حقوق بین‌الملل مدرن در مواجهه با جنگی پست مدرن (نبرد سایبری)

محمد آهنی امینه*

فاطمه زهرا فتح اللهی**

چکیده

بسیاری از تحلیل‌گران مسائل استراتژیک معتقدند جنگ سایبری پنجمین صحنه نبرد میان کشورها پس از زمین، دریا، هوا و فضا می‌باشد. در این جنگ که مشخصه جنگ‌های متعارف را نداشته و سلاح‌های به‌کار رفته در آن نیز متفاوت از نوع معمول است، قدرت کشورها براساس توان به‌کارگیری فناوری و شبکه‌های اطلاعاتی و کامپیوتری ارزیابی می‌شود. طی دو دهه گذشته نمونه‌های مشخصی از حملات سایبری علیه اهداف و تأسیسات صنعتی و نظامی به‌وقوع پیوسته که ازجمله می‌توان به حمله به تأسیسات صنعتی و زیربنایی و مؤسسات مالی استونی در سال ۲۰۰۷، حمله به تأسیسات اتمی ایران توسط کرم کامپیوتری "استاکس‌نت" و حمله بازیگران غیردولتی به شبکه اینترنتی برمه اشاره نمود. حقوق بین‌الملل بنا به دلائل متعددی در مواجهه صریح و قانونمند با این معضل امنیتی نیمه اول قرن بیست‌ویکم ناتوان و ناکارآمد به نظر می‌رسد. نوشتار حاضر به بررسی پیچیدگی‌های نبرد پست مدرن سایبری و وضعیت فعلی حقوق بین‌الملل برای مواجهه با آن می‌پردازد و در نهایت نتیجه می‌گیرد تنظیم یک چارچوب قانونی جامع و جدید برای مواجهه با حملات سایبری ضروری است.

واژگان کلیدی

حقوق جنگ، جنگ سایبری، حمله سایبری، حقوق بین‌الملل

---

* دکتری روابط بین‌الملل و رایزن حقوقی سفارت ایران در برلین Email: moahani@yahoo.com

** کارشناس ارشد ژئوپلتیک Email: fathollahiz@yahoo.com

تاریخ ارسال: ۹۳/۰۶/۱۸ تاریخ پذیرش: ۹۳/۰۹/۳۰

فصلنامه راهبرد / سال بیست و سوم / شماره ۷۲ / پاییز ۱۳۹۳ / صص ۱۴۹-۱۲۱

جستارگشایی

روز ۲۷ آوریل ۲۰۰۷ استونی مورد حمله اینترنتی قرارگرفت. طی چند ساعت تمام شبکه‌های اینترنتی بانک‌های اصلی این کشور از کار افتاد و علاوه بر توقف انتشار تمام روزنامه‌های اصلی آن کشور، ارتباطات دولتی نیز مختل شد. این حملات طی چند روز، بیشتر سایت‌های مهم را از کار انداخت و موجب بروز ناآرامی وسیعی در این کشور شد که زخمی شدن ۱۵۰ تن و کشته‌شدن یک تبعه روس بخشی از نتیجه آن بود.

در سال۲۰۱۰، تأسیسات نطنز دچار اشکالات فنی شد. موضوع این اشکال فنی یک حمله پیچیده بود که سانتریفیوژهای در حال چرخش را از کنترل خارج نمود. سلاح "استاکس‌نت" یک کرم رایانه‌ای بود که در اواخر مه۲۰۱۲ رسانه‌های امریکایی اعلام کردند به دستور مستقیم باراک اوباما رئیس جمهور ایالات متحده طراحی، ساخته و راه‌اندازی شد. گرچه در همان زمان احتمال این می‌رفت که امریکا تنها عامل سازنده نباشد، با این حال، در ژوئیه ۲۰۱۳ ، ادوارد اسنودن، کارمند سابق سرویس اطلاعاتی امریکا اعلام کرد این بدافزار با همکاری مشترک امریکا و اسراییل ساخته و علیه تأسیسات هسته‌ای ایران به‌کار گرفته شده است.

جامعه جهانی برای مواجهه با این تهدیدات نیازمند حقوق و قوانینی خاص است. برخی قوانین موجود حاوی ابزارهای محدودی برای واکنش به حملات سایبری هستند، مثلاً حقوق جنگ چارچوبی قانونی برای تنظیم برخی از حملات سایبری (که به سطح مخاصمه مسلحانه ارتقا یافته یا در بستر مخاصمه مسلحانه جاری صورت گیرند) فراهم می‌آورد. برخی دیگر از چارچوب‌های قانونی موجود، اعم از حقوق داخلی و حقوق بین‌الملل، به همین ترتیب نقشی اندک، پراکنده و نامنسجم در تنظیم حملات سایبری در بردارند، این ابزارها از کفایت و بسندگی لازم و کامل برخوردار نیستند.

این نوشتار درصدد یافتن پاسخ به این سؤال است که کدام یک از قوانین یا معاهدات بین‌المللی حاکم بر این منازعه می‌باشد؟ برخی معتقدند در این حوزه حقوق جنگ قابل اعمال است. اما بایستی در نظر داشت که این حملات تشابهی اندک با مخاصمات مسلحانه دارد که حقوق جنگ آن را قاعده‌مند می‌کند. اگر این حملات یک جنگ واقعی است، آیا قربانیان این حملات می‌توانند مدعی حق کاربرد زور متعارف، به‌عنوان دفاع از خود شوند؟ مثلاً آیا جمهوری اسلامی ایران قانوناً مجاز است در پاسخ به حمله سایبری استاکس‌نت اقدام به انجام حمله متعارف نظامی نماید؟ حقوق بین‌الملل جاری از کفایت و بسندگی لازم جهت مواجهه با حملات سایبری برخوردار نبوده و جامعه جهانی برای قاعده‌مند نمودن آن نیازمند تدوین معاهده‌ای

خاص می‌باشد. در ادبیات موجود در جنگ سایبری واژه‌های "حمله سایبری"،"نبرد سایبری"و"جرم سایبری" مستمراً به‌کار می‌رود، در حالی که نسبت به وجود تفاوت در معنای آنها توجه نمی‌شود. فقدان وضوح و شفافیت تعاریف مربوط به این واژه‌ها می‌تواند منجر به مشکلات بیشتر برای واکنش حقوقی معنادار به آنها شود.

سناریوهای مختلفی در این رابطه مطرح شده است. ویروسی که برای برهم زدن تصدیق اسناد مالی یا بازار سهام برنامه‌ریزی شده، ارسال پیام‌های جعلی که منجر به خارج‌کردن رآکتورهای هسته‌ای از مدار، یا رهاسازی آب پشت سدها می‌شود، قطع برق سیستم کنترل ترافیک هوایی که خطر اسقاط هواپیماها را در پی‌دارد، همگی می‌تواند از نتایج یک حمله سایبری مخرب باشد. با این حال تعریفی قابل قبول برای شناسایی این حوادث به‌عنوان حملات سایبری، یا نبرد سایبری وجود ندارد. فقدان وجود تعریف مشترک، تبیین سیاستی هماهنگ و یکسان برای دول درگیر در این عملیات را دشوار نموده است. از این رو ارائه یک تعریف از حمله سایبری اولین گام مهم برای مواجهه با تهدیدات روزافزون این حملات خواهد بود. به نظر می‌رسد یکی از مهم‌ترین تعاریف موجود، تعریف ارائه‌شده توسط ریچاردکلارک باشد. او نبرد سایبری را این‌گونه تعریف می‌کند: «عملیاتی که توسط دول ملی به منظور نفوذ در رایانه‌ها، یا شبکه‌های رایانه‌ای دولتی دیگر، با هدف ایجاد اختلال و ایراد خسارات صورت گیرد (Clark&Knake,2010, p.6)» .به همین ترتیب مایکل‌هایدن، مدیر سابق ناسا و سازمان سیا نیز تعریفی این چنین از جنگ سایبری ارائه داده است: «کوششی عامدانه برای ازکار انداختن یا تخریب شبکه‌های رایانه‌ای کشوری دیگر» (Gjelten, 2010).

مشکل این تعاریف آن است که در آنها هیچ تمایزی میان جرم سایبری، حمله سایبری و جنگ سایبری مشاهده نمی‌شود. علاوه برآن تعریف کلارک از یک منظر بسیار مضیق است. او حمله سایبری را به عاملیت دول ملی محدود نموده و حملات انجام‌شده توسط بازیگران غیردولتی را شامل نمی‌شود. تاکنون دو تلاش ویژه دولتی برای درک تهدید حملات سایبری، انجام شده است. یکی توسط دولت ایالات متحده و دیگری توسط سازمان همکاری‌های شانگهای. این دو تلاش منجر به دو فهم کاملاً متفاوت از این تهدیدات شده است. در سال ۲۰۱۱ اندکی پس از تشکیل فرماندهی سایبری ایالات متحده، ستاد مشترک ارتش امریکا واژه‌نامه‌ای برای کاربرد نظامی در عملیات سایبری منتشر ساخت. این واژه‌نامه حاوی اولین تعریف نظامی رسمی از حمله سایبری بوده و حمله سایبری را این‌گونه تعریف کرده است: «حمله سایبری عبارت است از اقدام خصمانه با استفاده از رایانه، سیستم‌هایا شبکه‌های مربوطه

به آن، با هدف ایجاد اخلال، یا تخریب یک سیستم حساس سایبری، اموال یا اعمال طرفین تخاصم .... یک حمله سایبری ممکن است از حامل‌های واسط، از جمله ابزار پیرامونی، انتقال‌دهنده‌های الکترونیک و کدهای جاسازی شده یا عملیات انسانی نیز استفاده نماید. فعال‌سازی یا نفوذ یک حمله سایبری ممکن است به لحاظ زمانی و مکانی از ابزار حمل آن متفاوت و مجزا باشد» (Cartwright, 2011,p.5).

ویژگی کلیدی این رویکرد آن است که حملات سایبری را به حملاتی محدود نموده که خصمانه بوده و با هدف ایراد آسیب به سیستم‌های سایبری مهم انجام شود. بنابراین تعریف، براساس اهداف حمله محدود شده است. در مقابل سازمان همکاری‌های شانگهای رویکردی"معنامحور" از حملات سایبری برگزیده و بر نگرانی نسبت به تهدیدات ناشی از کاربرد فناوری‌های نوین اطلاعات و ارتباطات علیه ثبات و امنیت بین‌المللی (اعم از فناوری‌های نظامی و غیرنظامی) تأکید نموده است. علاوه برآن انتشار اطلاعات مخرب سیستم‌های سیاسی، اقتصادی و اجتماعی و همچنین حوزه‌های معنوی، اخلاقی و فرهنگی سایر دول نیز به عنوان تهدیدات اصلی امنیت اطلاعاتی شناخته شده است. از این‌رو این سازمان ظاهراً حملات سایبری را در طیفی وسیع‌تر مد نظر گرفته و استفاده از فناوری سایبری برای تخریب و تضعیف ثبات سیاسی را نیز مشمول آن کرده است. برخی نگران‌اند که این تعریف تلاش سازمان برای توجیه سانسور و آزادی بیان از طریق شبکه اینترنت تلقی شود. به‌هرصورت برای ادامه بحث در این نوشتار، تعریفی مضیق از حمله سایبری در نظر گرفته می‌شود. تعریفی که بر تهدید ویژه تحمیل شده، توسط فناوری‌های سایبری متمرکز بوده و به قرار زیر می‌باشد: «حمله سایبری هر اقدامی است که به منظور تخریب کارکرد شبکه‌های رایانه‌ای انجام شده و یک هدف امنیت ملی یا سیاسی ورای آن وجود داشته باشد».

