نشریه‌ی علمی شهر ایمن
JOURNAL OF RESILIENT CITY
(JRC)

بررسی چالش های حقوق بین المللی در مواجهه با حملات سایبری و ارائه راهکارهای مناسب جهت برون‌رفت از چالش‌های مذکور

مهران جابری[۱]؛ آرامش شهبازی*[۲]؛ غلامرضا جلالی[۳]

۱- دانشجوی دکترای مدیریت فناوری اطلاعات دانشگاه علامه طباطبایی، تهران، ایران
۲- استادیار دانشگاه علامه طباطبایی (نویسنده مسئول)
۳- دانشیار دانشگاه عالی دفاع ملی

دریافت دست‌نوشته: ۱۴۰۰/۰۵/۰۶؛ پذیرش دست‌نوشته: ۱۴۰۰/۱۱/۲۰

واژگان کلیدی

حملات سایبری، حقوق بین‌الملل بشردوستانه، مسئولیت بین‌المللی دولت‌ها، مخاصمات مسلحانه

چکیده

جامعه بین‌المللی که در ابتدا متشکل از دولت‌هایی بود که وابستگی متقابل آنها را در کنار هم در یک اجتماع قرار می‌داد، به برکت تحولات بنیادین و چشمگیر ناشی از پیشرفت‌های حاصل از تکنولوژی، ارتباطات و نیاز به تأمین و تضمین ثبات در اثر تهدید ابزارها و سلاح‌های جدید از یک‌سو پذیرای بازیگران جدید در عرصه روابط بین‌المللی گردید و از سوی دیگر آگاهی و نیاز به همگرایی و همبستگی ناشی از وجود منافع مشترک و ارزش‌های انسانی در آن کاملاً بروز یافته است. قسمت‌های مختلفی متأثر از این بحث است. یکی از حوزه‌های مربوطه بحث مسئولیت بین‌المللی دولت بوده است. از دید کمیسیون حقوق بین‌الملل، محور استناد به مسئولیت، مفهوم دولت زیان‌دیده است. از سوی دیگر بحث تروریسم سایبری و تبیین مبانی و ارائه راهکارهای مربوط به آن است و همچنین حملات سایبری و بحث مخاصمات مسلحانه که باید مورد بررسی قرار گیرد. در تمامی این چالش‌ها حقوق بین‌الملل بایستی با ارائه راهکارهایی در جامعه بین‌المللی، بتواند از بروز زیان به افراد و دولت‌ها جلوگیری نماید.

۱- مقدمه

دستیابی بشر به تکنولوژی‌های جدید از جمله فضای سایبری و گسترش روزافزون استفاده از این بستر به دلیل ارزان بودن، سرعت بالا، راحتی در انتقال و دریافت داده‌ها در زمینه‌های مختلف و به‌تبع آن ایجاد بسترها و زیرساخت‌های مهم دولتی در بخش‌های اقتصادی، صنعتی، سیاسی و اجتماعی باعث وابستگی شدید به این فضا شده و برخی از بازیگران بین‌المللی به‌منظور تحمیل خواسته‌های غیر مشروعشان بر دولت‌ها به‌صورت مستقیم و غیر مستقیم از این فضا علیه دولت‌ها متوسل به زور شده و در صدد نفوذ، تخریب یا سرقت اطلاعات مهم و زیرساخت کشورها می‌باشند. لذا فناوری سایبری نیز که در بستر فضای سایبر معنا می‌یابد، به‌عنوان یکی از شیوه‌ها و ابزارهای نبرد امروزی در حال گسترش است و با توجه به مزایای متعددی که در استفاده از این ابزار وجود دارد، در سال‌های اخیر رغبت زیادی جهت کسب دانش و تخصص این‌گونه حملات از جانب کشورها و گروه‌های مختلف، صورت پذیرفته است. حتی تعداد قابل توجهی از کشورها اقدام به ایجاد واحدهای سایبری در نیروهای مسلح خود نموده‌اند که این، خود نشان از اهمیت این‌گونه حملات در جهان امروزی دارد. در مقابل این رغبت فزاینده متأسفانه

* نویسنده مسؤل: دانشگاه علامه طباطبایی، تهران، ایران؛ رایانامه: arameshshahbazi@gmail.com

مقررات جامع و مانعی در خصوص قاعده‌مندسازی حملات سایبری تا به امروز وجود نداشته است و یکی از دغدغه‌های جامعه کنونی بین‌المللی قاعده‌مندسازی این‌گونه حملات در بستر مقررات بین‌المللی است، از طرفی نیز هرچند که حقوق بین‌الملل نتوانسته از بروز منازعه جلوگیری کرده و آن را ریشه‌کن نماید، اما تا حدودی توانسته از شدت فجایع و بحث مخاصمات مسلحانه کم کند.

درعین‌حال در قواعد و مقررات حقوق بین‌الملل همچون بند ۴ ماده ۲ و ماده ۹۳ و ۱۴ و ۱۵ منشور و اصلاحیه‌ای که پس از وقایع یازده سپتامبر در ماده ۴ پیمان ناتو گنجانده شد مبنی بر اینکه ناتو معتقد است پاسخ به حملات سایبری درصورتی‌که به‌موجب آن حمله تمامیت ارزی و استقلال سیاسی و امنیت طرفین پیمان مورد تهدید قرار گیرد و این حملات هنجارهای عرفی عدم مداخله و یا هنجارهای بین‌المللی وابسته به آن را نقض کند اجازه مقابله به اعضای این پیمان داده می‌شود که به این نوع حملات و مقابله با آن اشاره می‌کند.

از این‌رو با افزایش حملات سایبری و همچنین با توجه به اوصاف حملات سایبری اگر این حملات در آستانه حمله مسلحانه باشد، می‌توان آن را به‌نوعی جنگ نامتقارن دانست که با توجه به این مسئله می‌توان قواعد حقوق بین‌الملل بشردوستانه را بر آن قابل اعمال دانست.

مطابق دستورالعمل تالین اقدامات سایبری زمانی مخرب است که کشوری به زیرساخت‌های سایبری کشور دیگر آسیب برساند. در ماده ۷۱ این دستورالعمل، دولت‌ها به ارائه گزارش اقدامات سایبری صورت گرفته در اعمال حقوق دفاع مشروع مورد نظر ماده ۱۵ منشور ملل متحد به شورای امنیت سازمان ملل ملزم می‌دارد. درعین‌حال چالش‌ها و مشکلات زیادی بر سر راه مواجهه با حملات سایبری وجود دارد. بحث از حملات سایبری و مخاصمات مسلحانه، بحث از حملات سایبری و مسئولیت بین‌المللی دولت‌ها در این زمینه و همچنین بحث تروریسم سایبری از جمله مواردی است که باید با توجه به قوانین و مقررات بین‌المللی آن را تبیین نمود.

۲- جنگ سایبری به‌عنوان شیوه‌ای جنگی

قواعد حقوقی عاملی برای ساماندهی به روابط اجتماعی است، بنابراین جریان‌های اجتماعی سیال و پویا اقتضا دارد تا قوانین لازم تصویب و اجرا گردند؛ حقوق مخاصمات مسلحانه نیز از این مجموعه خارج نیست و بخشی از حقوق بین‌الملل است که در هنگام مخاصمات مسلحانه بر روابط کشورها حاکم است و هدف آن تا حد امکان، کاهش آلام، صدمات و خسارات ناشی از جنگ است و مع‌الوصف هدف از آن جلوگیری از کارایی نظامی نیست [۱]، البته به فراخور تحولاتی که در نوع عوامل درگیر در مخاصمه، ابزارها و روش‌های جنگی رخ داده است، دستخوش تغییرات و دگرگونی‌هایی شده است. جنگ که در گذشته‌های نه‌چندان دور به‌مثابه یکی از ابزارهای سیاست ملی کشورها برای حل اختلافات بین‌المللی، تأمین یا بهبود منافع ملی انجام می‌شد، رفته‌رفته با خودنمایی بازیگران غیردولتی، شکل دیگری به خود گرفته است. نقش‌آفرینی این بازیگران که خود را در قلمرو جغرافیایی و حاکمیتی یک دولت محدود نمی‌دیدند، مستلزم بازنگری در قواعد مربوطه بود.

با تغییر و تحول طرف‌ها و عوامل درگیر در مخاصمات، شیوه‌ها و ابزارهای جنگی نیز تغییرات چشمگیری داشته‌اند، بهره‌گیری از روش‌های سایبری و خراب‌کاری توسط بدافزارهای رایانه‌ای از جمله روش‌ها و ابزارهای مخرب جدید به شمار می‌آید. شدت آثار جنگ‌های سایبری بسیاری از حقوقدانان و پژوهشگران را درباره امکان رسیدن به آستانه مخاصمه مسلحانه متقاعد کرده است. بدون شک خرابکاری و انهدام یک نیروگاه هسته‌ای توسط دولتی خارجی می‌تواند به‌عنوان حمله‌ای مسلحانه که در حوزه حقوق مخاصمات قرار می‌گیرد، ارزیابی شود (حملات سایبری به کشورهای استونی (۲۰۰۷) و گرجستان (۲۰۰۸) که به باور بسیاری از جانب روسیه هدایت شده‌اند از گسترده‌ترین موارد حملات سایبری دولتی بوده‌اند. در کنار حملات سایبری دولت از تروریسم سایبری و جرائم سایبری نیز می‌توان یاد کرد).

اینترنت که ساخت ارتش ایالات‌متحده آمریکا بود با سرعت غیر قابل باور در همه زمینه‌ها تسری یافت و جهانی شد. در چنین فضایی طرح دولت الکترونیک در دستور کار بسیاری از کشورها قرار گرفت. در کنار فواید بی‌شمار این وسیله ارتباط‌جمعی نمی‌توان خطرهای فراوان آن را برای

زندگی شخصی و اجتماعی افراد و جامعه نادیده گرفت. در واقع، به میزان گسترش و پیشرفت فضای الکترونیک و در بر گرفتن زیرساخت‌ها و امور حیاتی جامعه، به همان میزان نیز احتمال آسیب‌ها از آن افزایش می‌یابد.

مبنای حقوق مخاصمات مسلحانه اصل محدودیت توسل به شیوه‌ها و ابزارهای جنگی است و با اصول اولیه نظامی از قبیل اجتناب از هدر رفتن نیرو، سادگی عملیات، تمرکز نیرو، وحدت عمل و آزادی مانور مطابقت دارد. تمرکز نیرو بر روی اهداف اصلی و دور نگاه داشتن آن از اشخاص یا اشیائی که از ارزش نظامی کمی برخوردار بوده یا فاقد ارزش نظامی می‌باشد [۱] و اینکه طرف‌های مخاصمه نمی‌توانند سیاست‌های خود را با سبعیت و اقدامات غیر انسانی پیش برند. در واقع تنها هدف نظامی مشروع در جنگ تضعیف نیروها و قوای نظامی طرف متخاصم است، نمی‌توان به تسلیحاتی متوسل شد که باعث خسارات یا تلفات بیش از حد انسانی می‌شود و یا پیامدهایی دارد که با هدف یاد شده تناسبی ندارد. هدف حقوق بشردوستانه حمایت از اشخاص، اموال و اماکنی است که با پدیده خانمان‌سوز جنگ دست‌به‌گریبان هستند. از این‌رو برای محافظت از مواردی که هدف قرار دادن آنها ضرورت نظامی ندارند، دارای مقرراتی است. با توجه به آنکه هدف مشروع در مخاصمه تضعیف و کاستن از توان رزمی طرف مقابل است و نه نابودی آن، حقوق مخاصمات مسلحانه محدودیت‌هایی درباره ابزارها و شیوه‌های جنگی مقرر کرده است و هرگونه اقدامی که از هدف مشروع فراتر رود را قبول نمی‌کند. برای مثال، استفاده از ابزارها و شیوه‌هایی که به درد و رنج نیروهای متخاصم بیانجامد منع شده است (بند ۲ ماده ۳۵ پروتکل اول الحاقی به کنوانسیون ژنو). به‌عنوان یک اصل کلی و بنیادین حقوق بشردوستانه، افراد و اموال غیر نظامی از حملات و خطرات ناشی از عملیات نظامی مصون هستند (مواد ۵۱ و ۲۵ پروتکل اول الحاقی به کنوانسیون ژنو)، تأسیسات زیربنایی کشور اعم از آنکه دولتی باشند یا غیردولتی به دلیل کار ویژه و دخالت مؤثر آنها در ملزومات زیست اجتماعی مشمول حمایتند و از حمله مصون شناخته شده‌اند (مواد ۵۴ پروتکل اول و ۱۴ پروتکل دوم الحاقی).

نهادهای ملی و اجزای مهم کشور مانند نظام بانکی و اقتصادی، ارتباطات و مخابرات، پایانه‌ها و خطوط مواصلاتی، انرژی، سیستم آب‌رسانی و خدمات اورژانس نیز از این جمله‌اند. هدف قرار دادن این تأسیسات علاوه بر اینکه می‌تواند باعث تلفات و آسیب‌های جانی و مالی مستقیم یا غیر مستقیم شود، می‌تواند با هدف ارعاب مردم نیز انجام شود. به‌هرحال، این مراکز عمدتاً با شبکه‌های رایانه‌ای هدایت می‌شوند که نسبت به حملات سایبری آسیب‌پذیرند. بنابراین تعجب‌برانگیز نیست که امنیت سایبری تبدیل به یک نگرانی عمومی در جامعه بین‌المللی شده است و مجمع عمومی سازمان ملل متحد قطعنامه‌هایی درباره موضوعاتی دارد که تأکید بر انتشار و استفاده فناوری اطلاعات و ابزارهای تأثیرگذار بر منافع کل جامعه بین‌المللی می‌نماید و اظهار می‌دارد که سوء استفاده از فناوری اطلاعات می‌تواند تأثیر منفی شدیدی بر همه کشورها بگذارد و اینکه همه این تکنولوژی‌ها می‌توانند به‌صورت بالقوه با مقاصدی به کار گرفته شوند که با اهداف حفظ صلح و امنیت بین‌المللی در تعارض است. همچنین مجمع عمومی سازمان ملل برگزاری اجلاس جهانی جامعه اطلاعاتی را تأیید کرد که در دو فاز در ژنو در سال ۲۰۰۳ و در تونس در سال ۲۰۰۵ برگزار شد (برای اسناد تصویب شده در اجلاس رجوع کنید به: www.itu.int/wsis/index.html چشم‌اندازی دیگر می‌تواند قابلیت اعمال حقوق بشردوستانه در مخاصمات سایبری باشد).

یکی از چشم‌اندازهایی که از طریق آن یک حقوقدان بین‌المللی می‌تواند مسئله امنیت سایبری را مورد مطالعه قرار دهد حقوق جنگ است؛ یعنی قواعدی که استفاده از نیروهای مسلح را توسط کشورها در روابط بین‌المللی‌شان تنظیم می‌کند (چشم‌اندازی دیگر می‌تواند قابلیت اعمال حقوق بشردوستانه در مخاصمات سایبری باشد). در واقع، اگرچه آن‌گونه که تاکنون مشاهده شده این است که کشورهایی مورد حمله واقع شده‌اند و کشورهای دیگر مظنون به ارتکاب چنین اعمالی بوده‌اند، ولی شناسایی مرتکبان مشکل بوده است. در برخی موارد حمله‌های سایبری به‌خودی‌خود هدف بوده‌اند. برای مثال ایالات‌متحده آمریکا تاکنون هدف چندین حمله قرار گرفته که مصدر آن بنا بر ادعا، کشور چین بوده است (برای مثال حمله موسوم

به حمله تایوان در سال ۲۰۰۳ که به رایانه‌های دولتی برای چهار سال با نصب برنامه‌های مخفیانه برای دزدی اطلاعات رسوخ کرد). همچنین حمله‌های سایبری زمان صلح، کشور لیتوانی (در ژوئن ۲۰۰۸ بعد از آنکه مجلس لیتوانی قانونی را تصویب نمود که نمایش نمادهای شوروی را در ملأ عام ممنوع می‌نمود وب‌سایت‌ها مورد حمله قرار گرفتند) و مونته‌نگرو (یک حمله سایبری ۱۵۰ وب‌سایت، از جمله سرویس پست و چندین بانک را در مارس ۲۰۱۰ به تعطیلی کشاند. حمله نشأت گرفته از کوزوو بود) را مورد هدف قرار داده‌اند. در موارد دیگر حمله سایبری مقدم یا در متن یک عملیات یا مخاصمه مسلحانه بود. این حمله‌ها برای نمونه فوراً پس از آغاز عملیات نیروهای متحد در ۱۹۹۹ رخ دادند (جنگ سایبری کوزوو) هکرها تلاش کردند که ارتباط پست الکترونیک ناتو (پیمان آتلانتیک شمالی) را با پر نمودن آن مختل کنند. این در حالی بود که ایالات‌متحده آمریکا طرحی را بررسی می‌کرد که طی آن به شبکه‌های رایانه‌ای یوگسلاوی نفوذ نماید تا عملیات‌های نظامی آن را مختل کند، اما نهایتاً به دلیل شک در قانونی بودن این عمل، عملیات را لغو نمود. فدراسیون روسیه از جنگ سایبری در دومین جنگ چچن علیه وب‌سایت‌های شورشیان به‌منظور جلوگیری از ارسال تبلیغات ضد روسیه، استفاده نمود. حمله سایبری در گرجستان در ژوئیه - اوت ۲۰۰۸ که قبل و در خلال مخاصمه مسلحانه با فدراسیون روسیه روی داد باعث تعطیلی وب‌سایت‌های دولتی شد و سرعت اینترنت را کم نمود. افزون بر این وب‌سایت‌ها تغییر محتوا داده و محتوای آنها با تبلیغات ملی روسی جایگزین شد. همچنین حمله‌های سایبری چندین وب‌سایت رژیم غاصب سرزمین‌های اشغالی را طی عملیات ۲۰۰۸-۲۰۰۹ در نوار غزه مورد هدف قرار دادند.

۲-۱- حمله سایبری به‌مثابه حمله مسلحانه

حمله سایبری، مصداق سلاح جدیدی است که می‌تواند روش هدایت جنگ مدرن توسط بازیگران دولتی و غیردولتی را دگرگون سازد. سرشت بی‌مانند این تهدید و توانمندی مرتکبان جنگ‌های سایبری در آسیب رساندن، کشتار و تخریب فیزیکی از طریق فضای سایبری، تعریف سنتی توسل به زور را متحول ساخته است.

بند ۴ ماده ۲ منشور ملل متحد بیان می‌کند: «تمام اعضا در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگری که با مقاصد ملل متحد مغایرت داشته باشد خودداری خواهند کرد [۲]».

اگرچه معنای متداول و متبادر از واژه «زور» آن‌چنان گسترده است که اجبار نظامی و غیر نظامی را نیز در بر می‌گیرد، اما به نظر بیشتر حقوقدانان این مقرره ناظر به حالت نظامی و مسلحانه است. البته نوع ابزارها و سلاح‌های به کار رفته در اعمال زور حصری نیست. با این توصیف، عملیات‌های سایبری که دارای آثاری مشابه تسلیحات نظامی هستند، نباید مورد مناقشه قرار گیرد. بنا بر نظر دیوان بین‌المللی دادگستری، بند ۴ ماده ۲ منشور ملل متحد «به هرگونه کاربرد زوری صرف‌نظر از (نوع) سلاح به کار رفته»، تسری می‌یابد. بر این اساس، چون جنگ‌های سایبری دربردارنده سلاح‌های متعارف و کلاسیک نیستند، به‌خودی‌خود نمی‌توانند آن را از عنوان کاربرد زور مستثنا سازد.

