توسل حق دفاع مشروع در حملات سایبری در حقوق بین‌الملل

علی حیدری، بیژن حیدری

ali.heydari.4001@gmail.com

چکیده

یکی از شیوه‌های نوین تخاصم درصحنه بین‌المللی، حملاتی است که در بستر فضای سایبری صورت می‌گیرد، هرچند این حملات پتانسیل ایجاد تلفات گسترده و خسارات وسیع را دارند اما سرعت بالای تغییرات در این حوزه موجب گردیده است که حقوق بین‌الملل از وضع قواعد جدید متناسب با فضای سایبری عاجز بماند. استفاده از فضای سایبری برای دستیابی سریع و مؤثر به اهداف راهبردی، امروزه به ابزار جدید جنگی و مهم برای همه بازیگران دولتی و غیردولتی تبدیل شده است. شناساییِ قلمرو حقوقیِ آن نیز با موانعی در شرایط مختلف و از جمله حقوق جنگ و حق دفاع مشروع رو به روست که ورود حقوق بین‌الملل به بحث را با چالش مواجه کرده است. در این پژوهش با رویکرد توصیفی و استفاده مطالعات پیشین سعی شده است تا به بررسی ابعد موضوع مطرح شده پرداخته شود.

کلمات کلیدی: جنگ سایبری، حقوق بین‌الملل، حملات سایبری، دفاع مشروع.

۱ مقدمه

در این نوشتار، حملات سایبری بازیگران غیردولتی صرفاً به منظور احراز انتساب آ نها به یک دولت بررسی می‌شود. پژوهش حاضر نتیجه می گیرد که حمله ی سایبری را می توان وفق ماده‌ی ۴(۲) منشور ملل متحد، توسل به زور مسلحانه توصیف نمود. از سوی دیگر، حمله ی 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 اعطاء می‌نماید.

هم چنین، درواکنش به حمله ی سایبری که در حد حمله‌ی مسلحانه نباشد، اما حمله‌ی مسلحانه‌ی قریب الوقوعی را با تسلیحات متعارف تدارک ببیند، می‌توان به دفاع مشروع متوسل گردید.

گسترش فزاینده‌ی فن‌آوری اطلاعات و ارتباطات به تحول و دگرگونی جوامع در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی منجر شده است. جوامع، به نحو فزاینده‌ای به رایانه و شبکه‌های رایانه‌ای و خدمات حیاتی متکی به اینترنت وابسته شده‌اند. اهمیت جهانی فضای مجازی، آسیب‌پذیری‌هایی را نیز برای آن در پی داشته است؛ این بدین دلیل است که فن‌آوری و تخصص در زمینه‌ی سایبر، ساده و ارزان به دست

می‌آید؛ این امر به کشورهای ضعیف‌تر و حتی کنشگران غیردولتی امکان می‌دهد که به کشورهای دارای قدرت نظامی متعارف برتر، آسیب‌های قابل توجهی مانند از کار انداختن ژنراتورهای برق، قطع سیستم کنترل و ارتباطات فرماندهی، سرنگون کردن هواپیماها، ذوب راکتورهای هسته‌ای، انفجار خطوط لوله و تخریب تسلیحات را وارد نمایند (حسن بیگی، ۱۳۸۴).

در نتیجه‌ی بروز چنین تهدیداتی است که امنیت در فضای سایبر به دغدغه‌ی عمومی جامعه‌ی بین‌المللی بدل شده است. در این چارچوب، مجمع عمومی سازمان ملل متحد، مجموعه ای از قطعنامه‌ها را در خصوص پیشرفت‌های حاصل شده در خصوص اطلاعات و ارتباطات از راه دور و تأثیر آن بر امنیت بین‌المللی تصویب نموده و تأکید کرده است: «سوء استفاده‌ی جنایتکارانه از فن‌آوری های اطلاعاتی می‌تواند تأثیر شدیدی بر تمامی کشورها داشته باشد» (A/RES/56/121 of 19 December 2001). یکی از جنبه هایی که حقوقدانان بین‌المللی می‌توانند موضوع امنیت سایبری را از آن منظر بررسی نمایند، توسل حق دفاع مشروع در حملات سایبری است؛ حملات سایبری ارتکابی توسط کنشگران غیردولتی، صرفاً به منظور تبیین قابلیت یا عدم قابلیت انتساب به‌یک دولت بررسی می شود. بنابراین، پژوهش حاضر منصرف از جرایم سایبری ارتکابی توسط اشخاص حقیقی یا حقوقی خصوصی است که به لحاظ منافع شخصی بودن مانند سرقت پول از حساب‌های بانکی و علیه محرمانه داده‌ها و سیستم‌های رایانه‌ای صورت می‌گیرند. در ضمن «تروریسم سایبری» که عبارت است از تخریب یا اخلال گسترده‌ی داده‌ها، اطلاعات یا سامانه‌های رایانه‌ای یا ارتباطی از طریق فضای سایبر با انگیزه‌های سیاسی، مذهبی، ایدئولوژیکی و نژادی (پاکزاد، ۱۳۸۸) با این تحقیق ارتباط نمی‌یابد.

۲ مفهوم دفاع مشروع

«دفاع مشروع» امروزه استثنائی مهم بر اصل منع توسل به زور محسوب می‌شود. حق دفاع مشروع در «حملات مسلحانه» به‌عنوان یک اصل حقوق بین‌الملل عرفی است که در منشور به‌عنوان یک «حق ذاتی» به آن اشاره شده است. مفهوم عینی دفاع مشروع و اهمیت آن در چارچوب تحولات حقوق بین‌الملل در طول قرن گذشته به نحو قابل ملاحظه‌ای تغییر کرده است. در واقع با گسترش سازماندهی حقوق بین‌الملل در طی دهه‌های گذشته و بویژه فرایندی که با تأسیس جامعه ملل آغاز شده است مفهوم دفاع مشروع اهمیت قابل ملاحظه‌ای یافته است.

۳ مفهوم سایبری

واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضیدانی به نام نوربرت وینر Norbert Wiener در کتابی با عنوان «سایبرنتیک، کنترل و ارتباط در حیوان و ماشین» در سال ۱۹۴۸ به‌کار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی (و کامپیوترها) است.

سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای

کامپیوتر و اطلاعات است. در طی توسعه اینترنت واژه های ترکیبی بسیاری از این کلمه سایبر به‌وجود آمده است. از محیط سایبر (Cyberspace) نیز تعاریف گوناگونی به‌عمل آمده است که می‌توان در مجموع محیط سایبر را چنین تعریف کرد. محیط مجازی و غیرملموس موجود در فضای شبکه‌های بین‌المللی که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها ، ملت‌ها، کشورها و به‌طور کلی هرآنچه در کره خاکی به‌صورت ملموس و فیزیکی وجود دارد در یک فضای مجازی به‌شکل دیجیتالی وجود دارد و قابل استفاده و دسترس استفاده‌کنندگان و کاربران است و از طریق رایانه، اجزای آن و شبکه‌های بین‌المللی به‌هم مرتبط هستند.

۴ قانون‌گذاری در فضای سایبر

شیوه قانون‌گذاری در فضای سایبر، مبتنی بر دو نوع نگرش متفاوت به حاکمیت در فضای سایبر است. نگرش نخست، مبتنی بر انحصار دولت‌ها در عرصه قانون‌گذاری فضای سایبر است و نگرش دوم که ملهم از دکترین میراث مشترک بشریت است، مخالف ورود انحصاری دولت‌ها به این عرصه است. هر یک از این دو رویکرد، موجد روش‌های قانون‌گذاری مختلفی در فضای سایبر است. روش‌های قانون‌گذاری ملی، بین‌المللی و خودانتظامی در زمره روش‌های قانون‌گذاری در فضای سایبر به شمار می‌آیند.

اگرچه توسل به هر یک از روش‌های قانونگذاری با اشکالاتی در عرصه اجرا روبه‌روست، در این میان می‌توان رویکردی بینابین و مختلط را برگزید تا ضمن رفع نواقص دیگر روش‌ها، زمینه را برای نیل به تفاهم میان کشورها و گروه‌های فعال در زمینه فضای سایبر هموار سازد. نگرش دولت جمهوری اسلامی ایران، اساساً مبتنی بر شیوه قانون‌گذاری ملی است. با این حال، عملکرد ایران در سطح بین‌المللی و به‌ویژه در اتحادیه بین‌المللی مخابرات، حاکی از پذیرش روش مختلط در قانون‌گذاری در فضای سایبر است.