۱. بررسی اجزای تعریف

عبارت**"یک حمله سایبری ...."**: به معنای آن است که حمله، اعم از تهاجمی یا دفاعی، بایستی عامل باشد، نه غیرعامل. دولت‌ها احتمالاً هم از دفاع عامل و هم از دفاع غیرعامل استفاده می‌نمایند، اما دفاع غیرعامل را نمی‌توان یک حمله سایبری دانست. دفاع عامل شامل عملیات الکترونیکی برنامه‌ریزی‌شده برای حمله به سیستم‌های رایانه‌ای و از رده خارج کردن واسطه‌های حملات سایبری می‌شود.

عبارت **"... شامل هر اقدام انجام‌شده ...."**: باید در نظر داشت که استفاده از شبکه رایانه‌ای برای عملیات هواپیماهای بدون سرنشین، حمله سایبری محسوب نشده، بلکه نمونه‌ای از نبردهای متعارف با استفاده از فناوری پیشرفته است. اما استفاده از مواد انفجاری عادی برای قطع شبکه کابل زیردریایی که از طریق آن داده‌ها میان کشورهای تبادل می‌شود، یک حمله سایبری تلقی می‌شود. جنگ در نگاه سنتی آن در سه حوزه زمین، هوا و دریا تقسیم شده بود که هر کدام از آنها به‌واسطه خدمات نظامی خود مورد توجه قرار داشتند. نیروهای نظامی به‌صورت سنتی به جای زیرساخت‌ها، توسط حوزه‌های وظایف آنها سازمان یافته‌اند. وظیفه ارتش کنترل سرزمین است، نه رانندگی تانک و شلیک توپ. وظیفه نیروی دریایی کنترل دریاست، نه به‌کارگیری قایق‌ها و کشتی‌ها. وظیفه نیروی هوایی کنترل هواست، نه به پرواز درآوردن هواپیما و فروریختن بمب. هر کدام از این نیروهای باید به تمام ابزار و تسلیحاتی که تصور می‌شود برای کنترل حوزه وظائف خویش لازم دارند، اعم از هواپیما، قایق، موشک، توپخانه، شبکه‌های رایانه‌ای، دسترسی داشته باشند. به‌واسطه همین منطق، مأموریت یگان سایبری به‌کارگیری شبکه‌های رایانه‌ای دفاع سایبری و توان انجام عملیات سایبری با استفاده از هر ابزاری است. به واسطه کاربرد عبارت "هر اقدام" در این تعریف، یک حمله سایبری می‌تواند شامل هک، بمباران، قطع، آلوده ساختن، و اقداماتی از این دست شود. اما برای آنکه این عمل یک حمله سایبری تلقی شود، بایستی هدف آن تخریب یا اختلال در عملکرد شبکه‌های رایانه‌ای باشد.

عبارت **"... برای تخریب عملکرد ..."**: یک شبکه رایانه‌ای ممکن است از طرق مختلف در معرض تهدید قرار گیرد. **حملات عملی** در عملکرد سیستم رایانه اخلال نموده و این امر منجر به عملکرد بد شبکه خواهد شد. مثل ویروس، کرم رایانه‌ای، و تروجان. در مقابل **حملات معنایی**[1] سیستم عامل را حفظ می‌کند، اما صحت اطلاعاتی را که فرآوری کرده و اطلاعاتی که به آن واکنش نشان می‌دهد، هدف می‌گیرد. در نتیجه کارکرد سیستمی که هدف حمله معنایی قرار گرفته، دچار اخلال نشده و تصور نیز می‌شود که کار خود را به‌خوبی انجام می‌دهد، اما پاسخ‌های آن ناسازگار با واقعیت است. براساس تعریف فوق، جاسوسی سایبری اگرچه امنیت شبکه رایانه‌ای را با هدف انجام یک هدف نظامی در معرض خطر قرار می‌دهد، با این حال عملکرد یک سیستم رایانه‌ای را تخریب نکرده، بنابراین حمله سایبری محسوب نمی‌شود.

1. Semantic Attack

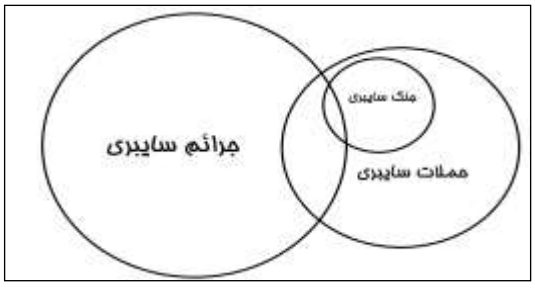
عبارت **"... از یک شبکه رایانه‌ای ...."**: هدف یک حمله سایبری باید یک شبکه رایانه‌ای باشد. شبکه رایانه‌ای سیستمی از رایانه‌ها و وسائلی است که از طریق کانال‌های ارتباطی با یکدیگر مرتبط‌اند. بایستی در نظر داشت که مفهوم رایانه چیزی بیش از یک کامپیوتر شخصی یا لپ‌تاپ است. شبکه رایانه شامل وسایلی است که کنترل آسانسورها، چراغ‌های راهنمایی و رانندگی، سیستم‌های تنظیم فشار در شبکه آب‌رسانی، وسایل منزل همانند تلویزیون، تلفن همراه و حتی ماشین‌های لباسشویی را در اختیار دارند. باگسترش رایانه‌ها در تقریباً تمامی وجوه فعالیت‌های بشری، امکان ایراد آسیب گسترده ناشی از یک حمله سایبری مستمراً در حال افزایش است.

عبارت **"... وجود یک هدف امنیت ملی یا سیاسی ورای حمله"**: وجود یک هدف امنیت ملی یا سیاسی موجب تمایز میان حمله سایبری و جرم سایبری ساده می‌شود. هرگونه اقدام تهاجمی که توسط بازیگر دولتی در عرصه سایبری انجام می‌شود، لزوماً دلالت بر امنیت ملی داشته، در صورت تأمین سایر عناصر تعریف، حمله سایبری محسوب می‌شود. جرم سایبری که توسط یک بازیگر غیردولتی با هدف امنیت ملی یا سیاسی ارتکاب می‌یابد، یک حمله سایبری است. از سوی دیگر یک جرم سایبری که توسط بازیگر غیردولتی با هدفی غیر از هدف امنیت ملی یا سیاسی به‌وقوع می‌پیوندد، همانند بسیاری از تقلب‌ها، دزدی‌های اموال خصوصی فرهنگی که مرتباً در عرصه اینترنت رخ می‌دهد، این عنصر از تعریف حمله سایبری را تأمین نکرده، صرفاً یک جرم سایبری (نه حمله سایبری) محسوب می‌شوند.

۲. مقایسه میان حمله سایبری، جرم سایبری و جنگ سایبری

برای درک بهتر مفهوم"حمله سایبری" و قائل شدن تمایز میان آن با"جرم سایبری"و"جنگ سایبری" شکل شماره (۱)می‌تواند مساعدت نماید:

شکل شماره (۱)- رابطه میان عملیات متعدد سایبری



(منبع: نویسندگان)

علی‌رغم آنکه هیچ تعریف عامی از مفهوم "حمله سایبری"و"جرم سایبری"وجود ندارد، با این وجود موضوع مهم برای فهم حمله سایبری، درک تمایز و اختلاف آن با جرم سایبری است. برخی از وجوه جرم سایبری به‌صورتی عام مورد شناسایی قرار گرفته است. معمولاً جرم سایبری استفاده از ابزار رایانه محور، برای ارتکاب اقدامات غیرقانونی شناخته شده و برخلاف حمله سایبری شامل طیف وسیعی از فعالیت‌های غیرمجاز می‌شود. در جرم سایبری علی‌رغم آنکه بعضاً شبکه‌رایانه هدف، تخریب می‌شود، اما لزوماً در تمام موارد این‌گونه نیست. علاوه بر آن غالباً در جرم سایبری هدف اقدام، امنیت ملی و سیاسی نیست. وجه تمایز آنها این است که برخلاف حملات سایبری، عامل تمام جرائم سایبری افرادند، و نه دولت‌ها[1]. علی‌رغم اهمیت تمایز میان جرم سایبری و حمله سایبری، اما به هنگام وقوع یک حادثه سایبری غالباً تشخیص آنها از یکدیگر کار آسانی نیست. بخشی از این مشکل از آنجا ناشی می‌شود که شناسایی هدف بازیگران کاری بس دشوار است.

همان‌گونه که در شکل شماره (۱) نشان داده شد، بیشتر جرائم سایبری منجر به یک حمله سایبری یا جنگ سایبری نمی‌شوند. یک عملیات، تنها زمانی که توسط یک بازیگر غیردولتی انجام، و انجام آن به لحاظ قانون داخلی یا بین‌المللی جرم باشد، یک جرم سایبری تلقی می‌شود. برای فهم بهتر عملیاتی که ممکن است جرم سایبری تلقی، اما حمله سایبری محسوب نگردد، موارد زیر را در نظر آورید:

اول: بازیگری غیردولتی با هدف امنیت ملی و سیاسی با استفاده از ابزار رایانه‌ای، عملی غیرقانونی مرتکب، اما این اقدام او منجر به تخریب شبکه‌های رایانه‌ای نمی‌شود. به عنوان مثال فردی ممکن است درجایی‌که براساس قوانین داخلی اعلام مخالفت سیاسی ممنوع است، از طریق اینترنت اعلام مخالفت سیاسی نموده و مرتکب جرمی سایبری شود.

دوم: هکری را در نظر آورید که بدون هیچ هدف امنیت ملی و سیاسی، و صرفاً جهت کسب منافع اقتصادی با استقاده از ابزار شبکه رایانه‌ای، سیستم حساب‌های آنلاین بانکی را تخریب نماید. در این مورد نیز یک جرم سایبری به‌وقوع پیوسته، اما حمله سایبری یا جنگ سایبری صورت نگرفته است.

سوم: بازیگری غیردولتی با استفاده از رایانه یا شبکه، درگیر عملیاتی غیرقانونی شده، اما کارکرد شبکه رایانه‌ای را تخریب نکرده و دارای هدف امنیت ملی و سیاسی نیز نبوده است. مثلاً فردی که اقدام به انتقال هرزه‌نگاری رایانه‌ای می‌کند، مرتکب جرم سایبری شده، اما حمله

سایبری انجام نداده است. جنگ سایبری هم می‌تواند منجر به حمله سایبری شود و هم منجر به جرم سایبری. جنگ سایبری شامل حملاتی می‌شود که:

۱. در بستر یک مخاصمه مسلحانه جاری صورت گرفته و منجر به تخریب کارکرد شبکه رایانه‌ای شود.

۲. اهداف امنیت ملی و سیاسی ورای آن باشد.