در مقابل، عده‌ای با توجه به اقدامات تدوین منشور ملل متحد که حاکی از تعمد دولت‌ها در عدم گسترش دامنه «زور» به فشارهای سیاسی یا اقتصادی بوده است، استناد به بند ۴ ماده ۲ منشور را درباره جنگ‌های سایبری که به تخریب یا تلفات مستقیم جانی منجر نمی‌شود را مورد تردید قرار داده‌اند. طرفداران این رویکرد به ماده ۴۱ منشور که در مورد تصمیمات و اقدامات غیر نظامی از قطع خطوط ارتباطی است، استناد می‌کنند که با اخذ ملاک از آن می‌توان دست کم عملیات‌های سایبری که کار ویژه آنها اختلال یا ممانعت در خدمات‌رسانی است را در زمره اقدامات غیر نظامی طبقه‌بندی کرد و از شمول بند ۴ ماده ۲ منشور خارج دانست؛ اما به نظر می‌رسد با تفسیری غایی از منشور با توجه به مقدمه آن که صیانت از نسل‌های آتی در برابر بلای جنگ را هدف سازمان ملل متحد دانسته و در ماده ۱ به هدف حفظ صلح و امنیت بین‌المللی تصریح داشته است، می‌توان گفت که هرگاه ابزارها شیوه‌های غیر خشونت‌بار، صلح و امنیت بین‌المللی را به مخاطره اندازد با اهداف

منشور ملل متحد مغایرت خواهد داشت (جنگ‌های سایبری از جانب دولت‌ها را مداخله در امور داخلی می‌توان تلقی کرد که از اصول سازمان ملل متحد است). گفتنی است که بند ۴ ماده ۲ منشور ملل آستانه‌ای از قبیل شدت یا مدت‌زمان ممنوعیت توسل به زور مشخص نکرده است. بنابراین، شمول این ممنوعیت گسترده‌تر از عنوان «تجاوز» (تجاوز در قطعنامه چنین تعریف شده است «به‌کارگیری نیروی نظامی توسط یک کشور علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی کشور دیگر یا به هر نحوی که با منشور ملل متحد سازگار نباشد». این قطعنامه هفت مورد از مصادیقی را که می‌تواند تجاوز تلقی شود را ذکر کرده است که البته این موارد حصری نیستند) (موضوع ماده ۳۹ منشور) یا «حمله مسلحانه» (موضوع ماده ۵۱ منشور و یا موضوع ماده ۲ مشترک کنوانسیون‌های ژنو) خواهد بود.

به نظر می‌رسد جنگ سایبری را می‌توان وفق ماده‌ی ۲ منشور ملل متحد، توسل به زور مسلحانه توصیف نمود. از سوی دیگر، حمله سایبری گسترده به زیرساخت‌های اساسی که خسارات مادی یا تلفات انسانی قابل قیاس با حمله‌ی مسلحانه با سلاح‌های متعارف را در پی داشته باشد، حق توسل به دفاع مشروع را به دولت قربانی اعطا می‌نماید. همچنین، در واکنش به حمله سایبری که در حد حمله مسلحانه نباشد، اما حمله مسلحانه قریب‌الوقوعی را با تسلیحات متعارف تدارک ببیند می‌توان به دفاع مشروع متوسل گردید.

همان‌طور که دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه بیان کرده است، باید میان شدیدترین صورت‌های کاربرد زور (که به آستانه حمله مسلحانه می‌رسند) و آن‌هایی که صرفاً اتفاقات مرزی هستند با توجه به «مقیاس و آثار» آن زور یا نیروی قهری تفکیک قائل شد. از این‌رو هر درگیری نظامی واجد عنوان حمله مسلحانه که مجوز دفاع مشروع است نخواهد بود. بنابراین، برای آنکه دولتی طبق ماده ۵۱ منشور ملل متحد به حق دفاع مشروع استناد کند می‌بایست حمله سایبری را نه‌تنها توسل به زور بلکه به‌مثابه حمله‌ای مسلحانه تلقی کند. البته منظور آن است که حمله سایبری خود موجد وضعیت مخاصمه مسلحانه شوند، نه آنکه یک مخاصمه کلاسیک و به‌عنوان یک روش جنگی به کار گرفته شوند.

بنابراین باید گفت آیا ابزارهای سایبری می‌توانند در حکم سلاح به کار گرفته شوند [۲]. در این باره گفته شده است این طراحی یا به کاربرد متداول از هر وسیله یا تعدادی از وسایل که باعث تلفات گسترده جانی و یا تخریب گسترده مالی می‌شود می‌بایست حائز شرایط یک «حمله مسلحانه انگاشته شود. در بند ۱ ماده ۴۹ پروتکل اول الحاقی نیز آمده است:

«حملات به معنای اعمال خشونت‌آمیز علیه طرف مقابل هستند اعم از آنکه تدافعی یا تهاجمی باشند».

معیاری که برخی حقوق‌دانان از جمله ژان پیکته در توصیف مخاصمه مسلحانه وفق ماده ۲ مشترک کنوانسیون‌های ژنو ارائه کرده‌اند نیز شایان توجه است. به نظر آنها، کاربرد زور در جایی به‌عنوان «حمله مسلحانه» شناخته می‌شود که دارای دامنه، مدت و شدت کافی باشد. با توجه به معیار اثر محور، درصورتی‌که کاربرد زور از طریق روش‌های سایبری به تلفات و خسارت گسترده جانی و مالی منجر شود و یا آنکه تأسیسات زیربنایی و مهم یک کشور را مورد هدف قرار دهد، می‌توان وقوع حمله مسلحانه را احراز کرد. این تأسیسات شامل مواردی است که برای تولید، انتقال یا توزیع انرژی به کار گرفته می‌شود یا مرتبط با حمل‌ونقل هوایی یا دریایی، خدمات بانکی و مالی، تجارت الکترونیک، آب‌رسانی، توزیع مواد غذایی، سلامت عمومی و سامانه‌ها و شبکه‌های مهم اطلاعاتی هستند. بر این اساس، حمله سایبری به نهادهای مهم یک کشور مانند بازار بورس که پیامدهای سوئی بر رفاه اجتماعی یک کشور به‌جا می‌گذارد، حمله‌ای مسلحانه تلقی می‌شود.

در ابتدا این‌گونه به ذهن متبادر می‌شود که حمله مسلحانه متضمن اعمالی خشونت‌آمیز است که به ایراد خسارت جانی یا تخریب اموال منجر می‌شود. در نتیجه حملات سایبری که چنین هدف یا پیامدی ندارند و برای ممانعت از خدمات‌رسانی و از کار انداختن یک برنامه طراحی‌شده‌اند را نمی‌توان حمله مسلحانه در نظر گرفت. در این باره مباحثی انجام شده است که به نظر می‌رسد بتوان حل آن را از فحوای بند ۲ ماده ۵۲ پروتکل اول الحاقی استنباط کرد؛ حال‌آنکه آنجا که تصرف، خنثی‌سازی یا بی‌اثر کردن برخی اموال (و بنا به تفاسیر بسیاری از دولت‌ها، یک

موفقیت) که می‌تواند مزیتی نظامی در بر داشته باشد، هدفی نظامی تلقی شده است و می‌تواند موضوع حمله واقع شود. بنابراین، از کار انداختن سیستم راداری یا موشکی یک کشور که مزیت نظامی غیرقابل‌انکاری دارد را به‌صرف اینکه موجب تلفات جانی یا تخریب نشده است را به‌سختی می‌توان حمله‌ای مسلحانه تلقی نکرد به‌گونه‌ای که حق دفاع مشروع را برای دولت زیان‌دیده پدید نیاورد.

چنانچه پیش‌تر بیان شد در آوریل ۲۰۰۷ تعدادی از تارنماهای مهم کشور استونی مورد حمله از نوع ممانعت از خدمات‌رسانی قرار گرفتند و در این میان، انگشت اتهام متوجه روسیه شد (گفتنی است در جریان حملات سایبری به استونی (۲۰۰۷) و گرجستان (۲۰۰۸)، مقامات روسی حاضر به پذیرش مسئولیت حملات سایبری نشدند و طرف‌های زیان‌دیده نیز نتوانستند مستنداتی حاکی از دخالت مستقیم کرملین یا مأموران یا مأذونین از جانب این کشور را پیدا کنند). این کشور موضوع را به شورای اتحادیه اروپا و ناتو گزارش کرد، اما ناتو این رخداد را به‌عنوان حمله‌ای مسلحانه که بتواند مجوز ورود این سازمان به‌عنوان دفاع مشروع دسته‌جمعی را فراهم آورد قبول نکرد. ناتو اعلام کرد در این برهه زمانی، حملات سایبری را یک کار نظامی مسلم نمی‌شناسد تا ماده ۵ پیمان ناتو درباره دفاع دسته‌جمعی مورد استناد قرار گرفت. این در حالی بود که وزیر دفاع استونی این وضعیت را با ماده ۳ قطعنامه تعریف تجاوز قابل‌تحلیل می‌دانست که مطابق آن «محاصره بندرها یا سواحل یک کشور توسط نیروهای نظامی کشوری دیگر» به‌منزله تجاوز قلمداد شده است. البته گفتنی است بر اساس ماده ۴۱ منشور ملل متحد، «قطع کامل یا جزئی روابط اقتصادی، مواصلاتی و ریلی، دریایی، هوایی، پستی، تلگرافی، رادیویی و دیگر وسایل ارتباطی» به‌عنوان اقداماتی که متضمن نیروی نظامی نیستند، به شمار آمده‌اند.

مایکل اشمیت، پژوهشگر برجسته قوانین برخوردهای مسلحانه این برداشت که حملات سایبری چون متضمن اعمال خشونت نیستند، «حمله» محسوب نمی‌شود را رد کرده و می‌گوید «حمله» اصطلاحی توصیفی و اثر محور است و منظور از «خشونت» پیامدهای خشونت‌بار است و نه اعمال خشونت‌آمیز، بر اساس ماده ۵۱ منشور ملل متحد و حقوق بین‌الملل عرفی، بروز مخاصمه مسلحانه به هر وسیله‌ای پیش‌شرط استناد به حق دفاع مشروع است؛ هارولد کوه، مشاور حقوقی وزارت امور خارجه ایالات‌متحده آمریکا اظهار داشت که حملات سایبری مشمول حقوق مخاصمات مسلحانه بوده و ممکن است باعث وضعیتی شود که مبنای موجهی برای جنگ پدید آورد. به‌زعم وی قواعد فعلی حقوق بین‌الملل بر فضای سایبر حاکمیت دارند و به انعقاد معاهداتی نیازی نیست که قواعد خاصی بر این قلمرو اعمال کنند. این اولین تحول تکنولوژیک نیست که سؤالاتی را در برابر حقوق بین‌الملل قرار می‌دهد؛ بنابراین شبکه‌های رایانه‌ای نظامی، اهدافی نظامی هستند که باید در هدف قرار دادن آنها اصولی مانند تفکیک و تناسب مورد ملاحظه قرار گیرد. بر همین اساس، دولت‌ها در قبال اقدامات سایبری که تخلف از هنجارهای بین‌المللی است توسط اشخاصی که تحت کنترل آنها عمل می‌کنند مسئولیت بین‌المللی دارند. به عقیده‌ی وی، توسل به زور و حمله که می‌تواند موجب دفاع شود، ممکن است با فعالیتی سایبری محقق شود. البته آستانه مشخصی برای میزان شدت یا خسارات پدید آمده برای احراز وضعیت مخاصمه در نظر گرفته نشده است.

۲-۲- ارزیابی بدافزار استاکس‌نت از نظر حقوق مخاصمات مسلحانه

حملات سایبری دارای اهداف گوناگون است که می‌توانند تهاجمی یا تدافعی باشند. چنین اهدافی می‌تواند ماهیت حمله را تغییر دهد به‌گونه‌ای که تا ممانعت از خدمات‌رسانی، جاسوسی، اقدامات خراب‌کارانه و حتی وضعیت مخاصمه مسلحانه جلو رود.

رویکردهای مختلفی درباره ماهیت حملات سایبری مطرح شده، اما تحت شرایطی حملات سایبری ممکن است به حمله‌ای مسلحانه برسد. بند ۱ ماده ۴۹ پروتکل اول حمله را به اعمال خشونت علیه طرف مقابل اعم از دفاع با تهاجم دانسته است. از این‌رو، باید دید که آیا خراب‌کاری در تأسیسات هسته‌ای یک کشور از طریق رایانه‌ای که در حوزه مقررات حقوق مخاصمات مسلحانه تلقی شود یا خیر. استاکس‌نت معادل دیجیتالی موشک‌های «شلیک کن و فراموش کن» تلقی می‌شود [۲] و این نگرانی را ایجاد کرده

است که جنگ سایبری ممکن است منجر به نتایج فاجعه‌باری در قرن بیست و یکم - قرن شبکه‌ای شده پیچیده - شود که جنگ اتمی ابرقدرتی قرن بیستم می‌توانست ایجاد کند.

استاکس‌نت یکی از معروف‌ترین بدافزارهایی است که برای در اختیار گرفتن سیستم کنترلی تأسیسات برنامه‌ریزی شد. در ابتدای سال ۲۰۱۰ یک شرکت امنیت رایانه‌ای در بلاروس این بدافزار را شناسایی و معلوم کرد که هزاران سیستم کنترل صنعتی را در گستره جهانی آلوده کرده است، البته آسیب چشم‌گیری گزارش نشده است. بنا بر یافته‌های کارشناسان، استاکس‌نت به‌گونه‌ای برنامه‌ریزی شد که سیستم‌های کنترل صنعتی ساخت شرکت زیمنس آلمان را مورد هدف قرار دهد. این بدافزار توسط یک حافظه جانبی وارد سیستم شده و از خلأها و نقاط آسیب‌پذیر مایکروسافت برای اهداف خود بهره گرفته است. انتخاب حافظه جانبی به‌عنوان حامل این بدافزار به این دلیل بوده که بسیاری از سیستم‌های کنترلی به اینترنت متصل نیستند. مهم‌ترین هدف این بدافزار، تأسیسات و تجهیزات غنی‌سازی اورانیوم ایران بوده است و به‌طور خاص برای هدف قرار دادن دستگاه‌های سانتریفیوژ و به هم ریختن سطوح کاری این دستگاه‌ها رساندن به سطح غیر قابل تحمل و کنترل دستگاه در صدد تخریب و نابودی چرخه غنی‌سازی بود. آثار بدافزار استاکس‌نت به‌گونه‌ای بوده است که نگاه کارشناسان را به فراتر از یک حمله سایبری سوق داده و بسیاری از جمله کارشناسان امنیت ملی ایالات‌متحده آمریکا را بر آن داشت تا استاکس‌نت را زمینه‌ساز جنگ‌های سایبری مورد ارزیابی قرار دهند و حتی عده‌ای از آن به‌عنوان سلاحی با آثار گسترده یاد کرده‌اند. به‌طوری‌که برخی با استناد به گفته مایکل هایدن، رئیس سابق سیا و آژانس اطلاعات ملی ایالات‌متحده آمریکا اظهار داشته‌اند که استاکس‌نت از جمله ابزارهای سایبری است که باعث آثاری فیزیکی می‌شود و همانند یک جنگ سایبری مرزها را طی کرده است؛ از این‌رو می‌تواند به‌عنوان حمله‌ای مسلحانه ارزیابی شود. این اقدام از منظر حقوق مخاصمات مسلحانه با حقوق جنگ نیز قابل بررسی است. درصورتی‌که این اقدام به‌مثابه توسل به زور تلقی شود، می‌توان آن را از منظر اصول و قواعد حقوق بشردوستانه مورد ارزیابی قرارداد.

به‌طورکلی در هر مخاصمه‌ای اصول بنیادین بشردوستانه‌ای نظیر اصول تفکیک، تناسب، ضرورت نظامی و پرهیز از ایراد رنج غیرضروری باید مد نظر قرار گیرد. بر اساس اصل تفکیک فقط اهداف نظامی می‌توانند مورد حمله قرار گیرند. اهداف نظامی، اهدافی هستند که به دلیل ماهیت، موقعیت هدف یا کاربری آنها از نظر نظامی مؤثر بوده و تخریب کلی یا جزئی و توقیف یا بی‌اثر ساختن آنها در زمان حمله مزیتی نظامی به شمار می‌آید (بند ۲ ماده ۵۲ پروتکل اول الحاقی.). مواد ۵۱ و ۷۵ پروتکل اول الحاقی برای حمایت از غیر نظامیان، طرف‌های مخاصمه را به اتخاذ برخی تدابیر حیاتی موظف دانسته و مقرر کرده که غیر نظامیان نباید مورد هدف مستقیم قرار گیرند و از حملاتی که خسارات جانبی آن باشد نیز مصون بمانند.

اگرچه حملات سایبری به‌ندرت تلفات جانی مستقیم دارند، اما به‌طور غیر مستقیم می‌توانند اصول تفکیک و تناسب را خدشه‌دار و متضمن پیامدهای سوء جانی و مالی بسیاری باشند. برای مثال، یک حمله سایبری به شبکه ارتباطی مخابراتی و خطوط تلفنی می‌توانند تماس با مراکز اورژانس و پلیس را قطع کرده و باعث تلفات جانی و مالی شوند. بدیهی است که هدف قرار دادن مراکز دارای انرژی‌های خطرناک مانند تأسیسات هسته‌ای یا سدها می‌توانند به‌مراتب آثار زیان‌بارتری داشته باشند. بر اساس ماده‌ی ۵۶ پروتکل اول الحاقی، تأسیسات دارای نیروهای خطرناک مانند سدها، آب‌بندها و نیروگاه‌های برق خسارات زیان‌بار شدید به جمعیت غیر نظامی شود، هرچند اهدافی نظامی باشند از حمله مصون هستند.

به‌هرحال میان حقوق توسل به زور و حقوق بشردوستانه باید تفکیک قائل شد. از آنجا که این دو نظام حقوقی ارتباطی باهم ندارند، ممکن است حمله سایبری از منظر حقوق توسل به زور (حقوق بر جنگ) همانند نظام حقوقی عام، عملی خلاف به شمار آید، اما الزاماً ناقض حقوق مخاصمات مسلحانه (حقوق در جنگ) به‌منزله نظام حقوقی خاص نباشد. برعکس پیش‌بینی حملات سایبری در چارچوب قواعد حقوق مخاصمات مجوزی برای تخطی از حقوق توسل به زور را فراهم نمی‌آورد؛ بنابراین حمله

سایبری به تأسیسات تولید برق هسته‌ای درصورتی‌که به یک دولت قابل انتساب باشد، هم مغایر با حقوق توسل به زور وهم ناقض حقوق مخاصمات می‌تواند باشد و موجب مسئولیت بین‌المللی آن دولت خواهد بود. علیرغم تعداد فزاینده موارد، هنوز به نظر نمی‌رسد که تحقیقات کافی در خصوص اینکه چگونه قواعد موجود توسل به زور در مورد حملات سایبری اعمال گردند، وجود ندارد. اکثر اندک نوشته‌های موجود در خصوص حقوق جنگ و حملات سایبری به‌وسیله دانشمندان و حقوقدانان آمریکایی صورت پذیرفته و در مجلات آمریکایی به چاپ رسیده است و اکثراً اسناد آمریکایی را در نظر گرفته است.

حملات سایبری در چارچوب طبقه‌بندی وسیع‌تری از آنچه به شکل سنتی به‌عنوان عملیات‌های اطلاعاتی شناخته می‌شود، قرار دارند. عملیات‌های اطلاعاتی (که جنگ اطلاعاتی یک زیر بخش آن در حوزه مخاصمات مسلحانه است) به‌کارگیری یکپارچه قابلیت‌های محوری جنگ‌اوری الکترونیک، عملیات‌های شبکه‌های کامپیوتری، عملیات‌های روانی، کمین‌های نظامی و عملیات‌های امنیتی در هماهنگی با پشتیبانی‌های خاص و توانایی‌های مربوطه برای تأثیر گذاشتن، مختل نمودن، تخریب یا گرفتن تصمیمات خصمانه بشری (با اراده و بی‌اراده) درحالی‌که از طرف خود حمایت می‌کنیم، می‌باشد (بر اساس یک مدرک دیگر عملیات‌های اطلاعاتی شامل هر عمل شامل کسب، انتقال، ذخیره یا تبدیل اطلاعاتی است که کاربرد نیروهای مسلح را بالا می‌برد. عملیات‌های اطلاعاتی تنها شامل جنگ اطلاعاتی نمی‌شود بلکه شامل تضمین اطلاعات است که شامل عملیات‌های اطلاعاتی می‌شود که با تضمین دسترسی به آنها، یکپارچگی، تصدیق و سندیت آنها، محرمانگی و عدم رد از آنها حفاظت و دفاع می‌نماید. این شامل ترمیم نظام‌های اطلاعاتی با وارد نمودن مفاهیم حمایت، تفتیش و توانایی واکنش به خطرات می‌گردد. بنابراین تضمین اطلاعات نه‌تنها شامل اقدامات نظامی می‌شود بلکه فعالیت‌های بخش دولتی و خصوصی را در بر می‌گیرد). بر اساس استراتژی ملی نظامی ایالات‌متحده آمریکا در عملیات‌های فضای سایبر، عملیات‌های شبکه‌های کامپیوتری (CNO) شامل حمله به شبکه‌های کامپیوتری (CNA)، دفاع از شبکه‌های کامپیوتری (CND)، و عملیات توانمندسازی بهره‌برداری از شبکه‌های کامپیوتری (CNE) می‌باشد. اگرچه این‌ها در مطبوعات به‌عنوان جنگ‌های سایبری شناخته می‌شوند ولی عملیات‌های توانمندسازی بهره‌برداری از شبکه‌های کامپیوتری متفاوت هستند زیرا این عملیات‌ها بر جمع‌آوری و ملاحظه اطلاعات حساس به‌جای اختلالات شبکه تمرکز دارند و می‌توانند مقدمه یک حمله باشند. آنها می‌توانند با هدف منتشر کردن اطلاعات برای مقاصد تبلیغاتی باشند، برای مثال با بد شکل نمودن و به هم ریختن یک وب‌سایت (برای مثال در حمله‌های سال ۲۰۰۸ گرجستان وب‌سایت‌های وزارت امور خارجه و بانک ملی تغییر شکل دادند و بد شکل شدند. محتوای این سایت‌ها با تصاویری از میخاییل ساکاشویلی و آدولف هیتلر جایگزین گردید). عملیات‌های توانمندسازی بهره‌برداری شبکه‌های کامپیوتری می‌تواند به‌قصد دزدیدن اطلاعات حساس از کامپیوترها باشد. در این رابطه درهای دام (Trap doors) و شنودها (Sniffers) به شکل ویژه ابزارهای مفیدی برای جاسوسی سایبری می‌باشند. ابزار اخیرالذکر به یک کاربر که از خارج نفوذ نموده اجازه می‌دهد که به نرم‌افزار در هر زمان، بدون آگاهی مالک آن، دسترسی داشته باشد. درحالی‌که مورد اول به برنامه‌هایی اطلاق می‌شود که از یک کامپیوتر دور اجرا شده و اطلاعات مبادله شده در یک شبکه را به‌منظور سرقت نام کاربری و رمز عبور جدا نموده و ثبت می‌کند. معهذا جاسوسی به‌وسیله حقوق بین‌الملل منع نشده اگرچه در سطح حقوق داخلی جرم انگاری شده است.

