انتساب حمله سایبری به دولت‌ها از منظر حقوق بین‌الملل

محمدعلی کریمی [۱]، محمد ستایش پور [۲]

[۱] کارشناس ارشد حقوق بین‌الملل، دانشگاه قم
karimi6447@gmail.com
[۲] استادیار حقوق بین‌الملل، دانشگاه قم
mohamadsetayeshpur@yahoo.com

چکیده

حمله سایبری به زیرساخت‌های هسته‌ای (استاکس نت ۲۰۱۰) و سامانه سوخت (۲۰۲۱) در ایران مهم‌ترین دلیل انتخاب این عنوان برای این پژوهش بود. افشاگری ادوارد اسنودن و مستند روزهای صفر ساخته الکس گیبنی موید نقش مسئولین دولت ایالات متحده (بوش و اوباما) در فرمان حمله سایبری به زیرساخت‌های هسته‌ای ج.ا.ایران بود. در حمله به سامانه سوخت ایران نیز نقش مستقیم یک دولت در این حمله سایبری ادعا شد. سال‌هاست که حملات سایبری متعددی علیه زیرساخت‌های حیاتی و حساس کشورهای مختلف صورت می‌گیرد و موجب خسارات می‌شود؛ اما به دلایل سخت بودن اثبات انتساب به دولت و شناسایی مهاجم و سازوکار حقوق بین‌الملل برای حمایت از کشور زیان‌دیده موجب شده تا بسیاری از سیاستمداران در این زمینه دچار سردرگمی باشند. ازآنجایی‌که دولت‌ها به حاکمیت فضای سایبری (معماری فنی که به اینترنت جهانی اجازه می‌دهد تا کار کند) و حاکمیت در فضای سایبری (نحوه استفاده دولت‌ها، صنعت و کاربران از این فناوری) توجه بیشتری می‌کنند، نقش قوانین بین‌المللی در سایبر زمینه اهمیت روزافزونی پیدا کرده است. حقوق بین‌الملل، روابط بین دولت‌ها و سایر ذی‌نفعان بین‌المللی (به‌ویژه سازمان‌های بین‌المللی) را از طریق ممنوعیت‌ها، الزامات و مجوزهای مختلف سازماندهی، منسجم و قاعده‌مند می‌کند. پژوهش حاضر گامی است مختصر در راستای شناخت بهتر این امر و کاربرد مناسب حقوق بین‌الملل در فضای سایبر، بازیگران درگیر، مسائل اصلی در کاربرد آن و مسیرهای بالقوه آینده که امید است مورد بهره‌برداری پژوهشگران قرار گیرد.

کلمات کلیدی: حمله سایبری، مسئولیت بین‌المللی، انتساب حمله سایبری، حقوق بین‌الملل.

۱ مقدمه

بررسی اسناد و تاریخچه اخبار رسانه‌ها در ژوئیه ۲۰۱۰، از حمله سایبری علیه زیرساخت‌های هسته‌ای ایران خبر می‌دهد که به دلیل پیچیدگی این رخداد، بسیاری از کارشناسان، عامل تهاجم را به نقش برخی دولت‌ها نسبت می‌دهند تا افراد و گروه‌های معاند.

