جنگ سایبری از منظر حقوق بین الملل با نگاه به دستورالعمل تالین

سهراب صلاحی[۱]
سید مهدی کشفی[۲]

چکیده

توسعه فناوری، اینترنت و ارتباطات و تجارت رایانه‌ای، با درنوردیدن ثغور، عرصه نوینی از فعالیت‌های انسانی را بازکرده و موجب تضعیف مشروعیت قوانین بر اساس مرزهای جغرافیایی شده است. پدیده حاضر، مرز جدیدی میان دنیای سایبری و دنیای حقیقی به وجود آورده که تهدید بزرگی در مقوله فقدان قانون و همچنین عدم امکان اجرای تمام و کمال قانون احساس می‌شود. استفاده دولت‌ها از فضای ناامن سایبری، زمینه را برای بسیاری از هم نوعان خود جهت خرابکاری، اخلال، ترور، جاسوسی و دیگر جرائم مرتبط هموار ساخته‌اند. اقدام به قانون‌گذاری در برخی کشورها، بسته به میزان پیشرفت در دنیای فناوری، جامعه بین‌المللی را نیز به فکر واداشته که بتواند در این آشفته بازار فضای مجازی، اقدامی هرچند اندک به‌منظور تلطیف این فضا انجام دهد. مقالات و کتب منتشره در سال‌های اخیر تاثیر شگرفی در توجه جهانیان به این جبهه جنگی داشته است. نوشتار حاضر به دنبال پاسخگویی به این سوال کلیدی است که جنگ سایبری چیست و آیا اقدامات مخرب سایبری از سوی کشورها می‌توانند موجد عناصر تجاوز و مشمول جرائم

۱. عضو هیئت علمی گروه حقوق دانشگاه جامع امام حسین (ع) تهران؛ نویسنده مسئول
Salahi.sohrab@gmail.com
۲. دانشجوی دکترای حقوق بین الملل دانشگاه آزاد اسلامی قشم واحد بین الملل

بین‌المللی، توسل به زور و بالتبع مسئولیت بین‌المللی دولت‌ها باشند؟ جهت یافتن پاسخ به چنین پرسشی باید به جستجو در اسناد بین‌المللی همچون منشور ملل متحد، کنوانسیون‌های حقوق جنگ و حقوق بشردوستانه و همچنین دستورالعمل تالین در خصوص جنگ‌های سایبری پرداخت. هرچند دستورالعمل اخیر، از نظر جرم انگاری و ارائه راهکار، با وجود کپی‌برداری از مواد کنوانسیون‌های با موضوع بشردوستانه، بالنسبه جامع و کامل بوده اما ماهیت ارشادی آن، مانع بزرگی در برابر لازم الاجرا و آمره بودن آن می‌نماید. با این وجود، بررسی آن به عنوان تنها منبع بین‌المللی با موضوع حقوق بین‌الملل قابل اعمال در نبردهای سایبری، خالی از لطف به نظر نمی‌رسد.

کلید واژگان: اقدامات مجرمانه سایبری، حقوق بین‌الملل، دستورالعمل تالین، حقوق بین‌الملل بشردوستانه، حقوق مخاصمات مسلحانه

مقدمه

پدیده رو به رشد حملات سایبری در دنیای مجازی، ذهن بسیاری از سیاست‌مداران و حقوق‌دانان را به خود مشغول کرده و این دل‌مشغولی منتج به مقالات و سخنرانی‌ها و ارائه راه حل‌هایی در جهت مقابله با این تهدید بین‌المللی شده است. شاید در گذشته‌ای قریب جنگ‌های زمینی، دریایی و هوایی را بارزترین نمونه روابط خصمانه دانسته و در مواجهه با آن، معاهدات و کنوانسیون‌های گوناگونی در سطح بین‌المللی به تصویب می‌رسید. اما امروزه با ظهور بد افزارهای گوناگون همچون *stuxnet* و *flame*، شبکه‌های گوناگون مجازی، رسانه‌ها و .... امنیت کشورها را به شدت در معرض تهدید قرار داده است. جنگ سایبری، جنگ نرم و جنگ پسانوین تنها بخشی از نام‌هایی است که بر این تهدیدات گذارده شده، با این وجود تک تک این واژگان باید حامل مفهومی از مفاهیم حقوقی بوده و با تعریف‌های مذکور در اسناد بین‌المللی مطابقت کنند.

به نقل از تارنمای سازمان ناتو، اولین حمله سایبری به واقعه کرم موریس در سال ۱۹۸۸ بازمی گردد؛ یکی از اولین کرم‌های شناخته شده که موجب اخلال در زیرساخت‌های سایبری در سر تا سر ایالات‌متحده شد. بنابراین رابرت تاپان موریس،[1] استاد کنونی موسسه فناوری ماساچوست، اولین سازنده کرم‌های رایانه‌ای بود که به گفته وی تنها به دنبال سنجش وسعت فضای اینترنت بوده است. در دسامبر سال ۲۰۰۶، ناسا[2] به دلیل واهمه از هک شدن، ایمیل‌ها با فایل‌های پیوستی خود را پیش از راه اندازی شاتل[3] بست. در آن زمان مجله *بیزینس ویک* گزارش داد که مزاحمان ناشناخته خارجی به برنامه اخیر پرتاب فضایی ایالات‌متحده دست پیدا کرده‌اند.

در آوریل ۲۰۰۷، شبکه‌های دولت استونی به دنبال کشمکش این کشور با روسیه بر سر حذف یادبود جنگ، توسط عوامل خارجی مورد آزار و اذیت قرار گرفته که منجر به اخلال موقت در سرویس‌های دولتی و بسته شدن بانکداری آنلاین این کشور شد. در ژوئن ۲۰۰۷ در پی حملات مستمر به شبکه‌های پنتاگون، ایمیل‌های طبقه‌بندی نشده وزارت دفاع امریکا مورد حمله سایبری قرار گرفت. اکتبر همان سال نیز وزارت امنیت کشور چین از سرقت اطلاعات از مناطق امنیتی این کشور خبر داد. حتی گرجستان نیز از حملات کذایی در امان نبوده و در سال ۲۰۰۸ مقارن با کشمکش این کشور با روسیه، شبکه‌های کامپیوتری آن مورد حمله مزاحمان خارجی قرار گرفت. تنها حمله ۲۰۰۹ به تجاوز هکران به

1. *Robert Tapan Morris*
2. *NASA*
3. *Shuttle*

زیرساخت‌های اینترنتی رژیم صهیونیستی در زمان حمله نظامی به نوار غزه اختصاص داشت. مقامات رژیم صهیونیستی، عاملان حمله مذکور را سازمانی تروریستی واقع در قلمرو شوروی سابق می‌دانستند و مدعی بودند که هزینه آن از سوی حماس یا حزب الله پرداخت می‌شود.

در ژانویه ۲۰۱۰، گروهی موسوم به ارتش سایبری ایران، سرویس موتور جستجوگر محبوب چین، به نام بایدو[1]، را مختل کردند. بدین نحو که کاربران در لحظه ورود به وبسایت، به صفحه‌ای با پیغام سیاسی ایران هدایت می‌شدند. این گروه با همان پیغام سابقه هک کردن سایت تویتر را نیز دارند. اما در اکتبر همان سال بدافزاری به نام استاکس نت در ایران، اندونزی و چند جای دیگر کشف شد که منجر به حدس و گمان‌هایی در خصوص استفاده از این سلاح سایبری علیه برنامه هسته‌ای ایران گردید. از سال ۲۰۱۱ تا ۲۰۱۳ نیز کشور کانادا، وزارت دفاع ایالات‌متحده و مؤسسات مالی کره جنوبی مورد حمله قرار گرفته و همچنین اقدامات امنیتی از طرف ناتو در مقابله با این حملات انجام گرفت. مهم‌ترین تجاوز سایبری در این بازه زمانی از سوی شرکت روسی، کاسپراسکای[2]، به نام "*Red October*" با هدف حمله به کشورهای اروپای شرقی، شوروی سابق و آسیای مرکزی کشف شد؛ هرچند آمریکای شمالی و اروپای غربی نیز به عنوان قربانیان این واقعه گزارش شدند[3].