در اینجا موضوع در رابطه با عملیات‌های توانمندسازی کاربرد شبکه‌های کامپیوتر نیست بلکه تنها شامل حمله به شبکه‌های کامپیوتری و دفاع از شبکه‌های کامپیوتری می‌باشد، یعنی آن عملیات‌های شبکه‌های کامپیوتری که از بهره‌برداری صرف فراتر رفته و با قصدی خصمانه همراه هستند: چنین حمله‌هایی با قصد جایگزین نمودن و تخریب اطلاعاتی که در کامپیوتر یا شبکه کامپیوتری هدف و با قصد ناتوان‌سازی و تضعیف قدرت فرماندهی دشمن، سیستم‌های کنترل و ارتباطات و یا ایراد خسارت بیرونی به کامپیوتر با شبکه‌های کامپیوتری هدف انجام می‌شوند. معمول‌ترین روش برای از کار انداختن کامپیوتر یا شبکه کامپیوتری جدا از

تخریب فیزیکی آن، از بین بردن سخت‌افزار آن می‌باشد یا نرم‌افزار آن یا لبریز نمودن آن با اطلاعات بسیار زیاد به‌منظور از بین بردن آن ابزارهای نرم‌افزاری محبوبی که برای مداخله در کارکرد کامپیوتر طراحی شده‌اند؛ اسب‌های تروجان، بمب‌های منطقی، ویروس‌ها و کرم‌ها هستند که می‌توانند با هک یا به‌سادگی به‌وسیله ضمیمه شدن به یک برنامه سالم و قانونی در کامپیوتر مقصد نصب گردند. یک ویروس، یک برنامه با تکرار و کپی شدن خودبه‌خود است که معمولاً به یک برنامه سالم در کامپیوتر هدف حمله، ضمیمه می‌شود، آن را تغییر می‌دهد و نتیجتاً دیگر برنامه‌ها و اگر کامپیوتر به شبکه متصل باشد، دیگر کامپیوترها را تحت تأثیر قرار می‌دهد. یک کرم کل موجودیت خود را تکرار و کپی می‌کند ولی برخلاف ویروس‌ها دیگر برنامه‌ها را تغییر نمی‌دهد. کرم آدرس‌های موجود در کامپیوتر هدف را ضبط نموده و پیام‌هایی از طریق سیستم ارسال می‌کند تا یک کاهش عمومی و نهایتاً از کار افتادن سیستم را موجب شود. ویروس‌ها و کرم‌ها می‌توانند در اسب‌های تروا (تروجان) پنهان باشند مانند یک قطعه از کد برنامه‌نویسی به‌ظاهر بی‌ضرر که در واقع برنامه‌ای مخرب را پنهان نموده یا دسترسی از راه دور را به یک کاربر از خارج شبکه اجازه می‌دهد.

مشهورترین تعریف حمله به شبکه‌های کامپیوتری محتملاً در سند DoD ایالات‌متحده آمریکا آمده است و آنها را به‌عنوان عملیات‌هایی برای مختل نمودن، رد کردن، تنزل یا تخریب اطلاعات موجود در خود کامپیوترها و شبکه‌های کامپیوتری، توصیف نموده است (United States National Military Strategy for Cyberspace Operations). این تعریفی که اغلب ذکر شده است تمایزی بین دو نوع حمله به شبکه‌های کامپیوتری قائل شده است. حملاتی که کامپیوترها و شبکه‌های کامپیوتری را هدف قرار می‌دهد و حملاتی که اطلاعات موجود در آن کامپیوترها و شبکه‌های کامپیوتری را هدف قرار می‌دهد. این روشن نیست که آیا تعریف DoD دربرگیرنده دست‌کاری شبکه کامپیوتری برای دستیابی به تأثیری خارجی در خود شبکه می‌شود یا خیر؟ این برخلاف حالتی است که ناکارآمدی صرف شبکه را باعث می‌شود. راهنمای اخیر حقوق بین‌الملل قابل اعمال در هوا و جنگ موشکی که به‌وسیله برنامه تحقیقاتی خط‌مشی بشردوستانه و مخاصمات (HPCR) در سال ۲۰۰۹ در هاروارد به تصویب رسید، تعریف سند DoD از حمله به شبکه‌های کامپیوتری را بازسازی نموده تا عملیات‌هایی را پوشش دهد که اطلاعات کامپیوتر را دستکاری می‌نماید و این با هدف به دست گرفتن کنترل کامپیوترها یا شبکه‌های کامپیوتری انجام می‌شود. تفسیر راهنما معین می‌نماید که حمله می‌تواند علیه یک کامپیوتر باشد یا کامپیوترهای معینی در یک شبکه یا کل شبکه و اینکه همه حملات به شبکه‌های کامپیوتری آن‌گونه که در ماده ۱ بخش e تعریف شده حمله نیستند، یعنی عمل نقض چه به‌صورت تجاوزکارانه و چه به‌صورت دفاعی باشد [۱۰]. هرچند تعاریف HPCR و DoD هر دو بر حملات به کامپیوترها به‌عنوان هدف تمرکز یافته‌اند و بنابراین این تعریف نیز حمله‌های معمولی بر تأسیسات شبکه‌های کامپیوتری را در بر می‌گیرد.

دکترین مشترک ایالات‌متحده آمریکا در خصوص عملیات‌های اطلاعاتی هنگامی‌که حملات علیه شبکه‌های کامپیوتری را به‌عنوان اعمال اتخاذ شده از طریق استفاده از شبکه‌های کامپیوتری برای مختل نمودن، رد کردن، تنزل دادن یا از بین بردن اطلاعات موجود در کامپیوترها و شبکه‌های کامپیوتری یا خود کامپیوترها با شبکه‌های کامپیوتری تعریف می‌کند، رویکرد مضیق‌تری اتخاذ نموده است، ولی حمله‌هایی که به‌قصد ایجاد آسیب خارجی به کامپیوترها یا شبکه‌های کامپیوتری را ذکر ننموده است [۴]. در اینجا اجبار (زور) سایبری (بر اساس فرهنگ انگلیسی آکسفورد سایبر به معنای امور مربوط به فناوری اطلاعات، اینترنت و واقعیت مجازی می‌باشد) و حمله‌های سایبری را به‌منظور تطابق با ادبیات حقوق بر جنگ مورد استفاده قرار می‌دهد [۱۱].

حملات به شبکه‌های کامپیوتری تا حدودی گمراه کننده هستند زیرا هدف عملیات‌های سایبری می‌تواند نه‌تنها شبکه‌های کامپیوتری بلکه کامپیوترهای منفرد و شخصی یا برخی کامپیوترها در یک شبکه به‌علاوه وب‌سایت‌ها باشد. بنابراین در زمینه این تحقیق حملات سایبری استفاده خصمانه از زور و اجبار سایبری می‌باشد که می‌تواند یک عمل مجرد باشد، می‌تواند اولین حمله در یک مخاصمه مسلحانه باشد، می‌تواند یک حمله در پس‌زمینه یک مخاصمه مسلحانه موجود و یا حتی واکنشی به حمله

قبلی معمولی یا سایبری باشد. با اشاره به اجبار یا زور سایبری نگارنده به عملیات‌هایی اشاره دارد که توسط کشوری علیه کشور دیگر چه به‌صورت حمله چه به‌صورت دفاع و از طریق استفاده از اطلاعات موجود در کامپیوترهای شخصی منفرد یا برخی کامپیوترها در یک شبکه با همه کامپیوترهای شبکه با قصد از کار انداختن کامپیوتر، شبکه کامپیوتری یا وب‌سایت هدف یا ایجاد خسارت بیرونی به شبکه یا کامپیوتر انجام می‌گیرد. این تعریف که بر کامپیوترها و شبکه‌های کامپیوتری به‌عنوان سلاح و نه به‌عنوان هدف تمرکز دارد و حملات جنبشی (که از طریق کامپیوتر و شبکه‌های کامپیوتری صورت می‌گیرد) بر امکانات کامپیوتری را پوشش نمی‌دهد و بنابراین از حوزه این پژوهش خارج است (بمباران امکانات ارتباطی از طریق عملیات جنبشی به معنای عملیات اطلاعاتی و نه حمله سایبری خواهد بود. قواعد حقوق بر جنگ و حقوق در جنگ موجود بدون مشکلاتی در رابطه با استفاده از سلاح‌های سنتی بر علیه کامپیوترها و شبکه‌های کامپیوتری اعمال می‌گردد)، جاسوسی سایبری و تبلیغات سایبری به‌منظور هدف عملیات نیز باید با شبکه را از کار بیندازند یا آسیب خارجی و فیزیکی وارد نمایند.

۲-۳- تعیین هویت و مشکلات انتساب

به‌طور سنتی، اقدامات دوران جنگ (که به‌اصطلاح «تلافی‌جویی خصمانه (Belligerent Reprisals)» نامیده می‌شوند) برای مجازات تخطی از قوانین برخوردهای مسلحانه و از طریق «انتقام به‌عین» مورد استفاده قرار می‌گرفتند. پروفسور یورم دینشتین، یکی از مفسران پیشروی قوانین برخوردهای مسلحانه، بر این مسئله تأکید دارد که برای خفیف‌ترین حملات سایبری، می‌توانیم با نمایش قابلیت‌های خود شروع کنیم؛ برای مثال، نفوذ به شبکه‌های رایانه‌ای فعال در حکومت مهاجم و درج پیام‌های تمسخرآمیز، درست مانند کاری که چینی‌ها با رایانه‌های پنتاگون و سیستم‌های رایانه‌ای دفاتر پیمانکاران عمده دفاعی آمریکایی انجام دادند. این حرکت معادل سایبری فرستادن یک رزم‌ناو برای نمایش قدرت حاکمیت در یک منطقه مورد مناقشه است.

۳- حمله سایبری از دیدگاه حقوق بین‌الملل

امروزه تهدیدها در قالب شبکه‌های رایانه‌ای و مخابراتی رو به افزایش است. بخش‌های کلیدی اقتصاد تمامی کشورها در حال حاضر، از جمله امکانات دولتی و خصوصی، بانکداری و امور مالی، حمل‌ونقل، تولید، پزشکی، آموزش‌وپرورش و دولت، همگی برای انجام عملیات روزانه وابسته به رایانه هستند. فضای مجازی ابزاری برای قدرت و ثروت است. هدف از حمله سایبری، دست‌یابی به اطلاعات سایر کشورها، ایجاد وقفه در تجارت و یا ایجاد خدشه در زیرساخت‌ها مانند آب، برق، حمل‌ونقل و... به‌نحوی‌که هزینه‌های اقتصادی را افزایش دهند. در تعریف عمومی حمله سایبری گفته می‌شود: «یک عملیات سایبری که انتظار می‌رود باعث تلفات یا خسارات انسانی شده یا به صدمه و خسارت به اشیا بیانجامد». اکثر حقوقدانان بر این باورند که حملات سایبری می‌تواند وضعیت مخاصمه مسلحانه به وجود آورد و از این نظر با حملات فیزیکی کلاسیک تفاوت ماهوی ندارد [۳].

گاهی به دلیل ناشناخته بودن منبع حمله، فضای مجازی به مکانی ایده‌آل برای جنگ تبدیل شده است. عدم وجود قوانین بین‌المللی باعث شده که هر کشوری به خود اجازه دهد تا بر ضد کشور دیگر وارد جنگ مجازی شود. با توجه به احتمال حملات تروریستی به فیبرهای نوری زیردریایی و زیرساخت‌های سایبری و اینکه این سلاح‌های سایبری فاقد قدرت تشخیص اهداف نظامی و عمومی هستند، تدوین قوانین جهانی امنیت سایبری ضروری است. در حال حاضر کشور ایالات‌متحده در جهان مرکز فرماندهی فضای مجازی را در پنتاگون راه‌اندازی کرده است که هدف از ایجاد آن حمله به شبکه‌های سایر کشورها و دفاع در مقابل حملات مجازی است. جنگ ویروس «استاکس‌نت» به تأسیسات اتمی نطنز بوده است [۵]. بر این اساس در این مبحث، حملات سایبری در حقوق بین‌الملل، اسناد و معاهدات بین‌المللی را مورد بررسی قرار می‌دهیم.

۱-۳- حمله سایبری در حقوق معاهدات و عرف‌های بین‌المللی

در سال ۱۹۹۹ وزارت دفاع آمریکا سندی ارائه کرد که در آن گستره معاهدات بین‌المللی و بخشی از حقوق بین‌الملل

که می‌تواند در مورد به‌کارگیری نبرد سایبری بر علیه کشورهای دیگر قابل اعمال باشد را مشخص نموده بود و از آن به‌عنوان مکملی برای قوانین مختلف آمریکا که هدایتگر این کشور در مورد جنگ‌ها - به معنای اعم - هستند و همچنین رفتار دولت این کشور در حوزه فضای مجازی به‌طور خاص استفاده کرد. ارزیابی مذکور در ابتدا نتیجه گرفت که جامعه بین‌المللی علاقه‌ای به ایجاد فوری بدنه قدرتمندی از قوانین در زمینه موضوع مد نظر ندارد. دومین نکته مطروحه در سند آن بود که هیچ محدودیت یا حوزه حقوقی‌ای وجود ندارد که شکل خاص نبرد سایبری مورد نظر ایالات‌متحده را مخاطب قرار دهد. سند مذکور به‌عنوان نکته سوم پیشنهاد کرده بود که شرایط مختلف هر نوع عملیات یا فعالیت برنامه‌ریزی‌شده خاص مورد تحلیل قرار گیرد تا مشخص شود که آیا قواعد حقوقی بین‌المللی کنونی قابلیت اعمال در این شرایط را دارند یا خیر.

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. به‌عنوان‌مثال، معاهده روابط از راه دور بین‌المللی (ITC) هرگونه مداخله زیان‌بار با استفاده از ارتباطات از راه دور را ممنوع می‌کند. 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 آن طوری که مد نظر بخش ۴ ماده ۲ منشور ملل متحد است تشکیل نمی‌دهد و بنابراین باعث ایجاد موضع‌گیری مشابهی در میان جامعه بین‌المللی نمی‌شود.

یک سند حقوقی بین‌المللی دیگر که استعداد مرتبط شدن با موضوع را دارد موافقت‌نامه اجتناب از فعالیت‌های خطرناک نظامی است که در سال ۱۹۸۹ بین ایالات‌متحده 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 به‌عنوان امکان ایجاد عرفی شناخته شود که حملات واقع شده در فضای مجازی را نوعی توسل به زور به شمار می‌آورد.

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 به‌عنوان تلاشی آشکار برای جلب نظر سازمان ملل به این موضوع شناخته می‌شود. این تلاش با استقبال اندکی در جامعه بین‌المللی مواجه شد و هرگز برای رأی‌گیری عمومی وارد مجمع عمومی سازمان ملل متحد نگردید.

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 به‌عنوان‌مثال 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.

۳-۲- حملات سایبری و ممنوعیت تهدید و توسل به زور در حقوق بین‌الملل

بند ۴ ماده ۲ منشور متحد بیان می‌کند که تمام اعضا در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا از هر روش دیگری که با مقاصد ملل متحد مغایرت داشته باشد خودداری خواهند کرد. مسئله این است که آیا حملات سایبری می‌تواند در قلمرو موضوعی این مقرره قرار گیرد. اگرچه معنای متداول و متبادر از واژه (زور) آن‌چنان گسترده است که اجباری نظامی و غیر نظامی را نیز در برمی‌گیرد اما به نظر بیشتر حقوقدانان این مقرره ناظر به حالت نظامی و مسلحانه است البته نوع ابزارها و سلاح‌های به کار رفته در اعمال زور حصری نیست. با این توصیف عملیات‌های سایبری که دارای آثاری مشابه تسلیحات نظامی هستند نباید مورد مناقشه قرار گیرد. بنا بر نظر دیوان بین‌المللی دادگستری بند ۴ ماده ۲ به هرگونه کاربرد زوری صرف‌نظر از نوع سلاح به کار رفته تسری می‌یابد. بر این اساس چون حملات سایبری دربردارنده سلاح‌های متعارف و کلاسیک نیستند به‌خودی‌خود نمی‌توانند آن را از عنوان کاربرد زور مستثنا سازد.

در مقابل عده‌ای با توجه به مقدمات تدوین منشور ملل متحد که حاکی از تعمد دولت‌ها در عدم گسترش دامنه زور به فشارهای سیاسی یا اقتصادی بوده است استناد به بند ۴ ماده ۲ منشور را درباره عملیات‌های سایبری که به تخریب یا تلفات مستقیم جانی منجر نمی‌شود را مورد تردید قرار داده‌اند. طرفداران این رویکرد به ماده ۴۱ منشور که در مورد تصمیمات و اقدامات غیر نظامی و اقدامات از قطع خطوط ارتباطی است استناد می‌کنند که با اخذ ملاک از آن می‌توان دست کم عملیات‌های سایبری که کار ویژه آنها اختلال یا ممانعت در خدمات‌رسانی است را در زمره اقداماتی غیر نظامی طبقه‌بندی کرد و از شمول ماده ۲ بند ۴ منشور خارج دانست؛ اما به نظر می‌رسد با تفسیری غایی از منشور با توجه به مقدمه آن که صیانت از نسل‌های آتی در برابر جنگ را هدف سازمان ملل متحد دانسته و در ماده ۱ به هدف حفظ صلح و امنیت بین‌المللی تصریح داشته است می‌توان گفت که هرگاه ابزارها یا شیوه‌های غیر خشونت‌بار صلح و امنیت بین‌المللی را به مخاطره اندازد با اهداف بین‌الملل متحد مغایرت خواهد داشت. گفتنی است که بند ۴ ماده ۲ آستانه‌ای از قبیل شدت یا مدت‌زمان برای ممنوعیت توسل به زور مشخص نکرده است. بنابراین شمول این ممنوعیت گسترده‌تر از عنوان تجاوز موضوع ماده ۳۹ منشور یا حمله مسلحانه موضوع ماده ۵۱ منشور و یا موضوع ماده ۲ مشترک کنوانسیون‌های ژنو خواهد بود [۳].

تاکنون برخی کشورها مانند ایالات‌متحده آمریکا، روسیه و استونی به‌صراحت دیدگاه خود را مبنی بر تلقی حمله‌ی سایبری به‌عنوان گونه‌ای از توسل به زور مسلحانه ابراز نموده‌اند. سند استراتژی نظامی ملی سال ۲۰۰۴ میلادی وزارت دفاع ایالات‌متحده آمریکا به سلاح‌هایی با آثار گسترده اشاره می‌نماید که بیشتر آثار مختل‌کننده دارند تا نابودکننده. این سند چارچوب حملات سایبری صورت گرفته نسبت به سیستم‌های اطلاعاتی بازرگانی یا علیه شبکه‌های حمل‌ونقل را از مصادیقی دانسته است که ممکن است به‌مراتب پیامدهای اقتصادی و روانی بیشتری از پرتاب یک سلاح کشنده داشته باشند. فدراسیون روسیه نیز بر این باور است که «تسلیحات اطلاعاتی می‌توانند آثار مخرب قابل‌مقایسه‌ای با آثار تسلیحات نابودی جمعی داشته باشند»؛ وزیر دفاع استونی، «محاصره سایبری» را معادل محاصره دریایی بندرها می‌داند که از دسترسی یک کشور به جهان ممانعت می‌کند.