۳. حقوق کیفری (همانند جنایات جنگی) را نقض نماید و

۴. برای انجام آن از ابزار شبکهو سیستم رایانه‌ای استفاده شود.

جنگ سایبری دارای تأثیری معادل حملات مسلحانه متعارف می‌باشد، اما حملات سایبری به صورت خلاصه دارای شرایط زیر می‌باشند:

۱. هم می‌تواند توسط دولت صورت پذیرد هم توسط بازیگران غیردولتی؛

۲. هدف آن بایستی تخریب کارکرد شبکه رایانه‌ای باشد؛

۳. یک هدف امنیت ملی و سیاسی بایستی در ورای آن باشد.

براین اساس جنگ سایبری همیشه تأمین‌کننده شرایط یک حمله سایبری می‌باشد، اما تمام حملات سایبری جنگ سایبری نیستند. تنها حملات سایبری که دارای تأثیراتی برابر با حملات مسلحانه متعارف، یا حملاتی که در چارچوب مخاصمات مسلحانه بوده و به سطح جنگ سایبری ارتقاء یابند، جنگ سایبری تلقی می‌شوند.

۳. حقوق جنگ و جنگ سایبری

در اینجا در نظر نیست که جزییات "حق جنگ[۲]" و "حقوق در جنگ[۳]" و قابلیت اعمال آنها در حملات سایبری مورد بررسی قرار گیرد، بلکه در نظر است تعیین شود به موجب "حق جنگ" چه زمانی یک حمله سایبری معادل حمله مسلحانه بوده تا بتوان واقعاً آن را جنگ سایبری نامید و چگونه حقوق حاکم بر جنگ، می‌توانند در حملات سایبری اعمال گردد.

اعمال حقوق جنگ نسبت به حملات سایبری به‌شدت چالش‌برانگیز است. عمده‌ترین معاهده حاکم بر حقوق جنگ کنوانسیون‌های چهارگانه ژنو می‌باشند که آخرین بار پس از خاتمه جنگ جهانی دوم به‌روزرسانی شده است. به هنگام تهیه این کنوانسیون‌ها، پیش‌بینی حملات سایبری برای تهیه‌کنندگان آن اساسا امکان‌پذیر نبوده است. چالشی که این کنوانسیون‌ها برای نظام‌مند نمودن حملات سایبری با آن روبه‌رو هستند، غیرقابل پیش‌بینی

2. Jus ad Bellum
3. Jus in Bello

بودن این حملات و نحوه مواجهه با حملاتی است که دارای هیچ نتیجه عینی و مستقیمی بر امنیت ملی نبوده، اما عملاً به آن آسیب وارد می‌نمایند. این واقعیت که چنین حملاتی هم به لحاظ کمّی و هم به لحاظ دامنه مستمراً در حال افزایش هستند، نشان‌دهنده ضرورت توافق دول در مورد شرایطی است که حمله سایبری منجر به حمله مسلحانه شده یا کاربرد زور را توجیه می‌نماید. با توجه به فقدان یک توافق جامع در این خصوص، افزایش مکرر حملات سایبری منجر به تقویت این نظر می‌شود که دولت‌ها مجازند برای پاسخ به حملات سایبری از تسلیحات متعارف استفاده نمایند.

در ابتدا لازم است به این سؤال پاسخ داده شود که چه زمانی یک حمله سایبری به سطح حمله مسلحانه ارتقاء می‌یابد که تمسک به حق دفاع از خود به موجب اصل ۵۱ منشور را مشروع نماید؟ همان‌گونه که گفته شد، بهترین ملاک برای تعیین یک حمله سایبری، به‌عنوان یک جنگ سایبری، بررسی این امر است که آیا حمله مذکور منجر به تخریبی فیزیکی، قابل مقایسه با حملات متعارف، شده است یا خیر؟ برای پاسخ به این سؤال لازم است هم متن منشور بررسی، و هم رویه دولت‌ها مورد عنایت قرارگیرد، زیرا یک جنگ تنها به‌واسطه یک حمله سایبری آغاز نمی‌شود. در رویه دولت‌ها نیز حمله سایبری مشروع، در پاسخ به یک حمله مسلحانه، وجود ندارد. بنابراین تحلیل حقوقی ارائه‌شده در اینجا ضرورتاً مبتنی بر موارد فرضی خواهد بود.

۳-۱. حق جنگ (حق کاربرد زور)

در اینجا مسئله تعیین قانون حاکم بر حق دولت‌ها برای کاربرد زور، به منظور دفاع از خود در مقابل حملات سایبری است. برای پاسخ به این سؤال بایستی سه مسئله بررسی شود:

۱. ممنوعیت کاربرد، و تهدید به آن در روابط بین‌الملل براساس بند ۴ اصل ۲ منشور؛

۲. استثنائات وارده بر ممنوعیت کاربردزور، و تهدید به آن براساس فصل هفتم منشور؛

۳. بررسی دو عنصر"ضرورت" و "تناسب" مربوط به حق جنگ در حقوق بین‌الملل عرفی و محدودیت‌ها و مشکلات موجود برای اعمال آن در حملات سایبری.

۳-۱-۱. ممنوعیت کاربرد زور و مداخله در امور داخلی، اصل حقوقی حاکم در روابط بین‌الملل

بند۴ اصل ۲ منشور ملل متحد اعلام می‌دارد دولت‌ها در روابط خارجی خویش از کاربرد زور، یا تهدید به آن، علیه تمامیت ارضی یا استقلال سیاسی دول دیگر، یا هر روش دیگری مغایر با

اهداف ملل متحد خودداری خواهند نمود. این ممنوعیت، منطبق با هنجار عدم مداخله در حقوق بین‌الملل عرفی است که دولت‌ها را از مداخله در امور داخلی دول دیگر منع می‌کند. دیوان دادگستری بین‌المللی نیز در قضیه نیکاراگوآ در مقابل ایالات متحده اعلام داشت، اگر مداخله شکل کاربرد زور یا تهدید به خود گیرد، هنجار عدم مداخله حقوق بین‌الملل عرفی متناظر با بند ۴ اصل ۲ منشور ملل متحد خواهد بود.

از آنجا که هزینه تمسک به حملات سایبری از هزینه مربوط به آغاز یک جنگ متعارف کمتر است و به دلیل آنکه دول صنعتی، عموماً وابستگی زیادی به شبکه‌های رایانه‌ای داشته و در مقابل حملات سایبری آسیب‌پذیرترند، حملات سایبری به عنوان سلاحی قدرتمند در دست ضعفا تلقی می‌شود. این تغییر در هزینه هم احتمال حملات سایبری را افزایش داده و هم امکان تفاسیر سیاسی گوناگون از حدود و ثغور بند ۴ اصل ۲ منشور را فراهم کرده است.

۳-۱-۲. استثناء امنیت جمعی و دفاع از خود

ممنوعیت کاربردزور یا تهدید به آن، در منشور ملل متحد دارای دو استثناء می‌باشد: ۱. امنیت جمعی مبتنی بر قطعنامه‌های لازم‌الاجرای شورای امنیت براساس فصل هفتم و ۲. دفاع از خود براساس اصل دفاع مشروع.

ارائه پاسخ براساس امنیت جمعی به لحاظ سیاسی قدری دشوار می‌باشد، زیرا صدور مجوز شورا معمولاً زمان‌بر بوده، یا به بن‌بست ختم می‌شود. اصل ۵۱ نیز اعلام می‌دارد در صورت وقوع یک حمله مسلحانه، هیچ چیز در منشور نمی‌تواند مخل حق ذاتی دفاع از خود به‌صورت جمعی و فردی باشد. موضوع اصلی برای تعیین مشروعیت دفاع از خود، وقوع یک تهاجم مسلحانه است. به تبع برای مشروعیت یک حمله سایبری نیز، ارتقاء آن به سطح تهاجم مسلحانه ضروری است تا دولت قربانی بتواند به‌صورت قانونی و مبتنی بر اصل ۵۱ به آن واکنش نشان دهد.

۳-۱-۳. رویکردهای موجود نسبت به استناد به اصل دفاع از خود در پاسخ به حملات سایبری

در مباحث علمی مربوط به اعمال حق کاربرد زور در مقابل حملات سایبری، جهت تعیین این امر که چه زمانی حمله سایبری منجر به یک حمله مسلحانه شده، تا ماشه استناد به حق دفاع از خود به‌صورت مسلحانه کشیده شود، سه رویکرد عمده تاکنون مطرح شده است: رویکرد ابزارمحور؛ رویکرد هدف‌محور و رویکرد تأثیرمحور.

رویکرد ابزارمحور. براساس این رویکرد، صرفاً وقوع یک حمله سایبری به تنهایی هیچگاه منجر به وقوع یک حمله مسلحانه در جهت اعمال اصل ۵۱ منشور نمی‌شود، زیرا که این حملات فاقد خصوصیت فیزیکی کاربرد مسلحانه زور، به‌شیوه سنتی هستند. از آنجا که در این حملات در مجموع از تسلیحات نظامی متعارف استفاده نمی‌شود، استناد به آن برای مشروعیت کاربرد حق دفاع از خود کارآیی ندارند. این گرایش درصورتی یک حمله سایبری را واجد شرایط مشروعیت استناد به اصل ۵۱ می‌داند که در آن تسلیحات نظامی استفاده شود. مثلاً بمباران سرورهای رایانه‌ای یا کابل‌های اینترنتی، شرایط یک حمله مسلحانه را کسب می‌کند. اصل ۴۱ منشور، اختلال کامل یا جزیی .... خطوط تلگراف، رادیو و سایر ابزار ارتباطاتی را حاوی کاربرد زور نمی‌داند. متن منشور نیز تا حدودی از نظریه "ابزارمحور" حمایت می‌کند. مجمع عمومی نیز فهرستی از اقداماتی را که به‌موجب اصل ۳۹ منشور منجر به تجاوز می‌شوند برشمرده است که تماماً حاوی کاربرد تسلیحات و نیروی نظامی می‌شوند. از آنجا که استفاده از تسلیحات و نیروهای نظامی به سادگی قابل شناسایی است، امتیاز مهم گرایش ابزارمحور سادگی در تشخیص آن است. با وجود این حملات سایبری، بدون استفاده از تسلیحات نظامی سنتی و متعارف، از ظرفیت ایجاد آسیب‌های به شدت مخربی برخوردارند.

رویکرد هدف‌محور. گرایش هدف‌محور با درک ضعف رویکرد ابزارمحور در مواجهه با خسارات ناشی از ابزار نامتعارف، هر حمله سایبری به سیستم‌های مهم رایانه‌ای را یک حمله مسلحانه تلقی می‌نماید. هدف اولیه این رویکرد مشروعیت بخشی به قاعده دفاع از خود پیشدستانه، برای یک حمله سایبری حاوی آسیبی قریب‌الوقوع است. علی‌رغم آنکه رویکرد هدف محور از سیستم‌های مهم ملی در مقابل تجاوز حمایت می‌کند، این گرایش، عمیقاً دفاع از خود قهری را که متضمن افزایش احتمال منازعات سایبری به نبردهای متعارف می‌باشد، افزایش می‌دهد. براساس این رویکرد در صورت یک وقوع یک حمله سایبری تنها به یک سیستم حیاتی کشور، می‌توان پاسخ نظامی متعارف داد. این گرایش با تسهیل احتمال خطر وقوع جنگ، امنیت جامعه بین‌المللی را در معرض خطر قرار می‌دهد.