این نکته نیز مبرهن است که وابستگی جوامع امروزی به فضای سایبری منجر به گزینه‌ای استراتژیک و مناسب جهت خرابکاری برای بازیگران دولتی و غیردولتی شده است. برای مثال، خرابکار سایبری قادر به دسترسی و حمله به بسیاری از خدمات عمومی و خصوصی دولت‌ها از قبیل آب، برق، سامانه‌های بانکی، هوانوردی و همچنین به دلیل پیوستگی سامانه‌ها به یکدیگر، حملات سایبری می‌توانند دارای اثرات علی و معلولی باشند. پس به درستی می‌توان سایبر را پس از زمین، هوا، دریا و فضا، پنجمین جبهه برای جنگ خواند؛ جبهه‌ای ایمن، ارزان و سهل‌الوصول برای مهاجم با حداقل تلفات و در عین حال ویران کننده، در عین حال حمایت از قربانیان آن در حقوق بین‌الملل در هاله‌ای از ابهام است.

حمایت از قربانیان در لوای حقوق بین‌الملل بشردوستانه مستلزم انطباق با تعریف تجاوز و وضعیت مخاصمه مسلحانه بین‌الملل بر طبق بند ۴ ماده ۲ منشور ملل متحد است، هرچند اسناد منتشره در زمینه حقوق بین‌الملل بشردوستانه مانند کنوانسیون‌های چهارگانه ژنو ۱۹۴۹ و دو پروتکل الحاقی ۱۹۷۷ به این کنوانسیون‌ها همچنین تلاش‌های سازمان صلیب سرخ جهانی در این موضوع قادر به پوشش جامع حمایتی برای قربانیان و جبران خسارت‌های وارده به این افراد نمی‌باشد، اما مطالعه و تطابق معاهدات و عرف‌های مطروحه در زمینه حقوق بین‌الملل بشردوستانه با پدیده‌های سایبری کنونی، می‌تواند راهگشای

1. *Baidu*
2. *Kaspersky*
3. *http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm*

قانون‌گذاری‌های آتی و تدوین و توسعه حقوق بین‌الملل در این زمینه باشد که دستورالعمل تالین ناتو به این مهم دست یازیده است. دستورالعمل مذکور توانسته با مطالعات دقیق توسط یک گروه کارشناسی، اقدامات صورت گرفته در فضای سایبری در فضای بین‌المللی را جرم‌انگاری نموده و با در نظر گرفتن حقوق «بر جنگ» و «در جنگ»، جواز و ممنوعیت هریک از اقدامات سایبری، که به اعتقاد کارشناسان می‌تواند مصداق ارکان و اجزای جنگ مسلحانه بین‌المللی قرار گیرند، را تبیین نماید.

پژوهش حاضر در پی تعریف دقیقی از فضای سایبری و اهمیت آن در دنیای کنونی، همچنین اهداف تهدیدات سایبری اخیر و گزیده‌ای از مناقشات عظیم سایبری با نگاه به عناصر جنایت تجاوز و تعریفی از مفهوم تجاوز و منع توسل به زور و طرح آن در موضوعات حقوق بین‌الملل بشردوستانه به عنوان استثنایی از قاعده منع توسل به زور و مسئولیت بین‌المللی دولت‌ها و همچنین پیشنهادهایی جهت رفع نقایص و بسط و توسعه و تحت شمول قرار دادن آن در حقوق بین‌الملل است.

تعریف فضای سایبری

بیش از سه دهه از برقراری اولین ارتباط در شبکه جهانی، که بعدها اینترنت نامیده شد، می‌گذرد. در آن زمان اندک افرادی نفوذ گسترده اینترنت در زندگی شخصی و شغلی انسان‌ها را پیش‌بینی می‌کردند. این شبکه غیرمتمرکز با واژه‌هایی رفیع، همچون ابزار توانمندسازی و دموکراتیزه کردن، توصیف می‌شد. اگرچه ادعای شکل یابی یک دهکده جهانی و در واقع حاکمیت یک فرهنگ خاص بر کل جهان، آنچه به آن «جهانی سازی» گفته می‌شد، که یک کدخدا آن را اداره نماید مبالغه آمیز بود، اما تحول ارتباطات و انتشار سریع لحظه‌ای آن و در نتیجه پیامدهای مثبت و منفی آن بر جوامع و تلاش بعضی قدرت‌ها برای مهندسی افکار جهانی از این طریق قابل کتمان نیست. به این دلیل بسیاری از دولت‌ها به‌وضوح از سوی این قدرت غیر متمرکز تهدید شده و به دنبال اعمال کنترل‌های متمرکزی بر چنین شبکه آشفته‌ای بوده‌اند. ایالات‌متحده اقدام به نظام‌مند کردن ارتباط کلامی از طریق قانون ناموفق نزاکت ارتباطات[1] و ایجاد محدودیت در استفاده از فناوری رمزنگاری توسط طرح بازیابی کلیدی نمود. بسیاری از قانون‌های سخت‌گیرانه از سوی برخی کشورها همچون چین و عربستان سعودی و بعضی کشورهای دیگر اعمال شد. اینترنت و سهامدارانش قاطعانه با اعمال چنین کنترل‌هایی مخالفت ورزیده که این امر به تنش‌ها و مجادله‌های گوناگونی بدل شد. (*Spinello, 2014: 1*).

۱. قانون نزاکت ارتباطات (*CDA*) مصوب ۱۹۹۶ اولین تلاش قابل توجه از سوی کنگره ایالات متحده برای تنظیم پورنوگرافی در اینترنت بود.

در سال ۱۹۸۴ نویسنده‌ای به نام ویلیام گیبسون برای اولین بار واژه فضای سایبری[1] را در رمان علمی تخیلی و موفق خود بانام «نورومنسر»[2] بکار برد. این رمان جمعیت کثیری از دانشمندان علم کامپیوتر فعال در زمینه طراحی و ساخت وب سایت‌ها که سازندگان بعدی دنیای آنلاین بودند را تحت تاثیر قرار داد. نظر گیبسون در مورد فضای دیجیتالی ارتباط و کنترل به بحث‌هایی در خصوص امنیت سایبر انجامید. در عبارت مشهوری در این رمان، گیبسون مجازا فضای مجازی را بدین گونه توصیف می‌کند: «توهم مبتنی بر رضایت طرفین که روزانه از طرف میلیاردها کاربر قانونی از هر ملیتی تجربه می‌شود . نمایش گرافیکی از داده‌های انتزاعی از بانک‌های هر کامپیوتر در سیستم انسانی. پیچیدگی غیرقابل تصور. خطوط نور در محدوده خارج از فضای ذهن، خوشه‌ها و صور فلکی داده‌ها. همچون چراغ‌های شهر که از دور نمایان هستند.» چنین تصویری از فضای ورا رو که به‌صورت پیچیدگی غیرقابل تصور تعریف شد، بسیار مهیج و متعالی است، اما دیدی موجز و واهی از شبکه‌های کنونی ارائه می‌دهد. در سال‌های اولیه قرن بیست و یکم، باید به شبکه‌ها و فضای سایبری رسید که وابسته به موضوعی متفاوت، مانند فضاهای نافذ با پیچیدگی قابل تصور، باشند (*Reverson, 2012: 15*). پیچیدگی‌های سایبری منجر به بروز بسیاری از تجاوزات شده که در دنیای مجازی عناوین مختلفی می گیرند اما، پیش از ورود به تعریف این مفاهیم، ابتدا باید فضای سایبری را از دیدگاه سازمان ملل از نظر گذراند. سازمان ملل فضای سایبری را بدین گونه تعریف می‌کند: "نظام جهانی سامانه‌های کامپیوتری که توسط اینترنت به هم متصل شده‌اند، زیرساخت‌های ارتباطات، نهادهای کنفرانس آنلاین، پایگاه‌های داده و سازمان‌های اطلاعاتی که به طور عام به نام شبکه شناخته می‌شوند." هرچند چنین نظامی عموما به معنای اینترنت است، اما این اصطلاح ممکن است برای اشاره به فضای اطلاعات الکترونیکی خاص و محدود از یک شرکت یا سازمان‌های نظامی و دولتی و غیره نیز مورد استفاده قرار گیرد (*Andress et al, 2014:4*).