۳-۳- حمله سایبری و استثناء دفاع از خود

ماده ۱۵ تنها استثناء مشخص ممنوعیت عام توسل به زور یک‌جانبه را تشریح می‌نماید. دولت‌ها می‌توانند در قبال یک حمله مسلحانه در قالب دفاع از خود به زور متوسل شوند. این قرائت با کلمات ساده موجود در ماده ۵۱، تاریخچه تهیه پیش‌نویس و موضع‌گیری‌های رسمی دولتی منطبق می‌باشد. این برداشت همچنین با تفسیر قابل استناد دیوان بین‌المللی دادگستری از ماده ۱۵ نیز منطبق است. به‌رغم تبیین برخی مسائل پس از حوادث یازده سپتامبر توسط شورای امنیت و دولت‌ها، با این حال کماکان ابهاماتی در خصوص زمان آغاز حمله مسلحانه جهت استناد به حق دفاع از خود وجود دارد. برای ایجاد حق دفاع از خود فردی یا جمعی لازم است یک حمله در حال وقوع بوده و یا قبلاً به وقوع پیوسته باشد. هرگونه واکنش قبل از این تاریخ منوط به تأیید شورای امنیت می‌باشد. بنابراین هیچ حق خود گمارده‌ای وجود ندارد که بتوان بر اساس آن علیه دولت دیگر به دلیل ترس از اینکه این دولت در حال طراحی یا گسترش سلاح‌هایی است که در یک عملیات نظامی فرضی قابل استفاده خواهد بود، حمله نمود.

در واقع عبارات صریح ماده ۱۵ به این نکته اشاره دارند که حق دفاع از خود در صورت وقوع یک حمله مسلحانه ممکن می‌باشد. متن ماده مذکور در قضایای مختلفی توسط دیوان بین‌المللی دادگستری مورد تفسیر قرار گرفته است. در قضیه نیکاراگوئه دیوان بیان داشت که حق دفاع از خود فردی یا جمعی صرفاً زمانی مطرح می‌شود که اعمال آن چنان گسترده باشند که با یک حمله مسلحانه برابری نمایند. به هنگام نتیجه‌گیری در مورد این مسئله که دفاع از خود یک‌جانبه در مقابل حمله مسلحانه ممکن است همچنین شامل «ارسال باندهای مسلح، گروه‌ها، چریک‌ها یا مزدوران از سوی یا به نمایندگی از یک دولت که علیه یک دولت دیگر از نیروی مسلح برابر با حمله مسلحانه واقعی نیروهای منظم، استفاده می‌نمایند»، شود تا حدودی بر تعریف مجمع عمومی از تجاوز مبتنی بوده است.

دیوان در آن قضیه ادعای ایالات‌متحده در خصوص مشروع بودن توسل به زور آن کشور علیه نیکاراگوئه به‌عنوان دفاع از خود جمعی السالوادور را مورد بررسی قرار داد. ایالات‌متحده استدلال می‌نمود که نیکاراگوئه با فراهم آوردن تسلیحات و تجهیزات برای شورشیان السالوادور ابتدا از زور غیر مشروع استفاده کرده است؛ اما دیوان به این نتیجه رسید که مشخص نگردیده، نیکاراگوئه مسئول فراهم آوردن تسلیحات و تجهیزات برای شورشیان السالوادور بوده است و حتی چنانچه این‌گونه می‌بود، عرضه تسلیحات مفهومی همانند حمله مسلحانه ندارد. به‌علاوه السالوادور نه به شورای امنیت گزارش داده و نه از ایالات‌متحده تقاضای یاری‌رسانی در امر دفاع از خود کرده است. با در نظر گرفتن قضیه نیکاراگوئه به این نتیجه می‌رسیم که تهدید به زور علیه یک دولت با حمله مسلحانه برابر نیست و دولت مورد تهدید می‌بایست اقداماتی غیر از اقدام در جهت دفاع مسلحانه از خود به عمل آورد، یا اینکه می‌بایست به دنبال مجوز شورای امنیت برای این عمل باشد. به‌علاوه دولت‌ها بر اساس مبانی مسئولیت دولت‌ها و ممنوعیت اقدام به‌مثل مسلحانه دارای محدودیت هستند. اقدام به مثل مسلحانه، نوعی توسل به زور با هدف انتقام، مجازات یا بازدارندگی عام می‌باشد. مجمع عمومی این اقدام به‌مثل مسلحانه را غیرقانونی اعلام داشته و دولت‌ها متعهدند از انجام آنها خودداری ورزند. حق دفاع از خود محدود به توسل به زوری است که به‌منظور دفع یک حمله در حال انجام، با هدف جلوگیری از حملات آینده دشمن پس از حمله اولیه یا از بین بردن آثار حمله دشمن همانند پایان بخشیدن به اشغال انجام پذیرد. دولت دفاع کننده در صورت وجود رعایت اصول ضرورت و تناسب می‌تواند با دفاع نیروهای دشمن حمله کننده را نابود نماید. در صورت ضرورت این حق همچنین می‌تواند شامل دفاع متناسب، در داخل سرزمین دشمن حمله کننده نیز باشد. توسل به زور تدافعی به‌مقتضای شرایط می‌تواند با تأخیر و پس از یک حمله مسلحانه غیرقانونی انجام گیرد. اندکی تأخیر جهت سازمان‌دهی عملیات دفاع قابل قبول خواهد بود.

توسل به زور در حالت دفاع از خود صرفاً در قبال دولتی ممکن است که قانوناً مسئولیت حمله مسلحانه را داشته است. دیدگاه کلی این است که برای استناد به حق دفاع از خود تنها نشأت گرفتن حمله دشمن از داخل سرزمین یک دولت کفایت می‌نماید. به‌علاوه چنانچه دولتی از کارگزاران خویش برای انجام حمله استفاده نماید، یا در اینکه نسبت به حملات کنترل نداشته، بلکه حمله‌کنندگان را پشتیبانی کرده، دارای مسئولیت قانونی خواهد بود. هرگونه توسل به زور در مقام دفاع از خود می‌بایست اصول ضرورت و تناسب را رعایت نماید. اصل ضرورت، توسل به زور نظامی را محدود به دستیابی به اهداف نظامی مشروع می‌نماید. اصل تناسب نیز مستلزم آن است که قربانیان غیر نظامی احتمالی متناسب باشند. چنانچه صدمات جانی بی‌گناهان با تخریب اموال غیر نظامیان در مقایسه با اهمیت هدفی، نامتناسب باشند آن حمله می‌بایست خاتمه پیدا کند [۶].

۴- حملات سایبری تحت حاکمیت حقوق بشردوستانه

هدف از حملات سایبری چیست؟ عملیات‌های مخرب سایبری را می‌توان به دو مقوله گسترده طبقه‌بندی کرد: حمله به شبکه کامپیوتری و بهره‌برداری از شبکه کامپیوتری (CAN) با هدف تغییر، تخریب، فریب، تنزل دادن و یا از بین بردن سیستم‌های دشمن یا شبکه‌ها یا اطلاعات و برنامه‌های مستقر درون سیستم‌ها و یا برنامه‌های در حال انتقال این سیستم‌ها و شبکه‌هاست [۱۲]؛ از سوی دیگر بهره‌برداری از شبکه کامپیوتری به دنبال استخراج اطلاعات است و ممکن است هیچ تخریب یا خرابکاری آشکار هم اصلاً نداشته باشد [۱۳]. CNE فرمی از جاسوسی کردن است و در حیطه فیزیکی در قواعد جنگ منع نشده بلکه این ممنوعیت از حوزه حقوق داخلی اعمال می‌گردد، از این‌رو حقوق جنگ به CNE نمی‌پردازد[۱].

مشکل اصلی در حوزه سایبری این است که غالباً اثرات حمله را نمی‌توان به‌آسانی از طریق CAN تشخیص داد زیرا این اثرات ممکن است خیلی سریع آشکار نباشند و نیتی که پشت این حمله است به‌آسانی با ابزارهای فنی قابل‌شناسایی نیست. مثلاً کرم استاکس‌نت را در نظر بگیرید که با ورود به سیستم‌عامل ویندوز بیش از یک سال در سیستم‌ها نفوذ کرد پیش از اینکه کارشناسان امنیتی سراسر جهان بتوانند

با کنار هم گذاشتن سرنخ‌هایی پی ببرند که این کرم حمله به سانتریفیوژهای غنی‌سازی اورانیوم در ایران را هدف قرار داده است[۲]. در فاز اولیه ساختن کد استاکس‌نت، کارشناسان امنیتی دریافتند که این کرم «قالب‌بندی سیستم را به سرقت می‌برد و با کمک سیستم‌های کنترل کننده آنها را به‌دلخواه خود طراحی می‌کند، به‌طور خلاصه اینکه به رقبا اجازه می‌دهد از طرح کلی خط تولید کارخانه نسخه کپی تهیه کنند [۱۴]. از این‌رو استاکس‌نت شبیه «نوعی جاسوسی صنعتی» است. همچنان که کارشناسان علی‌رغم چیزی که تصور می‌شد پیچیده‌ترین بدافزاری باشد که تاکنون کشف شده دقیق‌تر شدند، دریافتند که عملکرد جاسوسی استاکس‌نت اساساً بر همین مبناست و این کرم همچنین حامل یک payload مخرب بوده است. زمانی که این کرم به هدف مورد نظر رسید یک کنترلر صنعتی شروع به اجرای یک برنامه دوگانه نمود: یکی دستوراتی که به کنترلر ارسال می‌شد را با دستوراتی خرابکارانه جایگزین می‌کرد؛ درحالی‌که دیگری خاص یا مقصود اصلی کارهای تخریبی مورد اول را پنهان می‌کرد؛ اما کارشناسان همچنان هدف را نتوانسته‌اند شناسایی کنند، فقط هنگامی‌که اثرات این حمله آشکار شد (پس از اینکه استاکس سانتریفیوژهای نطنز از کار افتادند) که به‌طور قطعی مشخص شد این کرم سانتریفیوژها را مخفیانه به طرفی هدایت می‌کرده که از کنترل خارج شوند [۱۵] و ماهیت این کرم از هر دو نوع CNAو CNE گزارش شد.

همان‌طور که استاکس‌نت نشان داد، کشوری که بخواهد به حملات سایبری پاسخ دهد ممکن است در شناسایی نوع حمله سایبری ناتوان بماند یعنی اینکه نمی‌تواند مطمئن باشد که حمله از نوع CNA است یا CNE زیرا نمی‌تواند تشخیص دهد که مقصود از این حمله سایبری چه بوده است. پیامد این ابهام این است که این کشور نمی‌داند چه نوع رژیم حقوقی بر مسئله حاکم است؛ رژیم بین‌المللی یا داخلی.

۴-۱- مقصر (مباشر) در حملات سایبری کیست؟

در حملات سایبری، انتساب را می‌توان به شناسایی مباشر حمله سایبری، کامپیوتر یا موقعیت مکانی که این عملیات از آنجا سرچشمه گرفته ارجاع داد؛ مانند مقصود یک عملیات سایبری، انتساب هم برای یقین اطمینان یافتن فریبنده است به‌خصوص هنگامی‌که هویت مباشر مطرح می‌گردد [۲۵]. مانع فنی انتساب ریشه در ابزارهای چند هزار ساله‌ای دارد که فضای سایبر درصدد فائق آمدن بر ابهام آن می‌باشد[۳]. مثلاً رهگیری یک عملیات سایبری مبتنی بر اینترنت به آدرس IP کاربر می‌رسد که لزوماً به IP یا با کمک یک پنهان کننده معنی شناسایی مباشر آن نیست. یک مباشر می‌تواند با جعل در آدرس ردپایی دروغین از آدرس‌های IP خود بجای گذارد. حتی اگر فرض کنیم که آدرس IP که رهگیری شده به همانی برمی‌گردد که عملیات سایبری از آنجا صورت پذیرفته ردگیری کامپیوتر ممکن است به‌صورت تصادفی با یک botnet که بر این سیستم کنترل دارد از جانب مباشر صورت گرفته باشد[۴]. در این مثال کامپیوتر پاسخگو برای قسمتی از عملیات قابل شناسایی است حال‌آنکه بازیگر اصلی و مباشر عملیات ممکن است معلوم نباشد. انتساب همچنین می‌تواند روی عملیات سایبری تأثیر بگذارد و بدان پاسخ دهد- بدین‌صورت که تعیین کند این حمله تحت اعمال رژیم حقوق داخلی است یا حقوق جنگ بر آن حاکم است[۵].

گستره‌ای از انواع بازیگران در حوزه سایبری در کارند. جرائم garden - variety بازیگران غیردولتی با انگیزه‌های سیاسی[۶]، هکرهای کلاه‌سفید[۷]، هکرهای تحت حمایت دولت و بازیگران نظامی که اسامی‌شان بسیار است. از آنجایی که مقوله مباشر قطعاً نمی‌تواند رژیم حقوقی حاکم را تعیین کند اما جزئی مهم از محاسبات را تشکیل می‌دهد، مسئله انتساب نه‌تنها قابلیت اعمال قواعد حقوق جنگ را مشکل می‌کند بلکه به این مسئله دامن می‌زند که کشورها چگونه می‌توانند به قواعد حقوق جنگ در حوزه سایبر پایبند باشند درحالی‌که نمی‌دانند مهاجم اصلی کیست؟ ممکن است این مهاجم تحت لوای پرچم دروغین عمل کند و یا ردپایی جعلی از خود به جا گذارد و بدین‌ترتیب سبب شود یک کشور ثالث، کاملاً و به‌طور تصادفی قربانی عمل تلافی‌جویانه واقع شود و این مسئله می‌تواند تأثیر غیر مستقیمی بر شهروندان کشور قربانی و یا حتی شهروندان کشور خود

داشته باشد، همانند نوجوانی که شبکه برق یک شهر را هک می‌کند از طریق محاکم کیفری داخلی تحت پیگرد قرار می‌گیرد، اقدامات دولت خارجی نیز واجد پیگرد است و با وجود پیامدهای خرابکارانه ممکن است ذیل حقوق جنگ وارد شود[۸].

مسئله انتساب نه‌تنها قابلیت اعمال حقوق جنگ را پیچیده می‌کند بلکه این مسئله را پیش می‌کشد که دولت‌ها چگونه می‌توانند از قواعد حقوق جنگ متابعت کنند بدون اینکه قطعاً بدانند مهاجم اصلی در این خصوص کیست. این پیچیدگی را با دقت بیشتری ذیلاً بحث می‌کنیم. یک مهاجم ممکن است تحت لوای «پرچم دروغین»[۹] عمل کند و از این طریق موجب فریب یک کشور شود که از طرف این کشور دروغین مورد حمله سایبری قرار گرفته است و بدین‌ترتیب موجب برانگیختن یک Catalytic Conflict گردد و یا اینکه مهاجم ردپایی دروغین از خویش به‌جای گذاشته موجب شود یک کشور ثالث قربانی اقدام تلافی‌جویانه نسبت به شبکه‌های اینترنتی‌اش گردد و حتی اگر فرض اقدام متقابل محتمل باشد موجب اثرات غیر مستقیمی بر شهروندان من‌جمله شهروندان خودش در آن کشور شود[۱۰].

۴-۲- پیامدهای عملیات سایبری

توسل به زور و حمله مسلحانه عناصر کلیدی Jus ad bellum هستند و لزوماً واجد مفهومی فیزیکی می‌باشند. مخاصمه مسلحانه، حمله و عمل تجاوز مفاهیمی اساسی در Jus in bello هستند. حال این سؤال مطرح می‌شود که آیا درگیری سایبری هم نوعی از اینهاست؟

- در محیط سایبر عملیات فیزیکی در حوزه‌ای غیر فیزیکی رخ می‌دهد، اما از آن جهت که هک کردن یک نیروگاه هسته‌ای ممکن است با ایجاد تخریب سبب انتشار تشعشعات هسته‌ای گردد و از این جهت که حقوق بین‌الملل درصدد حمایت از موجودیت‌های خاص است، اعمال چنین رژیم حقوقی در حوزه سایبری را توجیه کند.
- برای تسری حقوق جنگ به درگیری سایبری، حقوقدانان روی پیامدهای ناشی از حملات سایبری تأکید دارند.

نکته قابل توجه این است که شدت این حملات باید به حدی مشخصی برسد تا تحت شمول قواعد حقوق جنگ قرار گیرد.

آیا مخاصمه مسلحانه‌ای وجود دارد که با عملیات سایبری در ارتباط باشد؟ حقوق زمان جنگ را می‌توان هنگامی در حوزه سایبر اعمال کرد که حقیقتاً یک مخاصمه مسلحانه در جریان باشد. در این حوزه تصمیمی با سیاست‌گذاران است که آیا حمله سایبری معادل با «توسل به زور» یا «حمله مسلحانه» است. حمله سایبری بیشتر در قالب تاکتیک نظامی است که در عرض سایر گزینه‌های تاکتیکی وجود دارد. لذا این تحلیل تا آنجا پیش می‌رود که یک مخاصمه مسلحانه حقیقتاً در جریان است.

۴-۳- نقش بخش خصوصی در مفاهیم حقوق جنگ در حوزه سایبری

قواعد حقوق جنگ در قبال دولت‌ها اعمال می‌شود. ظهور جنگ‌های نامتقارن به‌ویژه جنگ علیه تروریسم، شکل تازه به گفتمان حقوق جنگ داده و تجزیه‌وتحلیل نقش‌آفرینی بخش خصوصی را مطرح کرده است. تأکید اندکی در مورد نقش عناصر غیردولتی در مخاصمات مسلحانه صورت مهاجم این‌گونه استدلال کند که برای قطع ارتباطات و ضربه به نیروهای نظامی این حملات لازم بوده است، ولی با توجه به خسارات ناشی از این حملات به غیرنظامیان، این‌گونه حملات آشکار تجاوز به اصل تناسب خواهد بود. فرض کنید که اگر حملاتی به شبکه اورژانس شود و تعدادی از انسان‌ها به دلیل عدم ارائه خدمات اورژانسی جان خود را از دست بدهند، در این صورت آیا اصل تناسب مورد تعرض قرار گرفته؟ مسلماً پاسخ سؤال مثبت است.

۵- اصول کلی در رابطه با استفاده از تسلیحات

۵-۱- اصول حاکم بر تسلیحات در زمان مخاصمات مسلحانه و رابطه آنها با حملات سایبری

امروز، بشر در عصر فناوری اطلاعات زندگی می‌کند و در حال تجربه فناوری‌هایی است که در میدان‌های جنگ

استفاده می‌شوند. ظهور این فناوری‌ها شاید به چند دهه پیش بازمی‌گردند اما گسترش سلاح‌های جدید و یا روش‌های جنگ که بر چنین فناوری‌هایی تکیه می‌کنند نمایی جدید فراروی حقوق بشردوستانه بین‌المللی ایجاد کرده است. بررسی توسعه فناوری در سال‌های جاری به ما اجازه خواهد داد که نگاه دقیق‌تری را برای بحث در مورد تعدادی فناوری که به‌تازگی وارد میدان جنگ شده و یا می‌توان به‌طور بالقوه آنها را وارد در مخاصمات مسلحانه نمود، داشته باشیم. این پیشرفت‌ها، در فناوری‌های رایانه‌ای و اینترنتی به‌طور خاص مشهود است. در واقع جنگ‌های سایبری سطح جدید از پیشرفت و پیچیدگی به درگیری‌های مسلحانه افزوده است که ممکن است سؤالات جدیدی را در حقوق بشردوستانه بین‌المللی به همراه داشته باشد.

هنجارهای موجود در حقوق بشردوستانه بین‌المللی همچون استفاده بی‌رویه از سلاح، تمایز میان اهداف نظامی و غیرنظامی، تناسب و... می‌توانند و باید در جنگ‌های سایبری نیز اعمال شوند. اگر حمایت از انسان و انسانیت را پایه اصلی تعهد و اصل راهنمای حقوق بشردوستانه بدانیم، تفکیک میان منازعات می‌باشد، به‌هیچ‌عنوان دارای وجاهت و مشروعیت نخواهد بود. در واقع جداسازی حقوق مربوط به هریک از این دو دسته از مخاصمات، نتیجه‌ای جز محروم کردن دسته‌ای از انسان‌ها که تنها گناهشان زندگی در عصر تکنولوژی است نخواهد بود.