۱.۴ صلاحیت کیفری مراجع قضایی در فضای سایبر

مسألهٔ چگونگی تعیین مرجع قضایی صالح جهت رسیدگی به جرائم ارتکابی در فضای مذکور است. چون بر اساس قواعد سنتی مهم‌ترین ضابطهٔ تعیین صلاحیت مراجع قضایی کیفری، مکان وقوع جرم می‌باشد و در فضای جدید سایبر، که یک فضایی مجازی و فارغ از مکان می‌باشد، چنین ضابطه‌ای قابل اجرا نبوده و یا مستلزم تعدیل ویژه می‌باشد. در همین راستا برخی سعی کرده‌اند همان قواعد سنتی ناظر بر صلاحیت کیفری مراجع قضایی را با نگرشی جدید در این فضا اجرا کنند و برخی دیگر با طرح تئوری‌های نو در خصوص صلاحیت، از قبیل «فضای سایبر به‌عنوان یک فضای آزاد بین‌المللی» و یا پیش‌بینی دادگاهی ویژه به نام «دادگاه دیجیتالی یا سایبری» و یا صلاحیت «دادگاه ذی‌ارتباط منطقی با جرم» را مطرح کرده‌اند. کشور ایران در قانون مجازات جرائم رایانه‌ای در ماده ۲۸ تئوری اول یعنی اجرای قواعد سنتی با نگرشی جدید را اتخاذ کرده است. در این مقاله سعی شده است هر یک از تئوری‌های مطرح شده در این زمینه مورد نقد و بررسی قرار گیرد و در نهایت یک معیار تلفیقی ارائه گردد، با این توضیح که تا جایی که قواعد سنتی قابل اجرا باشند همان قواعد اجرا می‌شوند و در غیر آن صورت تئوری صلاحیت دادگاه ذی‌ارتباط منطقی با جرم

به‌عنوان ضابطه نهایی پذیرفته شود.

۲.۴ اعمال صلاحیت کیفری در مورد جرائم ارتکابی در فضای سایبر

تشخیص صلاحیت محاکم کیفری در فضای واقعی عمدتاً مبتنی بر مکان و مرز می‌باشد اما فضای سایبر فاقد مکان و حصری است. حال سؤال اینجاست که آیا این فضا دارای رژیم خاص حقوقی است؟ آیا قواعد سنتی حاکم بر انواع صلاحیت‌ها با توجه به ویژگی‌های فضای سایبر قابل اعمال است؟ می‌توان گفت تأکید کشورها بر حاکمیت واصل سرزمینی سبب عدم ایجاد رژیم خاص حقوقی برای صلاحیت کیفری در فضای سایبر شده است. همچنین در بین انواع صلاحیت اصل سرزمینی بیشترین چالش را با این فضا دارد. صلاحیت‌های حمایتی وتابعیتی نیز چالش‌هایی با این امر دارند هرچند که صلاحیت جهانی به‌دلیل عدم اتکاء به مکان و مرز کاربردی‌تر بنظر می‌رسد.

۵ بهره‌گیری از حقوق معاهدات و عرف‌های بین‌المللی

در حا حاضر تعداد اندکی معاهده‌ی بین‌المللی وجود دارند که می‌توانند تشکیل دهنده‌ی یک عرف بین‌المللی باشند که نهایتاً در تنظیم جنگ سایبری تا حدودی به کار رود. برای مثال، معاهده‌ی «کنوانسیون بین‌المللی مخابرات» و ماده‌ی ۳۵ آن، هر گونه مداخله‌ی زیان‌بار با استفاده از ارتباطات از راه دور را ممنوع می‌کند.

ماده‌ی ۳۷ همان نیز به گونه‌ای ممکن است بر جنگ‌های سایبری اثرگذار باشد. همچنین ماده‌ی ۱۹ بند ۲ و ماده‌ی ۲۰ این کنوانسیون نیز مستعد بهره‌گیری در این خصوص است (Schaap, 2009: 21).

یک سند حقوقی بین‌المللیِ دیگر که قابلیت ارتباط گرفتن با موضوع را دارد، موافقت‌نامه‌ی اجتناب از فعالیت‌های خطرناک نظامی است که در سال ۱۹۴۹ بین ایالات متحده آمریکا و شوروی به امضا رسیده بود. این موافقت‌نامه هر گونه مداخله‌ی زیان‌بار در «سیستم‌های فرماندهی و کنترلی دشمن» را ممنوع کرده بود. در اواخر قرن بیستم نیز با افزایش توجه رسانه‌ها و محافل دانشگاهی به مفهوم نوظهور جنگ سایبری، در جامعه‌ی بین‌المللی تلاش‌هایی برای مذاکراتی برای انعقاد معاهده‌هایی در این زمینه صورت گرفت. به‌طور نمونه، روسیه در اکتبر ۱۹۹۴ متولی تصویب قطعنامه‌ای در کمیته‌ی اول شورای امنیت سازمان ملل شد که به‌عنوان تلاشی آشکار برای جلب نظر ملل متحد به این موضوع شناخته می‌شود. این قطعنامه شامل فراخوانی برای دولت‌ها بود که از نظرهای آنها در مورد ایجاد نظام‌های حقوقی بین‌المللی به‌منظور تهدید، گسترش، ساخت و استفاده از سلاح‌های اطلاعاتی خاص حمایت کند. این تلاش با استقبال اندکی در جامعه‌ی بین‌المللی مواجه شد و هرگز برای رأی‌گیری عمومی وارد مجمع عمومی ملل متحد نشد (Hoisington, 2009).

اینک شاید با گذشت دو دهه از طرح اولیه‌ی آن و گسترش تهدیدات و حملاتی که برخی از آنها اشاره شد، جلب نظر جامعه‌ی بین‌المللی به دشواری گذشته نباشد، اما احتمالاً پس از آنکه حمله‌ی سایبری به حد مخاصمه‌ی مسلحانه رسید، یک نظام امنیتی بین‌المللی که شامل حقوق بشردوستانه بین‌المللی و حقوق بشر می‌شود، به جریان می‌افتد.

توسل به مفهوم دفاع مشروع نیز در خصوص این حملات مورد تردید واقع شده و امکان اعمال این حق

در این فضا به استناد ماده ۵۱ منشور ملل متحد و یا حقوق بین‌الملل عرفی از مهم‌ترین پرسش‌هایی است که بی‌پاسخ مانده است. به نظر می‌رسد در صورتی که حملات سایبری به زیرساخت‌های حیاتی یک کشور نفوذ کرده و پتانسیل ایجاد تخریب و اضمحلال در حد یک حمله مسلحانه را داشته باشند، مسلحانه فرض شده و دولت قربانی از حق دفاع مشروع برخوردار خواهد بود. برای مثال در خصوص حمله کرم رایانه‌ای استاکس‌نت در سال ۲۰۱۰ به تأسیسات هسته ای ایران، صرف نظر از مسئله انتساب آن به‌عنوان یک امر موضوعی، حق دفاع مشروع قابل اثبات است (غلامعلی قاسمی، سعید نامدار،۱۳۹۷).

۶ توسل به دفاع مشروع در موارد نقض اصل منع تهدید یا استفاده از زور

مبانی حقوقی دفاع مشروع به عنوان یک قاعده در حقوق بین‌الملل که خود استثنایی بر قاعده اصل منع تهدید و یا استفاده از زور می‌باشد، در ماده ۵۱ منشور ملل متحد آمده است. دفاع مشروع در طرح مسئولیت بین‌المللی دولت‌ها ۲۰۰۱ به‌عنوان یکی از معاذیر رافع وصف متخلفانه بین‌المللی ذکر شده است و از شرایط اساسی آن احراز تجاوز مسلحانه و رعایت شرط تناسب و ضرورت در اعمال حق دفاع مشروع است. از موارد دیگر در رعایت آن محدود و تحت کنترل بودن آن می‌باشد که باید به شورای امنیت در این باره گزارش داد و به‌محض ورود شورای امنیت به قایه دفاع مشروع منتفی می‌شود (احمدرضا توحیدی، ۱۳۹۷).

در استناد به دفاع مشروع در مقابل حمالت سایبری سه رویکرد وجود دارد:

الف. رویکرد ابزارمحور: در این رویکرد استفاده از تسلیحات نظامی متعارف برای استناد به دفاع مشروع اهمیت دارد. در این رویکرد در صورتی یک حمله سایبری واجد شرایط استناد به ماده ۵۱ منشور است که از تسلیحات نظامی استفاده شود، مثال: بمباران سرورهای رایانه‌ای یا کابل‌های اینترنتی.

ب. رویکرد هدف‌محور: براساس این رویکرد در صورت وقوع یک حمله سایبری واحد به یک سامانه حیاتی کشور، می‌توان پاسخ نظامی متعارف به این حمله داد.

ج. رویکرد تأثیرمحور: رویکرد تأثیرمحور به‌واسطه شدت تأثیرات یک حمله سایبری، آن را یک حمله مسلحانه تلقی می‌کند. رویکرد تأثیرمحور به‌دلیل مواضع میانه خود از مقبولیت بیشتری برخوردار است.

