۱۳۹۰)، **سایبر تروریس؛ تروریسم در عصر اطلاعات**، مجموعه مقالات تروریسم و مقابله با آن، چاپ اول، به اهتمام عباسعلی کدخدایی و نادر ساعد، تهران: مجمع جهانی صلح اسلامی.

مقالات

- شفیعی، محمد،(۱۳۷۵)، **بررسی مشروعیت دخالت‌های نظامی بشر دوستانه از دیدگاه حقوق بین‌الملل**، مجله حقوقی شماره ۲۰.

- ضیایی بیگدلی، محمدرضا،(۱۳۸۰)، **مشروعیت جنگ و توسل به زور از دید حقوق بین‌الملل**، مجله سیاست خارجی، سال ۵، ش۲.

منابع انگلیسی

- Gordon,Smith,(1997),**Driving Diplomacy into Cyberspace**,the World Today

- Kelsey,Jeffrey T.G.,(2008),**Hacking into International Humanitarian Law**: The Principles of Distinction and Neutralityin the Ageof Cyber Warfare, Michigan Law Review, Vol. 106.

- Koepsell,David,(2000),**the Ontology of Cyberspace**,Chicago: Open Court

- Rid,Thomas and Mcburney,Pete r,(2012),**Cyber-weapons**,the Rusi journal, No.1.

-Russia Today,26 Jan(2012),**US Launched Cyber Attacks on Other Nations**, https://rt.com/usa/news/us-attacks-cyber-war-615.

- Smith, w.Thomas, (2002), **The New Law of War: Legitimizing Hitech and Infrastructural Violence**, International Studies Quarterierly, Vol. 46, No. 3.

سایت

- https://rt.com/usa/news/us-attacks-cyber-war-615
- www.mosnews.com/news/2004/08/27/internetterror.shtml
- www.guardian.co.uk
- www.nsa.gov