هرچند دستورالعمل تالین فاقد تعریفی جامع و مانع است اما، اقدامات سایبری را در صورتی مخرب می‌داند که کشوری به زیرساخت‌های سایبری کشور دیگر آسیب برساند. همچنین درجای دیگر این دستورالعمل ذکر شده که زیرساخت سایبری عبارت است از منابع ارتباطات، ذخیره‌سازی و محاسباتی که بر اساس آن سامانه‌های اطلاعاتی عمل می کنند. ظاهرا این آسیب باید فیزیکی باشد چون اقداماتی از قبیل نظارت، خارج از تعریف گروه کارشناسی تنظیم‌کنندگان می‌نماید (*Schmitt,2013: 24,25*).

- تجاوز سایبری: تجاوز به اموال دیگران و یا ایجاد خسارت – مانند هک، خرابکاری و ویروس‌ها
- تقلب و دزدی سایبری: سرقت (پول و اموال) – برای مثال جعل کارت‌های اعتباری و نقض مالکیت معنوی

---

1. Cyberspace
2. Neuromancer

• هرزه نگاری سایبری: فعالیت‌های ناقض قوانین مربوط به هرزگی و نجابت

• خشونت سایبری: ایراد یا تحریک به وارد ساختن خسارت بدنی نسبت به دیگران و درنتیجه نقض قوانین مربوط به حمایت از اشخاص – همچون سخنان کینه توزانه و تعقیب و مزاحمت (Reyes et al, 2007: 27-28).

• تروریسم سایبری: حمله به سامانه‌های اطلاعاتی، کامپیوترها و داده‌ها یا به‌طور عام اختلال در زیرساخت‌های حیاتی سامانه‌های اطلاعاتی. به تعبیر پلیت[1] (۱۹۹۷) "تروریسم سایبری حمله‌ای با انگیزه سیاسی و قصد قبلی علیه سامانه‌های کامپیوتری، اطلاعاتی، برنامه‌های کامپیوتری و داده‌هاست که منتج به خشونت علیه اهداف غیر مبارز از سوی گروه‌های ملی یا عوامل مخفی می‌شوند"(Janczewski, 2008: 139).

• جنگ سایبری: جنگ سایبری توسعه سیاست‌ها در فضای مجازی توسط عوامل دولتی و غیردولتی است که به منزله و یا در پاسخ به تهدید جدی علیه امنیت ملی انجام می‌گیرد (Shakarian et al, 2013: 2). لازم به ذکر است که تاکنون در نظام، هیچ کشوری به جنگ سایبری استناد نکرده و تمام وقایع را به صورت حمله یا تجاوز خوانده‌اند. اما به عقیده نگارنده «جنگ سایبری را باید به‌کارگیری هدفمند قوای سایبری یک کشور، شامل مجموعه اقدامات پیوسته رایانه‌ای، در جهت تخریب، ضربه یا تصرف کشور هدف دانست که می‌تواند از طریق کنترل و تخریب زیرساخت‌های اطلاعاتی و امنیتی یک کشور انجام گیرد». آنچه در این تعریف ضروری می‌نماید لفظ «هدفمندی» و «پیوستگی» است که جنگ سایبری را از کنش و واکنش‌های آنی و کوتاه مدت دیگر اقدامات سایبری مجزا می‌کند.

گزیده‌ای از مناقشات بزرگ سایبری

در سال ۱۹۸۲، رئیس جمهوری ایالات‌متحده، ریگان، طرحی از سازمان سیا جهت انتقال نرم افزاری با کاربرد راه اندازی پمپ‌های خطوط لوله کشی، توربین‌ها، و سوپاپ‌ها را با اتحاد جماهیر شوروی به تصویب رساند. نرم افزار مذکور، که پس از آن توسط روس‌ها در کانادا به سرقت رفت، دارای امکانات پنهان بمب منطقی بوده که به جهت اختلال در سرعت‌های پمپ و تنظیمات سوپاپ‌ها طراحی شده بود. دبیر سابق نیروی هوایی ایالات‌متحده و مدیر سابق دفتر شناسایی ملی، توماس سی رید[2] در کتاب خود با نام «در آبیس: تاریخ محرمانه جنگ سرد[3]» نوشت که این بمب منطقی «به غیر هسته‌ای‌ترین انفجار و آتش

1. *Pollitt*
2. *Thomas C. Reed*
3. *At the Abyss: An Insider's History of the Cold War*

که تا به حال از فضا دیده شده بود، منجر گشت.» حمله کذایی تاثیر روانی و اقتصادی شگرفی بر اتحاد جماهیر شوروی گذارده و به عنوان یکی از عوامل پایان جنگ سرد شناخته شد[1].

همچنین ایالات‌متحده در سال ۱۹۹۱ از روش‌ها و ابزار جنگ سایبری در حمله به عراق بهره جست. فاز اول عملیات طوفان صحرا با عملیات هوایی استراتژیک و حملاتی بر ضد پدافندهای هوایی عراق، هواپیماها و فرودگاه‌ها، سامانه های فرماندهی و کنترل، امکانات ارتباط از راه دور، و عناصر کلیدی زیرساخت ملی همچون شبکه‌های حیاتی برق، شروع شد. علاوه بر این، ایالات‌متحده از سامانه‌های گسترده ماهواره‌ای و ارتباطی جهت پشتیبانی از این عملیات بهره برد.[2]

جنگ چچن علیه نیروهای روسی در سال ۱۹۹۴ و همچنین جنگ دوم ۱۹۹۷-۲۰۰۱ و کوزوو ۱۹۹۹ از دیگر نمونه‌های جنگ سایبری است. اما در همین سال‌ها یعنی سپتامبر ۲۰۰۰، هکرهای نوجوان رژیم صهیونستی اقدام به ساخت وب سایتی جهت هک کردن وب سایت‌های حماس و حزب‌الله در لبنان نمودند. این افراد در شش وب سایت سازمان‌های حماس و حزب‌الله در لبنان و تشکیلات ملی فلسطین عملیات خرابکارانه و تخریب انجام دادند. چنین حمله کوچکی منجر به جنگی سایبری و به سرعت بدل به اتفاقی بین‌المللی گشت. فلسطینی‌ها و سازمان‌های اسلامی حامی آن‌ها خواستار جنگ مقدس سایبری شدند[3]. بنابراین هکرها به سه وب سایت برجسته متعلق به پارلمان، وزارت امور خارجه، و وب سایت اطلاعات نیروی دفاع رژیم صهیونستی حمله کردند. متعاقبا، افراد مذکور به دفتر نخست وزیر رژیم صهیونستی، بانک رژیم صهیونستی و سازمان بورس تل آویو نیز حمله‌ور شدند.

در ژانویه ۲۰۰۱، این کشمکش منجر به حمله به بیش از ۱۶۰ وب سایت رژیم صهیونستی و ۳۵ وب سایت فلسطینی شد. ۵۴۸ از ۱۲۹۵ وب سایت رژیم صهیونستی فعال در خاورمیانه به طور کلی از بین رفت. این حملات همچنین علیه شرکت‌های تامین کننده زیرساخت‌های ارتباط از راه دور نیز صورت گرفت. سرانجام هکرهای فلسطینی با از بین بردن ارائه دهنده خدمات اینترنتی[4] رژیم صهیونستی، پیغامی مبنی بر توانایی آنان در بستن *ISPNetVision* رژیم صهیونستی، که میزبان حدود ۷۰ درصد تمام ترافیک اینترنت کشور است، ارسال نمودند.