ممنوعیت استفاده از ابزار یا روش‌های جنگی که ماهیتاً موجب ورود صدمه شدید و غیر ضروری هستند در تعداد زیادی از معاهدات من‌جمله اسنادی مانند اعلامیه سن‌پترزبورگ و اعلامیه‌ها و مقررات لاهه درج شده است (مقررات سال ۱۸۹۹ لاهه ماده ۳۲، مقررات سال ۱۹۰۷ لاهه، ماده ۲۳. پند (ه). این اصول کلی در رابطه با مخاصمات مسلحانه بین‌المللی و مخاصمات مسلحانه غیر بین‌المللی به‌صورت قابل‌اعمال هستند. در رابطه با ممنوعیت استفاده از این‌گونه ابزارها و روش‌ها، در مخاصمات مسلحانه داخلی بهتر است به نظر دیوان کیفری بین‌المللی برای یوگوسلاوی سابق در پرونده تادیچ در سال ۱۹۹۹ اشاره نماییم: «در واقع از دیدگاه اساسی انسانی و عقل سلیم نقض غرض است اگر استفاده از تسلیحاتی که در درگیری‌های مسلحانه بین دولت‌ها ممنوع شناخته شده، در دیگر موارد که دولت‌ها در صدد سرکوب شورش اتباع داخلی خود و در محدوده قلمرو خود هستند، استفاده از همان سلاح مجاز دانسته شود. آنچه در جنگ‌های بین‌المللی غیر انسانی است و در نتیجه ممنوع است در جنگ‌ها و شورش‌های داخلی هم ممنوع است» [۱۶].

دیوان بین‌المللی دادگستری در نظریه مشورتی در قضیه سلاح‌های هسته‌ای، رنج و صدمات غیر ضروری را به‌منزله «آسیبی بزرگ‌تر از آنچه برای نیل به اهداف مشروع نظامی غیر قابل‌اجتناب است»، ذکر می‌کند [۱۷]. در این راستا، قواعد و مقررات بین‌المللی در دو مسیر جداولی در امتداد هم در ۱۵۰ سال گذشته توسعه یافته‌اند: اولی شامل اصول کلی و مقررات مربوط به ابزارها و روش‌های جنگ، به‌عنوان نتیجه‌ای از به رسمیت شناختن ضروری‌های بشری و تحمیل محدودیت به انتخاب و استفاده از آنها. دوم شامل توافقنامه‌های بین‌المللی که ممنوعیت استفاده از سلاح‌های خاص مانند سلاح‌های شیمیایی و بیولوژیک، از سلاح‌های آتش‌زا، مین‌های ضد نفر و یا مهمات خوشه‌ای را ممنوع و یا محدود کرده است.

استفاده از قواعد حقوقی از قبل موجود، در رابطه با فناوری‌های موجود، این سؤال را مطرح می‌کند که آیا این قواعد و مقررات در پرتو ویژگی‌های فناوری‌های خاص و همچنین با توجه به تأثیرات قابل توجه انسانی این فناوری‌ها، به‌اندازه کافی واضح و روشن هستند؟ در حال حاضر احساس نیاز به قواعد و مقررات در بستر مسائل حقوقی مطرح شده توسط «جنگ سایبری» کاملاً مشهود است. در جنگ سایبری به ابزارها و روش‌های جنگی توسل می‌شود که به فناوری اطلاعات تکیه دارند و در زمینه یک درگیری مسلحانه استفاده می‌شوند، لذا پتانسیل نظامی در این فضا باید به‌طور کامل مورد بررسی قرار گیرد. با بررسی حملات سایبری خاصی که تاکنون اتفاق افتاده، درمی‌یابیم که یکی از طرفین درگیری به‌طور بالقوه می‌تواند به سیستم‌های رایانه طرف دیگر از اطراف مخاصمه حمله نماید، به‌عنوان‌مثال، با نفوذ و یا دستگیری سیستم‌های رایانه‌ای قرار می‌گیرند، در معرض حمله قرار گرفته به‌صورت

اتفاقی یا تعمدی آسیب‌دیده و یا نابود شوند، محتمل است [۱۸].

به نظر می‌رسد با وجود این ممنوعیت‌های سیاسی، مقررات دوستانه بین‌المللی برای انطباق با تحولات تکنولوژیک امروزی به‌اندازه کافی انعطاف‌پذیر است. شکی نیست که مقررات بشردوستانه بین‌الملل قابلیت تسری به سلاح‌های جدید و به تمام فناوری‌های جدید مورد استفاده در جنگ را داراست. به همین خاطر تدوین‌کنندگان پروتکل اول الحاقی به کنوانسیون ژنو به‌صراحت در ماده ۳۶، بررسی این مسئله که کاربرد سلاح‌های جدید با حقوق بین‌الملل مغایرتی نداشته باشد را پیش از ساخت این‌گونه سلاح‌ها به دولت‌های عضو تحمیل می‌کنند. البته با توجه به ماهیت متفاوت جنگ‌های سایبری، باید راه‌حل‌هایی منطبق با خصوصیت فضای سایبر، برای اعمال هرچه بهتر این اصول بنیادین ارائه گردد.

۵-۲- مسئولیت بین‌المللی دولت در حملات سایبری

منشأ حملات صورت گرفته در برابر دولت سه وضعیت می‌تواند داشته باشد: ۱. کاملاً مستقل، ۲. کاملاً دولتی، ۳. نیمه‌دولتی که در دو مورد آخر مسئولیت دولت بدیهی است، حملات صورت گرفته از سوی گروهی که تحت کنترل دولت عمل می‌کند منتسب به دولت می‌باشد و بنابراین دولتی که قربانی چنین اقداماتی می‌گردد می‌تواند از تمام ضمانت اجراهای مقرر در حقوق بین‌الملل بهره‌مند شود [۱۹] اما وقتی‌که ارگان حمله‌کننده خصوصی است به نظر می‌رسد که دولت‌ها تمایل دارند در فقدان یک تعهد عام‌الشمول حقوق بین‌الملل از مسئولیت اقدامات اشخاص خصوصی جز در موارد خیلی استثنایی شانه خالی کنند (در حقوق بین‌الملل اعمال و رفتار اشخاص خصوصی قابل انتساب به دولت نیست زیرا این اشخاص علی‌الاصول دارای سمتی از طرف دولت نیستند، لذا دولت فقط در قبال اعمال و رفتار خلاف موازین حقوق بین‌الملل مأموران و نمایندگان خود مسئول واقع می‌شود با این وجود اگر اشخاص خصوصی به‌صورت رسمی و قانونی از طرف و یا عملاً به نمایندگی از طرف او اقدام نمایند، اعمال آنها منتسب به دولت خواهد بود، ماده ۱۱ طرح مواد راجع به مسئولیت بین‌المللی دولت تحت عنوان «عمل اشخاص بدون نمایندگی از سوی دولت» در این زمینه مقرر می‌دارد: عمل شخص یا گروهی از اشخاصی که به نمایندگی از دولت انجام نگرفته باشد نباید از نظر حقوق بین‌الملل عمل دولت شناخته شود). همچنین اگر گروهی غیردولتی از دولت «الف» کمک آشکار و مؤثری به حمله‌کنندگان به دولت «ب» ارائه دهند مسئولیت بین‌المللی دولت اول محرز است.

۵-۲-۱- راهبرد برخی کشورها در حملات سایبری

کشورها در مورد توانایی حملات سایبری خود سکوت اختیار کرده‌اند و از اینکه خود را به قواعدی در چنین حوزه نوظهوری پایبند کنند اکراه می‌ورزند[۱۱]، البته ماهیت حوزه سایبر به‌تنهایی بر محرمانه بودن آن دامن می‌زند و به‌صورت کاملاً مخفی از جانب کاربرانی گمنام صورت می‌گیرد. به‌علاوه مشخص نیست که آیا عملیات سایبری قطعاً منجر به اعمال قواعد جنگ می‌گردد. از این‌رو تحقیقات حقوقی حوزه حملات سایبری تا حد زیادی درگیر فرضیه‌سازی به کمک محققانی است که قصد دارند سناریوهای متعدد سایبری کنونی را درون اصول و قواعد حقوق جنگ داخل کنند.

پس از آنکه نخستین هک شدن گوگل در ژانویه ۲۰۱۰ رخ داد و گوگل حملات صورت گرفته را به سرقت بردن مالکیت معنوی این شرکت خواند[۱۲]، در ماه مه ۲۰۱۱ یکی از دپارتمان‌های ایالات‌متحده، راهبردی بین‌المللی برای اداره کردن فضای سایبری منتشر کرد که حاکی از آن بود که آمریکا حق دفاع مشروع در برابر حملات مشروع را در مواردی برای خود مشروع می‌پندارد[۱۳] و پس از آن بود که پنتاگون اسناد مربوط به راهبردهای نوین و طبقه‌بندی شده خود در حوزه سایبر را منتشر کرد و با این اسناد حملات سایبری از جانب یک کشور خارجی را یک عمل جنگی تعبیر می‌کند [۲۰]، اندکی بعد دفتر مرکزی دپارتمان ایالتی از محرک‌هایی برای ایجاد «سایه» اینترنتی و سیستم‌های تلفن همراه خبر داد که قادرند برای پشتیبانی معاندین در کشورهایی که با سخت‌گیری از جانب رژیم ظالم مواجهند،

استفاده شود [۲۱].

کشور چین در پی مورد حملات سایبری قرار گرفتن از شکل‌گیری یک «ارتش آبی آنلاین» جهت تکمیل «ارتش سرخ سنتی» خود خبر داد و یک ژنرال سابق ارتش چین با اشاره به یک مجموعه هکرهای وطنی افزود «هک کردن مثل بازی پینگ‌پنگ برای ماست که بسیاری از مردم ما آن را بازی می‌کنند و ما در آن مهارت داریم» [۲۲].

در مورد قوانین سایبری به تصویب درآمده در جهان (دسامبر ۲۰۰۰)، از ۵۲ کشور تحقیقی به عمل آمد که نشان می‌داد قوانین سایبری ۳۳ کشور از جمله ایران، ایتالیا، اردن، بلغارستان، باکو و... به‌هیچ‌وجه به‌روز نشده است. قوانین ۹ کشور ازجمله برزیل، شیلی، چین، چک، دانمارک و... نسبتاً به‌روز و قوانین ۱۰ کشور از جمله استرالیا، کانادا، استونی، هند، ژاپن و... کاملاً به‌روز شده است. در خصوص کشور خودمان ایران باید بگوییم که مقامات رسمی کشور تصویب قانون و انجام سایر اقدامات لازم علیه جرائم سایبری را مقدمه‌ای برای مبارزه با این جرم چه در سطح داخلی و چه بین‌المللی می‌دانند.

معرفی جرائم سایبری به‌عنوان یکی از موضوعات کلیدی مطرح شونده در «کمیسیون سیاست‌گذاری جنایی و اصلاح قوانین کیفری» دلیل مستندی بر ادعای مذکور می‌باشد. انتخاب این موضوع به‌عنوان یکی از موضوعات مطرح شده در کمیسیون مذکور نشان می‌دهد که دولت نیاز به مبارزه با این نوع جرائم را بسیار ضروری خوانده و آگاه است که با همکاری‌های بین‌المللی و به‌کارگیری بهترین تجربیات بین‌المللی تحقق این هدف را تسهیل خواهد کرد.

اهداف اساسی این پروژه شامل تقویت دستگاه قضائی و ظرفیت‌های اجرایی قانونی کشور در رابطه با جرائم سایبری، تهیه آماری در مورد وقوع این نوع جرائم در کشور، توسعه یک مکانیسم پاسخ‌گویی ایده‌آل به این نوع جرائم و سرانجام ارتقاء آگاهی عمومی از جرائم سایبری در میان جمعیت کاربر اینترنت می‌باشد [۲۳].

۵-۲-۲- اقدامات بین‌المللی در مورد حملات سایبری

اولین سازمان بین‌المللی، سازمان همکاری شانگهای بود که حملات مجازی را به‌عنوان عامل مخرب برای اخلاق، معنویت و فرهنگ از سوی مهاجمان تعریف کرده است. در سپتامبر ۲۰۱۱ کشورهای عضو پیشنهاد تدوین شاخص‌های بین‌المللی برای یک سند جامع امنیت اطلاعاتی را به دبیر کل سازمان ملل ارائه دادند، این طرح از سوی کشورهای غربی حمایت نشد، زیرا رویکرد کشورهای غربی بیشتر بر جنبه‌های اقتصادی متمرکز بود.

در حال حاضر پروژه‌ای توسط دکتر Merezhko Alexander استاد حقوق بین‌الملل در حال تدوین برای ارائه به سازمان ملل است که طبق آن حملات سایبری به معنای استفاده از اینترنت و فناوری‌های وابسته به آن توسط یک دولت، بر ضد منافع اقتصادی، سیاسی، فناوری و اطلاعاتی یک حاکمیت دیگر است، ولی وی بیان می‌دارد که اینترنت میراث مشترک بشریت است و باید از حملات نظامی مصون بماند [۲۴].

۶- راهبرد بین‌المللی دولت‌ها

حقوق بین‌الملل نیز همچون سایر علوم در معرض اثرات مثبت و منفی پیشرفت فن‌آوری قرار دارد و برای انطباق خود با شرایط روز، ناچار به تعدیل، خلق و گاه انطباق قواعد موجود با زمینه‌های جدید می‌پردازد. چه‌بسا این سه گونه واکنش به‌صورت هم‌زمان و در یک ظرف زمانی که به تثبیت قواعدی حداقلی در زمینه جدید منجر می‌شود، عمل نماید. به‌واقع، چالش‌های نوینی که در برابر حقوق بین‌الملل قرار می‌گیرند، ظرفیت‌های این علم را محک زده و منجر به شکوفایی گستره‌ای جدید در چشم‌انداز منابع و ابزارهای تفسیر می‌شود. فضای سایبر از جمله چالش‌های اخیر حقوق بین‌الملل به شمار می‌رود که پرسش‌های بنیادینی را پیش روی حقوقدانان بین‌المللی قرار داده است.

هارولد کو (مشاور حقوقی وزارت امور خارجه ایالات‌متحده آمریکا) در کنفرانسی پیرامون مسئله فضای سایبر و امنیت ملی ایالات‌متحده آمریکا، بار دیگر پرسش چالش‌برانگیز و اخیر پیرامون نحوه اجرا و اعمال قواعد قدیمی حقوق جنگ بر شرایط نوین فضای سایبر را با توجه به توسعه و پیشرفت فناوری و قصد اجرای اصول بنیادین حقوق بشردوستانه مطرح نمود و از منظر راهبرد دولت متبوع خویش، دیدگاه اخیر

ایالات‌متحده آمریکا را دراین‌باره به تصویر کشید.

به‌زعم مشکلات بدیعی که این زمینه در خود دارد اما اصول حقوق بین‌الملل بر فضای سایبر قابل اعمال است. هرچند این دیدگاه در سطح جهانی بدین نحو نبوده و برخی دولت‌ها معتقدند که چنین نیست و باید قواعد معاهده‌ای جدید در این زمینه پاسخگوی مسائل مربوطه باشند.

فضای سایبر منطقه‌ای خارج از حیطه حقوق نیست و کسی نمی‌تواند در آن به فعالیت‌های خصمانه مبادرت ورزد بدون اینکه دچار محدودیتی بوده و یا از حیطه حقوق و قانون خارج باشد. حقوق بین‌الملل تا پیش از این نیز با نوآوری‌های جدید در عرصه علمی مواجه شده و آن حوزه‌ها را نیز تحت قاعده در آورده است؛ اما در اینجا برای آن دسته از افرادی که معتقدند حقوق به اندازه کافی در این عرصه وجود ندارد باید به دنبال ایجاد اجماعی در این خصوص بود که آیا و به چه تعداد دریافت و درک دیگر از این نکته نیاز وجود دارد. به همین دلیل، فزونی دریافت‌های مشترک در این باره موجب ثبات در این حوزه حقوقی می‌گردد و به پرسش‌های مطروحه پیرامون مسئولیت بین‌المللی دولت‌ها ناشی از جنگ و حملات سایبری پاسخ می‌دهد.

فعالیت‌های مزبور می‌تواند در برخی شرایط موجب مسئولیت بین‌المللی و مفهوم توسل به زور مندرج در منشور ملل متحد و عرف بین‌المللی باشد. این‌گونه فعالیت‌ها که تقریباً منجر به مرگ، صدمه یا خسارت جدی می‌شوند، می‌توانند به‌عنوان توسل به زور مطمح نظر قرار گیرند. مثال‌های مشترکی که برای فعالیت سایبری منجر به توسل به زور می‌شود، عبارتند از: عملیاتی که تأسیسات هسته‌ای را در یک بحران قرار می‌دهند؛ عملیاتی که منجر به باز شدن یک سد بر روی یک منطقه دارای جمعیت که منجر به آسیب شود؛ عملیاتی که منجر به اخلال در ترافیک هوایی شده و در نتیجه، تصادمات هوایی را در پی داشته باشند. در واقع، اگر آثار فیزیکی ناشی از یک حمله سایبری همانند رها کردن یک بمب یا شلیک یک موشک باشد، حمله سایبری مزبور نیز باید به‌عنوان ایجاد مسئولیت بین‌المللی و توسل به زور مورد ارزیابی قرار گیرد.

۶-۱- فرآیند تدوین قوانین جهانی

تقنین فضای سایبر در خلأ امکان‌پذیر نیست. قانون‌گذاری صحیح این فضا نیاز به شرایط باروری و ساختنی دارد. امروزه با توجه به آنچه پیش از این بیان شد، تدوین قوانین جهانی امنیت سایبری و ایجاد مسئولیت بین‌المللی برای دولت‌ها ضروری است [۷]. کشورهای غربی با توجه به آسیب‌پذیری‌هایی که در زمینه امنیت سایبری دارند و این موضوع روزبه‌روز خود را بیشتر بروز می‌دهد؛ این نیاز را به‌شدت احساس می‌کنند که باید قوانینی جهان‌شمول برای جنگ سایبری وضع شود.

کارشناسان روسیه و ایالات‌متحده آمریکا در یک کنفرانس امنیتی به رهبران جهان اعلام می‌کنند که برای جلوگیری از خطرات سلاح‌های سایبری، جهان به قوانین و التزام‌هایی در زمینه جنگ سایبری نیاز دارد. طرح سایبری به‌طور اختصاصی از سوی نیوزنایت (Newsnight)، از مؤسسه با نفوذ ایست‌وست در نیویورک مطرح شده و تحت عنوان اجرای کنوانسیون‌های ژنو و لاهه در زمینه فضای سایبری توصیف می‌شود. در سال پیش امنیت سایبری برای اولین بار در دستور کار کنفرانس سالیانه مونیخ قرار گرفت. در این اجلاس، نخست‌وزیر انگلیس، صدراعظم آلمان، وزرای امور خارجه ایالات‌متحده آمریکا و روسیه حضور یافتند. منطق پشت این حرکت این است که در دنیای درهم‌آمیخته مجازی ممکن است نیاز باشد که از مناطق ارائه‌دهنده تسهیلات و خدمات نظیر بیمارستان‌ها و مدارس، حفاظت شود. پیش‌نویس این طرح همچنین خواستار باز تعریف مفهوم دولت - ملت، با قلمروها و بازیگران جدید در فضای مجازی و فراتر از دولت‌ها، نظیر شرکت‌های چندملیتی و شهروندان است. این طرح همچنین بیان می‌کند، ابهاماتی که در مورد جنگ سایبری وجود دارد، باعث به تأخیر افتادن سیاست بین‌المللی در مقابله با آن است و اینکه شاید ایده‌های جنگ یا صلح برای عصر اینترنت که جهان می‌تواند خود را در حالت سومی غیر از جنگ یا صلح قرار دهد، بسیار ساده و پیش پا افتاده باشد. در این راستا تیم روسی - آمریکایی متذکر می‌شوند که تشخیص تفاوت بین اهداف شخصی و نظامی در فضای مجازی بسیار سخت است و ممکن است به علائم محافظت شده و کاملاً آشکار و محسوس نیاز داشته باشد. آنها می‌گویند که سلاح‌های

سایبری نه ویژگی‌های سلاح‌های قدیمی را دارند و نه مشمول قوانین فعلی جنگی می‌شوند؛ سلاح‌های سایبری می‌توانند در یک چشم به هم زدن از راه رسیده (ویروس‌هایی که به‌سرعت تکثیر و منتشر می‌شوند) و درحالی‌که فاقد قدرت تشخیص اهداف هستند، حمله کنند. جان بومگارنر (مدیر تحقیقاتی در زمینه تکنولوژی امنیتی در واحد پیامدهای سایبری ایالات‌متحده آمریکا) در صحبتی با نیوزنایت در مورد انواع تهدیداتی که در این زمینه وجود دارد می‌گوید: تکنولوژی‌های مخفیانه‌ای می‌تواند در سیستم‌های کامپیوتری کار گذاشته و اجرا شوند به‌طوری‌که شما اصلاً متوجه آن نشوید. «وی می‌گوید بعضی ظرفیت‌هایی که در حال حاضر وجود دارند عبارتند از: از کار انداختن شبکه‌های برق، ایجاد اختلال در منابع ذخیره آب و سیستم‌های تولیدی در صنایع. تقریباً هر روز گزارش‌هایی در مورد پیشامدهای سایبری می‌رسد. پروفسور پیتر سامر (Peter Sommer) از مدرسه اقتصاد لندن که اخیراً گزارشی را در مورد امنیت سایبری برای سازمان توسعه و همکاری اقتصادی (OECD) نوشته است می‌گوید: «این مسئله واقعاً اهمیت دارد ولی در مورد آن اغراق و جاروجنجال نیز زیاد شده است».