حتی برخی از کشورها از جمله روسیه و آمریکا برای خود حق دفاع مشروع در مواجهه با حملات سایبری قائل شده‌اند. مقامات روس اعلام کرده‌اند که حتی حق توسل به سلاح اتمی در مواجهه با حملات سایبری را دارند (K. Joanna, 2009).

این قبیل موضع‌گیری از جانب کشورهای قدرتمند و عضو دائم شورای امنیت و موضع‌گیری‌های مشابه از سوی کشورهای دیگر به نوعی بیانگر آینده خطرناک حملات سایبری و لزوم شناسائی آن توسط جامعه بین‌المللی را برای جهانیان گوشزد می‌کند.

۷ ضرورت انجام دفاع مشروع

پذیرش عمومی اصل ضرورت به سال ۱۸۴۳ برمی‌گردد. قواعد حقوقی حاکم بر جنگ (Jus ad bellum) نظیر ممنوعیت توسل به زور بند (۴) ماده (۲) منشور را می‌توان در مورد جنگ‌های سایبری نیز قابل تسری دانست و حملات سایبری را به‌مثابه نقض اصل منع توسل به زور توصیف کرد. در مورد قواعد در جنگ (Jus in Bello) نیز تقریباً اکثر قواعد حقوق بین‌الملل بشردوستانه نظیر لزوم رعایت «اصل تفکیک میان نظامیان و غیرنظامیان» قابل اجرا است. برای مثال در موردی که حملات سایبری با ایجاد اختلال رایانه‌ای در بیمارستان‌ها یا مراکز درمانی، حیات غیرنظامیان را در معرض تهدید قرار می‌دهد و یا در جایی که حملات سایبری عملکرد تاسیساتی را مختل می‌سازد که مستقیم یا غیرمستقیم جان و مال غیرنظامیان را در معرض آسیب قرار می‌دهد، اصل مذکور را که در مواد (۵۴) پروتکل اول ۱۹۷۷ الحاقی به کنوانسیون‌های ژنو ۱۹۴۹ و نیز ماده (۱۴) پروتکل دوم الحاقی نیز منعکس شده است، می‌توان قابل اعمال دانست.

همچون حملات مسلحانه فیزیکی آنچنان که دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه (نیکارگوئه علیه آمریکا)، ۱۹۸۶ میلادی بر معیار آستانه و شدت درگیری ها برای تلقی آن به‌عنوان حمله مسلحانه تأکید کرد، در حملات سایبری نیز باید معیار شدت و گستردگی این حملات برای تلقی آن به عنوان حمله مسلحانه و نقض اصل قاعده منع توسل به زور مطمح نظر قرار گیرد.

۱.۷ بیانیه ستاد کل نیروهای مسلح

بیانیه ستاد کل نیروهای مسلح شامل چهار ماده، دستاورد مهم و اقدام مؤثری در تبیین سیاست‌های کشور نسبت به تهدیدات و حملات فضای سایبری محسوب می‌شود. در ماده (۱) تحت عنوان کلیات، راجع به حقوق بین‌الملل قابل اعمال بر فضای سایبری بر لزوم توزیع عادلانه منافع و امتیازات یک فضای صلح‌آمیز سایبری که متضمن «دسترسی» و «حاکمیت منصفانه» برای تمام دولت‌ها باشد، تأکید شده است.

«اصل مسئولیت مشترک اما متفاوت دولت‌ها» (Common But Differentiated Responsibilities) از دیگر اصول مهم حقوق بین‌الملل است که در بیانیه مزبور بدان استناد شده است. همچنین در این بیانیه اصل برابری حاکمیت دولت‌ها و ممنوعیت توسل به زور و عمل تجاوزکارانه در فضای سایبری نیز قابل اعمال توصیف شده است.

در ماده (۲) این بیانیه ضمن تسری اصل حاکمیت سرزمینی و صلاحیت دولت بر تمامی اجزای فضای سایبری، تأکید شده است که «هرگونه استفاده عامدانه از زور سایبری با پیامدهای فیزیکی یا غیر فیزیکی که تهدیدی برای امنیت ملی بوده یا منجر به بی‌ثباتی آن به واسطه بی‌ثباتی سیاسی، اقتصادی، اجتماعی و فرهنگی شود، ناقض حاکمیت دولت است». همچنین بیان شده است که «عملیات بهره‌برداری سایبری در مواقعی که مستلزم نفوذ غیرمجاز به زیرساخت‌های سایبری (دولتی یا خصوصی) تحت کنترل دولت دیگری باشد، می‌تواند نقض حاکمیت دولتِ هدف تلقی شود».

۸ واکنش علیه حملات سایبری

با این فرض که کشور قربانی بتواند مبدأ حمله‌ی سایبری را شناسایی کند و آن را به کشوری انتساب نماید، چندین گزینه را بدین شرح در دسترس خواهد داشت:

توسل به شورای امنیت سازمان ملل متحد. کشور قربانی بر اساس ماده‌ی ۳۵ (۱) منشور ملل متحد می‌تواند وضعیت را به شورای امنیت ارجاع نماید؛ ممکن است شورای مذکور روش‌های مناسب را بر اساس ماده‌ی ۳۶ (۱) منشور جهت حل و فصل اختلاف توصیه نماید؛ در صورتی که شورا وضعیت را تهدیدی علیه صلح، نقض صلح یا اقدام تجاوزکارانه تلقی کند، می‌تواند اختیارات خود را بر مبنای فصل هفتم منشور اعمال کند. هر چند در نظر طراحان منشور ملل متحد چنانچه شورای امنیت سازمان ملل متحد، یک حمله‌ی سایبری را تهدیدی علیه صلح تلقی کند (Osterdahl, 1998)، می‌تواند به‌موجب ماده‌ی ۳۹ منشور ملل متحد توصیه‌هایی را ارائه نموده و برای جلوگیری از وخیم‌تر شدن بحران و به‌موجب ماده‌ی ۴۰ این منشور اقداماتی را پیشنهاد نماید و سرانجام به استناد مواد ۴۱ و ۴۲ منشور ملل متحد در خصوص اقدامات مبتنی بر عدم توسل به زور و یا توسل به زور اتخاذ تصمیم کند. شورای امنیت سازمان ملل متحد همچنین می‌تواند محاصره‌ی سایبری را بر کشور مسؤول حمله‌ی سایبری و به‌منظور ممانعت از استمرار یا تکرار حمله، تحمیل نماید.

در این راستا، مطابق با حقوق بین‌الملل یک دولت می‌بایست میان حمله و منبع آن ارتباط برقرار کند؛ زیرا قوانینی که بر پاسخ مشروع به یک تهاجم تصریح می‌کنند (پاسخ به تهاجم را مجاز می‌شمارند)، بر اساس دولتی بودن یا دولتی نبودن منشأ تهاجم متفاوت است؛ بنابراین اِشکالی که اینجا وجود دارد این است که مواد یاد شده تنها ناظر به دولت‌هاست پس برای منشأ غیردولتی نمی‌توان از این مواد بهره جست؛ بنابراین واقعیت این است که ممنوعیت موضوع بند ۴ ماده ۲ منشور در زمینه توسل به‌زور فقط در مورد دولت‌ها قابل‌اعمال و استناد است، نه درباره اشخاص. درصورتی‌که اقداماتی که در مقابله با این حملات صورت می‌گیرد در چارچوب موازین دفاع مشروع و استثناءهای اصل منع توسل به زور نباشد، خود نوعی نقض حقوق بین‌الملل به شمار می‌رود. از سوی دیگر، مطابق همین موازین، دفاع مشروع تنها زمانی میسر است که اقدامات در جهت دفاع از حملات دولت متجاوز صورت گرفته و حملات به‌طور قطعی به آن منتسب باشد نه به اشخاص خصوصی یا هر نهاد دیگر که احیاناً دست به حملات سایبری زده باشد. بدیهی است احراز دفاع مشروع و یا اقدام مقابله به‌مثل یا هر استراتژی حقوقی دیگر در این زمینه منوط به تحلیل و تبیین صحیح حملات سایبری به‌مثابه نقض اصول توسل به‌زور و شناسایی اصول حاکم بر این حملات در چارچوب حقوق جنگ خواهد بود؛ در غیر این صورت هرگونه اقدام تلافی‌جویانه خود می‌تواند موجبی برای طرح مسئولیت بین‌المللی دولت مرتکب باشد. به‌هر روی حملات سایبری اگر مصداقی از تجاوز یا توسل به‌زور محسوب نشوند، می‌تواند به‌عنوان مداخله در امور داخلی دولت، یک تخلف بین‌المللی تلقی شود. در صورت انتساب این اقدامات به دولت، طرح مسئولیت بین‌المللی دولت امکان‌پذیر خواهد بود. درصورتی‌که این حملات توسط افراد خصوصی که در استخدام دولت یا تحت کنترل دولت باشند به دولت منتسب می‌شود. اعمال «نظریه تقصیر» در حملات

سایبری موجب می‌شود تا با شناسایی «مقصر» حمله سایبری، «مرتکب» حملـه سـایبری نیز شناسایی شود. پس در این صورت امکان جبران خسارت به روش‌های مختلـف اعم از توقف عمل متخلفانه، پرداخت غرامت و جلب رضایت وجـود خواهـد داشت.