حملات تخریب‌گرانه رژیم صهیونستی بدین جا ختم نشد و این رژیم در سال ۲۰۰۷ طی عملیات باغ میوه[5]، حملات هوایی توسط هواپیماهای اف-۱۵ و اف-۱۶ و هواپیمای خبرنیوشی الکترونیکی[6] در منطقه دیر الزور در نیمه شب ششم سپتامبر ۲۰۰۷ که منجر به تخریب مجتمع الکبر با موشک‌های *AGM-65*

1. *David E. Hoffman, "CIA slipped bugs to Soviets" Washington Post, 27 february 2004*
2. *Jon Trux, "Desert Storm: A space-age war," NewScientist, 27 July 1991*
3. *"Cyber war Also Rages in MidEast," The Associated Press, 28 october 2000*
4. *ISP*
5. *Operation Orchard*
6. *ELINT aircraft*

Maverick و بمب‌های ۵۰۰ کیلوگرمی هدایت لیزری شد، انجام داد. هدف این حمله، راکتور اتمی در دست ساخت توسط تکنسین‌های کره شمالی جهت تولید پلوتونیم بود. گزارشی بیان می‌داشت که گروهی کماندوی رژیم صهیونستی در روز پیش از عملیات به منطقه اعزام شده تا قادر به مشخص نمودن هدف با لیزر باشند. منابع نظامی و صنعتی ایالات‌متحده بر این باور بودند که رژیم صهیونستی‌ها احتمالا از فناوری مشابه سیستم حملات شبکه‌ای هوابرد ساتر امریکا در رادار گریزی استفاده کرده‌اند. در می ۲۰۰۸، منابع اروپایی نیز مدعی منفعل شدن شبکه پدافند هوایی سوریه از سوی رژیم صهیونستی شدند؛ اطلاعات مشابهی نیز از سوی نشریات *Aviation Week* و *Space Technology* مطرح شد (*Schreier,2015:107-111*).

دستورالعمل تالین[1] ناتو در خصوص جنگ سایبری

در سال ۲۰۰۹، سازمان بین‌المللی نظامی واقع در تالین استونی با نام مرکز عالی همکاری دفاع سایبری که در سال ۲۰۰۸ از طرف ناتو به عنوان قطب علمی شناخته شده بود، از گروه بین‌المللی کارشناسان مستقل جهت نگارش دستورالعملی در خصوص قانون حاکم بر جنگ سایبری دعوت به عمل آورد. این پروژه که توسط متخصصین و محققان حقوق بین‌الملل طرح ریزی شد به دنبال تسری هنجارهای حقوقی و قانونی در اینگونه جنگ‌های نوین است. دستورالعمل حقوق بین‌الملل در خصوص جنگ سایبری یا دستورالعمل تالین، که از روندی کارشناس محور نشات گرفته در پی سندی غیر الزام‌آور جهت بسط قانون موجود به جنگ سایبری و همچنین تلاش جهت شفاف‌سازی بیشتر اسناد منتشره پیرامون اقدامات سایبری از سوی دولت‌ها و با توجه خاص به قوانین حقوق بر جنگ و حقوق در جنگ است.

بنابراین دستورالعمل تالین به بررسی حقوق حاکم بر جنگ سایبری پرداخته و به طورکلی دربرگیرنده حقوق بر جنگ، حقوق بین‌الملل حاکم بر توسل به زور از سوی کشورها به عنوان ابزار سیاست ملی، و حقوق در جنگ، حقوق بین‌الملل تنظیم‌کننده رفتار درگیری‌های مسلحانه (که با عنوان حقوق جنگ، حقوق مخاصمات مسلحانه یا حقوق بین‌الملل بشردوستانه نیز شناخته می‌شود) است. عناصر مرتبط حقوق بین‌الملل، مانند مسئولیت دولت‌ها و حقوق دریاها نیز در این دستورالعمل گنجانده شده است.

اقدامات سایبری که در سطح پایین‌تری از مفهوم "توسل به زور" و "مخاصمات مسلحانه" به انجام می‌رسند، در این مقاله مورد بحث واقع نشده است. به عنوان مثال دستورالعمل هیچ گونه اشاره‌ای نسبت به حوزه‌های دیگر قابل اطلاق در حقوق بین‌الملل، همچون حقوق بشر یا حقوق مخابرات، ندارد. مشروعیت فعالیت‌های سایبری تنها در ارتباط با حقوق بر جنگ، مفاهیم توسل به زور و حمله مسلحانه، یا در زمینه

1. *Tallinn Manual*

مخاصمات مسلحانه و حقوق در جنگ مورد سنجش قرار می‌گیرد. اگرچه یکایک کشورها و کسانی که تحت صلاحیت دادگاه‌های آنان قرار می‌گیرند باید منطبق با قانون ملی، مقررات و قانون‌گذاری داخلی خود رفتار کنند، اما دستورالعمل کذایی ملزم به چنین رفتاری نیست. سرانجام، دستورالعمل در خصوص موضوعات مسئولیت کیفری کشورها و حقوق داخلی یا بین‌الملل کاوشی انجام نمی‌دهد.

به طور خلاصه، این دستورالعمل، برخلاف آنچه در کاربرد رایج از آن استنباط می‌شود، در مورد امنیت سایبری نگارش نشده است. جاسوسی سایبری، سرقت مالکیت معنوی و طیف گسترده‌ای از اقدامات کیفری در فضای مجازی تهدیداتی جدی و واقعی علیه کشورها، سازمان‌ها و افراد خصوصی تلقی می‌شوند. واکنش کافی به چنین اقداماتی، مناسبات ملی و بین‌المللی را طلب می‌کند که دستورالعمل تالین به دلیل عدم ایفای نقش لازم توسط حقوق بین‌الملل در خصوص توسل به زور و مخاصمات مسلحانه، این مناسبات را مدنظر قرار نمی‌دهد. حقوق بین‌الملل فاقد کارایی لازم جهت مقابله با تهدیدات حادث در حوزه سایبری است.

تاکید دستورالعمل تالین، در معنای دقیق، بر اقدامات سایبری علیه تجهیزات سایبری، به عنوان مثال به کارگیری اقدامات سایبری علیه زیرساخت‌های حیاتی یک دولت یا حمله سایبری با هدف سامانه‌های کنترلی و فرماندهی دشمن، است. بنابراین هدف این دستورالعمل حول محور اقدامات سایبری علیه تجهیزات مادی، همچون حمله هوایی و بمباران مرکز کنترل سایبری، نمی‌چرخد. همچنین حملات نظامی الکترونیک سنتی، مانند انداختن پارازیت، را نیز دربر نمی‌گیرد. چنین اقداماتی قبلا تحت حقوق مخاصمات مسلحانه تعریف شده‌اند. در آخر باید خاطرنشان کرد که دستورالعمل تالین دربرگیرنده هردو مخاصمات مسلحانه بین‌المللی و غیر بین‌المللی است (*Schmitt,2013:16-19*).

دستورالعمل فوق الذکر را می‌توان نمونه تقریبا جامعی از جرم انگاری و قانون‌گذاری در پدیده سایبری در سطح بین‌الملل دانست اما به دلیل ماهیت صرفا علمی، غیر الزام‌آور بودن و ارشادی آن، استناد صرف به آن در این نوشتار خالی از اشکال نیست. از این رو در بحث‌های آتی به دنبال مدد از دیگر اسناد و مطالعات بین‌المللی در خصوص تبیین موضوعات حقوق بین‌الملل در برابر اقدامات سایبری خواهیم بود، بنابراین چون قرار دادن اقدامات سایبری علیه کشورها تحت شمول مفهوم تجاوز، تعریفی دقیق از این مفهوم را می‌طلبد، در بخش بعدی ابتدا مفهوم تجاوز و منع توسل به زور در حقوق بین الملل تعریف شده سپس به تطابق این نظریات با اقدامات سایبری خواهیم پرداخت.

مفهوم تجاوز و منع توسل به زور در روابط بین‌الملل

اولین معاهداتی که در آن‌ها تجاوز تعریف و اعمال تشکیل دهنده آن برشمرده شده، معاهدات معروف به معاهدات لندن یا پیمان‌های عدم تجاوز است که در تاریخ‌های ۳، ۴ و ۵ ژوئیه ۱۹۳۳ میان اتحاد جماهیر شوروی سابق و برخی کشورهای دیگر از جمله ایران، افغانستان، استونی، لتونی، ترکیه، رومانی و لهستان منعقد شده است. طبق این معاهدات، موارد زیر تجاوز محسوب شده و عامل آن متجاوز شناخته می‌شود:

۱) اعلان جنگ به یک کشور.
۲) حمله و تهاجم مسلحانه به قلمرو یک کشور.
۳) محاصره دریایی یک کشور.
۴) کمک به گروه‌های مسلح جهت حمله به قلمرو یک کشور و اعطای پناهندگی به آنان.
۵) حمله مسلحانه به کشتی‌ها و هواپیماهای یک کشور

با این حال مفهوم تجاوز جایگاه رفیعی در منشور ممل متحد داشته و این امر موجب مباحثات گسترده‌ای در کنفرانس سانفرانسیسکو گردید (ضیائی بیگدلی، ۱۳۸۰، ص ۲۸). همان‌گونه که دولت‌های بزرگ ذی نفوذ در اجلاس تدوین منشور ملل متحد اصل تساوی حاکمیت همه اعضای جامعه بین‌الملل را پذیرفتند، به ممنوعیت مطلق تهدید یا اعمال زور نیز، تن دادند. نماینده آمریکا در اجلاس سانفرانسیسکو اعلام کرد که منع توسل به زور در روابط بین‌الملل یک ممنوعیت کلی و مطلق است. این گونه بود که بر اساس ماده ۲ (۴) منشور ملل متحد «کلیه اعضا باید در روابط بین المللی خود از تهدید یا استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی هر دولت و یا از هر طریق دیگری که با مقاصد ملل متحد تباین داشته است، خودداری ورزند».