در ژوئن ۱۹۸۲، اوج جنگ سرد، یک ماهواره اعلام خطر آمریکایی انفجار عظیمی را در سیبری شناسایی کرد. آیا موشکی شلیک شده بود؟ یک آزمایش اتمی بود؟ به نظر می‌رسد که یک انفجار در خطوط انتقال گاز شوروی بود. علت آن نقص در سیستم کنترل کامپیوتری‌ای بود که جاسوسان شوروی از یک شرکت کانادایی دزدیده بودند. بر اساس خاطرات توماس رید، از فرماندهان سابق نیروی هوایی ایالات‌متحده آمریکا، آنها نمی‌دانستند که سیا نرم‌افزار آن را طوری دست‌کاری کرده بود که پس از مدتی از کنترل خارج شده و سرعت پمپ‌ها و تنظیمات دریچه‌ها را به حالتی برگرداند که باعث افزایش فشار تا حدی بسیار فراتر از میزان تحمل اتصالات لوله‌ها بشود. به گفته او، نتیجه‌ی این کار بزرگ‌ترین انفجار و آتش غیر اتمی بود که تاکنون از فضا مشاهده شده بود (www.economist.com).

این یکی از اولین نمایش‌های قدرت یک بمب منطقی بود. اکنون پس از سه دهه، که سیستم‌های کامپیوتری حساس زیادی به اینترنت متصل شده‌اند، آیا دشمنان می‌توانند از بمب‌های منطقی مثلاً برای قطع کردن برق از آن‌سوی دنیا استفاده کنند؟ یک مقام ارشد نظامی آمریکایی می‌گوید این موضوع مرا تا حد مرگ می‌ترساند. از نظر مایک مک کانل، از رؤسای سابق سازمان جاسوسی ایالات‌متحده آمریکا، آثار یک جنگ سایبری تمام‌عیار خیلی شبیه یک جنگ هسته‌ای است. وی می‌گوید: جنگ سایبری هم‌اکنون آغاز شده است و ما داریم آن را می‌بازیم (http://jang-syberi.blogfa.com). آخرین تلاش‌ها برای تدوین مواد قانون برخوردهای مسلحانه که در نهایت به تصویب پروتکل الحاقی اول ۱۹۷۷ پیمان ژنو انجامید، تأکید دارد که حملات نباید علیه شهروندان غیرنظامی یا «اهداف غیرنظامی» انجام شود. تفسیرهایی که از سوی کمیته بین‌المللی صلیب سرخ در ژنو مورد تأیید قرار گرفته‌اند تأکید دارند که هیچ استثنای مجازی برای این محدودیت‌های قید شده وجود نداشته و اینکه آنها درست همان‌طور که در خصوص روش‌های سنتی جنگ کاربرد داشته‌اند، در زمینه حملات سایبری نیز قابل استفاده خواهند بود. تعداد بسیار زیادی از تحلیلگران قوانین، این تفسیر را مورد تأیید قرار داده‌اند.

اما اشتباه بزرگی است اگر بکوشیم که اقدامات تلافی‌جویانه سایبری را نیز در این چارچوب جای دهیم. با وجود اینکه بسیاری از مواد پروتکل الحاقی اول حالا دیگر بخشی از قوانین عرفی محدود کننده اقدامات جنگی هستند، اما با این حال بعضی کشورها به‌صورت رسمی این پروتکل را نپذیرفته‌اند، و برخی دیگر از کشورها (از جمله انگلیس، فرانسه، آلمان، کانادا و استرالیا) که این پروتکل را پذیرفته‌اند، این کار را تنها پس از لحاظ کردن قیودی رسمی به پروتکل انجام دادند که حق تلافی‌جویی غیرنظامی به‌عین را در برابر دشمنانی که محدودیت‌های ذکر شده در پیمان را زیر پا می‌گذارند، برای آنها محفوظ بدارد. حتی اگر تمام حملات سایبری را به لحاظ قانونی معادل «حمله مسلحانه» بدانیم و فرض را بر این بگذاریم که تمام محدودیت‌های قانونی برخوردهای مسلحانه در قلمروی سایبر نیز کاربرد دارند، آنگاه ادعای کمیته بین‌المللی صلیب سرخ که حملات سایبری تلافی‌جویانه هرگز نباید علیه

شهروندان یا «اهداف غیرنظامی» اجرا شوند، چندان قانع کننده به نظر نمی‌رسد.

جنگ در دریا متفاوت است. هدف این جنگ‌ها، نه یورش و تصرف قلمرو که حملات پی‌درپی و آسیب رساندن به دشمن است. از روش‌های متداول برخوردهای دریایی می‌توان به ایجاد اختلال در مراودات تجاری دشمن، از طریق تصرف و برخی اوقات غرق کردن کشتی‌های بازرگانی اشاره کرد. در این جنگ‌ها دیگر لازم نیست که کشورهای متخاصم نگران شهروندان غیرنظامی ساکن در مناطق جنگی باشند، اما در قدیم، دریا نیز مرامنامه عرفی خود را داشت که تعیین‌کننده رفتار مناسب با خدمه کشتی تصرف شده بود. طرفین جنگ هیچ تمایلی به تحریک کشورهای بی‌طرفی نداشتند که اگر کشتی‌های خودشان مورد حمله قرار می‌گرفت یا احساس می‌کردند که به‌واسطه رفتارهای غیر قابل پذیرش رزم‌ناوها تهدید می‌شوند، ممکن بود وارد جنگ شوند. بنابراین قدرت‌های دریایی، چه در کشتی‌های جنگی و چه در کشتی‌های بازرگانی، در برخورد با خدمه‌ای که خود را تسلیم می‌کردند، رفتار قابل‌قبول و کنترل شده‌ای داشتند. بنابراین در جنگ‌های کلاسیک دریایی، تمایز در میان اهداف مجاز و غیر مجاز تعریف می‌شد و نه میان اهداف نظامی و غیر نظامی؛ به‌طور نمونه، مهاجمانی که به کشتی‌های بازرگانی یورش می‌بردند، وارد یک کشتی می‌شدند، ملیت آن را مشخص کرده و اگر این کشتی متعلق به دشمن بود، هم کشتی و هم بار آن را به‌عنوان «غنیمت جنگی» به تصرف خود درمی‌آوردند. اگر یک کشتی جنگی تصمیم داشت که کشتی دیگری را غرق کند، این کار را تنها پس از تلاش برای کمک به خدمه کشتی و تأمین امنیت جانی آنها انجام می‌داد. تا پایان قرن نوزدهم، به سبب فناوری‌های بدوی دریایی، رعایت چنین احتیاط‌هایی در زمان تصرف کشتی دشمن برای مهاجمان به کشتی‌های تجاری، امکان‌پذیر و بی‌خطر بود. اما در قرن بیستم این سیستم فرو پاشید، زیرا ارتباطات رادیویی برای آن دسته از کشتی‌های تجاری که مورد حمله قرار می‌گرفتند، این امکان را فراهم می‌ساخت که از رزم‌ناوهای کشورهای هم‌پیمان درخواست کمک کنند و این مسئله سوار شدن به کشتی هدف، جست‌وجوی آن، و کسب اطمینان از امنیت جانی خدمه کشتی، پیش از غرق کردن آن را برای مهاجمان به کار پر مخاطره‌ای بدل می‌کرد. از سوی دیگر در همین زمان بود که زیردریایی‌ها و هواپیماها ظرفیت خود را به‌عنوان اسلحه‌ای قدرتمند در دریا نشان دادند. اما آنها فاقد هرگونه قابلیتی برای ورود مهاجمان به کشتی هدف و انجام جست‌وجوهای لازم بودند. در نتیجه در طول جنگ‌های جهانی، حملات مرگبار بدون اخطار به روندی عادی و معمول تبدیل شد. به‌علاوه هم‌پیمانان دریایی با استفاده از ناوگان‌های سطحی خود مسیر کشتیرانی دشمن را سد می‌کردند و با این کار مانع از عبور تمام کشتی‌های بی‌طرف، حتی آنهایی که غذا و سوخت حمل می‌کردند، می‌شدند.

اگر ما هنوز جنگ‌های زمینی و دریایی را در دو دسته مختلف و متمایز طبقه‌بندی می‌کنیم، به‌طور قطع باید برخوردهای سایبری را در دسته دوم قرار دهیم، به‌علاوه برخوردهای سایبری حقیقتاً شباهت‌های بیشتری با جنگ‌های دریایی اولیه دارند تا برخوردهای دریایی قرن بیستم. در برخورد سایبری، مهاجمان درعین‌حال که با خطرات بسیار اندکی روبه‌رو هستند، می‌توانند بدون تهدید جان شهروندان غیرنظامی، خسارات اقتصادی قابل‌توجهی را به هدف مورد نظر خود وارد آورند. نفوذگران سایبری نیز مانند مهاجمان دریایی گذشته، به‌طور معمول، به هیچ نحو، با شهروندان کشور هدف برخورد نداشتند. بنابراین، مهاجمان سایبری نیز انگیزه‌هایی را که نیروهای زمینی را به اعطای مصونیت به شهروندان غیر نظامی دشمن وامی‌داشت، در برابر خود نمی‌بینند.

البته ما هنوز دلایل بسیار خوبی داریم که در برخورد سایبری و زمانی که پای جان شهروندان غیرنظامی در میان است، محدودیت‌های بشردوستانه را مد نظر قرار دهیم؛ اما حملات سایبری می‌توانند بدون خسارات جانی، ضربات سختی را به اقتصاد وارد آورند؛ بنابراین تنظیم قواعدی برای ممانعت از کشته شدن شهروندان در جریان تبادل آتش میان طرفین در این بحث چندان قابل توجیه به نظر نمی‌رسد، بلکه بیشتر منطقی است که در پی قوانینی باشیم که مانع از آن شود که شرایط سخت اقتصادی یا دیگر مزاحمت‌های شخصی به شهروندان آسیبی برساند. بنابراین ما به وضع مصونیت کامل برای آنچه پروتکل الحاقی اول

«اهداف غیر نظامی» می‌نامد (یعنی تجهیزات، تأسیسات و زیرساخت‌هایی اقتصادی که به دستیابی به مقاصد «نظامی» اختصاص نیافته باشد) نیازی نداریم.

در بمباران‌های جنگ‌های قرن بیستم، تأسیسات صنعتی تولید سلاح، از دید راهبردسازان جنگ، اهداف درجه دوم محسوب می‌شد: زیرا نسبت به دیگر تأسیسات غیر نظامی مناسب‌تر، و نسبت به زیرساخت‌های کاملاً نظامی نامناسب‌تر بودند. اما در این تحلیل‌ها نگاشت خوبی بر روی واقعیت برخوردهای قلمروی سایبر وجود ندارد. برخوردهای سایبری نیازی به زیرساخت‌های تخصصی ندارند. رایانه‌ها و ابزارهای توسعه نرم‌افزاری که ممکن است در این قبیل حملات مورد بهره‌برداری قرار گیرند، به‌سختی قابل‌تمایز از آن دسته ابزارهایی هستند که تنها برای مقاصد تجاری با پژوهش‌های غیر نظامی استفاده می‌شوند، اگر اساس قابل تمایز باشند. اگر بکوشیم به «بخش فناوری‌های پیشرفته (High-Tech)» دشمن به‌عنوان یک هدف نظامی حمله کنیم، احتمالاً در یک قیاس نسبی، میزان آسیبی که به اهداف غیرنظامی وارد خواهیم آورد می‌تواند قابل‌مقایسه با خسارات بمباران‌های جنگ جهانی دوم باشد، اما این بار با توجیه‌پذیری بسیار کمتری زیرا امروزه دیگر از قابلیت‌های فراوانی برای تشخیص و تمیز اهداف برخورداریم. با این حال اگر منحصراً بر روی شبکه‌های رایانه‌ای نظامی متمرکز شویم، دیگر با چنین مسئله‌ای مواجه نخواهیم بود.

در قدیم، قانون برخوردهای مسلحانه در پی تعریف تمایز «نظامی» از «غیر نظامی»، نه‌تنها از منظر تشخیص اهداف مجاز، که همچنین از دید کیفیت مشارکت در نبرد بود. به‌طور عمده به این علت که اگر شهروندان غیر نظامی، عرف منع مشارکت در جنگ را نادیده می‌گرفتند، مبارزان نظامی نیز دیگر نمی‌توانستند عرف تمایز میان اهداف نظامی و غیر نظامی را رعایت کنند. در نوشتارهای قدیمی‌تر، از مبارزان غیر نظامی با عنوان «خائن» یا «جنایتکار جنگی» یاد شده است. با این حال، در این معاهده‌ها به وجود برخی از استثنائات (حتی در جنگ‌های زمینی) نیز اشاره شده است. «پیمان لاهه در خصوص جنگ‌های زمینی» و «پیمان سوم ژنو» سال ۱۹۴۹، چتر حمایت از اسرای جنگی را به اعضای ارتش‌ها و دیگر افراد خارج از چارچوب ارتش‌های منظم، البته در صورت برخوردار بودن از شرایطی خاص، گسترش داد. اما هیچ‌یک از این حمایت‌ها در برخوردهای سایبری چندان معنادار به نظر نمی‌رسد. یورش‌های سایبری تقریباً همیشه به‌صورت مخفیانه هدایت می‌شوند: به‌طور قطع وزارت دفاع ایالات‌متحده آمریکا اگر تصمیم به حمله به یک شبکه رایانه‌ای داشته باشد، هیچ‌گاه یک پیام مخرب سایبری را با ایمیلی که به‌منزله یک آدرس بازگشت و تعیین‌کننده هویت فرستنده است، برای کسی نخواهد فرستاد. امروزه در اینترنت، جرائم و فعالیت‌های جاسوسی سایبری بسیار زیادی به وقوع می‌پیوندد طوری که هیچ کشوری نمی‌تواند ادعا کند که به هویت غیر نظامی پیام‌های دریافتی خود اطمینان داشته و می‌تواند ارسال پیام‌های آلوده را به‌منزله «خیانت» تلقی کند. مبارزان سایبری در قلمروی دشمن حضور فیزیکی نخواهند داشت. بنابراین دستگیری آنها توسط دشمن بسیار غیرمحتمل است، در نتیجه دیگر نیازی به حمایت پیمان ژنو از اسرای جنگی نیز وجود ندارد. نفوذگران غیرنظامی نیز با نظم اصولی ارتش و در پیروی از دنباله‌ای از دستورات قابل شناسایی عمل نمی‌کنند. به‌علاوه، درحالی‌که نیروهای غیر نظامی در نبردهای سنتی برای داشتن عملکردی مؤثر تا اندازه‌ای به آموزش‌های نظامی مقدماتی نیاز دارند، چنین مسئله‌ای برای نفوذگران غیر نظامی صادق نیست. مهارت‌هایی که این افراد به آنها نیاز دارند کاملاً در بخش‌های غیر نظامی صنعت فناوری اطلاعات توسعه‌یافته و شکوفا شده‌اند. از آنجا که امروزه تهدیدات غیر نظامی بسیار زیادی شبکه‌های رایانه‌ای را هدف قرار داده است، توسعه‌گران تجاری و دانشکده‌های علوم رایانه در حال حاضر بر امنیت شبکه برای مصارف غیر نظامی متمرکز شده‌اند؛ و درک ضرورت امنیت رایانه به معنای درک چگونگی اجرای حملات سایبری است (با این حال، در این معاهده‌ها به وجود برخی از استثنائات حتی در جنگ‌های زمینی نیز اشاره شده است. «پیمان لاهه در خصوص جنگ‌های زمینی و پیمان سوم ژنو» سال ۱۹۴۹، چتر حمایت از اسرای جنگی را به اعضای ارتش‌ها و دیگر افراد خارج از چارچوب ارتش‌های منظم، البته در صورت برخوردار بودن از شرایطی خاص، گسترش داد). برنامه درسی دانشکده‌های علوم رایانه روزبه‌روز بیش از پیش به

تدریس فنون مرتبط با حملات سایبری اختصاص می‌یابد، رقابت‌هایی سازمان‌دهی شده و (قانونی) وجود دارد که در آنها دانش‌آموزان و دانشجویان به رقابت برای ثبت سریع‌ترین و مؤثرترین نفوذ به رایانه‌های هدف می‌پردازند («کنفرانس بین‌المللی تسخیر پرچم دانشگاه کالیفرنیا، سانتا باربارا» ۲۰ سپتامبر، ۲۰۱۱). دانشکده‌ها نیز فراخوان‌هایی را برای جذب دانشجویانی منتشر می‌کنند که بتوانند با نرم‌افزارهای آلوده و مخرب کارکرده و حتی خود اقدام به نوشتن چنین نرم‌افزارهایی بکنند (جورج لدلین، «آسیب فزاینده عدم وجود آموزش‌های مناسب در خصوص بدافزارها»، بخش ارتباطات انجمن ماشین‌آلات رایانه‌ای (ACM) فوریه ۲۰۱۱، صفحات ۳۴-۳۲). به‌راحتی می‌توان شهروندانی با چنین مهارت‌هایی را معادل شبه‌نظامیان حوزه فناوری‌های پیشرفته تصور کرد. به‌طور قطع، اگر یک برخورد سایبری علنی با یک دشمن شناخته شده وجود داشته باشد، افراد زیادی را می‌توان در بخش خصوصی یافت که از مهارت‌های فنی لازم برای مشارکت در اقدامات تلافی‌جویانه برخوردار باشند.

در اینجا دوباره بهتر است با استناد به تجارب گذشته، در پی یافتن شیوه‌های خلاقانه‌تری برای بررسی برخوردهای سایبری باشیم. از آنجا که برخوردهای سایبری شباهت‌های بیشتری با جنگ‌های دریایی کلاسیک دارند، بهتر است به یاد آوریم که حکومت‌ها غالباً در موقعیت‌های خاص از دریانوردان توانمندی که عضو نیروی دریایی نبودند، درخواست کمک می‌کردند. پیش از میانه قرن نوزدهم، کشتی‌هایی جنگی با عنوان «مزدور ناوها» در دریا حضور داشتند که از طرف حکومت‌ها مأموریت می‌یافتند به کشتی‌های دشمن حمله کنند. سهم آنها درصدی از غنائمی بود که می‌توانستند از کشتی‌های تجاری دشمن به دست آورند. این دریانوردان با دزدان دریایی ساده تفاوت داشتند (هرچند شباهت‌های آشکاری نیز میان آنها وجود دارد) زیرا از سوی مقامات رسمی کشورهای پشتیبانی یک به‌اصطلاح «حکم ضبط اموال بیگانگان» برای آنها صادر می‌شد.

۶-۲- حل‌وفصل اختلافات ناشی از جنگ سایبری

بعد از آنچه بیان شد و فرض بر وقوع جنگ یا حملات سایبری و شناسایی دولت خاطی و در پی ایجاد مسالمت بین دو کشور درگیر در جنگ سایبری به بررسی چگونگی حل‌وفصل اختلافات به وجود آمده بین این کشورها می‌پردازیم و به توضیح انواع روش‌های حل‌وفصل اختلافات بین‌المللی و ترمیم و آغاز دوباره رابطه حقوقی طرف‌های درگیر می‌پردازیم.

۶-۲-۱- جبران خسارت

دولت مسئول فعل متخلفانه بین‌المللی متعهد دو اقدام می‌باشد [۸]:

یکی توقف رفتار متخلفانه و دیگری ارائه تضمین‌های مناسب از سوی دولت مسئول برای عدم تکرار آن فعل، هر دو موضوع، ابعادی از احیاء و ترمیم رابطه حقوقی است که بر اثر نقض آسیب دیده است. توقف، جنبه سلبی دارد و به دنبال پایان بخشیدن به رفتار متخلفانه در حال اجرا است درحالی‌که ارائه تضمین‌ها، کارکردی پیشگیرانه دارد و می‌توان آن را تقویت اجرای تعهد در آینده توصیف کرد. در هر دو، تداوم اعتبار تعهد نقض شده یک فرض ضروری است زیرا اگر اجرای تعهد پس از نقض آن متوقف شده باشد، مسئله توقف و ارائه اطمینان و تضمینات مطرح نمی‌شود (در این خصوص مقایسه کنید با بند (۱) ماده ۷۰ کنوانسیون ۱۹۶۹ وین راجع به حقوق معاهدات).