در اواخر ماه مه ۲۰۱۲، رسانه‌های آمریکایی اعلام کردند که استاکس‌نت مستقیماً به دستور اوباما، رئیس‌جمهور وقت آمریکا طراحی، ساخته و راه‌اندازی شد [۱۴]. گرچه در همان زمان احتمال این می‌رفت که آمریکا تنها عامل سازنده نباشد، در ۷ ژوئیه ۲۰۱۳، ادوارد اسنودن در مصاحبه‌ای با اشپیگل اعلام کرد: این بدافزار با همکاری مشترک آژانس امنیت ملی ایالات متحده آمریکا و اسرائیل طی عملیاتی به نام «عملیات بازی‌های المپیک» ساخته شده‌است [۲۱]. در سال ۲۰۱۶، الکس گیبنی مستندی به نام روزهای صفر در مورد استاکس‌نت منتشر کرد که در آن، این ویروس محصول مشترک ایالات متحده آمریکا و واحد ۸۲۰۰ ارتش اسرائیل معرفی شده‌است [۲۲]. اما این حمله سایبری پایان کار نبود و هم‌زمان با اعتراضات به گران شدن بنزین در ایران (اکتبر ۲۰۲۱)، حمله سایبری به جایگاه‌های پمپ‌بنزین در ایران صورت گرفت که سبب بروز اختلال در روند سوخت‌گیری برای مردم شد. این اختلال از بسیاری از شهرهای ایران گزارش شد[۱]. این حمله سایبری سبب شد تا خرید بنزین با نرخ دولتی، موسوم به بنزین سهمیه‌ای، از مدار خارج شود و سوخت‌گیری فقط با نرخ آزاد فقط در برخی از پمپ‌بنزین‌ها ممکن باشد[۲].

خبرگزاری ایلنا گزارش داد که در ساعات اولیه شروع رخداد، ۳۰٪ از پمپ‌بنزین‌های کشور توان سوخت‌رسانی به‌صورت دستی و آفلاین را داشتند و در تهران بزرگ فقط ۱۲ جایگاه فعال بود[۳].

سازمان صداوسیمای جمهوری اسلامی ایران اعلام کرد: عامل این حمله سایبری احتمالاً یک «کشور خارجی» بوده است. چند مقام نظام جمهوری اسلامی هم در اظهار نظرهایی متفاوت، این حمله را مرتبط با حوادث آبان ۹۸ و اقدام «دشمن» دانستند.

وب‌سایت خبر آنلاین، رژیم صهیونیستی را عامل حمله سایبری معرفی کرد[۴].

آنتونیو گوترش، دبیرکل سازمان ملل، در اولین سخنرانی خود در افتتاحیه نشست سران مجمع‌عمومی سازمان ملل متحد در سال ۲۰۱۷، تشدید تهدیدات امنیت سایبری را به‌عنوان یک تهدید اصلی برای امنیت بین‌المللی برجسته کرد.

برای درک وخامت این تهدیدها، کافی است نگاهی به نمونه های اخیر حمله های سایبری داشته باشیم که علاوه بر تهدید جنگ سایبری، این حمله ها منجر به توقف کار بیمارستان‌ها، قطع شبکه‌های برق، توقف فعالیت شهرهای بزرگ و حتی یکپارچگی فرایندهای دموکراتیک شده است [۹].

هرچند رسانه دولت آمریکا (صدای آمریکا) پس از مناقشه بر سر اعلام نقش یک کشور متخاصم در حمله سایبری به جایگاه‌های سوخت ایران، اعلام کرد ایمیلی دریافت کرده که بر اساس آن، گروه «گنجشک درنده» علاوه بر پذیرش مسئولیت این حمله، مسئولیت حملات سایبری به شرکت راه‌آهن و وزارت راه و شهرسازی را نیز به عهده گرفته است.

هرچند این دو حمله سایبری در اینجا ذکر گردید، بی شک حملات زیادی به زیرساخت‌های جمهوری اسلامی ایران صورت گرفته که کنترل شده و یا شدت آن کم بوده است؛ اما این پرسش برای افکار عمومی

[۱] خبرگزاری مهر. ۲۶-۱۰-۲۰۲۱
[۲] خبرگزاری تسنیم. ۲۷-۱۰-۲۰۲۱
[۳] خبرگزاری ایلنا. ۲۷-۱۰-۲۰۲۱
[۴] خبر آنلاین. ۲۸-۱۰-۲۰۲۱

باقی است که چگونه می‌توان نقش یک کشور در حمله سایبری را اثبات کرد و نکته دوم اینکه چگونه می‌توان از مسیر حقوق بین‌الملل برای کشور ایجاد بازدارندگی کرد و حق خود را از مجامع بین‌المللی مطالبه کرد؟

۲ مبانی نظری و ادبیات مفهومی

۱.۲ فضای سایبری چیست؟

فضای سایبری[۵] مفهومی برای بیان و تفسیر فناوری یکپارچه دیجیتال است[۶] و حاکی از فضای غیرقابل‌لمس ابری بین رایانه‌ها و فضای داده‌ای که اطلاعات دائماً در شبکه‌های محلی یا جهانی در حال تبادل هستند.