بدین ترتیب طبق منشور ملل متحد تهدید به زور یا اعمال آن تحت هر شرایطی به استثنای مواردی در فصل هفتم (اقدامات اجرایی دسته جمعی) و ماده ۵۱ (دفاع مشروع) تصریح گردیده، ممنوع شده است. در عین حال امید آن بود که موارد مجاز توسل به زور در روابط بین‌الملل دستاویز پیشبرد منافع سیاسی و اقتصادی دولت‌های صاحب امتیاز وتو نگردد، اما چنین نشد. به علاوه قدرت‌های بزرگ در بسیاری از موارد برای وادار ساختن دولتی دیگر به منظور نادیده گرفتن و عدول از حاکمیتش و یا برای کسب هرگونه امتیاز غیرداوطلبانه از آن دولت، فشارهای اقتصادی را در دستور کار خود قرار دادند و بعضی دولت‌های ضعیف را از نظر اقتصادی فلج می‌کردند. فقدان هرگونه قاعده‌ای که این نوع رفتار را ممنوع گرداند شدیدا مورد اعتراض کشورهای جهان سوم واقع می‌گردید و در بسیاری از موارد آن‌ها را مجبور به کسب حمایت دولت‌های سوسیالیستی در دوران جنگ سرد کرد. مشکل غامض‌تر اینکه، با وجودی که توسل به زور در منشور ملل متحد به عنوان عامل تهدیدکننده صلح و امنیت جهانی شناخته شد ولیکن

تعریف «جنایت تجاوز» به عنوان مهم‌ترین عامل تهدیدکننده صلح و امنیت تا اجلاس کامپلا (۲۰۱۰) در هاله‌ای از ابهام ماند (صلاحی، ۱۳۹۴، صص ۲۴۷-۲۴۹).

اولین کنفرانس بازنگری اساسنامه دیوان کیفری بین‌المللی در ۳۱ می ۲۰۱۰ در کامپلا (پایتخت اوگاندا) رسما آغاز به کار نمود و در این اجلاس، بند اول ماده ۸ مکرر اساسنامه به تصویب رسید که در ارتباط با تعریف جرم تجاوز اشعار می‌دارد: «برنامه‌ریزی، تدارک، شروع یا اجرای اقدام تجاوزکارانه توسط صاحب منصبی که به نحو موثری اقدام سیاسی یا نظامی یک دولت را کنترل یا هدایت می‌کند، با توجه به ماهیت، شدت و گستره آن، موجب نقض آشکار منشور ملل متحد می‌شود». در بند دوم نیز به احصای مصادیق جنایت تجاوز پرداخته و بیان می‌دارد: «تهاجم یا حمله به سرزمین دولت دیگر به وسیله نیروهای مسلح یک دولت، یا هر نوع اشغال نظامی هرچند موقت که از چنین تهاجم یا حمله‌ای ناشی شود، یا هر نوع ضمیمه کردن تمام یا بخشی از سرزمین دولت دیگر با استفاده از نیروهای مسلح، بمباران سرزمین دولت دیگر یا به کار بردن سلاح علیه سرزمین دولت دیگر ...»(صلاحی،۱۳۹۱، ص،۱۶۲).

جایگاه اقدامات سایبری از منظر منع توسل به زور و مفهوم تجاوز

موضوع قابل بحث در این بخش تحت شمول قرار دادن اقدامات سایبری در حوزه قواعد منع توسل به زور در روابط بین‌الملل است. اگرچه لازم به ذکر است که قصد اعمال فشار جهت شناسایی و تشخیص عملیات سایبری به عنوان اعمال نیروی نظامی مستکفی نیست. هرچند نیروی نظامی چیزی جز شکل افراطی از مداخله، همچون فشار دیپلماتیک و اقتصادی، به‌منظور وادار کردن کشور قربانی به انجام عملی خاص نخواهد بود. به همین ترتیب، اگر عملیات سایبری بدین منظور مورد استفاده قرار گیرد، به راحتی آن را می‌توان از اقسام اعمال زور قرار داد (*Roscini,2014:45*).

همان‌گونه که مشاهده شد، عملیات سایبری می‌تواند از سوء استفاده سایبری جهت جمع آوری اطلاعات، شناسایی و نظارت گرفته تا حملات سایبری و همچنین از حذف، خراب کردن و تغییر داده و نرم افزار گرفته تا ایجاد خسارات بر زیرساخت‌های اموال و اشخاص را شامل می‌شود. چنین تنوع اقدامات در عملیات سایبری موجب نظریات گوناگون در تحت شمول قرار دادن آن در اقسام اعمال زور شده است (*Ibid: 52*).

کارشناسان حقوقی در نشست تالین پیوسته به دنبال حکمی حقوقی در خصوص اقسام توسل به زور و یا بسط حقوق بر جنگ بوده‌اند، بدین جهت به رأی مشورتی دیوان بین‌المللی دادگستری استناد شد. در

رأی مشورتی مذکور با عنوان تسلیحات هسته‌ای، دیوان مقرر داشت که "توسل به زور"، همان‌گونه که درخصوص دفاع مشروع ذکر شد، می‌تواند صرف نظر از به کارگیری هر نوع سلاح تحقق یابد[1].

بنا بر چنین رویکردی، توسل به اقدامات سایبری علیه دیگر کشورها، خواه به تنهایی خواه در جریان اقدامات دیگر، نیز می‌تواند واجد شرایط حقوق بر جنگ باشد. همچنین می‌تواند دارای چارچوب قانونی محکم جهت اقدامات دفاعی در برابر مخاصمات مسلحانه و یا اقدامات سایبری صرف باشد. اگرچه این طرز نگرش نسبتا در سطح جهانی پذیرفته شده است اما پرسش اینجاست که چگونه می‌توان این هنجارها را در فضای سایبری به کار بست.

دیوان بین‌الملل دادگستری در تفسیر بند ۴ ماده ۲ منشور که اعمال زور علیه کشورها را تحریم می‌کند، ضمن رأی نیکاراگوئه بیان می‌دارد که چنین ممنوعیتی قاعده‌ای عرفی در حقوق بین‌الملل را تشکیل می‌دهد، همچنین در رأی اقدامات نظامی، دیوان این بند را سنگ بنای منشور می‌داند.

پس اقدامات سایبری را می‌توان تحت شمول بند فوق الذکر دانست، مشروط بر اینکه به موجب قانون مسئولیت بین‌المللی دولتی چنین اقداماتی توسط دولت‌ها و یا حداقل قابل انتساب به دولت‌ها باشند. همان‌گونه که توسل به زور الزاما شامل اعمال مستقیم نیروی نظامی توسط دولت‌ها و یا گروه‌ها یا افراد تحت کنترل آن‌ها نیست، در اقدامات سایبری نیز، برای مثال بد افزارهای مخرب یک گروه شورشی و آموزش نحوه استفاده از آن، می‌تواند تحت شمول اعمال زور قرار گیرد (*Weller, 2015: 1112-1114*).

دستورالعمل تالین توسل و تهدید به توسل به زور را در اقدامات سایبری تعریف نموده و هردو آنان را ممنوع دانسته است. چنین اقداماتی مغایر اصل تمامیت ارضی و استقلال سیاسی کشورها و همچنین اهداف سازمان ملل تلقی شده‌اند. تاثیرات و اندازه اقدامات سایبری به جهت اطلاق به توسل به زور و غیرقانونی خواندن آنان را باید با اقدامات غیر سایبری در سطح توسل به زور مقایسه نمود (*Schmitt,2013:45-53*).