توقف رفتار ناقض تعهد بین‌المللی نخستین شرط محو آثار رفتار متخلفانه است. این شرط به همراه جبران خسارات یکی از دو نتیجه کلی مترتب بر فعل متخلفانه بین‌المللی است. توقف رفتار متخلفانه عمدتاً کانون اصلی مشاجراتی است که از رفتار ناقض تعهد بین‌المللی ایجاد می‌شود. نه‌تنها دولت‌ها بلکه ارگان‌های سازمان‌های بین‌المللی همچون مجمع عمومی و شورای امنیت نیز در مواقعی که با نقض‌های شدید حقوق بین‌الملل مواجه می‌شوند خواستار توقف آن رفتارها می‌شوند.

تعهد به جبران کامل خسارت وارده به دولت زیان‌دیده، دومین تعهد کلی دولتی است که مرتکب فعل متخلفانه بین‌المللی شده است. دیوان دائمی دادگستری بین‌المللی به این اصل کلی نتایج و آثار ارتکاب فعل متخلفانه بین‌المللی

در کارخانه کورزوف اشاره کرده است:

این یک اصل حقوق بین‌الملل است که نقض هر تعهد، تعهد به جبران آن را به شکلی مناسب در پی دارد. از این‌رو جبران خسارت عنصر لاینفک قصور در اجرای یک کنوانسیون است و ضرورتی ندارد که به این مسئله در خود آن کنوانسیون تصریح شود. در نتیجه اختلافات راجع به جبران خسارت که بر اثر قصور در اجرای کنوانسیون مطرح می‌شوند اختلافات مربوط به اجرای آن کنوانسیون است (Factory at Chorzow, Jurisdiction, 1927, P.C.I.J., Series A, No. 9, at p. 21). محور تمامی آثار فعل متخلفانه ممکن است بسته به نوع و میزان زیان و خسارت وارده مستلزم آن باشد که برخی با تمامی اشکال جبران خسارت به کار گرفته شود [۹]. از میان اشکال مختلف جبران خسارت که عبارتند از: اعاده به وضع سابق، پرداخت غرامت و جلب رضایت؛ پرداخت غرامت معمول‌ترین روش جبران خسارت در رویه بین‌المللی است. در پرونده Gabcikovo - Nagymaros Project دیوان اعلام کرد که این قاعده پذیرفته شده حقوق بین‌الملل است که دولت زیان‌دیده محق است از دولت مرتکب فعل متخلفانه بین‌المللی بابت خسارت وارده به او غرامت بگیرد (Gabcikovo-Nagymaros Project ..., op.cit, para. 152). به همین ترتیب پذیرفته شده که دیوان یا دادگاه بین‌المللی که برای رسیدگی به ادعای مسئولیت دولت صلاحیت دارد به‌عنوان یکی از ابعاد آن صلاحیت مجاز است که بابت خسارات وارده به پرداخت غرامت حکم دهد.

جلب رضایت نوع دیگری از جبران خسارت است که دولت مسئول می‌تواند در ایفای تعهد خویش به جبران کامل خسارت ناشی از فعل متخلفانه بین‌المللی ارائه کند. شکل مناسب جلب رضایت به اوضاع و احوال بستگی دارد و نمی‌توان از پیش آن را تعیین کرد (در داوری پرونده Rainbow Warrior، دیوان در عین رد ادعاهای نیوزیلند برای استرداد یا توقف و صدور و رأی به پرداخت غرامت، اعلامیه‌های گوناگونی را از باب جلب رضایت صادر کرد و به‌علاوه توصیه کرد به طرفین در پایان دادن به وضعیت نامناسب موجود کمک شود. به‌ویژه دیوان داوری توصیه کرد که فرانسه مبلغ دو میلیون دلار به صندوقی که برای ترویج و تشویق روابط دوستانه و نزدیک میان شهروندان دو کشور تأسیس می‌شود کمک کند).

باید میان نقض‌های مختلف حقوق بین‌الملل تمایزی کیفی قائل شد. دیوان بین‌المللی دادگستری در قضیه بارسلونا تراکشن به این مسئله پرداخت: باید میان تعهدات یک دولت در قبال جامعه بین‌المللی در کل و تعهدات او در برابر دولتی دیگر در زمینه حمایت دیپلماتیک تفکیک قائل شویم. تعهدات دسته قبل به دلیل ماهیتشان به همه دولت‌ها مربوطند. با توجه به اهمیت حقوق ذی‌ربط، می‌توان گفت که تمامی دولت‌ها در حمایت از آنها دارای منفعت حقوقی هستند، آنها تعهداتی عام‌الشمول هستند.

اظهارات دیوان آشکارا حاکی از آن است که در چارچوب مسئولیت بین‌المللی، برخی تعهدات در قبال جامعه بین‌المللی کشورها در کل وجود دارد و به دلیل اهمیت حقوق ذی‌ربط تمامی دولت‌ها در حمایت از آنها دارای منفعت حقوقی هستند. نقض‌های شدید ناشی از قواعد آمره حقوق بین‌الملل عام نه‌تنها برای دولت مسئول بلکه برای تمامی دیگر دولت‌ها، نتایجی را در بر دارد. دیگر اینکه تمامی دولت‌ها می‌توانند برای نقض تعهداتی که در قبال جامعه بین‌المللی در کل وجود دارد به مسئولیت استناد کند.

۶-۲-۲- توسل به شورای امنیت سازمان ملل

با فرض آنکه کشور قربانی قادر باشد که منشأ حملات را شناسایی کند و رفتار را به یک کشور منتسب کند، چند روش جبران خسارت وجود دارد. اول اینکه قربانی یا یک عضو دیگر سازمان ملل متحد می‌تواند وضعیت را طبق بند ۱ ماده ۳۵ منشور ملل متحد به شورای امنیت ارجاع دهد و شورا ممکن است روش‌های مناسبی را برای حل اختلاف پیشنهاد کند (بند ۱ ماده ۳۶). درصورتی‌که شورای امنیت تشخیص دهد که وضعیت منجر به تهدید علیه صلح، نقض صلح یا عمل تجاوز می‌شود، می‌تواند اختیارات خود به‌موجب فصل هفتم منشور را اعمال کند. نتیجه اینکه آیا حملات یا جنگ‌های سایبری می‌توانند نقض صلح یا عمل تجاوز (برخی وضعیت مذکور در قطعنامه ۳۳۱۴ مورخ ۱۴ دسامبر ۱۹۷۴ در تعریف تجاوز می‌توانند به نحو مطلوبی

حملات سایبری را نیز پوشش دهند. درهرصورت، فهرست مشخص شده در تعریف تجاوز جامع نبوده و برای شورای امنیت الزام‌آور نیست) محسوب شوند یا خیر این است که آنها و حتی برخی عملیات‌ها تخلیه اطلاعات کامپیوتری CNEمی‌توانند به نحو بالقوه‌ای منجر به تهدید صلح شوند. حتی اگر در دیدگاه نویسندگان (قطعنامه) این مفهوم محدود به استفاده از اجبار مسلحانه مرسوم باشد، حوزه‌اش به‌تدریج توسعه یافته و تقریباً هر چیزی می‌تواند به‌وسیله شورای امنیت به‌عنوان تهدید صلح قلمداد شود (این مشهور است که نویسندگان منشور عمده مفهوم را تعریف نکرده رها نمودند). مشخصاً ارزیابی به اوضاع و احوال هر مورد بستگی دارد. برای مثال ازآنجا که سند DoD ایالات‌متحده آمریکا تأکید دارد این واقعیت که یک حمله به شبکه‌های کامپیوتری خسارات گسترده، اختلال اقتصادی و از دست دادن زندگی ایجاد نموده می‌تواند به‌شدت اقدام شورای امنیت را تسریع نماید.

افزون بر این هر حمله به شبکه‌های کامپیوتری که توسط کشورهایی که با یکدیگر اختلاف دارند مانند هند و پاکستان یا ترکیه و یونان در منازعات طولانی جهانی انجام شود، خطر به آتش کشیدن منازعه را دارد. از سوی دیگر ممکن است حملات کامپیوتری را در بین قدرت‌های اقتصادی اصلی غرب ببینیم (شاید به شکل جاسوسی اقتصادی) که مشخصاً در صورت کشف صلح را تهدید نمی‌کند.

اگر شورای امنیت حمله سایبری را به‌عنوان تهدید صلح قلمداد نمود، قادر است طبق ماده ۳۹ منشور توصیه‌هایی بنماید، طبق ماده ۴۰ تدابیری برای جلوگیری از بدتر شدن بحران اتخاذ کند و تدابیری شامل استفاده از زور یا عدم استفاده از زور طبق مواد ۴۱ یا ۴۲ اتخاذ نماید. خصوصاً ماده ۴۱ در زمره اقداماتی که شامل استفاده از زور نمی‌شوند، قطع کلی یا جزئی تلگراف، رادیو و دیگر وسایل ارتباطی را فهرست نموده است. در این صورت شورای امنیت باید یک انسداد سایبری را بر کشور مسئول حملات سایبری، به‌منظور جلوگیری از ادامه یا تکرار حمله، تحمیل کند (اشمیت پیشنهاد می‌دهد که حملات سایبری به‌عنوان ابزار اجرای قطعنامه‌های شورای امنیت ممکن است گامی معتدل در بین ابزارهای غیراجباری ماده ۴۱ و استفاده آشکار از زور طبق ماده ۴۲ باشد).

۶-۲-۳- توسل به یک دیوان بین‌المللی

اگر در جنگ سایبری کشور مسئول مورد شناسایی قرار گیرد ممکن است به‌منظور به دست آوردن جبران خسارت نقض بند ۴ ماده ۲ منشور و اصل عدم‌مداخله نزد یک دیوان بین‌المللی، برای مثال دیوان بین‌المللی دادگستری، فراخوانده شود. با این حال ممکن است برآورد میزان خسارات اطلاعات دقیق و خسارات وارد شده به دلیل محرمانگی کار و کسب بی‌میل باشند. افزون بر این دیوان بین‌المللی دادگستری مانند دیگر دیوان‌های بین‌المللی صلاحیت اجباری ندارد و بنابراین دو طرف باید در خصوص رجوع پرونده به قضاوت توافق کنند. گزینه دیگر در خواست نظر مشورتی از دیوان بر طبق ماده ۹۶ منشور ملل متحد است. چنین نظریاتی اختیاری هستند و الزام‌آور نمی‌باشند، اگرچه ممکن است این نظریات در شکل‌گیری قاعده حقوق بین‌الملل عرفی به نحو قاطعانه‌ای سهیم باشند.

برخی مفسرین پیشنهاد می‌دهند که جدا از به وجود آمدن مسئولیت دولت، حمله‌های سایبری منجر به تجاوز دربردارنده مسئولیت کیفری بین‌المللی افراد مسئول نیز می‌شوند (افراد متهم به جرم تجاوز ارضی مسلماً می‌توانند نزد دادگاه داخلی نیز محاکمه شوند. مشکل دیگر که خارج از موضوع این مقاله است این است که آیا نسل‌کشی، جرائم جنگی و جرائم علیه بشریت نیز می‌توانند از طریق ابزارهای سایبری ارتکاب یابند). کنفرانس بازبینی اساسنامه دیوان کیفری بین‌المللی در سال ۲۰۱۰ نهایتاً تعریفی از تجاوز را تصویب نمود که تعریف تجاوز مندرج در قطعنامه ۳۳۱۴ مجمع عمومی سازمان ملل در سال ۱۹۷۴ را نمونه قرار داده بود، اما به‌منظور تطابق با اصل قانونی بودن، بدون در بر گرفتن ماده ۴ که اعلام کننده ماهیت غیر حصری فهرست موارد تجاوز مندرج در اعلامیه بود. در سال ۲۰۰۸ برخی هیئت‌های نمایندگی نگرانی‌شان را از این موضوع بیان نمودند که جمله‌بندی تعریف حمله‌های سایبری را مستثنا می‌نماید (در بر نمی‌گیرد) و از طرح قبلی حمایت کردند که اشکالی از حمله به غیر از استفاده از نیروهای

مسلح را در بر می‌گیرد که ثبات سیاسی و اقتصادی با اعمال حق تعیین سرنوشت را تحت تأثیر قرار می‌دهند یا امنیت، دفاع با تمامیت ارضی یک یا چند کشور نقض می‌کند.

درحالی‌که این صحیح است که برخی موارد فهرست شده در بند ۲ ماده ۸ مکرر اساسنامه دیوان نیز می‌توانند برخی حملات سایبری را با استناد قیاسی با حملات جنبشی (برای مثال وزیر دفاع استونی حملات سایبری را با انسداد بنادر ۲۰۰ سال پیش مقایسه نمود) پوشش دهند اما این شک‌برانگیز است که آیا چنین رویکردی با تفسیر موسعی مطابق با ماده ۲۲ اساسنامه می‌باشد یا خیر که توسعه مصداق یا مفهوم با قیاس را ممنوع نموده است. از سوی دیگر شرط رهبری که مسئولیت را محدود می‌کند به اشخاص که در مقامی هستند می‌توانند به نحو مؤثری بر اقدامات سیاسی و نظامی یک کشور اعمال کنترل نمایند، محتملاً تعقیب هکرهایی را که کنترل نظام عملیات موشکی یک کشور را به دست گرفته و از آن برای انجام یک تجاوز علیه کشور دیگر استفاده می‌نمایند، مستثنا نمی‌کنند. بنابراین اثر برابر ساز فناوری سایبری می‌تواند طیف محدود افرادی را که شاید جرم تجاوز را انجام دهند، توسعه دهد.

۷- چالش‌های مواجهه با حملات سایبری و راهکارهای مقابله با آن‌ها

اقداماتی که در فضای سایبری رخ می‌دهد از ماهیت نامشخصی برخوردار است. همین ماهیت مبهم، تأثیر چالش‌های امنیتی منبعث شده از فضای سایبر را بر زندگی واقعی و عرصه فیزیکی محیط سیاسی، اجتماعی و اقتصادی جوامع افزایش می‌دهد. چالش‌های امنیتی ایجاد شده در فضای سایبر به‌تناسب ماهیت طراحان آن از ویژگی‌های خاصی برخوردارند. برای مثال بازیگران دولتی و تروریست‌ها معمولاً با اهداف شبه‌جنگی به طراحی حملات سایبری می‌پردازند. در مقابل هکرها یا گروه‌های تبهکار اقتصادی معمولاً اهداف شبه‌جنگی نداشته و به دنبال کسب منافع مالی یا شخصی هستند.

به‌طورکلی می‌توان گفت تکنولوژی‌های اطلاعاتی در منابع، نوع و ابزارهای تهدید، تحولی شگرف ایجاد نموده‌اند. این تکنولوژی‌ها هم از لحاظ کمی (تعدد و تنوع منابع تهدید) و هم از لحاظ کیفی (پیچیده‌تر و کارآمد شدن ابزارهای سنتی تهدید) ابزارهای تهدید امنیت ملی را متحول کرده‌اند. در گذشته منابع تهدید امنیت دولت‌ها مشخص بود اما امروز چنین تعریفی وجود ندارد. فناوری‌های نوین اطلاعاتی، تهدیدها و آسیب‌پذیری‌های امنیتی متعددی را متوجه کشورها اعم از بزرگ یا کوچک، پیشرفته یا در حال توسعه ساخته‌اند زیرا گسترش تکنولوژی‌های ارتباطی- اطلاعاتی فاصله موضوعات داخلی و خارجی را محو کرده و افراد جوامع را با تهدیدهای فرا ملی پیوند داده است. همچنین این تکنولوژی‌ها با خلق موجودیت‌های بدون ساختار فیزیکی و مجازی و فارغ از محدودیت‌های طبیعی نه‌تنها حاکمیت ملی در برخورد با تهدیدهای امنیتی تضعیف نموده بلکه قدرت تأثیرگذاری و عدم تعیین تهدیدها را نیز افزایش داده است.

اگرچه درگیری در فضای سایبر به علت مبهم بودن منشأ تهدیدها و انگیزه‌های آنها یک پدیده غیرسیاسی تلقی می‌شود، اما واقعیت امر آن است که حملات سایبر در واقع ادامه سیاست محسوب می‌شوند. یعنی همان‌گونه که جنگ، ادامه فعالیت سیاسی با ابزاری دیگر است؛ حملات سایبری نیز ماهیتی سیاسی دارند. بر اساس چنین مفهومی تنها آن دسته از حملات سایبری را می‌توان حملات شبه‌جنگی دانست که طراحان آن، اهداف سیاسی را دنبال کنند. یعنی می‌توان گفت ستیز و دشمنی سیاسی در دنیای واقعی با کمک تکنولوژی‌های اطلاعاتی در فضای سایبر دنبال می‌شود. بر همین اساس فضای سایبر یک فضای سیاسی است. بنابراین اگر هدف مهاجمان سایبری دستیابی به منافع مالی یا شخصی از طریق ابزار مجرمانه همانند دزدی، کلاه‌برداری یا اخاذی باشد، این اقدامات صرفاً ماهیت مجرمانه دارد اما اگر هدف اصلی مهاجمان سایبر، وارد آوردن آسیب‌های جدی بر نهادهای دولتی، شهروندان یا تخریب و نابودی زیربناها و ساختارهای حیاتی نظامی و غیرنظامی باشد، این اقدامات جزو اقدامات جنگی محسوب می‌شود.

محیط سایبر به‌سرعت در حال تغییر است. این تغییرات و سیال بودن فضای مجازی، چالش بسیار بزرگی را برای کشورهایی نظیر ایالات‌متحده آمریکا به وجود آورده

است؛ زیرا این کشور بر فضای سایبری که تفکرات و اندیشه‌های نوین در آن پدید می‌آید و شیوه‌های نوین درگیری طراحی می‌شود کنترلی ندارد. با گسترش روزافزون دسترسی جهانی به اینترنت و رشد تعداد کاربران نه‌تنها ترافیک جهانی در فضای سایبر افزایش یافته بلکه بازیگران جدیدی در عرصه امنیت سیاسی، اجتماعی، اقتصادی و فرهنگی جهان، نمود یافته‌اند که به‌راحتی می‌توانند ماهیت و هویت خود را پشت حکومت‌ها و جنبش‌های اجتماعی مخفی کرده و ضمن طراحی حملات مختلف برای آسیب رساندن به زیرساخت‌های حیاتی یک کشور، زمینه چالش‌های سیاسی و امنیتی را به وجود آورند. ازآنجایی‌که فضای اینترنت بسیار گسترده‌تر از محیط سیاسی کشورهاست؛ دولت‌ها نمی‌توانند بر این فضای مجازی کنترلی داشته باشند. این مسئله بر شدت چالش‌های ایجاد شده در چنین فضایی می‌افزاید. این مسئله زمانی که با پیچیدگی‌های عمیق فضای مجازی همراه می‌شود، زمینه مناسبی را برای افزایش درگیری و تضاد در این فضا به وجود می‌آورد. همین مورد، مفهوم سنتی جنگ را نیز تغییر داده است. در گذشته جنگ مبتنی بر حمله و دفاع بود. اما در حال حاضر به علت پیچیدگی تکنولوژی‌های رایانه‌ای و محیط متغیر و سیال فضای سایبر مفهوم حمله و دفاع تغییر یافته است؛ به‌گونه‌ای که امروزه دولت‌های مختلف جهان برای تأمین امنیت خود مفهوم دفاع در جنگ‌های سنتی را با مفهوم نرم‌افزاری آن در فضای سایبر تلفیق کرده و در راستای نظامی نمودن این فضا گام برداشته‌اند. در واقع دولت‌های مدرن کنونی می‌کوشند با تلفیق چهار فضای درگیری در زمین، دریا، هوا و فضا با بعد مجازی، درگیری جنگ‌های سایبری را مدیریت نمایند؛ اما این‌رویکرد هرچه بیشتر سبب افزایش تنش در فضای مجازی می‌شود.

بنابراین می‌توان گفت اگرچه نقش گروه‌های غیردولتی در فضای سایبر افزایش یافته است اما به‌وضوح می‌توان مشاهده کرد که در زمینه مدیریت جنگ‌ها در فضای سایبر همچنان کنترل نهایی و مسلط با دولت‌های ملی است. علاوه بر این از آنجایی که جنگ چهره‌ای دیگر از سیاست و در واقع دنباله آن به‌حساب می‌آید، مهم‌ترین راهکار مدیریت جنگ‌های سایبری تدوین یک ساختار سیاسی بین‌المللی به‌وسیله دولت‌های مدرن ملی خواهد بود. این مسئله نقش دولت‌ها را در فضای مجازی افزایش می‌دهد. بنابراین امروزه شرط اصلی موفقیت مدیریت بحران‌های مجازی، درک فضای سایبر به‌عنوان یک محیط سیاسی است که نیازمند تدوین ارزش‌ها و هنجارهای بین‌المللی به‌وسیله دولت‌های جهان می‌باشد.