فضای سایبر و مجازی خدمات متعددی در حوزه روابط اجتماعی، بانکداری، حمل‌ونقل (جاده‌ای، دریایی، هوایی)، شبکه‌های اداری، رسانه‌های دیداری و شنیداری، پزشکی، آموزش و...ارائه می‌کنند و عموماً مردم از بستر خدماتی و غیرنظامی آنها استفاده می‌کنند. در کنار این امر، ساختارهای نظامی و امنیتی کشورها نیز از این فضاها بهره‌گیری و استفاده می‌کنند و به‌نوعی ساکنین این فضاها هستند[۷].

۲.۲ حملات سایبری در بستر مجازی

بدون شک، همان‌طور که ذکر شد، یکی از پیچیده‌ترین ابزاری که تاکنون از آن برای اهداف تروریستی بهره برده شده است، اینترنت است. تنها در دنیای اینترنت است که دولت‌ها، گروه‌های فشار، تروریست‌ها و... می‌توانند با هزاران نام مجازی و بدون این که ردی از خود بر جای بگذارند، حمله‌ای را که ممکن است آغازگر جنگی باشد، به راه‌اندازند. حمله سایبری به حمله هدایت شده از طریق فضای سایبر با توسل به ابزارها و تجهیزات سایبری را گویند[۸]. در این راستا، سیاست‌مداران نیز فضای سایبر را پنجمین قلمرو جنگ‌افروزی بعد از زمین، دریا، هوا، فضا تعریف می‌کنند[۹].

۱.۲.۲ حمله و جنگ سایبری چیست؟

حمله سایبری هر گونه اقدام تهاجمی است که بسترهای اطلاعاتی، شبکه‌های رایانه‌ای، زیرساخت‌های حیاتی، حساس و مهم، دستگاه‌های شخصی یا گوشی‌های هوشمند و... را هدف قرار می‌دهد [۱۲].

مهاجم می‌تواند شخص، گروه، دولت یا فرایندی باشد که سعی می‌کند بدون مجوز، به داده‌ها، عملکردها یا سایر مناطق محدود شده سیستم دسترسی پیدا کند که عموماً نیت مهاجم مخرب است [۲۳].

بسته به زمینه، حملات سایبری می تواند بخشی از جنگ سایبری یا تروریسم سایبری باشد. یک حمله سایبری می‌تواند توسط دولت‌ها، افراد، گروه‌ها، جوامع یا سازمان‌های مستقل به کار گرفته شود و ممکن است از یک منبع ناشناس سرچشمه بگیرد. محصولی که حمله سایبری را تسهیل می‌کند، گاهی اوقات سلاح

[5] Cyber Space

[۶] تعریف دیکشنری آکسفورد

[۷] توکل، اکبر. فصلنامه علوم و فنون نظامی. زمستان ۱۳۸۵

[8] Law Journal of Science

[9] Technology, Vol. 18, Issue 1, 2008, pp. 293-324

سایبری نامیده می‌شود. حملات سایبری در چند سال اخیر با نرخ هشداردهنده‌ای افزایش یافته است. برای مثال، بر اساس اعلام مسئولین روس، در سال ۲۰۲۲، شمار حملات سایبری علیه روسیه به میزان ۸۰ درصد افزایش یافت [۸].

در ایران نیز این حملات به‌صورت فزاینده رشد داشته است و بر اساس اعلام کارشناسان حوزه امنیت، عمده حملات سایبری صورت گرفته در ایران پس از فیشینگ، حملات DDOS، باج‌افزار و بدافزارها، بالاترین درصد حملات سایبری را تشکیل می‌دهند و همچنین «عامل نفوذی» بیشترین و پررنگ‌ترین علت این حملات شناخته می‌شود.