تهدیدات سایبری از دیدگاه حقوق و عناصر جنگ

پیش‌نیاز اعمال حقوق مخاصمات مسلحانه، وجود مخاصمات مسلحانه است که با وجود اهمیت فراوان در بحث این نوشتار نمی‌گنجد چون تاکنون هیچ یک از موجودیت‌های بین‌المللی گزارشی از وقوع جنگ سایبری ارائه نداده‌اند. تنها نمونه کاربرد حقوق مخاصمات مسلحانه را در عملیات سایبری ضمن

---

۱. مشروعیت تهدید یا استفاده از تسلیحات هسته‌ای، رأی مشورتی ۸ جولای ۱۹۹۶، مذکور در گزارش دیوان بین المللی دادگستری ۱۹۹۶

مخاصمات مسلحانه بین‌المللی میان گرجستان و روسیه در سال ۲۰۰۸ می‌توان مشاهده کرد که در پیشبرد جنگ مذکور انجام گرفت. برای مثال اگر حمله هکرها پس از جنگ میان دو کشور رخ دهد آنگاه هکرهای مسبب این حمله سایبری به‌طور مؤثر همانند سربازان در جنگ شرکت داشته، جنبه حقوقی پیدا می‌کنند (*Gladyshev et al, 2015: 139*).

حقوق بین‌الملل در خصوص عملیات سایبری نیازمند جنگجویان نظامی است تا از قواعدی از قبیل اصل ضرورت نظامی، تمایز میان نظامیان و غیر نظامیان، تناسب، احترام به افراد و اشیای مورد حمایت، بی طرفی و منع روش‌های جنگی خاص (مانند نقض تعهد) پیروی کند. اگرچه تردیدهایی در خصوص اعمال قوانین جهت عملیات سایبری در طول مخاصمات مسلحانه وجود دارد اما اختلاف‌هایی در مورد سهولت یا دشواری ارزیابی چنین عملیات‌هایی تحت این قواعد مطرح می‌شود. ناکامی در تعریف جنگ و بیان اقسام روش‌های جنگی، گنجاندن اقدامات سایبری در حقوق جنگ را دشوار می‌کند. برای مثال اختلال در سامانه‌های اطلاعاتی افراد را نمی‌توان معادل حمله به غیر نظامیان دانست چون حمله به عنوان خشونت علیه دشمن تعریف می‌شود و به دلیل اینکه ممکن است از اینترنت جهت عملیات نظامی استفاده شود و همچنین به علت ارتباط فناوری‌های اطلاعاتی مختص نظامیان و غیر نظامیان، این اقدام سایبری مشروع شناخته شود (*Reveron,2012*).

بسط حملات سایبری در استثنائات منع توسل به زور

با اینکه هیچ تعریف معتبر و حقوقی از "جنگ سایبری" یا "حمله سایبری" در حقوق بین‌الملل عمومی و معاهدات خاص، حقوق عرفی و دکترین موجود نیست اما توصیفاتی عملی بر پایه فناوری و نحوه عملکرد آن وجود دارد. وزارت دفاع ایالات‌متحده تعاریفی از مفاهیم اقدامات سایبری از قبیل حمله به شبکه‌های رایانه‌ای، دفاع از شبکه‌های رایانه‌ای و استثمار شبکه‌های رایانه‌ای را ارائه داده است. بدین ترتیب حمله به شبکه‌های رایانه‌ای به صورت " استفاده از رایانه جهت ایجاد اختلال، تنزل یا تخریب اطلاعات موجود در رایانه و شبکه‌های رایانه‌ای یا خود رایانه‌ها و شبکه‌ها" تعریف شده است؛ همچنین تعریف دفاع از شبکه‌های رایانه‌ای به شرح زیر است: "حفاظت، نظارت، تحلیل، تشخیص و واکنش از طریق فعالیت‌های مجاز شبکه‌های کامپیوتری و سامانه‌های اطلاعاتی وزارت دفاع" و سرانجام استثمار شبکه‌های رایانه‌ای بدین صورت تعریف شده است: "اقدامات و قابلیت‌های جمع‌آوری اطلاعات از طریق شبکه‌های رایانه‌ای جهت گردآوری داده‌ها از هدف یا شبکه‌ها یا سامانه‌های اطلاعاتی خودکار". درمجموع اینگونه اقدامات، در صورت حادث شدن در درگیری‌های نظامی، می‌توانند جنگ سایبری محسوب شوند.

اگرچه کمیته بین‌الملل صلیب سرخ در تبیین حوزه سایبر در جنگ در مطالعات عرفی حقوق بین‌الملل بشردوستانه سال ۲۰۰۵ از خود بی پروایی نشان نداد اما، به‌صورت علنی در دست کم دو متن رسمی موضع سازمانی خود را در قابلیت اعمال حقوق بین‌الملل بشردوستانه در اقدامات سایبری در درگیری‌های مسلحانه اظهار نمود. کامل‌ترین بیانیه کمیته بین‌الملل صلیب سرخ به قرار زیر است:

این حقیقت که یک فعالیت نظامی خاص به‌طور ویژه نظام‌مند نشده، به معنی استفاده بی‌حد و حصر از آن نیست. از نظر کمیته بین‌الملل صلیب سرخ، ابزار و روش‌های جنگی موسوم به فناوری سایبری، همانند هر نوع سلاح یا سیستم جدید که تاکنون وجود داشته و در مخاصمات مسلحانه استفاده می‌شده، موضوع حقوق بین‌الملل بشردوستانه قرار می‌گیرد. در مجموع، علی رغم نوین بودن فناوری، محدودیت‌های قانونی درمورد ابزار و روش‌های جنگی موسوم به فناوری سایبری اعمال می‌شود. در حالی که ماده قانونی حقوق بین‌الملل بشردوستانه در تحریم صریح آن وجود ندارد، واضح است که اقدامات سایبری در مخاصمات مسلحانه تنها می‌تواند در چارچوب حقوق موجود قرار گیرد. کمیته بین الملل صلیب سرخ به دنبال توسعه خود در ارتباط با استفاده از فضای سایبری با مقاصد نظامی و دستیابی به تاثیر بالقوه نظامی آنها با نظر به مشارکت و نظارت حقوق بین‌الملل بشردوستانه خواهد بود.

به همین نحو کمیته صلیب سرخ در سازمان ملل، صریحا جنگ سایبری و در نتیجه کاربرد حقوق بین‌الملل بشردوستانه مورد اطلاق کمیته بین‌الملل صلیب سرخ را به نحو ذیل منحصر به همراهی و تداخل حملات مسلحانه و اقدامات سایبری نموده است:

... کمیته بین‌الملل صلیب سرخ توجه کشورها را به پیامدهای بالقوه حقوق بین‌الملل بشردوستانه در جنگ سایبری، یعنی حمله به شبکه‌های رایانه‌ای در طول وضعیت مخاصمات مسلحانه، جلب کرد. این پیامدها می‌تواند شامل حالات فاجعه‌آمیز همچون مداخله در سامانه‌های کنترل عبور و مرور هوایی و در نتیجه تصادم و سقوط هواپیماها، قطع جریان آب و برق شهرها یا تخریب تاسیسات هسته‌ای و شیمیایی باشند. بنابراین کمیته فوق خواستار الزام تمام طرفین مخاصمات در رعایت قواعد حقوق بین‌الملل بشردوستانه در خصوص ابزار و روش‌های جنگ سایبری با لحاظ اصول تفکیک، تناسب و احتیاط در حمله شد (*Saxon,2013: 210-220*).