رویکرد تأثیرمحور. رویکرد تأثیرمحور، به واسطه شدت تأثیرات یک حمله سایبری، آن را یک حمله مسلحانه تلقی می‌کند. رویکرد تأثیرمحور به دلیل مواضعی میانه بین رویکردهای"هدف‌محور" و "ابزارمحور"، از مقبولیت زیادی برخوردار است. نظرات مختلف رویکرد تأثیرمحور به واسطه درجه شدت، اعم از شدت صرف آسیب، یا شدت آسیب نهایی،

اندازه‌گیری می‌شود. مشکل موجود در رویکرد تأثیرمحور نتایجی است که موجب مشروعیت استناد به دفاع از خود می‌شود. مثلاً حمله‌ای را به یک سیستم کنترل ترافیک هوایی، یا یک شبکه برق منطقه‌ای منجر به خارج شدن آنها از مدار شده، یا حمله‌ای مثل سال حمله سایبری سال ۲۰۰۷ به وبسایت‌های استونی را در نظرگیرید. کدام یک از این حملات تأثیرات عظیمی برجای خواهد گذارد؛ به‌گونه‌ای که بتوان آن را به عنوان حمله مسلحانه توجیه و در پاسخ به آن از نیروهای دفاعی استفاده نمود؟ تمام این حملات کم یا زیاد می‌توانند منجر به مرگ شده و به زیرساخت‌های اقتصادی آسیب وارد نمایند، اما برای کشور متجاوز پیش‌بینی نتیجه این حملات بسیار دشوار می‌باشد. "دانیل سیلور" مشاور سابق سازمان سیا و آژانس امنیت ملی ایالات متحده، استدلال نموده که معیارکلیدی برای تعیین این امر که چه زمانی یک حمله سایبری منجر به حمله مسلحانه می‌شود، شدت آسیب وارده می‌باشد(silver, 2002, pp.90-91). یک حمله سایبری تنها زمانی که جرحی بوده یا به اموال آسیب رساند، توجیه‌کننده دفاع از خود خواهد بود. حتی در آن صورت نیز باید شدت آن مشابه نتایج کاربرد زور مسلحانه باشد. براساس این معیار یک حمله سایبری به سیستم کنترل ترافیک هوایی که منجر به آن شود که هواپیماها با یکدیگر تصادم نمایند، به عنوان یک حمله مسلحانه تلقی خواهد شد، زیرا که این یک اقدام قهری بوده که منجر به ایراد تلفات جانی و وارد آمدن آسیب‌های مهمی به اموال شده است. اما یک حمله سایبری به وبسایت یا نفوذ صرف به یک سیستم رایانه‌ای مهم، به‌صورت عمومی یک حمله مسلحانه تلقی نمی‌شود. شایان ذکر است محاسبه "هدف حمله" که برای ارائه تعریف حمله سایبری مورد بررسی قرار گرفت، در اینجا نیز توصیه می‌شود. براین اساس حمله مذکور بایستی با هدف امنیت ملی و سیاسی ارتکاب یافته باشد. یک اقدام سایبری فاقد نتایج امنیت ملی، یک حمله سایبری محسوب نشده و به تبع از یک جنگ سایبری فاصله بسیار زیادی خواهد داشت.

۳-۲. حقوق در جنگ

علی‌رغم آنکه تاکنون حملات سایبری مستقلاً به عنوان یک مخاصمه مسلحانه مطرح نشده‌اند، به‌طور سنتی این حملات در پاسخ به اقدامات تحریک‌آمیز در مخاصمات، یا به منظور زمینه‌سازی برای یک حمله متعارف قریب‌الوقوع مورد استفاده قرار گرفته‌اند. در این بخش در نظر است به بررسی روابط میان الزامات حقوقی در جنگ‌های سنتی و کاربرد حملات سایبری در مخاصمات مسلحانه متعارف پرداخته شود.

۳-۲-۱. الزامات حقوق عرفی جنگ

استفاده از نیروهای مسلح در پاسخ به یک حمله سایبری نه تنها بایستی منطبق با منشور ملل متحد و محدودیت‌های حقوق بین‌الملل عرفی بر نیروهای مسلح باشد، بلکه باید با دو عنصر "تناسب"و"ضرورت" حقوق بین‌الملل عرفی نیز همخوان باشد. علی‌رغم آنکه اصول مذکور در حقوق بین‌الملل عرفی واضح است، اعمال این اصول در پاسخ دولت‌ها به حملات سایبری مشاجره‌انگیز است. ارزیابی این امرکه آیا استناد به دفاع مشروع، با اصول "تناسب" و "ضرورت" همخوان بوده یا خیر، عملاً حتی برای حملات متعارف نیز دشوار است. به‌علاوه این مقررات تنها بر بخش کوچکی از حملات سایبری، قابل اعمال‌اند که به‌واسطه قطعنامه‌های شورای امنیت یا به‌واسطه اصل ۵۱ منشور مبتنی برحق دفاع ازخود مشروع باشند. در نتیجه تنها برخی از حملات سایبری به درستی یک جنگ سایبری محسوب می‌شوند. از آنجا که حملات سایبری عموماً با فوریت همراه نبوده، مهلک و مخرب نیستند و صرفاً قادر به ایجاد نقص در سیستم‌های شبکه‌ای، آن هم به‌صورت موقت‌اند، به‌نظر می‌رسد فضای مجازی می‌تواند چالش‌هایی بر اعمال اصول "تناسب" و "ضرورت" و همچنین تمایز و بی‌طرفی، موجود در حقوق جنگ تحمیل کند.

الف) ضرورت. علی‌رغم آنکه ارزیابی عنصر ضرورت در یک حمله سایبری ممکن است دشوار باشد، این دشواری منبعث از مباحثی است که ریشه در جنگ سایبری نداشته و منحصر به حقوق حملات سایبری در جنگ نیز نمی‌باشد. عنصر ضرورت در حق کاربرد زور، به وجود یک امتیاز محکم نظامی وابسته است که بایستی از یک منازعه خاص حاصل شود. یک حمله سایبری منفرد در صورتی که منجر به پیشبرد اهداف نظامی نشود، می‌تواند غیرضروری تشخیص داده شود.

ب) تناسب. عنصر تناسب در الزامات حقوق عرفی جنگ انجام حمله‌ای را که انتظار رود به‌صورت تصادفی منجر به بروز تلفات جانی و ایراد جراحت به غیرنظامی شده، یا به اموال غیرنظامی آسیب‌هایی وارد ساخته که بیش از امتیاز نظامی قطعی و مستقیم پیش‌بینی شده از آن باشد ((additional protocol I,1977,Artc:51(5)(b))، منع نموده است. در حقوق جنگ لازم است تصمیم‌گیرندگان جهت بررسی عنصر تناسب، میان امکان بروز تلفات و ایراد آسیب به اموال غیرنظامی از یک سو، و کسب منافع نظامی ناشی از این حملات را از سوی دیگر، توازن برقرار سازند ((additional protocol I,1977,Artc:51(5)(b)54,57(2)(a)(iii)) به دلیل ماهیت آسیب حملات سایبری، تبیین عنصر تناسب در این حملات کاری بس دشواری است. از آنجا

که معمولاً علی‌رغم شدت حملات سایبری، تأثیر مستقیم این حملات غیرمهلک یا موقت می‌باشد، ارزیابی دقیق تناسب این حملات براساس معیارهای پیش‌گفته یعنی، جرح و قتل غیرنظامیان و ایراد خسارت به اموال غیرنظامی، کار دشواری است. ضروری است نحوه ارزیابی آسیب موقت وارده بر سیستم‌های حیاتی مشخص و شفاف شود، زیرا یک حمله سایبری که انتقال اطلاعات از طریق اینترنت را مختل می‌کند، ممکن است علی‌رغم آنکه موجب دردسر مردم می‌شود، دارای نتایج شدیدتری نیز باشد. به عنوان مثال، یک حمله سایبری می‌تواند موجب اختلال در انتقال اطلاعات حیاتی بیماران یک بیمارستان شده و از این طریق باعث مرگ بیماران شود. براین اساس تحلیل عنصر تناسب برای یک "حمله انکار سرویس توزیع شده[۴]"، نسبت به یک حمله متعارف، با شک و تردید بیشتری همراه است. درحقوق جنگ جهت بررسی عنصر تناسب، پیش‌بینی نتایج احتمالی یک عملیات ضروری است، اما در بستری سایبری وجود تردیدهای فزاینده، تحلیل این عنصر را با مشکل مواجه می‌نماید. هنگام تصمیم‌گیری در مورد مشروعیت حملات برنامه‌ریزی شده، دولت‌ها ممکن است بیش از حد دچار تردید شوند.

پ) تمایز. یکی دیگر از چالش‌های قانونی در بستر حملات سایبری مربوط به اصل تمایز می‌باشد که دولت‌ها را ملزم می‌نماید میان نظامیان و غیرنظامیان تفاوت قائل شده و حملات را صرفا به اهداف نظامی محدود کنند. فرماندهان نظامی بایستی تسلیحاتی با دقت هدف‌گیری بالا به‌کار برده و میان اهداف نظامی و غیرنظامی تمایز قائل شوند. با توسیع این عبارت می‌توان اعلام داشت که حقوق جنگ انجام حملات سایبری در منازعه را که غیرقابل کنترل و غیرقابل پیش‌بینی بوده یا در آنها تمایزی میان اهداف نظامی و غیرنظامی وجود ندارد، ممنوع ساخته است.[۲] بند ۲ ماده ۵۴ پروتکل اول الحاقی حملاتی را که منجر به محرومیت جمعیت غیرنظامی از ضروریات حیات، همانند غذا یا تأمین آب شرب شود، ممنوع ساخته است.

در حملات سایبری تحت شرایطی خاص، قائل شدن تمایز به راحتی امکان‌پذیر است. به‌عنوان مثال حمله سایبری به یک سیستم کنترل ترافیک هوایی نظامی، که صرفاً منجر به تصادم وسایل ترابری نظامی شود، همخوان با اصل تمایز است. اما برخی حملات سایبری دیگر، مثلاً حمله به بخش بانکی غیرنظامی یا بیمارستان‌ها، موزه‌ها، یا اماکن عبادی، آشکارا ناقض اصل تمایزند.

4. DDos (Distributed Denial of Service attack)

بررسی چنین مواردی سهل است، اما معمولاً در بستر حمله سایبری تحلیل عنصر تمایز پیچیده‌تر خواهد بود، زیرا که اهداف مورد نظر می‌تواند در آن واحد توسط بازیگران متعدد بهره‌برداری شوند. حدود ۹۵ درصد از مخابرات نظامی، از طریق شبکه‌های غیرنظامی برقرار می‌شوند. این امر شبکه‌های غیرنظامی را به اهداف نظامی جذابی مبدل می‌کند. از آنجا که بیشتر فضای مجازی دارای کاربری غیرنظامی می‌باشد، تقویت، تحکیم و الزام به قائل شدن تمایز در فضای مجازی می‌تواند بسیار بیش از بستر نبردهای متعارف چالش برانگیز باشد.