رجوع به دادگاه بین‌المللی. کشور مسؤول حمله‌ی سایبری را می‌توان جهت جبران غرامت ناشی از نقض ماده‌ی ۲(۴) منشور ملل متحد و اصل عدم مداخله، به یک دادگاه بین‌المللی از جمله دیوان بین‌المللی دادگستری، احضار نمود. با این وجود باید توجه داشت که تعیین میزان خسارات ناشی از یک حمله‌ی سایبری، امری دشوار است؛ زیرا مؤسسات مالی ممکن است در تهیه‌ی اطلاعات دقیق و تعیین میزان خسارات مردد باشند؛ همچنین دیوان بین‌المللی دادگستری مانند سایر دادگاه‌های بین‌المللی، فاقد صلاحیت اجباری است؛ بنابراین، هر دو طرف اختلاف باید در خصوص ارجاع قضیه به دیوان توافق نمایند.

وفق ماده‌ی ۹۶ منشور ملل متحد، گزینه‌ی دیگر می‌تواند درخواست نظریه‌ی مشورتی از دیوان بین‌المللی دادگستری در خصوص مشروعیت یا عدم مشروعیت حملات سایبری باشد. چنین نظریاتی اختیاری و غیرالزام‌آورند؛ هرچند در شکل‌گیری یک قاعده‌ی عرفی بین‌المللی مؤثر می‌باشند (Conforti, 2005).

۹ مقابله به مثل و اقدام متقابل

کشور قربانی یک حمله‌ی سایبری می‌تواند به مقابله به مثل و اقدامات متقابل غیر نظامی علیه حمله‌کننده متوسل شود. بر اساس ماده‌ی ۴۹(۱) طرح مسئولیت بین‌المللی دولت، دولت صدمه‌دیده می‌تواند علیه دولت مسئول تخلف بین‌المللی، برای وادار ساختن دولت مذکور به ایفای تعهدات خود، به اقدامات متقابل مبادرت ورزد (حلمی،۱۳۸۷). حملات سایبری و تبلیغات سایبری با هدف ایجاد شورش و منازعه‌ی داخلی در کشور هدف، امری غیرقانونی بوده و با اصول ممنوعیت توسل به زور و ممنوعیت مداخله در امور داخلی سایر کشورها مغایر است؛ این‌گونه مداخلات کشور صدمه دیده را قادر می‌سازد اقدامات متقابل متناسب و سازگاری با حدود و شرایط مذکور در مواد ۵۰ تا ۵۲ طرح مسئولیت بین‌المللی دولت اتخاذ نماید.

پرسشی که در این راستا مطرح می‌شود، این است که آیا کشور قربانی یک حمله‌ی سایبری می‌تواند به اقدام متقابل مبتنی بر توسل به زور علیه حمله‌کننده مبادرت ورزد؟

پاسخ مثبت به این پرسش در صورتی است که در ماده‌ی ۵۱ منشور یا حقوق بین‌الملل عرفی، توسل به دفاع مشروع در مقابل حمله‌ی سایبری امری مجاز باشد. در نتیجه‌ی ماده‌ی ۵۰(۱) طرح مسئولیت بین‌المللی دولت ممنوع باشد، کشور قربانی حمله‌ی سایبری نمی‌تواند واکنش نشان دهد؛ مگر آنکه حمله‌ی سایبری شدید بوده و آثار گسترده‌ای داشته باشد؛ در این صورت به استناد ماده‌ی ۵۱ منشور ملل متحد، کشور مذکور محق به واکنش می‌باشد. وضعیتی که مدنظر کمیسیون حقوق بین‌الملل از تصویب ماده‌ی ۵۰ طرح مسئولیت بین‌المللی دولت بوده، ناظر بر کشوری است که در برابر نقض پیشین مثلاً یک معاهده‌ی بازرگانی توسط کشور دیگر، به زور مسلحانه متوسل گردد بر اساس ماده ۵۰(۱) طرح مذکور، چنین اقدام متقابلی که تناسبی با اقدام اولیه ندارد، منع شده است.

۱.۹ توسل به زور مسلحانه به استناد دفاع مشروع

پرسش این است که حمله‌ی سایبری از کدام ویژگی‌ها، گستردگی و پیامدها باید برخوردار باشد تا بتوان علیه آن به زور مسلحانه متوسل شد؟ پاسخ این پرسش در ادامه خواهد آمد.

شرایط تلقی حمله‌ی سایبری معادل حمله‌ی مسلحانه: ماده‌ی ۵۱ منشور ملل متحد مقرر می‌کند: در صورت وقوع حمله ی مسلحانه علیه یک عضو ملل متحد تا زمانی که شورای امنیت اقدامات لازم برای حفظ صلح و امنیت بین‌المللی را به عمل آورد، هیچ یک از مقررات این منشور به حق ذاتی دفاع از خود اعم از فردی یا دسته‌جمعی لطمه‌ای نخواهد رسانید؛ کشور قربانی توسل به زور سایبری در صورت تلقی چنین حمله‌ای به‌عنوان یک حمله‌ی مسلحانه، می‌تواند به دفاع مشروع متوسل شود.

پرسش مهم این است که آیا یک حمله‌ی سایبری به شبکه‌ی رایانه‌ای یک زیرساخت غیرنظامی می‌تواند در صورت دارا بودن معیار مقیاس و تحقق نتیجه، به‌نحو بالقوه یک حمله‌ی مسلحانه تلقی شود؟

در صورتی که به زیرساخت‌های مهم حمله شود و چنین حمله‌ای با تلفات و خسارات گسترده همراه باشد، پاسخ مثبت است؛ اما در خصوص اینکه زیرساخت‌های مهم کدامند، توافقی وجود ندارد. مجمع عمومی سازمان ملل متحد اعلام نموده است که هر کشور باید زیرساخت‌های مهم اطلاعاتی را خود تعیین نماید (A/RES/58/199 of 23 December2003).

۲.۹ امنیت سایبری؛ ظرفیت‌های حقوق بین‌الملل

از نمونه‌های جدید و مهم تهدیدهای سایبری، می‌توان به حمله جاسوسی Solarwinds در سال ۲۰۲۰ اشاره کرد، که سازمان‌ها و شرکت‌های آمریکایی و ایمیل مقامات وزارت امنیت آمریکا مورد حملات گسترده قرار گرفتند. دامنه این حمله‌ها که ادعا می‌شد توسط هکرهای روسی صورت گرفته، آنچنان گسترده بود که مؤسسه ملی بهداشت، پنتاگون، وزارت انرژی و همچنین مشتریان کمیسیون بورس اوراق بهادار نیز در فهرست آسیب‌دیدگان این حمله قرار گرفتند. تهدیداتی نیز که در سایه همه‌گیری کووید-۱۹ پیش آمد، به‌ویژه در نشست‌های غیررسمی شورای امنیت (Arria Formula) مورد بحث قرار گرفت و بر ثبات سایبری، پیشگیری از درگیری و ظرفیت‌سازی تأکید شد. از آنجا که تهدیدهای امنیت سایبری هر روزه، رواج، پیچیدگی و شدت بیشتری می یابند، دولت‌ها و جامعه فنی و صنعتی بر تقویت امنیت سایبری تمرکز کرده‌اند. درواقع، امنیت و ثبات فضای سایبری، سنگ بنای بحث در مورد فضای سایبری، حاکمیت اینترنت و آزادی اینترنت قرار گرفته است.

نگرانی جامعه بین‌المللی در این زمینه، موجب شد از سالهای ۱۹۹۸ مجمع عمومی ملل متحد آغاز به تصویب قطعنامه‌های سالانه نماید و تأکید کند که فناوری اطلاعات بالقوه می‌تواند برای مقاصدی مغایر حفظ ثبات و امنیت بین‌المللی به کار گرفته شود.

مجمع عمومی در قطعنامه ۳۲/۵۸ از دبیر کل درخواست کرد تا گروهی متشکل از کارشناسان دولتی را برای پیشبرد رفتار مسئولانه دولت‌ها در فضای سایبری در چارچوب امنیت بین‌المللی تشکیل دهد. این کار گروه که متشکل از ۲۵ عضو بود، از زمان آغاز به کار در سال ۲۰۰۴ تاکنون ۶ کارگروه تشکیل داده

است و آخرین کارگروه، کار خود را در ماه مه ۲۰۲۱ با تصویب یک گزارش به اتفاق آراء به پایان رسانید. در دوره‌های پیشین، مهم‌ترین دستاورد گروه کارشناسان دولتی، پذیرش کاربرد حقوق بین‌الملل در فضای سایبری (۲۰۱۳) و معرفی هنجارهای غیرالزام آور داوطلبانه رفتار مسئولانه دولت در سال ۲۰۱۵ بوده است. مذاکرات دور ۲۰۱۶-۲۰۱۷ این کارگروه به علت اختلاف نظر کارشناسان در مورد مسائل مربوط به کاربرد حقوق بین‌الملل به‌ویژه حقوق بشردوستانه، اقدامات متقابل و دفاع مشروع سایبری با شکست مواجه شد و نتیجه‌ای در پی نداشت.