حمله سایبری هرگونه تلاش عامدانه برای سرقت، افشای، تغییر، غیرفعال کردن یا از بین بردن داده‌ها، برنامه‌ها یا سایر دارایی‌ها از طریق دسترسی غیرمجاز به شبکه، سیستم کامپیوتری یا دستگاه دیجیتال است که در صورت تشدید و سازماندهی دولت‌ها و گروه‌ها در حملات سایبری علیه اهداف مشترک و کشورهای هدف، این امر را جنگ سایبری گویند.

عوامل تهدید، حملات سایبری را به دلایل مختلف از دزدی کوچک گرفته تا اقدامات خصمانه و جنگی انجام می‌دهند. آن‌ها از تاکتیک‌های مختلفی مانند حملات بدافزار، کلاهبرداری و سرقت رمز عبور برای دسترسی غیرمجاز به سیستم‌های هدف خود استفاده می‌کنند [۱۶].

حملات سایبری می‌تواند موجب اختلال کسب‌وکارها و نابودی آنها شود. میانگین هزینه خسارت نفوذ و دسترسی به داده‌ها ۳۵.۴ میلیون دلار است[۱۰]. اما برخی از حملات سایبری می‌توانند بسیار پرهزینه‌تر از سایرین باشند. حملات باج‌افزاری باعث شده تا ۴۰ میلیون دلار باج پرداخت شود. کلاهبرداری‌های مربوط به ایمیل تجاری (BEC) در یک حمله ۴۷ میلیون دلار از قربانیان سرقت کرده است. حملات سایبری که اطلاعات شناسایی شخصی مشتریان (PII) را به خطر می‌اندازد، می‌تواند منجر به از دست دادن اعتماد مشتری، جریمه‌های نظارتی و حتی اقدامات قانونی شود. طبق یک برآورد، جرایم سایبری تا سال ۲۰۲۵ سالانه ۵.۱۰ تریلیون دلار برای اقتصاد جهان هزینه خواهد داشت [۱۶].

۳ اِعمال قوانین حقوق بین‌الملل در حوزه فضای مجازی

با استثنائات معدودی (به‌ویژه کنوانسیون بوداپست در مورد جرایم سایبری و کنوانسیون اتحادیه آفریقا که هنوز در مورد امنیت سایبری و حفاظت از داده‌های شخصی اجرا نشده است)، قوانین بین‌الملل برای تنظیم فضای سایبری قوانین خاصی ندارد. علاوه بر آن، این فناوری هم جدید و هم پویا است؛ بنابراین، برای چندین سال، سؤالات باز وجود داشت که آیا قوانین بین‌المللی موجود اصلاً در مورد فضای سایبری اعمال می‌شود یا خیر؟

امروزه، اکثر کشورها و چندین سازمان بین‌المللی، از جمله کمیته اول مجمع‌عمومی سازمان ملل متحد در

[۱۰] این برچسب قیمت شامل هزینه‌های کشف و پاسخ به تخلف، خرابی و درآمد از دست‌رفته و آسیب بلندمدت به یک کسب‌وکار و برند آن می‌شود.

مورد خلع سلاح و امنیت بین‌المللی، G ۲۰، اتحادیه اروپا، آسه‌آن[۱۱] و سازمان کشورهای آمریکایی (OAS)[۱۲] تأیید کرده‌اند که قوانین بین‌المللی موجود برای استفاده از فناوری اطلاعات و ارتباطات (فضای سایبر) اِعمال شود. با این حال، در طول دهه گذشته، کشورها و ایالات متعددی در این زمینه شروع به مذاکره و گفت‌وگو کردند.