ت) بی‌طرفی. آخرین معضل مربوط به ارزیابی مشروعیت یک حمله سایبری در جنگ آن است که یک حمله سایبری ممکن است ظاهراً یا واقعاً ریشه در سرزمین یک دولت بی‌طرف داشته باشد. دولت‌ها می‌تواند همانند سوییس به‌صورت دائمی بی‌طرف باشند، یا تنها در خلال یک مخاصمه اعلام بی‌طرفی کند، اما اصل بی‌طرفی دربردارنده حقوق و مسئولیت‌هاست. حق اساسی دولت بی‌طرف، مصونیت از تعرض است. تکلیف اساسی آن نیز عدم جانبداری، و بی‌طرفی مطلق است. درخصوص تعهد دول بی‌طرف نسبت به جلوگیری از استفاده از امکانات آنها توسط متخاصمین، نظرات متفاوتی وجود دارد. برخی معتقدند دول بی‌طرف ملزم به ممانعت از استفاده از تسهیلات ارتباطی خویش توسط طرفین تخاصم نبوده، اما مجاز به کمک به آنها جهت ایجاد چنین تسهیلاتی نمی‌باشند. گروهی دیگر معتقدند که حمله به سرزمین دول بی‌طرفی که نخواهند یا نتوانند از حملات غیرقانونی که ریشه در سرزمین آنها دارند، جلوگیری نمایند، مشروع است. اینان مدعی هستند که دولت‌ها، نه تنها متعهدند که خود از ارتکاب به حملات سایبری خودداری کنند، بلکه نبایستی اجازه استفاده آگاهانه از قلمرو خود برای انجام عملیات علیه حقوق سایر دول دهند.

برخی ویژگی‌های حملات سایبری موجب دشواری ارزیابی اصل بی‌طرفی می‌شود. حملات سایبری می‌تواند به‌صورت مخفیانه از رایانه‌های "زامبی" واقع در یک کشور، برای ضربه زدن به شبکه‌های موجود در کشور دیگر، از طریق مجموعه‌ای از سرورها و رایانه‌ها استفاده نماید. تحلیل و ارزیابی چنین حملاتی به موجب اصل بی‌طرفی به دو دلیل با مانع مواجه می‌شود. یکی آنکه کشور بی‌طرف قادر به کسب اطلاع از بهره‌برداری رایانه‌های خود برای انجام حملات سایبری نبوده، به تبع از نقض بی‌طرفی خود مطلع نمی‌شود. علاوه برآن براساس اصل بی‌طرفی پاسخ‌های قانونی به حمله، مبتنی بر هویت وکشور منشاء حمله تعیین می‌شود. ناتوانی در انتساب مسئولیت حمله به دولتی معین، مانع از بررسی نقض اصل بی‌طرفی خواهد شد.

۳-۲-۱. اهداف مشروع در بستر حمله سایبری

در حقوق جنگ سه گروه افراد اهدافی مشروع تلقی می‌شوند: رزمندگان، غیرنظامیانی که مشارکت مستقیم در مخاصمه دارند و غیرنظامیانی که مستمراً می‌رزمند.

براساس بند ۳ اصل ۵۱ پروتکل الحاقی اول کنوانسیون ژنو، غیرنظامیان به میزانی که مشارکت مستقیم در مخاصمه دارند، مصونیت خویش را از دست خواهند داد. به‌علاوه براساس حقوق بین‌الملل عرفی، که توسط کمیته بین‌المللی صلیب سرخ نیز مورد تأیید قرارگرفته، غیرنظامیانی را که مستمراً در حال نبردند، می‌توان هدف گرفت. مشارکت غیرنظامیان در حملات سایبری، و تهدید به چنین حملاتی، عملاً امکان تمایز میان مشارکت مستقیم، عملکرد مستمر خصمانه، و سایر انواع مشارکت در نزاع را غیرشفاف نموده است. به‌طور سنتی طراحان غیرنظامی سیستم‌های تسلیحاتی، شرکت‌کننده مستقیم در تخاصم محسوب نمی‌شوند. برنامه‌نویسانی که با اطلاعات نظامی کار می‌کنند می‌تواند درست تا لحظه انجام حمله، اقدام به دستکاری رمزها و کدها نمایند. فعالیت مستمر چنین غیرنظامیانی، می‌تواند مشمول آماده‌سازی، اجرا، یا فرماندهی عملیات گشته و به عنوان مشارکت مستقیم در تخاصم محسوب شود. درنتیجه غیرنظامیان درگیر در حملات سایبری به‌دلیل انجام اعمالی که منجر به تغییر وضعیت آنها براساس حقوق جنگ می‌شود، هدفی مشروع برای حمله متقابل تلقی شوند.

۳-۲-۲. فاعل حمله مشروع سایبری

دلایلی متعددی وجود دارد که دولت‌ها را علی‌رغم وجود عواقب حقوقی، تشویق به استفاده از غیرنظامیان در عملیات سایبری می‌نماید. اولاً غیرنظامیان از توان فنی و تخصصی بیشتری نسبت به دولت‌ها برخوردارند. علاوه بر آن عاملیت غیرنظامیان دولت‌ها را قادر می‌سازد مشارکت خود در عملیات سایبری را کتمان کنند. گفته می‌شود مبتنی بر همین استدلال گروه "ناشی" که متشکل از جوانان طرفدار کرملین بود، مسئولیت حمله سایبری سال ۲۰۰۷ علیه دولت استونی را برعهده گرفت.

جئوفری اس کورن، قاضی و دستیار سابق حقوق جنگ امریکا در این رابطه عنوان داشته که دیگر معیار مربوط به مشارکت مستقیم منسوخ شده، پیشنهاد نمود معیاری نوین برای افراد مجاز به انجام حملات سایبری و انطباق آن با حقوق جنگ تعیین شود. انجام وظیفه براساس سلسله‌مراتب فرماندهی معیاری منطبق با حالت رزمندگی است، زیرا اعضای نیروهای مسلح تحت مسئولیت فرمانده قرار داشته و در درون یک سلسله‌مراتب نظامی شامل آموزش، انضباط

و وفاداری یگانی عمل می‌کنند. براین اساس کورن استدلال می‌کند که تنها افرادی که تحت نظارت یک فرمانده عمل می‌کنند، بایستی واجد شرایط ناقض حقوق جنگ باشند، زیرا عمل آنان در چارچوب ساختار فرماندهی و انضباط قرار داشته که قادر به جلوگیری از بروز تخلفات یا تنبیه آنهاست. براساس این استدلال، دولت‌ها برای انجام وظایف دولتی که مستلزم رعایت حقوق جنگ است، مجاز به به‌کارگیری پیمانکاران غیرنظامی نیستند.

۴. تلاش سازمان‌های فراملی برای تنظیم قواعد واکنش به حملات سایبری

علی‌رغم آنکه تاکنون هیچ چارچوب جامع حقوقی بین‌المللی، حاکم بر تمام حملات سایبری وجود ندارد، تلاش‌های پراکنده و جسته و گریخته‌ای انجام شده است که برخی امکانات را برای کنترل این تهدید فزاینده ایجاد می‌کند. در این بخش به بررسی این مکانیسم‌های قانونی پرداخته خواهد شد.

۴-۱. سازمان ملل متحد

سازمان ملل متحد تاکنون اقدامات محدودی درخصوص امنیت سایبری انجام داده است. علی‌رغم آنکه مجمع عمومی سازمان تاکنون در این رابطه چندین قطعنامه صادر کرده، این قطعنامه‌ها مبهم و متضمن اقدام خاصی از سوی اعضای سازمان نیست. در اوت ۱۹۹۹ سازمان ملل متحد، با هدف درک بهتر مفاهیم امنیت فناوری‌های اطلاعاتی در حال ظهور، میزبان نشستی کارشناسی در ژنو بود. قطعنامه‌ای که به دنبال این نشست از سوی مجمع عمومی سازمان در سال ۲۰۰۲ منتشر شد، بحث و بررسی بیشتر در خصوص امنیت اطلاعات را خواستار شد (U.N G.A A/RES/57/53,2002) اما اقداماتی اندک در این رابطه به عمل آمد. در سال‌های ۲۰۰۳ و ۲۰۰۵ سازمان میزبان برگزاری دو اجلاس سران بود، که در آن به امنیت اطلاعات فراخوانی شد، اما بار دیگر نتایجی قطعی حاصل نشد. در ژوئیه ۲۰۱۰ که متخصصان امنیت سایبری بیش از ۱۵ کشور جهان، از جمله قدرت‌های بزرگ سایبری مثل امریکا، چین، و روسیه گرد هم آمده بودند، سازمان گامی به جلو برداشته و توصیه‌هایی به دبیرکل ارائه و کشورها را به اقدامات زیر فراخواند (U.N Doc. A/65/201, 2010).

۱. گفتگوهای بیشتر میان دولت‌ها؛

۲. اعتمادسازی، ایجاد ثبات و کاهش مخاطرات ... از جمله تبادل نقطه‌نظرات ملی درخصوص استفاده از اطلاعات و تکنولوژی‌های ارتباطی در مخاصمات؛

۳. تبادل اطلاعات درخصوص قانون‌گذاری اطلاعات ملی و فناوری‌های ارتباطی مربوط به استراتژی‌های امنیتی و سیاست‌ها و کاربرد فناوری‌ها؛

۴. شناسایی اقدامات لازم برای حمایت از ایجاد ظرفیت در کشورهای کمتر توسعه‌یافته؛

۵. یافتن امکاناتی برای تشریح اصطلاحات و شرایط مشترک.

به‌هرصورت درحال حاضر نقش سازمان ملل متحد در خصوص امنیت سایبری تقریباً در حد انجام مذاکره و تبادل اطلاعات باقی‌مانده است.

۴-۲. پیمان آتلانتیک شمالی (ناتو)

ناتو به دلیل فقدان یک دکترین اصولی و استراتژی سایبری جامع، به حمله سایبری سال ۲۰۰۷ استونی، از خود واکنشی نشان نداد، اما پس از آن مواجهه با تهدیدات سایبری را مد نظر قرار داد. این پیمان در اجلاس سران در سال ۲۰۰۸ در بخارست، به‌طور رسمی حملات سایبری را مورد بررسی قرار داده و دو بخش متمرکز بر حملات سایبری به این شرح ایجاد کرد:

الف) اداره مدیریت دفاع سایبری. این اداره بر توان دفاعی کشورهای عضو متمرکز است. اطلاعات کمی در خصوص آن منتشر شده، این اعتقاد وجود دارد که بر توان رهگیری سریع الکترونیکی جهت شناسایی تهدیدات، همچنین تبادل سریع اطلاعات جاسوسی سایبری متمرکز می‌باشد تا در نهایت به یک اتاق عملیات جنگی برای دفاع سایبری مبدل شود.

ب) مرکز عالی دفاع مشترک سایبری. هدف این مرکز توسعه استراتژی و دکترین دفاع بلندمدت سایبری می‌باشد.