به دنبال افزایش تنش‌ها میان قدرت‌های سایبری و شکست گروه کارشناسان دولتی در دور پیشین، مجمع عمومی در سال ۲۰۱۸ قطعنامه‌ای با حمایت روسیه مبنی بر ایجاد کارگروه بازبررسی تحولات در زمینه ارتباطات و اطلاعات در چارچوب امنیت بین‌المللی (OEWG) به تصویب رساند. تأسیس این کارگروه به انشعاب تلاش‌های سازمان ملل در این زمینه منجر شد و کارگروه باز به موازات گروه کارشناسان دولتی موظف شد موضوعات اساسی را که گروه کارشناسان در مورد آنها به اجماع رسیده‌اند، به بحث گذارد. نخستین گزارش این کارگروه به اتفاق آراء کشورهای شرکت‌کننده در مارس ۲۰۲۱ تصویب شد، که به‌دلیل مشارکت مستقیم دولت‌ها در تصویب آن می‌تواند از جایگاه مهم‌تری نسبت به سایر گزارش‌ها و اقدامات در این زمینه برخوردار باشد.

این گزارش، فراوانی، پیچیدگی و تنوع رویدادهای خرابکارانه فناوری اطلاعات و ارتباطات و همین‌طور افزایش احتمال استفاده از ابزارهای سایبری در مخاصمات آینده توسط تروریست‌ها و گروه‌های تبهکار و آثار بالقوه ویرانگر آنها را از جمله افزایش تعداد حملات سایبری خصمانه که خدمات عمومی ضروری مثل امکانات پزشکی، خدمات مالی، انرژی، آب، حمل و نقل و بهداشت را به مخاطره می‌اندازند، شناسایی کرده است. موضوع دومی که در این گزارش بدان پرداخته شده، هنجارها و اصول است و بر ارتباط و محدودیت‌های هنجارهای غیرالزام‌آور داوطلبانه برای صلح، امنیت و ثبات بین‌المللی تأکیده شده است. همچنین بر وظایف دولت‌ها برای جلوگیری از گسترش ابزارهای مخرب و بر لزوم گزارش‌دهی آسیب‌پذیری‌ها تأکید می‌کند. در این گزارش مشارکت فعال و مستمر دولت‌ها در گفتگوهای سازمانی منظم تحت نظارت سازمان ملل نیز مورد تأکید قرار گرفته است.

۱۰ الزامات حقوقی دفاع مشروع علیه حمله‌ی سایبری

به هنگام توسل به دفاع مشروع علیه یک حمله‌ی سایبری که در حد حمله‌ی مسلحانه باشد باید الزامات «ضرورت»، «تناسب» و «فوریت» رعایت شود (Din stein, 2005).

ضرورت بدین معنی است که توسل به زور آخرین گزینه و راهکار است؛ لذا باید سایر راهکارها ناکارآمد بوده یا احتمالاً ناکارا و بی‌فایده باشند. به‌عنوان یک الزام و شرط حداقلی، ضرورت بر این دلالت دارد که کشوری که درصدد دفاع مشروع است، باید دریابد که حمله‌ی سایبری یک تصادف نبوده و موضوع را نمی‌توان با توسل به روش‌های کمتر قهرآمیز حل و فصل نمود؛ روش‌هایی چون جلوگیری از دسترسی نفوذگران سایبری به شبکه‌ها و وب‌سایت‌های هدف حمله از طریق توسل به دفاع سایبری. در خصوص الزام تناسب باید گفت که

در عمل، واکنش یکسانی به حمله‌ی سایبری امکان‌پذیر نمی‌باشد. چرا که گاهی کشور قربانی فاقد فناوری توسل به حمله‌ی سایبری بوده و یا متجاوز فاقد یک شبکه‌ی به حد کافی توسعه‌یافته برای حمله به آن است (Greenberg, 1998).

سرانجام اینکه، الزام فوریت بیانگر آن است که هدف غایی دفاع مشروع تنبیه مهاجم نمی‌باشد، بلکه هدف، دفع حمله‌ی مسلحانه است. چنین الزامی به‌ویژه در خصوص حملات سایبری باید به نحو انعطاف‌پذیری به کار رود؛ چرا که برای مثال، در فرض استفاده‌ی متجاوز از «بمب های هوشمند یا زمانی» خسارات واقعی مدت‌ها پس از حمله‌ی سایبری ایجاد خواهد شد؛ امری که واکنش در قالب دفاع مشروع را با تأخیر مواجه می‌سازد.

۱۱ عملیات سایبری و حمله مسلحانه در معنای ماده ۵۱ منشور سازمان ملل متحد

تهدیدهای سایبری که شاید بتوان گفت برای اولین بار در سال ۱۸۳۴ با هک سیستم تلگراف فرانسه و ربودن اطلاعات مالی بانکی آغاز شد به چنان قدرت انهدام و ویران‌گری رسیده است که امروزه دولت‌ها از امکان تلقی برخی عملیات سایبری به‌عنوان حمله مسلحانه در مفهوم ماده ۵۱ منشور ملل متحد و توسل به دفاع مشروع فردی یا حتی جمعی در مواجه با آن، سخن می‌گویند.

در مواجهه با این تهدیدها، رویکرد اصلی حقوق بین‌الملل آن است که هر قاعده در دنیای واقعی قابل سرایت و اعمال است بر فضای مجازی؛ (برای نمونه نک به بند ۶۹ آخرین گزارش گروه کارشناسان دولتی در مورد رفتار مسؤولانه در فضای مجازی، بند ۷ آخرین گزارش گروه کاری نامحدود و قطعنامه شورای حقوق بشر در مورد اینترنت) ـ گویی که فضای مجازی همان آرایه ادبی است به کنایه از دنیای واقعی ما. از این منظر، حمله مسلحانه قلمداد کردن عملیات سایبری ممکن بوده و در نتیجه علاوه بر موضع بسیاری از دولت‌ها، بسیاری از صاحب‌نظران حقوقی از جمله کارشناسان مورد مشورت در دستورالعمل تالین ۲ نیز بر این نظر هستند که «دولت قربانی عملیات سایبری که به سطح حمله مسلحانه رسیده باشد، می‌تواند به حق دفاع مشروع ذاتی خود متوسل شود» (تأکید اضافه شده است، قاعده ۷۱). این کارشناسان، عملیات سایبری را هنگامی حمله مسلحانه قلمداد می کنند که «گستره و تأثیر» آن مشابه آستانه‌ای باشد که برای تلقی توسل به زور به حمله مسلحانه در دنیای واقعی اعمال می‌شود و در نتیجه بر این نظر هستند که چنانچه عملیات سایبری منجر به «صدمات جدی یا مرگ تعدادی یا ایراد خسارت یا نابودی اموال» شود، یعنی آثار فیزیکی همانند یک حمله مسلحانه به بار آورد، می‌تواند به‌عنوان حمله مسلحانه در مفهوم ماده ۵۱ منشور تلقی گردد (بند ۸، قاعده ۷۱).

این کارشناسان دو مبنای عمده برای چنین نتیجه‌گیری عنوان می‌کنند: نخست، نظر دیوان بین‌المللی دادگستری در مورد قابل اعمال بودن ممنوعیت توسل به زور و همچنین ماده ۵۱ منشور بر هر نوع «سلاح» (بند ۳۹ نظریه مشورتی دیوان در مورد سلاح های هسته‌ای)؛ و دوم وجود اجماع بر آنکه حمله‌های غیرکینتیک (یا غیرجنبشی) به مانند شیمیایی یا بیولوژیک در صورت ایراد آثاری مشابه با حمله‌های کینتیک می‌تواند در

گستره مفهوم حمله مسلحانه مندرج در منشور قرار گیرد (بند ۴ قاعده ۷۱).