بر اساس بررسی صورت گرفته، به‌صورت رسمی، حملات سایبری از ابتدای ۲۰۰۰ خودنمایی کرد. در این سال‌ها، حملات سطحی و قابل توجه نبودند تا اینکه در سال‌های ۲۰۰۸، ۲۰۱۰[۱۳] و ۲۰۱۳ حملات سایبری با نام‌های استاکس‌نت و کانفیکر[۱۴]، Worm ۲۰۰۸، سال ۲۰۱۱ شبکه پلی‌استیشن سونی و Spamhaus[۱۵] ۲۰۱۳ سطحی جدی‌تر را به سیاست‌گذاران و حقوق‌دانان ارائه نمودند.

پژوهشگر معتقد است که سال ۲۰۱۰ را می‌توان نقطه عطفی در حوزه حقوق بین‌الملل معرفی کرد. تا قبل از این تاریخ، عمده تهاجمات سایبری به لحاظ خسارت محدود بوده؛ اما در این سال، حمله سایبری خصمانه علیه زیرساخت‌های هسته‌ای ایران از طریق ویروسی بنام استاکس‌نت صورت گرفت.

تقریباً از آغاز سال ۲۰۱۲، برخی کشورها شروع به ارائه دیدگاه‌های خود در مجموعه‌ای از سخنرانی‌ها و بیانیه‌ها کردند. در سال ۲۰۱۸، دادستان کل بریتانیا بیانیه مهمی از دیدگاه‌های این کشور ارائه کرد.

در سال‌های بعد، کشورهای دیگر (عمدتاً اروپایی) شروع به ارائه دیدگاه‌های دقیق خود کردند؛ از جمله استرالیا، استونی، فنلاند، فرانسه، آلمان و هلند. تلاش‌های جاری در سازمان ملل و در زمینه‌های منطقه‌ای مانند OAS اکنون به دنبال گسترش فهرست کشورهای دارای نظرات حقوق بین‌الملل در فضای سایبری است. با این حال، هنوز اکثریت قریب به‌اتفاق دولت‌ها سکوت کرده‌اند.

اینکه چرا این کشورها سکوت می‌کنند، اغلب نامشخص است. برخی ممکن است بخواهند از گرفتار شدن در مناقشات بین‌المللی در بین کشورهایی که صحبت کرده‌اند، اجتناب کنند. با این حال، برای دیگران، ممکن است موضوع مربوط به اهلیت قانونی باشد. بسیاری از کشورها فاقد پرسنل یا منابع لازم برای درک مسائل مربوط به اعمال قوانین بین‌المللی در فضای سایبری هستند؛ بنابراین، یک مسئله آغازین برای اعمال حقوق بین‌الملل، ایجاد ظرفیت قانونی کافی برای همه دولت‌ها است تا در شکل‌دهی آنچه که حقوق بین‌الملل در مورد مسائل سایبری می‌گوید، نظر داشته باشد.

۱.۳ اختلاف‌نظرها در حوزه فضای سایبر

در میان آن دسته از کشورهایی که در مورد اعمال قوانین بین‌الملل در فضای سایبری موضع‌گیری کرده‌اند، تعدادی اختلافات «وجودی» وجود دارد؛ ادعاهای رقابتی مبنی بر اینکه یک قاعده یا رژیم حقوقی بین‌المللی به طور کامل شامل یا حذف شده است. به‌عنوان مثال، در چارچوب سازمان ملل، چند کشور در دسترس بودن حقوق بشردوستانه بین‌المللی، حق دفاع از خود، وظیفه احتیاط لازم، و حق اتخاذ اقدامات متقابل با

[۱۱] Association of Southeast Asian Nations (اتحادیه کشورهای جنوب شرق آسیا که بیشتر با نام اختصاری آسه‌آن)
[۱۲] همه کشورهای مستقل قاره آمریکا (۳۵ کشور) عضو سازمان کشورهای آمریکایی هستند.
[۱۳] حمله استاکس‌نت به زیرساخت‌های هسته‌ای ایران
[۱۴] یک کرم رایانه‌ای است که از اکتبر سال ۲۰۰۸ ظاهر شد و سیستم‌های عامل ویندوز را مورد هدف قرار داد.
[۱۵] کمپانی Spamhaus متهم است که منبع اصلی تولید اسپم و توزیع آن در سرویس‌دهنده اینترنتی در جهان است.