اهمیت فعالیت هماهنگ دولت‌های جهان برای مقابله با بحران‌های جهانی در فضای سایبر به‌اندازه‌ای است که اکثر کارشناسان، عدم موفقیت ایالات‌متحده آمریکا در برخورد با بحران‌های بسیار پیچیده مجازی را ناشی از یک‌جانبه‌گرایی این کشور در این عرصه می‌دانند. البته همکاری جهانی دولت‌ها برای مدیریت فضای سایبر باید مبتنی بر گفتگو و مذاکره سیاسی باشد، زیرا اتخاذ راهکارهای نظامی تنها منجر به افزایش پراکندگی و تشتت در این فضا می‌شود. مذاکرات سیاسی دولت‌های مدرن ملی در حکم یک سرمایه مهم سیاسی، زمینه تدوین ارزش‌ها و هنجارهای بین‌المللی برای قانونمند کردن این فضا را به وجود می‌آورد. در واقع این سرمایه سیاسی از طریق مذاکره سیاست‌مداران برجسته کشورها که توانمندی تطابق با پیچیدگی‌های فضای سایبر را دارند، شکل می‌گیرد. از آنجایی که در فضای سایبر شناسایی هویت و مکان مهاجم، مقاصد و اهداف آنها سبب ایجاد چالش‌های جدی برای تشخیص به‌موقع یک تهاجم، واکنش در مقابل آن و ارزیابی دقیق میزان خسارت پس از تهاجم می‌شود لزوم اتخاذ یک چارچوب سیاسی بین‌المللی برای مقابله با چالش‌های فضای سایبر، امروزه یکی از اولویت‌های اصلی امنیت ملی کشورهای جهان محسوب می‌شود.

البته تأمین امنیت سایبر در بعد داخلی نیز از اهمیت بسیار زیادی برخوردار است؛ به‌گونه‌ای که امروزه کشورهای اروپایی و ایالات‌متحده آمریکا بیشتر از گذشته به انجام فعالیت‌های سازمان‌یافته در مورد فضای سایبر می‌پردازند. البته در ایالات‌متحده آمریکا هنوز هیچ تفاهم ملی در مورد میزان اهمیت تهدیدهای سایبر حاصل نشده است. به‌هرحال امروزه دو دسته تفکر در این کشور در مورد تأمین امنیت

سایبر شکل گرفته است. گروهی تهدیدهای سایبر را یک مسئله امنیتی تلقی نموده و مسئولیت مقابله با آنها را بر عهده نیروی نظامی می‌دانند. در مقابل، گروهی با حضور نظامیان در این عرصه مخالفند و تأمین امنیت مجازی را مسئله‌ای مدنی می‌دانند. با این وجود وزارت دفاع ایالات‌متحده آمریکا نقش تعیین‌کننده‌ای در تعریف منافع این کشور در فضای سایبر ایفا می‌کند.

دیدگاه بریتانیا نیز درباره جنگ سایبر تا حدی شبیه به آمریکا است. این کشور جنگ سایبر را به‌صورت اقدامات تأثیرگذار بر سیستم‌های اطلاعاتی دیگران و دفاع از سیستم‌های اطلاعاتی خودی برای کسب حمایت از اهداف ملی تعریف می‌کند. علاوه بر این، بریتانیا از یک چارچوب قانونی برای مدیریت فعالیت‌های اطلاعاتی و مقابله با جرائم رایانه‌ای برخوردار است.

اگرچه این اقدامات می‌تواند در فضای داخلی تا حدی امنیت سایبری را تأمین کند اما برای تأمین امنیت فضای مجازی در بعد جهانی باید همه دولت‌های مدرن غربی و غیر غربی در قالب تعامل‌های سیاسی، یک چارچوب ارزشی و هنجاری را برای تدوین قوانین بین‌المللی برای به نظم درآوردن فضای مجازی شکل دهند. البته ذکر این نکته بسیار مهم، ضروری است که دولت‌های غربی نباید در تدوین ارزش‌ها و هنجارهای بین‌المللی برای قانونمند کردن فضای سایبر نظرهای خود را بر کشورهای غیر غربی تحمیل کنند؛ زیرا چنین اقدامی سبب می‌شود فضای سایبری کشورهای غیر غربی تحت انقیاد قوانین کشورهای غربی قرار گیرد. این مسئله سبب می‌شود، دول غیر غربی قوانینی را برای فضای مجازی خود اجرا کنند که هیچ سنخیتی با محیط داخلی آنها ندارد.

یکی از راهکارهایی که می‌توان در زمینه رفع چالش‌ها ارائه داد، ایجاد سیستم‌های جامع نظارتی و کنترلی از طریق کنوانسیون‌های بین‌المللی با عنوان منع توسل به حملات سایبری همانند منع استفاده از سلاح‌های شیمیایی و منع توسل به زور مهم‌ترین عامل پیشگیری از حملات سایبری می‌باشد. از دیگر سو، مسئولیت بین‌المللی دولت‌ها می‌تواند در کاهش نگرانی‌های ناشی از توسعه شبکه‌ای رایانه‌ای و اینترنتی کارآمد باشد. همچنین حقوق بین‌الملل عرفی نیز با وجود نسبی رویه کشورها و اعتقاد حقوقی به‌ویژه در خصوص حق دفاع مشروع علیه حملات سایبری می‌تواند در این زمینه نقش پر رنگ در سطح جرائم بین‌المللی ایفا نماید.

یکی از مهم‌ترین راهکارهایی که می‌تواند در زمینه مواجهه با حملات سایبری به کمک حقوق بین‌الملل بیاید، تنظیم و تصویب قوانین و مقررات جامع و کامل است که بتواند از میزان حملات سایبری جلوگیری کند، زیرا یکی از مهم‌ترین چالش‌های حقوقی در مواجهه با حملات سایبری نبود ضمانت اجرایی کافی است. کشورها در مورد توانایی حملات سایبری خود سکوت اختیار کرده‌اند و از اینکه خود را به قواعدی در چنین حوزه نوظهوری پایبند کنند اکراه می‌ورزند، البته ماهیت حوزه سایبر به‌تنهایی بر محرمانه بودن آن دامن می‌زند و به‌صورت کاملاً مخفی از جانب کاربرانی گمنام صورت می‌گیرد؛ به‌علاوه مشخص نیست که آیا عملیات سایبری قطعاً منجر به اعمال قواعد جنگ می‌گردد. از این‌رو تحقیقات حقوقی حوزه حملات سایبری تا حد زیادی درگیر فرضیه‌سازی به کمک محققانی است که قصد دارند سناریوهای متعدد سایبری کنونی را درون اصول و قواعد حقوق جنگ داخل کنند.

پس از آنکه نخستین هک شدن گوگل در ژانویه ۲۰۱۰ رخ داد و گوگل حملات صورت گرفته را به سرقت بردن مالکیت معنوی این شرکت خواند، در ماه مه ۲۰۱۱ یکی از دپارتمان‌های ایالات‌متحده ، راهبردی بین‌المللی برای اداره کردن فضای سایبری منتشر کرد که حاکی از آن بود که آمریکا حق دفاع مشروع در برابر حملات مشروع را در مواردی برای خود مشروع می‌پندارد و پس از آن بود که پنتاگون اسناد مربوط به راهبردهای نوین و طبقه‌بندی شده خود در حوزه سایبر را منتشر کرد و با این اسناد حملات سایبری از جانب یک کشور خارجی را یک عمل جنگی تعبیر می‌کند. اندکی بعد دفتر مرکزی دپارتمان ایالتی از محرک‌هایی برای ایجاد سایه اینترنتی و سیستم‌های تلفن همراه خبر داد که قادرند برای پشتیبانی معاندین در کشورهایی که با سخت‌گیری از جانب رژیم ظالم مواجهند، استفاده شود. درعین‌حال به نظر می‌رسد که کشورها با راهکارهای این‌چنینی می‌توانند تا حدودی در مواجهه با

حملات سایبری موفق باشند اما این همه ماجرا نیست و برای مقابله بهتر باید قوانین بازدارنده در نظر گرفت.

۸- نتیجه‌گیری

فضای سایبر به‌عنوان بارزترین جلوه عصر ارتباطات و اطلاعات همانند همه دستاوردهای بشری، تهدیدها و فرصت‌های بسیاری را فرا روی جوامع بشری قرار داده است. این حوزه هم با اقبال جهانی مردم و کاربران خصوصی روبه‌رو شده و هم مورد توجه فزاینده دولت‌ها برای ارائه خدمات عمومی مانند دولت الکترونیک و حتی نظامی قرار گرفته است.

متأسفانه نظام حقوقی بین‌الملل در مقابله با تکنولوژی‌های مخرب و فناوری‌های پیشرفته همچون جنگ سایبری بسیار کند و عقب افتاده است و ماهیت نظام حقوق بین‌الملل اجازه نمی‌دهد که تا وقتی دولت‌ها خود را به‌موجب یک سند الزام‌آور حقوقی متعهد نساخته باشند، امکان استناد به مسئولیت آنها فراهم گردد.

مهم‌ترین نکته، نیاز عاجل به تدوین کدهای استانداردسازی قواعد رفتاری در فضای سایبری و در چهارچوب جهانی است. رهنمودهای فرا ملی مشابهی در عصرهای مختلف و در زمینه‌های دیگر مانند تجارت، ارتباطات و حمل‌ونقل وجود دارند. نهادهایی همچون سازمان مالکیت معنوی و سازمان بین‌المللی دریانوردی تنها دو نمونه از همکاری‌های موفق در زمینه‌های تخصصی در سطح بین‌المللی می‌باشند. به‌طور مشابه می‌توان به آژانس بین‌المللی ایجاد شده تحت حمایت سازمان ملل متحد برای مدیریت و سرپرستی این چارچوب در واکنش به حملات سایبری یاد کرد، این آژانس می‌تواند استفاده صلح‌آمیز از فناوری دیجیتال شبکه و جلوگیری از سوء استفاده از این فناوری را تضمین کند. چنین آژانسی همچنین می‌تواند به‌عنوان یک مجمع بین دولتی برای حل‌وفصل دیپلماتیک حوادث خصمانه واقع شده در فضای سایبر و تسهیل همکاری‌های بین‌المللی در رابطه با جرائم رایانه‌ای و تروریسم سایبری عمل نماید. با ایجاد چنین نهادی در این فضاست که خشونت‌ها و تجاوزهای مکرر، موضوع معاهداتی در فضای دیجیتالی جدید در بستر سازمان ملل متحد خواهد بود. از دیگر سو برقراری ارتباط میان اقدامات خصمانه سایبری با مسئولیت بین‌المللی متجاوزین سایبری و مجازات آن‌ها، کاهش برداشت‌های نادرست و محاسبات اشتباه، و تدوین چارچوبی از قوانین و انتظارات در خصوص رفتار دولت‌هایی که محدود کننده جنگ سایبری هستند و سایر اقدامات آسیب‌رسان در فضای سایبری، باید در دستور کار قرار گیرد. نکته دیگر نحوه برخورد دولت‌ها با دشمنان نظامی خود در مقوله امنیت سایبری است، تا اینکه ثبات فضای بین‌المللی تضمین شود.

۹- پانوشت‌ها

1. An exception to this general rule would be a CNE gathering information prefatory to an attack during an armed conflict. In this instance, jus in bello rules may permit the perpetrator of a CNE to Targeted.
2. The earliest version of Stuxnet was apparently released in the summer of 2009. In September 2010 an industrial control systems-security expert in Hamburg announced that he had reverse-engineered the virus's payload and discovered its ultimate purpose: sabotaging certain Siemens-made programmable logic controllers operating under certain conditions. The certain controllers operating under certain conditions are now widely believed to have been those at an Iranian nuclear site. Michael Joseph Gross, A Declaration of Cyber-War, VANITYFAIR, April 2011, http://www.vanityfair.com/culture/ features/2011/04/stuxnet-201104.html.
3. See Clark & Landau, supra note 32, at 26-27 (describing how the Internet's reliance on packet switching and network-layering allows for anonymity).
4. A botnet is "a network of thousands or even millions of computers under the control of an Attacker that is used to carry out a wide range of services." Tyler Moore, Introducing the Economics of Cyber security: Principles and Policy Options, in Proceedings of a Workshop on Deterring Cyberattacks, supra note 32, at 3.6. In this regard, a botnet can serve as a force multiplier" by Allowing one actor to harness the capacity of thousands or millions of computers. See David Gerwitz, 10 Things You Should Know About the Pentagon's New Cyber warfare Strategy, ZDNET Government (June 2, 2011, 5:00 AM), http://www.zdnet.com/blog/government/10things-you-should-know-about-thepentagons-new-cyberwarfare-strategy/10429 ([A]ny small group with a pile of PCs (or even PlayStations) can mount a hugely damaging attack, especially if they make use of zombie botnets as a force multiplier.").
5. Hollis, supra note 29 at 405 (“If you do not know who authored an attack, how can you know whether to treat it as a crime or an act of war?").
6. See Eneken Tikk, Kadri Kaska & Liis Vihul, International Cyber Incidents: Legal Considerations, 31-32 (2010) (describing the emerging trend of patriotic hacking).
7. See Definition of: white hat hacker, PCMAG. COM, http://www. pcmag.com/encyclopedia_term/ 0,2542,t=white+hat+hacker&i=54434,00.asp (last visited Jan. 6, 2012) (defining "white-hat hackers” as the "good guys" i.e., "concerned employees or security professionals who are paid to find vulnerabilities").
8. See Schmitt, Cyber Operations and the Jus in Bello, supra note 29, at 131 ("[A]ny (cyber] operation by or attributable to a State which results in damage to or destruction of objects or injury to or death of individuals of another State would commence an international armed conflict.")
9. See Dancho Danchev, Should a Targeted Country Strike Back at the Cyber Attackers?, ZERO DAY, (May 10, 2010, 2:03 PM), http://www.zdnet.com/blog/security/should-a-targeted-country-strike-backat-thecyberattackers/6194 (describing "false flag cyber operations" as "impersonating a particular country" in order to "engineer[] cyber warfare tensions by relying on the negative reputation of 'usual' suspects") 49 A catalytic conflict is one in which a third party instigates conflict between two other parties. "NRC REPORT, supra note 31, at 312.
10. A catalytic conflict is one in which a third party instigates conflict between two other parties. "NRC

REPORT, supra note 31, at 312.

11. See Scott J. Shackelford, Estonia Three Years Later: A Progress Report on Combating Cyber Attacks, 13 J. INTERNET L. 22, 22(2010) ("Many nations, including the United States, have found mutual Benefit in the status quo strategic ambiguity.").
12. David Drummond. A New Approach to China. The Official Google Blog (Jan. 12. 2014, 3:00 PM), available at: http://googleblog.blogspot.com/2010/01/new-approach-to-china.html
13. E×EC. Office of the President, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World 10, 14 May 2011 hereinafter.

۱۰- مراجع

[۱] آنتونی پ.و. راجرز و پل مالرب، قواعد کاربردی حقوق مخاصمات مسلحانه، ترجمه کمیته ملی حقوق بشردوستانه تهران: انتشارات امیرکبیر، ۱۳۸۷.

[۲] خلف رضایی، حسین، حملات سایبری از منظر حقوق بین‌الملل، فصلنامه مجلس و راهبرد، شماره ۷۳، ۱۳۹۰.

[۳] خلف رضایی، حسین، حملات سایبری از منظر حقوق بین‌الملل (مطالعه موردی: استاکس‌نت)، مجله مجلس و راهبرد، شماره ۳۷، بهار ۱۳۹۲.

[۴] روسکیتی، مارکو، حمله‌های سایبری و ممنوعیت تهدید استفاده از زور، سالنامه حقوق ملل متحد ماکس پلانک، شماره ۱۴، ۲۰۱۰.

[۵] پور قهرمانی، بابک و علی صابرنژاد، ضرورت تدوین قواعد بین‌المللی برای مبارزه با جنگ سایبری، چهارمین همایش بین‌المللی تحولات جدید ایران و جهان به دانشگاه بین‌المللی امام خمینی، ۱۳۹۱.

[۶] الن اگنل، ماری، مشروعیت توسل به زور علیه عراق: بررسی نظریه پیش‌دستی در دفاع از خود، ترجمه سید حسین سادات میدانی، مجله سیاست خارجی، شماره ۵۶، بهار ۱۳۸۲.

[۷] قاجار قیونلو، سیامک، مقدمه حقوق سایبر، تهران: انتشارات بنیاد حقوقی میزان ، ۱۳۹۱.

[۸] ابراهیم گل، علیرضا، مسئولیت بین‌المللی دولت‌ها، تهران: انتشارات شهر دانش، ۱۳۹۰.

[۹] حلمی، نصرت‌الله، مسئولیت بین‌المللی دولت و حمایت سیاسی، تهران: انتشارات میزان ۱۳۹۰.

[10] Commentary on the HPCR manual on International Law Applicable to Air and Missile Warefare, March 2010.

[11] J.A. Simpson, E.S.C. Weiner, The Oxford Compact English Dictionary, 2003.

[12] National Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities 80 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) [Hereinafter NRC REPORT).

[13] David D. Clark & Susan Landau, Untangling Attribution, in Proceedings of a Workshop on Deterring Cyberattacks 25, 28 (National Research Council ed., 2010).

[14] Kim Zetter, How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History, WIRED, July 11, 2011, http://www.wired.com/threatlevel/2011/7/howdigital-detectives-decipheredstuxnet/All/1.

[15] William J. Broad, John Markoff & David E. Sanger, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, N.Y. TIMES, Jan. 15, 2011, www.nytimes.com/2011/1/16/world/middleeast/16stuxnet.html.

[16] Icty the Prosecutor V. Dusko Tadic Aka (dule), decision on the defence motion for interlocutory appeal on jurisdiction, 2 October 1995, case no. it-94-1-ar72, appeals chamber, icty, para 119.

[17] ICJ, advisory opinion on legality of the threat or use of nuclear weapons, para 95.

[18] Eric Talbot Jensen, cyber warfare and precautions against effectsof attacks, op.

[19] Van Dyke (1940) the Responsibility of States for International Cyber Attacks, 34, AM. J. INT'L L. 58. p. 79.

[20] Siobhan Gorman & Julian E. Barnes, Cyber Combat: Act of War, WALL ST. J., May 31, 2011, available at: http://online.WSJ.COImanicle/SB10001424052702304563104576355623135782718.html.

[21] James Glanz & John Markoff, U. S. Underwrites Internet Detour Around Censors, N. Y.

[22] TIMES, June 12, 2011, available at: http://www.nytimes.com/2011/06/12/world/12internet.html?pagewanted=1&_=1&hp.

[23] Leo Lewis, China's Blue Army of 30 Computer Experts Could Deploy Cyber Warfare on Foreign Powers, Australian, May 27, 2011, available at: http://www.theaustralian.com, au/australian-it/chinas-blue-armycouldconduct-cyber-warfare-on-foreignpowers/story-e6frgakx-1226064132826.

[24] http://www.ghazavat.com opcit. p. 8-12.

[25] Wisj.com. Retrieved on 2011-11-08. Gorman, Siobhan. (2012-06-04) WSJ: U.S. Backs Talks on Cyber Warfare.

[26] Rose McDermott, Decision Making Under Uncertainty, in Proceedings of a Workshop on Deterring Cyberattacks, supra note 32, at 227, 229 ("[U]unlike most military attacks, cyber attacks defy easy assessments of perpetrator and purpose.")

نشریه‌ی علمی-پژوهشی شهر ایمن
JOURNAL OF RESILIENT CITY
(JRC)

Mehran Jaberi, Aramesh Shahbazi*, Gholamreza Jalali

1. Ph.D. student of information technology management at Allameh Tabataba'i University

2. Associate Professor at Allameh Tabataba'i University (corresponding author)

3. Associate Professor at Supreme National Defense University

Abstract

The international community, which was initially made up of states whose interdependence brought them together in a community, due to the fundamental and significant developments resulting from the advances in technology, communication and the need to provide and guarantee the stability due to the threat of new tools and weapons, on the one hand, new actors were accepted in the field of international relations, and on the other hand, awareness and the need for convergence and correlation resulting from the existence of common interests and human values have been fully revealed in it. Various parts are affected by this discussion. One of the relevant areas has been the discussion of the government's international responsibility. From the point of view of the International Law Commission, the axis of reference to responsibility, the concept of the state has been damaged. On the other hand, it is about cyber terrorism and explaining the basics and providing related solutions, as well as cyber-attacks and the discussion of armed conflicts that should be investigated. In all these challenges, international law should be able to prevent harm to individuals and governments by providing solutions in the international community.

Key Words: Cyber-attacks, International humanitarian law, International responsibility of governments, Armed conflicts

* Corresponding author: Aramesh Shahbazi, Tehran, Iran;.arameshshahbazi@gmail.com