با وجود مشابهت عملکرد عملیات سایبری با یک حمله شیمیایی از لحاظ غیرکینتیک بودن، در این واقعیت تردیدی نیست که در مورد اول ما با یک برنامه کامپیوتری مواجه هستیم که جز در فضای رایانه‌ای وجود ندارد و جز به کمک رایانه اثر نخواهد کرد و در مورد دوم با یک عنصر شیمیایی موجود در عالم واقع. به دیگر سخن، تأثیر یک عملیات سایبری به خودی خود و مستقیم نیست بلکه به دلیل تأثیری است که بر عملکرد کامپیوتر و شبکه‌ها و افزاره‌های متصل به آن گذاشته و در نتیجه عملکرد نادرست سیستم‌های کامپیوتری، ممکن است خسارتی به اموال یا لطمه‌ای به افراد وارد شود. دقیقاً به دلیل همین تفکیک است که اخیرا، اشمیت و بیلر در مقاله‌ای در مورد ابزار یا روش جنگی بودن عملیات سایبری، می‌نویسند از آنجا که در هیچ سلاح دیگری این مرحله میانی وجود ندارد که از خود هدف خواسته شود که زیان مورد نظر را پدید آورد، عملیات سایبری که متشکل است از مجموعه کدهایی که دستور اقدامات زیان‌آور را به یک سیستم رایانه‌ای می‌دهد، نمی‌تواند در مفهوم «سلاح» یا «ابزار» جنگی قرار گیرد بلکه توصیف درست از آن، در ذیل «روش جنگی» است. با توجه به اینکه اشمیت خود بانی و موتور اصلی دستورالعمل‌های تالین است، بعید نیست در دستورالعمل تالین ۳ که شروع آن کلید خورده است، تغییراتی در تقسیم‌بندی عملیات سایبری به سلاح و روش جنگی صورت گیرد (قاعده ۱۰۳ دستورالعمل تالین ۲ در حال حاضر ابزارهای سایبری را سلاح سایبری و سیستم‌های متصل به آن و روش‌های سایبری را تاکتیک، تکنیک و آیین‌های سایبری هدایت مخاصمات می‌خواند). با آنکه مقاله اشاره شده در بالا در مقام بیان تبیین یک قاعده از هدایت مخاصمات در حقوق بشردوستانه است (و خود تأکید می‌کند که چنین تفکیکی تأثیری در اجرای قواعد حقوق بشردوستانه ندارد)، چنین روشنگری نمی‌تواند بدون تأثیر در حوزه های دیگر حقوق و به‌خصوص حقوق توسل به زور باشد. برای نمونه، اگر عملیات سایبری در هر شکل و ابعاد به مانند توسل به حیله که صرفاً یک روش جنگی است، به‌طور طبیعی نمی‌تواند در مفهوم «سلاح» قرار گیرد و در نتیجه، از نظر موضوعی از دامنه شمول نظریه مشورتی دیوان در مورد سلاح‌های هسته‌ای در مورد قابل اعمال بودن ماده ۲ و ۵۱ منشور بر هر «سلاحی» خارج می‌شود.

در زمان تدوین دستورالعمل تالین ۲، این بحث مطرح شد که آیا استفاده از «سلاح» برای تحقق حمله مسلحانه ضروری است یا خیر. پیش از ادامه این بحث، اشاره به این مطلب ضروری است که در دستورالعمل تالین ۲، کارشناسان بر تفاوت میان «تجاوز» و «حمله مسلحانه» اذعان داشته و هر «تجاوزی» را لزوماً مساوی با «حمله مسلحانه» نمی‌دانند (بند ۲ قاعده ۷۱)، که خود تأییدی است بر تفکیک میان «تجاوز مسلحانه» یا همان حمله مسلحانه با سایر اشکال «تجاوز». با این حال، در بحث ضرورت استفاده از سلاح، نظر اکثر کارشناسان بر این بود که لازم نیست حمله مسلحانه با استفاده از سلاح باشد ـ امری که با تعریف تجاوز مسلحانه می‌تواند در مغایرت باشد – اما این نظر را نیز رد نکردند که واژه «مسلحانه» بودن صرفاً بر استفاده از سلاح اطلاق می‌شود و در نتیجه جز عملیات سایبری که با استفاده از سلاح سایبری در مفهوم قاعده ۱۰۳ انجام گیرد، سایر عملیات‌های سایبری صرف نظر از گستره و آثار نمی‌تواند به‌عنوان حمله مسلحانه در مفهوم ماده ۵۱ منشور در نظر گرفته شود.» (بند ۵ قاعده ۷۱). با این توصیف، اگر طبقه‌بندی اشمیت در مورد روش جنگی بودن عملیات سایبری پذیرفته شود، این دو دیدگاه قطعاً غیر قابل جمع خواهند شد، یعنی یا بایستی

قائل به تعمیم حمله مسلحانه به عملیات سایبری به صرف آثار بود و یا با توجه به اینکه عملیات سایبری صرفاً مجموعه‌ای از دستورهای کامپیوتری است و در نتیجه هیچ اقدام مسلحانه‌ای در عالم واقع صورت نگرفته است، در صورت وجود سایر شرایط آن را صرفاً مشمول مداخله، توسل به زور و یا حتی تجاوز دانست و نه حمله مسلحانه.

چنانچه قایل به نظر اول شویم، یعنی تنها آثار را به عنوان معیار حمله مسلحانه بودن عملیات سایبری در نظر بگیریم، آیا این امر منجر نمی‌شود که بتوان سایر روش‌هایی را نیز که منجر به مرگ و آسیب گسترده می‌شوند، برای نمونه تحریم‌های اقتصادی یک‌جانبه، در مفهوم حمله مسلحانه ماده ۵۱ قرار گیرد؟ مقایسه عملیات سایبری با تحریم‌ها از این جهت جالب توجه می‌نماید که آثار تحریم، به‌خصوص خسارات و لطمات معمولاً فوری نبوده، بلکه در طولانی‌مدت رخ دهد. این تأثیر مشابه همان اتفاقی بود که در مورد ویروس استاکس‌نت روی داد؛ با وجود اینکه کدهای دستوری مختلف مدت‌های مدیدی بود که در سیستم‌های رایانه‌ای وارد شده بودند (گفته می‌شود حدود چهار سال)، اما امکان تلقی آن به‌عنوان «حمله مسلحانه» تنها زمانی در نظر گرفته شد که خسارات گسترده‌تر وارد شده بود (ذکر این مطالب ضروری است که تاکنون نه استاکس‌نت و نه هیچ عملیات سایبری دیگر به‌عنوان حمله مسلحانه مورد شناسایی دولت‌ها قرار نگرفته و حتی در مورد استاکس نت، کارشناسان تالین در مورد حمله مسلحانه قلمداد کردن آن تردید داشتند، با وجود آنکه همه موافق بودند که این عملیات توسل به زور بوده است. (بند ۱۰، قاعده ۷۲)). حال، چرا بایستی تفاوتی بین کدهای دستوری زیان‌بار و وضع قوانین تحریمی زیان‌بار قائل شد زمانی که ـ همان‌طور که همه تجربه کرده‌ایم ـ هر دو موجب مرگ و آسیب می‌شوند؟ در این خصوص، توجه به این مسأله مهم است که با وجود اینکه از موارد تجاوز مندرج در اساسنامه دیوان بین‌المللی کیفری، توسل به روش «محاصره بنادر و سواحل توسط نیروهای مسلح دولت دیگر» (بند ج ماده ۸ مکرر اساسنامه دیوان بین‌المللی کیفری) است که در معنای سنتی، جنگی است اقتصادی برای ممانعت از ورود کالا و افراد به قلمروی کشور دشمن (تفسیر جنایت تجاوز، ص. ۴۴۳) اما آنچه این روش را تبدیل به تجاوز می‌کند، حضور نیروهای مسلح دولت محاصره‌کننده است که می‌توانند عملاً مانع ورود و خروج کالا و خدمات شوند (همان، ص. ۴۴۴) و نه صرف تحریم.

رویه دیوان بین‌المللی دادگستری در تبیین تفاوت میان توسل به زور و حمله مسلحانه به صرف اشاره به گستره و آثار نبایستی توجه را از این مطلب دور کند که در هر سه پرونده فعالیت‌های نظامی و شبه نظامی در نیکاراگوئه، سکوهای نفتی و فعالیت های مسلحانه در کنگو، تردید یا حتی بحثی در مسلحانه بودن اقدامات انجام شده در مفهوم عادی و کلاسیک و واقعی آن نبود؛ بلکه محل تردید، تعیین آستانه یا مصادیق حمله مسلحانه در توجیه اقدامات نظامی متقابل در قالب دفاع مشروع بود. از این دیدگاه، صرف در نظر گرفتن معیار گستره و آثار بدون بستر آن، که همان عملیات نظامی مشروحه در هر پرونده‌ای بود، به‌مثابه حکایت نادان خواندن فیل در شعر مولاناست (دکتر کتایون حسین نژاد، ۱۴۰۱).