توجه به فعالیت‌های آنلاین را به چالش کشیده‌اند.

وجود (یا عدم وجود) یک یا چند مورد از این چارچوب‌های قانونی در فضای سایبری، پیامدهای قابل توجهی برای اعمال قوانین بین‌المللی دارد که بر نحوه انجام عملیات سایبری دولت‌ها در درگیری‌های مسلحانه، توانایی آنها برای پاسخ به فعالیت‌های سایبری مخرب انجام شده توسط سایر کشورها و اقداماتی که آنها باید برای محافظت از حقوق کشورهای ثالث در برابر آسیب‌های ناشی از قلمرو خود انجام دهند.

حتی در مواردی که دولت‌ها می‌پذیرند که یک قاعده یا رژیم حقوقی بین‌المللی خاص در فضای سایبری اعمال می‌شود، سؤالات تفسیری اساسی اغلب برای بحث باقی می‌مانند. رژیم‌های حقوقی بین‌المللی مانند عدم مداخله، حاکمیت و حقوق بشر در کاربردهای خود در فضای مجازی با ابهامات زیادی مواجه هستند.

برای مثال، وظیفه عدم مداخله، از امور بین‌المللی و خارجی دولت‌ها در برابر مداخله «اجباری» سایر کشورها محافظت می‌کند.

با این حال، هیچ اتفاق‌نظری در مورد اینکه این وظیفه از «امور» محافظت می‌کند، وجود ندارد، چه رسد به اینکه چه چیزی اجبار را از فعالیت سایبری غیر اجباری متمایز می‌کند. به همین ترتیب، حاکمیت بدون شک یکی از ویژگی‌های اصلی معماری نظم حقوقی بین‌المللی است. با این حال، به نظر می‌رسد که کشورها در مورد اینکه آیا حاکمیت صرفاً یک اصل اساسی است که سایر قواعد حقوقی بین‌المللی (مانند عدم مداخله) بر آن استوار است یا اینکه یک قاعده مستقل است که می‌تواند مستقیماً توسط برخی عملیات سایبری دولت‌های خارجی نقض شود، اختلاف نظر دارند.

۲.۳ انتساب در حملات سایبری

انتساب سایبری، فرایند ردیابی، شناسایی و مقصر دانستن عامل حمله سایبری یا سایر سوءاستفاده‌های هکری است و اثبات این امر می‌تواند بسیار دشوار باشد؛ زیرا معماری زیربنایی اینترنت، راه‌های متعددی را برای مهاجمان ارائه می‌دهد تا ردهای خود را پنهان کنند. شرکت‌ها اغلب فاقد منابع یا تخصص مورد نیاز برای ردیابی مجرمان سایبری هستند؛ بنابراین سازمان‌هایی که نیاز به اسناد سایبری دارند، معمولاً کارشناسان امنیت اطلاعات خارجی را استخدام می‌کنند. با این حال، انتساب سایبری می‌تواند چالش‌برانگیز باشد، حتی برای کارشناسان امنیت سایبری [۲۰].

۱.۲.۳ تکنیک‌های انتساب در حملات سایبری

محققین جرایم سایبری تکنیک‌های تخصصی و متفاوت زیادی برای انجام اسناد سایبری در دسترس دارند، اما انتساب قطعی و دقیق سایبری همیشه امکان‌پذیر نیست. محققان از ابزارهای تجزیه‌وتحلیل، اسکریپت‌ها و برنامه‌ها برای کشف اطلاعات مهم در مورد حملات استفاده می‌کنند.