علی‌رغم فشار زیاد کشورهای شرق اروپا، حملات سایبری تا اجلاس سال ۲۰۱۴ در ولز بریتانیا تنها درچارچوب اصل۴ پیمان ناتو قرار می‌گرفت که در صورت وقوع حمله سایبری، کشورهای عضو را به مشورت با یکدیگر فراخوانده، اما آنها را مجبور به مساعدت به یکدیگر براساس اصل ۵ پیمان نمی‌کرد. در ۶ سپتامبر ۲۰۱۴ دبیرکل ناتو پا را از آن فراتر نهاده و به‌طور رسمی اعلام داشت این سازمان راهبرد جدیدی را در زمینه دفاع سایبری اتخاذ کرده که بر اساس آن اگر عضوی مورد حمله سایبری دشمن قرار گیرد این حمله معادل حمله نظامی کلاسیک تلقی شده و تمامی اعضای ناتو باید شرایط را دفاعی تلقی کنند. در این استراتژی حمله سایبری به یک عضو به منزله تعرض به کل اعضای پیمان تلقی، و بر لزوم دفاع جمعی در برابر حمله نظامی تأکید شده است. به این ترتیب، حمله سایبری ویرانگر به شبکه‌ها و سرورهای یکی از اعضای ناتو می‌تواند به عنوان اعلام جنگ به آن کشورها تلقی شود. در

استراتژی جدید ناتو به سرعت زیاد حملات سایبری اشاره و عنوان شده است که حمله با موشک‌های قاره‌پیمای بالستیک دست‌کم به ۳۰ دقیقه زمان نیاز داشته، یا حملات دریایی ماه‌ها زمان می‌برد، اما حملات سایبری تنها در ۳۰ میلی‌ثانیه می‌توانند انجام شود. علاوه بر آن ناتو گروهی از صاحب نظران را برای بررسی این مسئله و تدوین استراتژی ناتو در مقابل حملات سایبری منصوب نمود که نتیجه کار آنها در سال ۲۰۱۳ تحت عنوان دستورالعمل تالین در حقوق بین‌الملل قابل اعمال در نبردهای سایبری در شهر تالین در کشور استونی ارائه شد.

۴-۳. شورای اروپا

شورای اروپا، تاکنون نسبت به هر سازمان فراملی دیگری، بیشترین اشتیاق را جهت تنظیم قواعد مربوط به امنیت سایبری، به‌خصوص جرم سایبری، از خود نشان داده است. این شورا در سال ۲۰۰۱ کنوانسیون جرایم سایبری شورای اروپا را به‌عنوان اولین معاهده بین‌المللی درخصوص جرایم ارتکابی ازطریق اینترنت و شبکه‌های رایانه‌ای اعلام کرد. این کنوانسیون صورت ابتدایی سیاست مشترک کیفری اتحادیه، با هدف دفاع در مقابل جرایم سایبری، از طریق قانون‌گذاری و انجام همکاری‌های بین‌المللی بود. ایالات متحده نیز در سال ۲۰۰۶ به این کنوانسیون پیوست.[۳] حملات سایبری مندرج در کنوانسیون جرایم سایبری فوق، به محرمانه‌بودن، یکپارچگی و در دسترس بودن داده‌ها و سیستم‌های رایانه‌ای، به‌خصوص دسترسی غیرقانونی به آنها، همچنین مداخلات اطلاعاتی و سیستمی در آنها مربوط است. به نظر نمی‌رسد مفاد آن قابل اعمال بر عملیات دولتی (خواه با هدف اعمال قانون، خواه با هدف امنیت ملی) باشد. برای مثال اصل ۲ آن اعلام می‌دارد که ضروری است دول عضو، قانون‌گذاری و سایر اقدامات لازمه ... را به منظور ایجاد یک بخش دفاع کیفری براساس حقوق داخلی خود جهت دسترسی بدون مجوز به تمام یا بخشی از سیستم رایانه‌ای انجام دهند. این کنوانسیون می‌تواند از طریق الحاق سایر کشورها، محدودیت‌هایی اندک بر حملات سایبری اعمال نماید. براساس اصل ۲۳ کنوانسیون، متعاهدین توافق نمودند به منظور انجام تحقیقات و بازرسی در خصوص جرائم کیفری مربوط به سیستم‌های رایانه‌ای و اطلاعات، تا حد امکان با یکدیگر همکاری نمایند. اگرچه غیرمستقیم و غیرمصرح، اما از آنجا که انجام حملات سایبری کشورهای عضو این کنوانسیون علیه سایر دول عضو می‌تواند باعث اضمحلال اهداف کنوانسیون شود، این توافق می‌تواند تاحدی حملات سایبری طرف‌های کنوانسیون را علیه یکدیگر محدود نماید.

مع‌الوصف اینکه در اثر نقض کنوانسیون، چه عواقب و پیامدهایی متوجه دول عضو می‌شود، همچنان نامشخص است.

۴-۴. سازمان کشورهای امریکایی

سازمان کشورهای امریکایی اقدامات اولیه برای تنظیم قواعد مربوط به حملات سایبری را به‌عمل آورده است. در آوریل ۲۰۰۴ سازمان مذکور قطعنامه‌ای از تصویب گذارند که عنوان می‌داشت دول عضو بایستی امتیازات اجرای اصول مورد نظر کنوانسیون سال ۲۰۰۱ جرایم سایبری شورای اروپا را ارزیابی و امکان الحاق به آن را بررسی کنند. این سازمان همچنین استراتژی جامع امنیت سایبری بین‌الامریکایی را تصویب نمود که یکی از اهداف آن سیاست‌گذاری و قانون‌گذاری جرایم سایبری است تا از کاربران اینترنتی حفاظت نموده و با وجود احترام به حقوق خصوصی کاربران اینترنت، سد راه سوءاستفاده از رایانه‌ها و شبکه‌های رایانه‌ای شود. به منظور حصول به این نتیجه سازمان مذکور با استقرار یک گروه کارشناسی جهت ارائه کمک‌های فنی به کشورهای عضو برای تهیه پیش‌نویس و وضع قوانینی که جرم سایبری را مجازات، از سیستم‌های اطلاعات حفاظت، و استفاده از اینترنت در فعالیت‌های غیرقانونی را منع کند، توافق نموده است. مجموعه یکسانی از قوانین که کشورهای عضو بتوانند به‌واسطه آن با جرایم سایبری و حملات سایبری مقابله کنند، ارائه نشده است.

۴-۵. سازمان همکاری‌های شانگهای

سازمان همکاری‌های شانگهای نیز گام‌های اولیه مهمی برای همکاری در حوزه امنیت سایبری برداشته است. در قطعنامه یکاترینبورگ[5] که در ۱۶ ژوئن ۲۰۰۹ صادر شد، کشورهای عضو سازمان بر اهمیت موضوع تأمین امنیت اطلاعات بین‌المللی به‌عنوان یکی از عوامل کلیدی سیستم عمومی امنیت بین‌المللی تأکید دارند. سازمان همچنین امکان تأسیس مرکز اقدامات قانونی بین‌المللی در خصوص حملات سایبری را مطرح نموده است. این سازمان مدلی را ارائه داده که احتمالاً در تعارض با مدل غربی است که در پی جلوگیری از تداخل در آزادی بیان است.

در مجموع می‌توان عنوان داشت که تلاش‌های بین‌المللی جهت قاعده‌مندسازی حملات سایبری هنوز در مرحله جنینی قراردارد. به استثنای کنوانسیون جرم سایبری شورای اروپا، بیشتر موافقت‌نامه‌های بین‌المللی تاکنون از بحث درخصوص استراتژی‌های آتی فراتر نرفته‌اند.

5. Yekaterinburg Declaration

۵. سایر چارچوب‌های قانونی حاکم بر حملات سایبری

علاوه بر حقوق جنگ، برخی چارچوب‌های حقوقی دیگر نیز موجودند که به‌طور مستقیم معطوف به حملات سایبری نبوده، حاوی ابزاری هستند که می‌تواند حملات سایبری را نیز قاعده‌مند نمایند. این رژیم‌های حقوقی عمدتاً پیش از ظهور حملات سایبری شکل‌گرفته و به صراحت حملات سایبری را مد نظر ندارند. اما درصورتی که حمله‌ای از طریق روش‌های مندرج در آنها انجام شود، می‌توانند برای بررسی حمله سایبری نیز مورد استناد قرارگیرند. از کنار هم گذاشتن رژیم‌های متعدد بین‌المللی که هرکدام از آنها برخی وجوه حملات سایبری را قاعده‌مند می‌سازند، می‌توان یک رویه قانونی به‌هم بافته، و صرفاً بخشی از حملات سایبری را تنظیم کرد. در این بخش به بررسی این چارچوب‌ها پرداخته می‌شود.

۵-۱. حقوق بین‌الملل سنتی اقدام متقابل

حقوق بین‌الملل عرفی اقدام متقابل، بر چگونگی واکنش دولت‌ها نسبت به تخلفات بین‌المللی، حاکم است. تخلفاتی که به سطح یک مخاصمه مسلحانه ارتقاء نیافته تا بتوان آنها را تحت عنوان دفاع از خود توجیه نمود. براساس این قاعده درصورت تخلف یک دولت از حقوق بین‌الملل، دولت زیان‌دیده می‌تواند با اقدامات متقابل خود به آن پاسخ دهد. برخی حملات سایبری به سطح مخاصمه مسلحانه ارتقاء نمی‌یابد، اما هنجار عدم مداخله حقوق بین‌الملل عرفی را نقض می‌کنند. این تخلفات، دولت زیان‌دیده را مستحق انجام اقدامات متقابل، جهت الزام دولت مسئول به قانون می‌نماید. اصول مسئولیت بین‌المللی دولت‌ها اعلام می‌دارد اقدامات متقابل بایستی موقت بوده، دولت مسئول را به‌دلیل تخلفات قبلی آن هدف گرفته، و ابزاری جهت جلوگیری از تخلف دولت مسئول در اختیار قراردهد (U.N. A/56/10, Artc:49). در صورت توقف تخلف از حقوق بین‌الملل، اقدام متقابل نمی‌تواند ادامه یابد. همچنین هیچگاه اقدام متقابل نمی‌تواند تخلف از اصول اساسی حقوق بشر، ممنوعیت اقدامات تلافی‌جویانه، یا هنجارهای قطعی و محرز بین‌المللی را توجیه نماید. این اقدامات همچنین بهانه‌ای برای قصور در حل‌وفصل مسالمت‌آمیز اختلافات، یا مصونیت دیپلمات‌ها نیست (U.N. A/56/10, Artc:50, Para:2). دولت زیان‌دیده باید پیش از تمسک به اقدامات متقابل، به‌صورت کلی دولت مسئول را به خودداری از انجام اقدامات خلاف فراخوانده، اعلام دارد که تصمیم به انجام اقدامات متقابل گرفته، و پیشنهاد مذاکره برای حل موضوع را دهد(U.N. A/56/10, Artc:52). براساس حقوق عرفی اقدامات متقابل، دولت مهاجم که به‌واسطه حملات سایبری تعهدات خود را نسبت به عدم

دخالت در امور دولت حاکم دیگری نقض نماید، می‌تواند مشمول اقدامات متقابل قانونی دولت زیان‌دیده شود. چنین اقدامات متقابلی می‌تواند از "دفاع غیرعامل" سایبری (مثل فایروال‌ها) که جهت دفع حملات سایبری به کار گرفته می‌شوند فراتر رفته و با هدف خشکاندن ریشه حمله منجر به "دفاع عامل" نیز منجر شود. پیش از آنکه دولتی تحت عنوان عمل متقابل اقدام به دفاع عامل نماید، بایستی نشان دهد که یک اقدام خلاف بین‌المللی منجر به آسیب‌رسانی به آن شده، دولت مسئول را شناسایی، و نسبت به سایر قیود پایبند بماند. عمل متقابل بایستی به منظور تشویق دولت متخلف جهت عمل به تعهداتش برنامه‌ریزی شود.