با وجود آنکه عملیات سایبری می‌تواند آثار بسیار مخربی داشته باشد، اما، همگام با صاحب‌نظرانی که ماده ۵۱ منشور سازمان ملل متحد را استثنایی نه بر منع توسل به زور بلکه بر اقدامات جمعی سازمان ملل متحد ذیل فصل هفتم منشور و تحت لوای شورای امنیت و محدود به موارد تجاوز مسلحانه‌ای می‌دانند که اقتضای

اقدام فوری پیش از اتخاذ تدابیر ضروری توسط شورای امنیت تامین صلح و امنیت را دارد. به دلیل ماهیت مجازی، چنین عملیاتی نمی‌تواند در مفهوم حمله مسلحانه قرار گیرد. این ایده، منصرف از این استدلال است که حتی اگر عملیات سایبری را حمله مسلحانه بدانیم، متناسب‌ترین دفاع در برابر آن به احتمال قوی مقابله مجازی با آن و نه استفاده از بمب و موشک است.

۱۲ تأثیر و شدت حملات سایبری

حملات سایبری می‌تواند از بسیاری جهات بر سازمان‌ها تأثیر بگذارد، از اختلالات جزئی در عملیات گرفته تا خسارات عمده مالی. صرف نظر از نوع حمله سایبری، هر نتیجه‌ای نوعی هزینه دارد، چه پولی و چه غیر پولی. پیامدهای حملات سایبری ممکن است هفته‌ها و یا ماه‌ها بعد بر روی کسب‌وکارها تأثیر بگذارد. در ادامه پنج منطقه‌ای که ممکن است آسیب ببیند آورده شده است:

- خسارات مالی
- از دست دادن بهره‌وری
- خسارت به اعتبار
- مشکلات مداوم تجاری
- بدهی‌های قانونی

حملات باج‌افزار به‌عنوان یک نگرانی بزرگ شیوع بیشتری پیدا کرده است. در پایان سال ۲۰۱۶ هر ۴۰ ثانیه یک تجارت قربانی حمله باج‌افزار می شد. بر اساس گزارشی از Cybersecurity Ventures انتظار می‌رود این میزان تا امسال هر ۱۱ ثانیه افزایش یابد. این حمله سایبری زمانی اتفاق می‌افتد که از نرم‌افزار مخربی برای محدود کردن دسترسی به سیستم رایانه‌ای یا داده‌ها استفاده شود، تا زمانی که قربانی، باج خواسته شده توسط مجرم را پرداخت کند.

از زمانی که افراد از سیستم‌های تجاری آسیب‌پذیر بهره‌مند می‌شوند، جرائم سایبری افزایش یافته است. غالباً مهاجمان به دنبال باج گرفتن هستند: ۵۳ درصد از حملات سایبری منجر به خسارت ۵۰۰،۰۰۰ دلاری یا بیشتر شده است.

اهداف حملات سایبری: ایجاد اختلال در یک سرور، به‌کار گرفتن کامپیوتر افراد به‌عنوان سپر، دسترسی به اطلاعات یک سیستم کامپیوتری، ورود به اتصالات اینترنتی که پهنای باند زیادی دارند، مطالعه و زیر نظر گرفتن یک سازمان به‌صورت غیر مجاز، دسترسی و سرقت اطلاعاتی که در یک کامپیوتر نگهداری می‌شود.

۱۳ دفاع مشروع علیه حمله‌ی سایبری از منظر حقوق بین‌الملل عرفی

همان‌گونه که آورده شد، به‌موجب ماده‌ی ۵۱ منشور ملل متحد، می‌توان به دفاع مشروع علیه حمله‌ی سایبری متوسل شد. پرسش این است که آیا قاعده‌ی عرفی در این خصوص وجود دارد؟ در قضیه‌ی نیکاراگوئه، دیوان بین‌المللی دادگستری دریافت که هویت کاملاً مجزایی میان قواعد عرفی بین‌المللی توسل به زور و مقررات ناظر بر آن در منشور ملل متحد وجود ندارد و حقوق بین‌الملل عرفی صرف نظر از حقوق بین‌الملل معاهدات به وجود و کارکرد خود ادامه می‌دهد؛ حتی اگر هر دو نظام حقوقی محتوای یکسانی داشته باشند (Nicaragua case, 1986).

ایالات متحده آمریکا، در خصوص حق دفاع مشروع در تقابل با حملات سایبری، مواضعی را اتخاذ نموده است. بر اساس ارزیابی وزارت دفاع این کشور، کشور حامی حملات سایبری، حق توسل به دفاع مشروع را برای طرف مقابل ایجاد می‌کند.از منظر این وزارتخانه ، هرگاه یک حمله‌ی شبکه‌ای رایانه‌ای هماهنگ، سیستم کنترل ترافیک هوایی یک کشور و یا سیستم‌های بانکداری و مالی آن را مختل کند، دریچه‌ی چندین سد را باز کند و در نتیجه سیل جاری شود و هر یک از این اقدامات تلفات گسترده غیرنظامیان و یا خسارات مادی را در پی داشته باشد، کشور اخیر، قربانی و هدف یک حمله‌ی مسلحانه یا عملی برابر با یک حمله‌ی مسلحانه واقع شده است (www.au.af.mil).

رویه‌ی سازمان‌های بین‌المللی مربوطه، شکل دیگری از رویه‌ی کشورها است که در ارزیابی وجود یک قاعده‌ی حقوق بین‌الملل عرفی باید مورد توجه قرار گیرد (انجمن حقوق بین‌الملل، ۱۳۸۴).

حقوق بین‌الملل عرفی نیز با توجه به وجود نسبی رویه‌ی کشورها و اعتقاد حقوقی، به‌ویژه در خصوص حق دفاع مشروع علیه حملات سایبری، می‌تواند نقشی را در این زمینه ایفاء نماید. این فرایند ادامه دارد و می‌تواند به شکل‌گیری یک قاعده‌ی عرفی در سال‌های پیش رو منجر گردد. ضمن آنکه همکاری‌های بین‌المللی در سطوح منطقه‌ای و جهانی می‌تواند در مقابله با حملات سایبری که پدیده‌ای بدون مرز است، نقش مؤثری ایفاء نماید. در این راستا ضرورت انعقاد معاهده‌های خاص در مورد ممنوعیت حملات سایبری بیش از پیش احساس می‌شود.

۱۴ آزادی اطلاعات در فضای سایبر از منظر حقوق بین‌الملل

در فرهنگ سیاسی و فلسفی کمتر واژه‌ای به اندازه «آزادی» به بازی گرفته شده است. در حالی که عده‌ای آزادی را به مفهوم رهایی از هر گونه قید و بند دانسته‌اند، جمعی دیگر آن را اطاعت از عقل و اقدام به قانون معنی کرده‌اند. گویی رمز این همه اختلاف و ابهام در خود واژه آزادی نیز نهفته باشد. امروزه آزادی بیان به‌صورت گسترده یکی از حقوق بشر تلقی می‌شود؛ بدین معنی که انسان‌ها «به‌خاطر انسان بودنشان» حق آزادی بیان دارند. در کنار پذیرش عمومی مفهوم آزادی بیان، از طرف دیگر توافقی عمومی نیز وجود دارد که باید برای آزادی بیان حد و مرز مشخص کرد؛ دیگر فضای سایبر یک فضای تک‌بعدی وب‌سایتی نیست . امروز

مخاطب بدون اینکه احساس کند در میان چندین وجه از اشکال سایبر است. می‌توان فضای سایبر را به‌مثابه دریاچه‌ای در نظر گرفت که ابعاد گوناگون آن مانند جزایر کوچک و بزرگی هستند که شناگران در این فضا هر از چند گاهی به یکی از این جزایر سر می‌زنند. امروزه دیگر فعالیت در یک عرصه از فضای سایبر نمی‌تواند یک فعالیت اثرگذار و جامع باشد، بلکه بسیاری از مراکز مهم و تأثیرگذار در تمام ابعاد این فضا با محتواهای مختلف در موضوعات مشترک فعال هستند.