مهم‌ترین موضوع مطرح در اقدامات سایبری سردرگمی در مورد حدود و تعریف زمانی رخداد این پدیده و اصطلاح "حمله" در حقوق بین‌الملل بشردوستانه و "حمله نظامی" در حقوق بر جنگ است. با توجه به بیانیه تفسیری کمیته بین‌الملل صلیب سرخ که اصطلاح حمله را معادل اقدام نظامی می‌داند، یقینا حمله به شبکه‌های سایبری لزوما باید در این زمینه صورت گرفته تا بدان لفظ حمله اطلاق شود. اما صلیب سرخ در بیانیه اخیر خود، عدم قطعیت قانونی را بیان کرد:

... بی‌شک با وجود مخاصمات مسلحانه، حقوق بین‌الملل بشردوستانه در صورت توسل به اقدامات سایبری در معیت سلاح‌های سنتی بکار گرفته خواهد شد. اما وخامت مسئله در زمانی بروز خواهد کرد که حقوق بین‌الملل بشردوستانه بخواهد در وضعیت اقدامات سایبری صرف در مخاصمه کارایی پیدا کند. آیا چنین وضعیتی را می‌توان تحت کنوانسیون‌های ژنو و دیگر معاهدات بشردوستانه، مخاصمه نظامی دانست؟ آیا نوع وضعیت در اطلاق آنان تفاوت خواهد داشت؟ پاسخ به این پرسش‌ها تنها به عملکرد دولت‌ها در آینده برخواهد گشت.

بنابراین حمله سایبری به استونی در ۲۰۰۷ و به‌کارگیری کرم استاکس نت علیه نیروگاه هسته‌ای نطنز ایران در ۲۰۱۰ را نمی‌توان مشمول حقوق بین‌الملل بشردوستانه دانست چرا که مفهوم "حمله" در آن‌ها تحقق نیافته‌اند (*Ibid:223*).

اما در صورت حمله و تحقق جنگ و توسل به زور، استناد به یکی از استثنائات منع توسل به زور از نظر سازمان ملل، حق دولت‌ها در دفاع مشروع، است که در ماده ۵۱ منشور ملل متحد منعکس شده است. ماده مذکور مقرر می‌دارد که: "در صورت وقوع حمله مسلحانه علیه یک عضو ملل متحد تا زمانی که شورای امنیت اقدام لازم برای حفظ صلح و امنیت بین‌المللی را به عمل آورد هیچ یک از مقررات این منشور به حق ذاتی دفاع از خود، خواه فردی یا دسته جمعی لطمه‌ای وارد نخواهد کرد. اعضا باید اقداماتی را که در اعمال این حق دفاع از خود به عمل می‌آورند فورا به شورای امنیت گزارش دهند. این اقدامات به هیچ وجه در اختیار و مسئولیتی که شورای امنیت بر طبق این منشور دارد و به موجب آن برای حفظ و اعاده صلح و امنیت بین‌المللی و در هر موقع که ضروری تشخیص دهد اقدام لازم به عمل خواهد آورد تاثیری نخواهد داشت."

حق دفاع مشروع منحصرا جهت جبران خسارت از قربانی حمله نظامی مطرح شده، از آنجا که چنین حمله‌هایی ذیل بند ۴ ماده ۲ منشور و حقوق عرفی به "توسل به زور" و الزامات قانونی آن شده است. در مقابل، دفاع مشروع، واکنش دفاعی مؤثر (از نظر ماهیت، ذات، استمرار و محدوده) بوده که در غیر اینصورت دربرگیرنده توسل غیرقانونی به زور از سوی یک کشور خواهد بود. بنابراین می‌توان استدلال نمود که دفاع سایبری منفعل، که تنها سعی بر بازدارندگی حمله دارد، دفاعی قانونی است. تنها درخصوص دفاع فعال، خواه در ماهیت سایبری و خواه فیزیکی، قانون دفاع مشروع مستقیما از سوی دولت یا گروه درگیر در مخاصمه به منصه ظهور می‌رسد.

علاوه براین، تنها دولت‌ها از حق دفاع مشروع برخوردارند، بنابراین نهادهای خصوصی، همچون شرکت‌هایی که مورد حملات سایبری قرار می‌گیرند، نمی‌توانند بر طبق حق دفاع مشروع و صرفنظر از شدت آن واکنشی نشان دهند. واکنش آنان تابع قوانین داخلی و بین‌المللی خواهد بود. اما، حمله سایبری علیه دولت‌های ملی ممکن است حملات نظامی تلقی شده و دولت مذکور به‌طور مؤثر از خود دفاع به

عمل آورد. لازم به ذکر است که الزامات دفاع مشروع از قبیل فوریت، قطعیت و فقدان زمان برای تامل باید وجود داشته باشد (*Committee on Deterring Cyberattacks,2010:162-163*).

مواد ۱۳ تا ۱۷ دستورالعمل تالین به دفاع مشروع و شرایط توسل به دفاع از قبیل ضرورت، تناسب و فوریت و همچنین حق دفاع مشروع اختصاص یافته است. در ماده ۱۷ این دستورالعمل، دولت‌ها را به ارائه گزارش اقدامات سایبری صورت گرفته در اعمال حق دفاع مشروع مورد نظر ماده ۵۱ منشور ملل متحد به شورای امنیت سازمان ملل ملزم می‌دارد (*Schmitt,2013:53-65*).

حملات سایبری و مسئولیت بین‌الملل دولت‌ها

در کنار اهمیت بلامنازع اینترنت، رایانه‌ها و زیرساخت‌های سایبری برای هر کشور و ارکان و نهادهای وابسته به آن، استفاده ناصحیح و خصمانه از آن‌ها نیز می‌تواند بسیار خطرناک جلوه کند. از این‌رو دولت‌های ملی محتاج اطمینان خاطر از شبکه‌های حامی امنیت و اقتصاد ملی خود می‌باشند. بنابراین نقض امنیت و اصل تمامیت ارضی یک کشور باید برای کشور متخاصم مسئولیت آور بوده تا راه سوء استفاده از این ابزار مفید، ارزان و قابل دسترس بسته شود.

در این قسمت درصدد پاسخ به پرسشی هستیم که آیا استفاده ناصحیح از فضای سایبری و ایجاد ضربه و آسیب به دولت‌های دیگر می‌تواند مسئولیت بین‌المللی برای دولت متجاوز به بار آورد؟ پاسخ به این سوال مثبت خواهد بود، مشروط بر اینکه استفاده نادرست از اینترنت عمل غیر قانونی بین‌المللی تلقی گردد. با این استدلال که با توجه به بین‌المللی بودن قلمرو اینترنت، دولت‌ها باید این قلمرو را مطابق حقوق بین‌الملل اداره کرده و بنابراین استفاده از فضای سایبری موضوع حقوق بین‌الملل قرار گیرد. همانگونه که هارولد کوه، مشاور حقوقی اسبق وزارت امور خارجه امریکا، بیان داشت:" اصول حقوق بین‌الملل در فضای سایبری کارآمد خواهند بود ..." اما چالش‌های اساسی، مانند مسئله مسئولیت دولت‌ها درقبال اعمال اتباع خود، پیش روی حقوق مسئولیت بین‌المللی است. مع الوصف مسئول شناختن دولت‌ها بنا بر اعمال اتباع آن‌ها امری دشوار است مگر اینکه تنها حالتی متصور شود که دولت‌ها مستقیما موجب حمله و اخلال در زیرساخت‌های سایبری دولتی دیگر شوند.

دیوان بین‌المللی دادگستری بارها به مسئولیت بین‌المللی دولت‌ها به دلیل نقض تعهدات بین‌المللی استناد نموده است. در معروف‌ترین این موارد، قضیه تنگه کورفو، دیوان مقرر داشت که صرف وجود مین در محدوده سرزمینی دولت آلبانی نمی‌توان دولت مذکور را مسئول دانست بلکه دیوان به دلیل عدم اطلاع به وجود منطقه مین‌گذاری شده در دریای سرزمینی به کشتی‌های کشورهای ثالث از سوی آلبانی، حکم به مسئولیت بین‌المللی وی را صادر کرد. از نظر دیوان، این التزام متکی بر سه اصل کلی است: اصول ابتدایی

بشری، آزادی ارتباطات دریایی و تعهد هر دولت اجازه نمی‌دهد که آگاهانه از قلمرو خود برای اعمالی مخالف با حقوق کشورهای دیگر استفاده کند. دیوان در این مقوله شرایط واقعی دیگری را نیز در نظر گرفت که اگر آلبانی در لحظات آخر، برای مثال کمتر از ۲۴ ساعت از لحظه برخورد کشتی‌های جنگی انگلستان، از مین گذاری اطلاع می‌یافت، عدم اطلاع او به کشورهای ثالث به دلیل سختی و یا عدم امکان مجاز شمرده می‌شد. مسئله مسئولیت بین‌المللی در قضایای دیگری مانند کنگو علیه اوگاندا، ژنوساید بوسنی و غیره نیز مطرح شد.