علی‌رغم آنکه اقدامات متقابل ابزاری ارزشمند برای مواجهه با حملات سایبری که به سطح یک حمله مسلحانه ارتقاء نیافته، در اختیار دولت‌ها قرار می‌دهد، لازم است:

۱. هویت مهاجم و رایانه یا شبکه‌ای منشاء این حملات به‌درستی مشخص شود؛

۲. طرف مقابل بایستی اقدامات متقابل را هزینه‌دار بداند؛

۳. این هزینه باید زیاد باشد که مانع مهاجم برای استمرار اقدامات غیرقانونی شود و

۴. به دلیل اشتراک زیرساخت‌های سایبری، یا استفاده از رایانه افراد به عنوان ابزار حمله، بدون رضایت آنها، انجام اقدام متقابل صرفاً آسیب‌رسان به عامل حملات غیرقانونی دشوار است.

حقوق اقدامات متقابل عرفی نیز صرفاً پاسخگوی بخشی از معضل مربوط به حملات سایبری بوده و برای مواجهه با چنین معضلی به سایر رژیم‌های حقوق بین‌الملل که مستقیماً حملات سایبری را قانونمند کنند، نیاز است.

۵-۲. حقوق ارتباطات از راه دور

حملات سایبری با استفاده از ارتباطات باسیم بین‌المللی، می‌تواند مشمول حقوق ارتباطات از راه دور شوند. مقررات ارتباطات از راه دور بین‌المللی می‌تواند درخصوص حمله سایبری به امواج الکترونیک یا شبکه‌های ارتباطات از راه دور بین‌المللی، مورد استناد قرارگیرند. دول عضو این اتحادیه می‌توانند هر ارتباط از راه دور غیردولتی را که قادر به ایجاد مخاطره برای امنیت دولت، یا قوانین، یا انتظام اجتماعی آن باشد، قطع نموده یا ارائه خدمات ارتباطات از راه دور بین‌المللی را به‌صورت کامل یا صرفاً برای ارتباطاتی خاص، یا نوع خاصی از مکاتبات، ورودی، خروجی یا تبادل، را به‌حالت تعلیق درآورند. مشروط به آنکه بلافاصله از طریق دبیرکل، این اقدام به سایر دول اعلام گردد. دول عضو همچنین بایستی علیه مداخلات مخربی که ارائه خدمات رادیویی، یا سایر خدمات ایمنی را به مخاطره افکنده یا شدیداً در ارائه خدمت ارتباطات از راه دور ایجاد

اخلال، یا آن را مسدود نماید، قانون وضع نموده و تمام اقدامات لازم را جهت حصول اطمینان نسبت به محرمانه بودن مکاتبات بین‌المللی به عمل آورند؛ مگر آنکه این محرمانه بودن مغایر با قوانین داخلی یا کنوانسیون‌های بین‌المللی باشد. علی‌رغم محدودیت‌های فوق، قانون ارتباطات از راه دور بین‌المللی به‌صورتی خاص استفاده از ارتباطات از راه دور را در جهت اهداف نظامی همانند حملات سایبری منع نکرده است. اتحادیه ارتباطات از راه دور علیه مداخله مخرب دقت به خرج داده است، اما تخلفات و تجاوزات نظامی از این مقررات را بدون نیاز به یک مکانیسم گزارش‌دهی یا اعمال محدودیت‌های دیگر در استفاده از آن مجاز می‌دارد. این استثناء می‌تواند حملات سایبری را در برگرفته و حتی ممکن است نبرد سایبری را نیز شامل شود. علاوه بر این استثنای نظامی، مقررات اتحادیه ارتباطات از راه دور بین‌المللی، از چارچوب حقوقی ضعیفی برای تنظیم حملات سایبری برخوردار است.

۵-۳. قانون هوانوردی

حملات سایبری که هوانوردی غیرنظامی را هدف گرفته یا در آن مداخله نماید، می‌تواند در تعارض با سه معاهده اصلی هوانوردی قرار گیرد: ۱. کنوانسیون سال ۱۹۴۴ شیکاگو در خصوص هوانوردی غیرنظامی بین‌المللی.۲. کنوانسیون مونترال برای سرکوب اقدامات غیرقانونی علیه هوانوردی غیرنظامی.۳. پروتکل سال ۱۹۸۸ برای سرکوب اقدامات خشونت‌آمیز غیرقانونی علیه فرودگاه‌هایی که در خدمت هوانوردی غیرنظامی بین‌المللی است. مثلاً اختلال درکنترل ترافیک هوایی، تغییر فهرست مسافران پرواز، یا افزودن نام یک کشور به فهرست کشورهای پرواز ممنوع، می‌تواند براساس قانون هوانوردی نمونه‌هایی از حملات سایبری تلقی شوند.

الف) کنوانسیون شیکاگو

کنوانسیون شیکاگو یک نهاد تخصصی زیر نظر سازمان ملل متحد جهت هماهنگی و تنظیم مسافرت هوایی بین‌المللی تشکیل داد. این کنوانسیون همچنین مجموعه مقررات مربوط به فضا، هواپیمایی، هوانوردی، ثبت و ایمنی ایجاد کرده و تصریح دارد تمام دولت‌ها بایستی ایمنی ناوبری هواپیماهای غیرنظامی را در نظر داشته باشند. در صورتی که دولتی با حملات سایبری خود پروازهای غیرنظامی را هدف قراردهد، اقدامی مغایر با حفاظت مد نظر کنوانسیون، در مداخله در امور مربوط به پروازهای غیرنظامی انجام داده است. این حملات همچنین می‌تواند در تعارض با اصلاحیه سال ۱۹۸۴ علیه استفاده از سلاح برای هدف‌گیری هواپیماهای

غیرنظامی در حال پرواز نیز باشد. با این حال، کنوانسیون، دول عضو را مجاز می‌دارد در خلال جنگ یا اعلام حالت فوق‌العاده، درصورت اطلاع به شورا، تعهدات خود را کاهش دهند.

ب) کنوانسیون مونترال

این کنوانسیون به صورتی کلی اقدامات خاص غیرقانونی را که می‌تواند امنیت هوانوردی غیرنظامی را با مخاطره مواجه نماید، مطرح می‌کند. اصل یک آن اعلام می‌دارد یک فرد هنگامی مجرم شناخته می‌شود که عامدانه و غیرقانونی مجموعه‌ای از اقدامات منجر به عدم امکان پرواز انجام داده، یا تلاش به انجام آن داشته، یا به‌صورتی جدی امنیت یک هواپیما را در خلال پرواز مثلاً از طریق تخریب، یا ایراد آسیب به تأسیسات ناوبری هوایی یا اخلال درکارکرد آن....یا با ارائه اطلاعات غیرواقعی، به‌مخاطره افکند. به نظر نمی‌رسد این موافقتنامه قادر به اعمال محدودیت بر حملات سایبری باشد، مگر آنکه این حملات مثلاً به‌واسطه مداخله درسیستم عامل هواپیما، منجر به عدم امکان پرواز شده، یا امنیت یک هواپیما را درخلال پرواز (مثلاً مداخله در کنترل ارتباطات ترافیک هوایی یا سایر جنبه های ناوبری هوایی) باخطر مواجه کند.

پ) پروتکل مونترال

پروتکل مونترال این چارچوب قانونی را، از هواپیمای در حال پرواز، به انجام اقدامات خشن مخاطره‌آمیز برای امنیت افراد در فرودگاه، یا احتمال آن .... یا اقداماتی که عملیات امن چنین فرودگاهی را در معرض خطر قراردهد، گسترش داده است. اصل دوم پروتکل اعلام می‌دارد فردی که عامدانه و غیرقانونی با استفاده از هر یک از طرق زیر، یا تلاش به آن، امنیت در فرودگاه مذکور را با مخاطره مواجه نموده یا احتمال آن را ایجاد نماید، مجرم تلقی می‌شود:

الف) در فرودگاه در حال سرویس به هوانوردی غیرنظامی بین‌المللی، عملی خشونت‌بار علیه یک فرد انجام داده و منجر به مرگ یا ایراد جراحت شدید او شود یا احتمال آن رود.

ب) تأسیسات و تسهیلات یک فرودگاه بین‌المللی را که در خدمت هوانوردی غیرنظامی بین‌المللی است، یا هواپیمای (خارجی از سرویس) مستقر در آن را تخریب، یا آسیبی جدی به آن وارد و در نتیجه در خدمت رسانی فرودگاه ایجاد اخلال نماید.

این پروتکل حملات سایبری تضعیف‌کننده امنیت فرودگاه‌های بین‌المللی را ممنوع ساخته است.

۵-۶. حقوق فضا

با توجه به اینکه عملیات رایانه‌ای ماهواره‌ها، بخشی همگرا با ارتباطات از راه دور بین‌المللی در عملیات نظامی است، حملات سایبری می‌تواند با اعمال محدودیت حقوق فضا نیز مواجه شوند. این امکان وجود دارد که معاهدات فضای خارج جوّ، ماه، و ایراد آسیب به اشیاء سماوی و همچنین مقررات ماهواره، برای قاعده‌مندسازی حملات سایبری مورد استفاده قرار گیرند. معاهدات مربوط به ایراد آسیب به اشیاء سماوی، یا ماه، بر اساس تعریف ما آشکارا بر حملات سایبری، قابل اعمال بوده، برای جلوگیری از اطاله کلام به آن پرداخته نمی‌شود. البته این معاهدات نیز برای تنظیم حملات سایبری، شامل تعهدات اندکی هستند. معاهده فضای خارج جوّ سال ۱۹۶۷، آزادی بهره‌برداری از فضا را اعلام و استفاده از آن را با اهداف مخرب خاص، ممنوع دانسته است. این معاهده عنوان می‌دارد:"دول عضو این معاهده متعهد می‌شوند که هیچ شیء حامل تسلیحات هسته‌ای، یا سایر انواع تسلیحات کشتار جمعی را در مدار زمین قرار نداده، چنین تسلیحاتی را بر اجرام آسمانی نصب نکرده، یا آنها را به هر شکلی در فضای خارج جوّ مستقر نسازند." معاهده فضای خارج جوّ به صراحت استفاده نظامی از فضا، همانند استقرار ماهواره شناسایی نظامی در مدار زمین، ماهواره‌های سنجش از راه دور، سیستم‌های نظامی مکان‌یاب جهانی و استقرار فضایی یک سیستم موشکی ضد بالستیک را مجاز می‌دارد.