۱.۱۴ مزیت‌ها و محدودیت‌های فضای سایبر برای آزادی بیان

پیش از وارد شدن به بحث‌های خاصی که فضای سایبر در مورد اصل آزادی بیان به‌وجود آورده لازم است مفهوم آن در حدی که مورد توجه اسناد بین‌المللی حقوق بشری بوده، تبیین شود. بر این پایه، اعلامیه جهانی حقوق بشر (۱۹۴۸) در ماده ۱۹ خود مقرر می‌دارد: «هرکس حق آزادی عقیده و بیان دارد و این حق مستلزم آن است که از داشتن عقیده بیم نداشته باشد و در دریافت و انتشار اطلاعات و افکار، به تمام وسایل ممکن بدون ملاحظات آزاد باشد بی‌گمان این ماده همانند دیگر مفاد این سند به شکل کلی تنظیم شده و استیفاء این حقوق ایجاب می‌کرد که این مفاهیم دقیق‌تر و شفاف‌تر تعریف شده و حدود و ثغور آنها مشخص شود. از این رو در سال ۱۹۷۶ میثاق بین‌المللی حقوق مدنی و سیاسی به‌تصویب دولت‌های عضو سازمان ملل رسید. در این سند دو ماده ۱۸ و ۱۹ به تبیین این موضوع پرداخته‌اند. ماده ۱۸ حق آزادی تفکر آگاهی و دین را به رسمیت می‌شناسد که آزادی عقیده موضوع ماده ۱۹ را نیز دربر می‌گیرد. تأکید اصلی این ماده، محترم شمردن آزادی تفکر درباره همه موضوع‌های مربوط به ایمان شخصی و تعهد به دین یا اعتقاد خاص است و آن‌گونه که در بند ۲ ماده ۴ میثاق آمده، حتی در شرایط خاص و اضطراری هم نباید آن را خوار شمرد و تحقیر کرد. البته این ماده میان آزادی تفکر آگاهی و دین یا عقیده و آزادی ابراز آنها تفکیک قائل شده است. گروه نخست تحت حمایت مطلق هستند تا اندازه‌ای که طبق ماده ۱۷ و بند ۲ ماده ۱۸ هیچ‌کس را نمی‌توان مجبور کرد تا افکار خود را آشکار کند یا به دین یا عقیده خاصی بگرود. ولی، بر گروه دوم محدودیت‌هایی اعمال شده که در جای خود به آنها اشاره خواهد شد.

ماده ۱۹ با عنوان آزادی عقیده حق داشتن اعتقاد بدون مداخله را با هیچ استثناء یا محدودیتی به رسمیت می‌شناسد (بند ۱). در اینجا نیز میان اصل این حق و آزادی ابراز آن تفکیک صورت گرفته و در بند ۲ میثاق آمده حتی در شرایط خاص و اضطراری هم نباید آن را خوار شمرد و تحقیر کرد. البته این ماده میان آزادی، تفکر، آگاهی و دین یا عقیده و آزادی ابراز آنها تفکیک قائل شده است.

۱۵ نتیجه‌گیری

با پیشرفت فناوری، فضای سایبری به‌عنوان فضای پنجم در حقوق بین‌الملل دیر زمانی نیست پا به عرصه ظهور گذاشته است. مثل اکثر پیشرفت‌هایی که فناوری به همراه داشته است در این باره هم از این فضا برای اعمال خرابکارانه استفاده شده است. ماهیت غیرملموس فضای سایبری و تهدیداتی که این فضا برای امنیت وحاکمیت دولت‌ها دارد و ویژگی‌هایی که حملات سایبری دارد، تدوین و تطبیق قوانین بین‌المللی بر

این نوع فعالیت‌های سایبری را ایجاب می‌کند. با توجه به عناصری که برای یک جنگ می‌توان برشمرد، با نگاهی به مقررات بین‌المللی، از جمله منشور ملل متحد، نظریات تفسیری دیوان بین‌المللی دادگستری در قضایای ترافعی یا مشورتی، کنوانسیون‌های چهارگانه ژنو ۱۱۸۱، پروتکل‌های الحاقی ۱۱۷۷ آن و رویه دولت‌ها، می‌توان ابزارهای به‌کار رفته در حملات سایبری را با نگاه غایت‌محور به عنوان ابزار جنگی شناسائی کرد و این نوع حملات را تحت عنوان «زور» که در منشور ملل متحد آمده است، قلمداد نمود. علاوه بر این، با به‌کار بردن معیارهای شناخت حملات سایبری می‌توان این نوع حملات را به‌عنوان ناقض اصول منع تهدید و عدم توسل به زور و اصل عدم مداخله در امور داخلی کشوها بر شمرد. با در نظرگرفتن ملاحظات ذکرشده، کشورها در هنگام مواجهه با حملات سایبری با رعایت مقررات و موازین بین‌المللی حق توسل به دفاع مشروع و اقدامات متقابل را دارا می‌باشند. با توجه به اهمیت این اصول برای جامعه بین‌المللی که به‌عنوان قواعد آمره بین‌المللی نیز شناسایی شده‌اند، ماهیت حقوقی حملات سایبری باید توسط نهادهای ذیربط همچون دیوان بین‌المللی دادگستری با ارجاع دعوای ترافعی به دیوان یا درخواست نظریه مشورتی، همچنین توسط شورای امنیت سازمان ملل متحد که طبق فصل هفتم منشور ملل متحد مسئولیت اصلی حفظ صلح و امنیت بین‌المللی را به دوش می‌کشد و به‌عنوان مرجع اصلی احراز وقوع تجاوز طبق قطعنامه تعریف تجاوز باید به این عرصه ورود پیدا کنند.

نکته حائز اهمیت دیگر در مورد مسئولیت دولتها در قبال فعالیت‌های سایبری است. در هنجار ۱۳(ج) این گزارش مقرر شده است که دولت‌ها نباید آگاهانه اجازه دهند که با استفاده از فناوری اطلاعات و ارتباطات از قلمروشان برای اعمال مغایر حقوق بین‌الملل استفاده شود.

این هنجار که به مفهوم مراقبت مقتضی (Due Diligence) معروف است، اخیراً در حوزه سایبری به‌عنوان راهکاری امیدوارکننده برای پاسخگویی دولت‌ها در قبال عملیات سایبری که از قلمرو آنها سرچشمه می‌گیرند یا از قلمروی آنها عبور می‌کند، بسیار مورد توجه قرار گرفته است.

با وجود تلاش‌ها و اقدامات برشمرده شده توسط کشورهای عضو سازمان ملل و حقوقدانان بین‌المللی در نهایت، دست‌یابی به راه حل اصلی در تنظیم مقررات سایبری دشوار به نظر می‌رسد. از سویی، دولت‌های غربی و ذی‌نفعان عرصه سایبری، بر این نظرند که حقوق بین‌الملل موجود برای تنظیم رفتار دولت‌ها در فضای سایبر کافی است و تنها باید به چگونگی عملیاتی کردن این قواعد پرداخت. اما در مقابل، برخی کشورها مانند ایران، روسیه و کوبا معتقدند در حقوق موجود شکاف‌ها و ناکارآمدی‌هایی وجود دارد که نیازمند تنظیم قواعد جدید در این زمینه از طریق تدوین یک معاهده جدید و یا تحول حقوق بین‌الملل عرفی است.

حتی در رویکرد معتقدان به ضرورت قواعد جدید نیز همسویی وجود ندارد. برخی دولت‌ها بر معاهده‌ای متمرکز هستند که از دولت‌ها در برابر مردم محافظت می‌کند و برخی دیگر به‌دنبال معاهده‌ای هستند که از مردم در برابر دولت‌ها محافظت کند.

مراجع

[۱] توحیدی، محمدرضا، «ارزیابی ماهیت حقوقی حملات سایبری با نگاهی به منشور سازمان ملل متحد»، ۱۳۹۷.

[۲] اسمعیل‌زاده ملاباشی، پرستو، عبدالهی، محسن، زمانی، سیدقاسم، «حملات سایبری و اصول حقوق بین‌الملل بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)»، فصلنامه مطالعات حقوق عمومی، دوره ۸۷، شماره ۲، صفحه ۵۸۲، تابستان ۱۳۹۶.

[۳] آهنی امینه، محمد، «حقوق بین‌الملل مدرن و جنگ سایبری در فضای مجازی»، مؤسسه انتشاراتی جهان جام جم، ۱۳۹۷، صفحات ۱۰۶-۱۱۰.

[۴] پاکزاد، بتول، «ماهیت تروریسم سایبری» مجله‌ی تحقیقات حقوقی دانشگاه شهید بهشتی، ویژه‌نامه‌ی شماره‌ی ۴، بهار ۱۳۹۰.

[۵] پاکزاد، بتول، تروریسم سایبری، رساله‌ی دکتری حقوق کیفری و جرم‌شناسی، دانشکده‌ی حقوق دانشگاه شهید بهشتی، ۱۳۸۸.

[6] Abraham M. Denmark, James Mulvenon. (2010). Contested Commons: The Future of American Power in a Multipolar World, Center for New American Security (CNAS).

[7] Hess, Charlotte. (1996). “Untangling the Web: The Internet as a Commons.” Workshop in Political Theory and Policy Analysis”, Indiana University.

[8] Schmitt, Michael N. (2013). Tallinn Manual on the International Law: Applicable to Cyber Warfare, Cambridge University Press.

[9] Robertson Jr., H.B., “Self-Defense Against Computer NetworkAttack Under International Law”, in: Schmitt/O’Donnell (eds).

[10] Computer Network Attack and International Law, 2001. Roscini, M., Threats of Armed Force and Contemporary International.

[11] Schmitt, M. (2017). Computer network attack and the use of force in international law: thoughts on a normative framework. In The Use of Force in International Law (pp. 379-431). Routledge.

[12] Shackelford, S. J. (2009). From nuclear war to net war: analogizing cyber attacks in international law. Berkeley J. Int’l Law, 27, 192.