بر اساس تحلیل‌های ارائه شده، می‌توان مسئولیت دولت‌ها به جهت اعمال غیرقانونی بین‌المللی دولت‌ها در فضای مجازی مبنی بر تلاش بر نقض حقوق دیگر کشورها در سرزمین آنان را متصور شد. تلاش دولت‌ها در نقض حقوق دیگر کشورها می‌تواند بدین گونه ارزیابی شود که نخست استفاده از اینترنت فی‌نفسه غیرقانونی نیست، دوم انتقال داده از رایانه‌ها الزاما منشأ فعالیت‌های مضر نیستند و سرانجام وجود هزاران رایانه در سرزمین یک دولت به خودی خود به فعالیت‌های مضر تلقی نمی‌شود. بنابراین به محض اطلاع از انجام فعالیت‌های مضر در قلمرو یک کشور و عدم کنترل مؤثر از سوی وی، دولت مذکور باید مسئول شناخته شود حتی اگر اطلاع رسانی از سوی دولت قربانی انجام گیرد (*Tsagourias,2015:67-69*).

در بخش دوم، مواد ۶ تا ۸، دستورالعمل تالین در خصوص مسئولیت بین‌المللی دولت‌ها سخن گفته شده است. دستورالعمل مذکور دولت‌ها را در نقض تعهدات بین‌المللی در اقدامات سایبری مسئول دانسته و همچنین این اقدامات را تعریف نموده است. با این وجود اقدامات سایبری از درون یک کشور بدون کنترل مؤثر آن دولت را از مقوله مسئولیت مستثنی دانسته است (*Schmitt,2013:35-40*).

نتیجه‌گیری

هرچند تاکنون مقررات نظام‌مندی در خصوص اقدامات سایبری و تعریف و گنجانیدن آن در موضوعات حقوق بین‌الملل از سوی سازمان ملل صورت نگرفته اما برخی کشورها همچون ایران، آمریکا، انگلستان و آلمان متضرر از جرائم و حملات سایبری، نوشتارهایی حقوقی صادر نموده‌اند. هرچند چنین تلاش‌هایی از منظر بین‌المللی لازم الاجرا نبوده و در قیاس با مقوله با اهمیت فضای سایبری، که بسیاری آن را پنجمین جبهه جنگی می‌دانند، ناچیز می‌نماید اما می‌تواند جرقه و راهنمایی در تدوین مقررات بین‌المللی محسوب گردد.

با اینکه در مجامع سیاسی انتقادات زیادی به دستورالعمل تالین پیرامون حقوق بین‌الملل قابل اعمال در جنگ‌های سایبری به دلیل تفسیر موسع آن از توسل به زور و قانونی انگاشتن توسل به دفاع مشروع در قالب فضای سایبری، وارد آمده اما با گزارش‌های روزانه از تهاجم انواع کرم‌ها، ویروس‌ها و بد افزارها به زیرساخت‌های سایبری کشورها، مسئله تجاوزات سایبری به حریم کشورها واقعیت غیرقابل انکار بوده و جز گنجانیدن آن در قالب زور و حقوق مخاصمات مسلحانه نمی‌توان قواعد و مقرراتی برای آن تعیین نمود.

دستورالعمل فوق‌الذکر تنها انعکاسی از نظرات گروه کارشناسان مستقل و فاقد هرگونه رسمیتی است، همچنین در مقدمه این سند به صراحت ذکر شده که مفاد حاضر نظریات سازمان ناتو و یا کشورهای متبوع کارشناسان نیست. حقوقدان بین‌الملل هنگام مطالعه دستورالعمل تالین با سندی جدید مواجه نشده بلکه اسناد گوناگون بین‌المللی درخصوص حقوق مخاصمات مسلحانه، بشر دوستانه و مسئولیت بین‌الملل دولت‌ها با جایگزینی اصطلاحات سایبری می‌باشند.

در شرایط کنونی، بررسی قانون حمله به شبکه‌های رایانه‌ای تحت موازین حقوق بین‌الملل پیچیدگی‌های زیادی دارد. تحت قوانین حقوق بر جنگ نیاز به تاثیرات عینی مانند مرگ، مجروحیت یا تخریب اموال عینی ثابت مانده اگرچه راه‌های وصول بدان‌ها غیرمستقیم شده است. قصد و غرض مهاجم نقش بسیار مهمی در تعیین واکنش دولت قربانی ایفا می‌کند. قطعا، قرارگرفتن حمله شبکه رایانه‌ای تحت حمله نظامی و درنتیجه لازم الاجرا شدن حق دفاع مشروع، مستلزم مقیاس و ابعاد کافی خواهد بود.

همان‌گونه که در بخش‌های پیشین گفته شد، اقدامات سایبری در جریان مخاصمات مسلحانه و نظامی به راحتی مصداق پیدا کرده و می‌توان الزامات حقوق بین‌الملل و خصوصا حقوق مخاصمات مسلحانه را بر آن وارد، کرد اما صرف اقدامات سایبری جهت تجاوز به یک کشور تاکنون عنوان مجرمانه‌ای در حقوق بین‌الملل به خود نگرفته و نام‌گذاری آنان به عنوان جنگ، تجاوز و ... عملا مصداق خارجی پیدا نکرده است.

منابع

۱. ضیائی بیگدلی، محمدرضا (۱۳۸۰)، حقوق جنگ، چاپ دوم، تهران، دانشگاه علامه طباطبایی

۲. صلاحی، سهراب (۱۳۹۴)، اشغال عراق؛ اهداف راهبردی و استنادات حقوقی، تهران، نشر میزان

۳. صلاحی، سهراب (۱۳۹۱)، بازخوانی دلایل اشغال عراق از منظر حق توسل به زور و بررسی آثار آن در پرتو حقوق بین‌الملل کیفری، فصلنامه حقوق، مجله دانشکده حقوق و علوم سیاسی، دوره ۴۲، شماره ۴، زمستان ۱۳۹۱، صفحات ۱۵۷-۱۷۶

4. Andress, Jason & Winterfeld, steve (2014), ***Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners****, second edition, USA, Elsevier*

5. Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy (2010), ***Proceedings of a Workshop on Deterring cyberattacks Informing Strategies and Developing Options for U.S. Policy****, Washington D.C., The National Academies Press*

6. Gladyshev, Pavel; Marrington, Andrew & Baggili, Ibrahim (2015), ***Digital forensics and cyber crime****, New York, Springer International Publishing*

7. Janczewski, Lech J. Colarik, Andrew (2008), ***Cyber Warfare and Cyber Terrorism****, New York, Idea Group Inc (IGI)*

8. Reverson, Derek S. (2012), ***Cyberspace and national security: threats, opportunities, and power in a virtual world****, USA, Georgetown University Press*

9. Reyes, Anthony; O'Shea, Kevin; Steele, Jim; Hansen, Jon R. jean, Captain Benjamin R. Ralph, Thomas (2007), ***Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors****, USA, Elsevier*

10. Roscini, Marco (2014), ***Cyber Operations and the Use of Force in International Law****, first Edition, USA, Oxford University Press*

11. Saxon, Dan (2013), ***International Humanitarian Law and the changing technology of war****, Netherlands, Koninklijke Brill NV*

12. Schmitt, Michael N. (2013), ***Tallin Manual on the International Law Applicable to Cyber Warfare****, New York, Cambridge University Press*

13. Shakarian, Paulo; Shakarian, Jana & Ruef, Andrew (2013), ***Introduction to Cyber warfare: A Multidisciplinary Approach****, USA, Elsevier*

14. Spinello, Richard A. (2014), ***Cyberethics: Morality and Law in Cyberspace****, fifth edition, USA, Jones & Bartlett Learning*

15. Tsagourias, Nicholas & Buchan Russell (2015), ***Research Handbook on International Law and Cyberspace****, UK, Edward Elgar Publishing Limited*

16. Weller, Marc (2015), ***The Oxford Handbook of the Use of Force in International Law****, first Edition, UK, Oxford University Press*

17. Schreier, Fred (2015), ***On Cyberwarfare****, DCAF Horizon 2015 Working Paper No. 7*