از آنجا که حملات سایبری بعید است که منجر به وقوع کشتار جمعی از نوع مورد نظر این معاهده شود، بعید است بتوان حملات سایبری را دارای مشخصه‌های ممنوع‌شده توسط معاهده فضای خارج جوّ دانست. مقررات مربوط به ماهواره‌ها، مسیر بالقوه دیگری برای قاعده‌مندسازی حملات سایبری ارائه می‌دهد. موافقتنامه سال ۱۹۷۱ سازمان ارتباطات از راه دور ماهواره‌ای بین‌المللی و کنوانسیون سال ۱۹۷۹ سازمان ماهواره‌های دریایی بین‌المللی، حاوی مقررات وجوه صلح‌آمیز قابل اعمال بر ماهواره‌ها، شبیه به معاهده فضای خارج جوّ می‌باشد. به هرصورت علی‌رغم این واقعیت که ماهواره‌ها در حملات سایبری ایفای نقش می‌کنند، این معاهدات کاربردهای ضعیفی در قانون‌مندسازی حملات سایبری دارند. سازمان ارتباطات از راه دور ماهواره‌ای، که در ابتدا به عنوان یک تشکل بین‌الدولی دارای اختیار پیشبرد .... طراحی، توسعه، احداث، استقرار، عملیات و تعمیر و نگهداری بخش فضایی سیستم ماهواره‌ای ارتباطات از راه دو تجارت جهانی بود، در سال ۲۰۰۰، به بخش خصوصی واگذار شد. به همین ترتیب، سازمان ماهواره‌های دریایی بین‌المللی به میزان زیادی موقوف به منافع بین‌الدولی شده، در نتیجه هیچ سازمانی در جایگاهی قرارندارد تا مقررات عمومی مربوط به حملات سایبری را اعلام دارد.

۵-۵. حقوق دریاها

کنوانسیون سال ۱۹۸۲ ملل متحد در خصوص حقوق دریاها، به خصوص اصول ۱۹، ۱۰۹ و ۱۱۳، به‌صورت ضمنی قابل استفاده در حملات سایبری در دریا می‌باشد. اصل ۱۹ عبور بی‌ضرر یک شناور دریایی را از طریق دریای سرزمینی ملتی دیگر، مادامی که صلح، انتظام و امنیت دولت ساحلی را به مخاطره نیندازد، مجاز می‌دارد. این التزام عموماً تحت عنوان حقوق بین‌الملل عرفی، مورد پذیرش قرار گرفته است. اعمالی که به‌واسطه اصل ۱۹ منع شده، عبارت‌اند از:

الف) هر تهدید، یا کاربرد زور علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولت ساحلی، یا به طریقی دیگر که ناقض اصول حقوق بین‌الملل مندرج در منشور ملل متحد باشد.

ب) اقدام به جمع‌آوری اطلاعات به منظور ایراد صدمه به دفاع یا امنیت دولت ساحلی؛

پ) تبلیغات با هدف تأثیرگذاری بر دفاع یا امنیت دولت ساحلی؛

ت) مداخله در سیستم ارتباطی یا هر تأسیسات یا تسهیلات متعلق به دولت ساحلی.

از این مقررات به خصوص بند"د" می‌توان ممنوعیت حملات سایبری با استفاده از سیستم‌های رایانه‌ای مستقر در شناورهای دریایی را استنتاج نمود. کنوانسیون حقوق دریاهای ملل متحد پخش غیرمجاز برنامه رادیو تلویزیونی را عبارت می‌داند از انتقال امواج رادیو یا تلویزیونی مغایر با مقررات بین‌المللی از یک کشتی یا تأسیسات مستقر در دریای آزاد که عموم مردم را مخاطب قرار دهد، به استثنای پیام‌های ناشی از اضطرار. با توجه به توافق بر سر شبکه رایانه‌ای عمل‌کننده در سیستم ارسال پیام کشتی، این ممنوعیت می‌تواند به حمله سایبری نیز تسری یابد. به‌واسطه منع تخریب کارکرد سیستم‌های ارتباطاتی در دریا، این مقررات حفاظت‌های اندکی در مقابل وقوع حملات سایبری در دریای آزاد، یا حملاتی که منشأ آنها دریای آزاد است، اعلام می‌دارد.

در مجموع حقوق بین‌الملل حاکم بر ارتباطات از راه دور، هوانوردی، فضا و دریا، در چارچوب بسترهایی خاص، ابزاری بالقوه موثر برای بررسی حملات سایبری تأمین می‌نماید. همچنان این مقررات متداخل و درهم و برهم، قاصر از تأمین مکانیزمی جامع برای مواجهه با تمام اشکال حملات سایبری هستند.

فرجام

ظهور ویروس استاکس‌نت در سال ۲۰۱۰ در تأسیسات هسته‌ای جمهوری اسلامی ایران نشان از آسیب‌پذیری دولت‌ها مقابل حملات سایبری داشت. زیرساخت رایانه‌ای کشورهای جهان طی سالیان اخیر آسیب‌پذیری بیشتری یافته‌اند، اما واکنش به این تهدیدات با سرعتی همپایه آنها پیش نرفته است. در شرایط فعلی دولت‌ها برای مواجهه با این تهدیدات فزاینده، بایستی بر مجموعه‌های محدود، اما تکه‌تکه حقوقی که برای مواجهه با چالش تهدیدات سایبری طراحی نشده‌اند، متکی شوند.

حملات سایبری حاکی از وقوع تهدیداتی نوین و فزاینده‌اند که حقوق موجود بین‌الملل و قوانین داخلی کشورها برای مواجهه با آن تاکنون چارچوب‌های ویژه‌ای تبیین نکرده‌اند. از حقوق مخاصمات مسلحانه تنها می‌توان در پاسخ به حملات سایبری که به سطح حمله مسلحانه ارتقاء یافته، یا در بستر یک مخاصمه مسلحانه جاری به‌وقوع پیوسته باشند، بهره‌برداری نمود. اکثر حملات سایبری به سطح مخاصمه مسلحانه ارتقاء نمی‌یابند. اما ظاهراً مشروط به آنکه حمله سایبری اولیه یکی از تعهدات بین‌المللی دولت مسئول را نقض نماید، به موجب حقوق بین‌الملل عرفی دولت قربانی حق دارد به منظور اجبار دولت مسئول، به انطباق با هنجارهای بین‌المللی و خودداری از انجام حملات سایبری از درون قلمروی ارضی خویش، یا عدم اجازه به انجام به چنین عملیاتی، اقدامات متقابل و ضروری (غیرمسلحانه) را طراحی نماید.

در حالی که دفاع عامل، عمومی‌ترین نوع اقدامات متقابل است که می‌توان در پاسخ به حمله سایبری از آن استفاده نمود، این دفاع تنها یکی از انواع دفاع است. محدودیت اساسی بر یک اقدام متقابل مجاز، آن است که اقدام مذکور بایستی متناسب با آسیب‌های وارده به دولت قربانی باشد. به علاوه اقدامات متقابل بایستی به منظور بازگشت به شرایطی باشد که هم دولت مرتکب عمل و هم دولت قربانی به وظایف قانونی خویش در ارتباط با طرف مقابل بازگردنده شوند. این اقدامات متقابل بایستی موقتی بوده و به محض اینکه انجام حملات سایبری متوقف شد، اقدامات متقابل نیز متوقف شوند.

فضای مجازی یک شبکه از مجموعه شبکه‌هایی است که هزاران هزار تأمین‌کنندگان خدمات اینترنتی در سراسر جهان را شامل می‌شود. هیچ دولت یا سازمان خاصی قادر به آن نیست به تنهایی از شبکه‌های داخلی خود، دفاع سایبری موثر نماید. با وجود آنکه توسعه هنجارهای بین‌المللی مفیدند، این هنجارها تاکنون تعریفی از حمله سایبری توسط بازیگران دولتی و غیردولتی ارائه نداده‌اند. دامنه مشکل، جهانی است، راه‌حل آن نیز بایستی جهانی باشد.

به نظر می‌رسد انعقاد یک سند بین‌المللی سایبری، با دو هدف عمده یک انجام هماهنگی بین‌المللی و دیگری مواجهه صحیح با چالش حملات سایبری، ضروری است. سند مذکور بایستی حاوی دو ویژگی اساسی باشد: ۱. تعریفی روشن از حمله سایبری و جنگ سایبری ارائه دهد.

۲. چارچوبی مشخص برای تحکیم همکاری‌های بین‌المللی جهت تبادل اطلاعات، جمع‌آوری مدارک و پیگرد افرادی دخیل در حملات فرامرزی سایبری، مقرر دارد. چنین چارچوبی باید چالش‌های مربوط به جرم‌انگاری این جرائم را تعیین نموده و حق افرادی که از اینترنت و فناوری‌های مربوط به آن، صرفاً برای اعلام مخالفت سیاسی قانونی استفاده می‌کنند، محفوظ دارد.

پانوشت‌ها

۱. بر این اساس علی‌رغم آنکه ممکن است جرایم سایبری توسط عناصر دولتی و در خارج از حوزه صلاحیت آنها به‌وقوع پیوندد، عملیات دولت‌ها حتی درصورت غیرقانونی بودن، جرم سایبری تلقی نمی‌شود.

۲. براساس بند ۲ ماده ۵۲ پروتکل اول الحاقی، اهداف نظامی که هدف گرفته می‌شوند بایستی دارای دو ملاک باشند: اول اینکه در خدمت اهداف نظامی باشند و دوم اینکه هدف‌گیری آنها حاوی یک امتیاز قطعی نظامی باشد.

۳. کنوانسیون امکان پیوستن برخی دول از جمله ایالات متحده به آن را در نظر گرفته است.

منابع فارسی

خبر سایت دویچه وله فارسی، تحت عنوان " ناتو: حمله سایبری جدی به یکی از اعضاء پاسخی نظامی دارد"، مورخ ۶ سپتامبر ۲۰۱۴

منابع لاتین

Cartwright, James E. (Nov. 2011), ***Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands***, The cice chairman of the joint chefs of staff, Washington D.C. Directories of the Joint Staff Directories on Joint Terminology for Cyberspace Operations.

Clarke A. Richard & Knake, Robert K. (2010), ***Cuber War: The Next Threat to National Security and What to Do about It***, Harper Collins Publishers.

Gjelten, Tom (Sept 22, 2010), ***Extending the Law of War to Cyberspace***, Nat Pub Radio http://www.npr.org/templates/story/story.php?storyId=130023318

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1) (8 June 1977).

Schmitt, Michael (1999), "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", ***Columbia Journal of Transnational Law***, Vol.37.

Silver, Daniel, ***Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter***, in Computer Network Attack and International Law 73, 2002 ,Michael, Schmitt & Brian O Donnell, Available at: http://archive.org/stream/computernetworka76nava /computernetworka76nava_djvu.txt

U.N General Assembly, A/RES/57/53, 30 December 2002

U.N. Doc. A/56/10 (2001)

U.N. Doc. ST/LEG/SER B/25 (2012), ***Chapter III Countermeasures***, p.304, Avalable at: http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf

U.N. Secretary-General, ***Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security***, 4, U.N. Doc. A/65/201 (July 30, 2010).