محققان جرایم سایبری اغلب قادر به کشف اطلاعات مربوط به زبان برنامه‌نویسی و اطلاعات مربوط به آن، از جمله کامپایلر مورد استفاده، زمان کامپایل، کتابخانه‌های مورد استفاده و ترتیب اجرای رویدادهای مربوط به یک حمله سایبری هستند. به‌عنوان مثال، اگر محققین بتوانند تشخیص دهند که یک بدافزار با استفاده از صفحه‌کلید چینی، روسی یا زبان‌های دیگر نوشته شده است، این اطلاعات می‌تواند به محدود کردن

مظنونان برای انتساب سایبری کمک کند. محققینی که تلاش می‌کنند انتساب حمله سایبری را انجام دهند، هر ابرداده مرتبط با حمله را نیز تجزیه‌وتحلیل می‌کنند. ابرداده‌ها، از جمله آدرس‌های IP منبع، داده‌های ایمیل، پلتفرم‌های میزبانی، نام‌های دامنه، اطلاعات ثبت‌نام دامنه و داده‌های منابع شخص ثالث، می‌توانند به ایجاد انتساب کمک کنند؛ زیرا سیستم‌های مورد استفاده برای حملات سایبری اغلب با گره‌های خارج از شبکه مورد هدف ارتباط برقرار می‌کنند. با این حال، این نقاط داده را نیز می‌توان به‌راحتی جعل کرد.

محققان همچنین ممکن است ابرداده‌های جمع‌آوری‌شده از حملات متعددی را که سازمان‌های مختلف را هدف قرار می‌دهند، تجزیه‌وتحلیل کنند. انجام این کار، کارشناسان را قادر می‌سازد تا بر اساس تکرار داده‌های جعلی که شناسایی می‌کنند، برخی مفروضات و ادعاها را انجام دهند. به‌عنوان مثال، متخصصان امنیتی ممکن است بتوانند یک آدرس ایمیل ناشناس را از یک حمله ردیابی کنند و آن را بر اساس نام‌های دامنه استفاده شده در حمله که قبلاً توسط یک عامل تهدید خاص مورد استفاده قرار گرفته بودند، به مهاجم پیوند دهند. رویکرد دیگر برای محققان، بررسی تکنیک‌ها، رویه‌ها و تاکتیک‌های مورد استفاده در حمله است؛ زیرا مهاجمان سایبری اغلب سبک‌های متمایز و قابل‌تشخیص خود را دارند. محققان گاهی اوقات قادر به شناسایی عاملان بر اساس سرنخ‌های مربوط به روش‌های حمله، مانند تاکتیک‌های مهندسی اجتماعی یا استفاده مجدد از بدافزارهای مورد استفاده در حملات قبلی هستند.

دانستن آنچه در صنایع خاص یا شرکت‌های خاص اتفاق می‌افتد نیز می‌تواند به بازرسان جرایم سایبری در پیش‌بینی حملات کمک کند. به‌عنوان مثال، شرکت‌های صنعت گاز طبیعی زمانی که قیمت گاز افزایش می‌یابد، پول بیشتری را صرف اکتشاف می‌کنند و در نتیجه در معرض خطر بیشتری برای سرقت داده‌های مکانی قرار می‌گیرند. درک انگیزه‌های مهاجم همچنین می‌تواند به اسناد سایبری کمک کند. کارشناسان امنیتی برای درک اهداف مجرمان تلاش می‌کنند؛ زیرا همیشه به پول مربوط نمی‌شود. هدف بازرسان این است که بفهمند آیا مجرمان سایبری فقط در کمین هستند یا برای مدت طولانی جاسوسی کرده‌اند. آنها همچنین سعی می‌کنند کشف کنند که آیا هکرها در طول حملات خود به دنبال داده‌های خاصی هستند یا خیر و چگونه سعی می‌کنند از آنچه پیدا می‌کنند استفاده کنند.

اگرچه انتساب سایبری یک علم دقیق نیست، اما این تکنیک‌های انتساب می‌تواند به بازرسان جرایم سایبری کمک کند تا مهاجمان را بدون تردید معقول شناسایی کنند [۲۰].

حقوق بین‌الملل فقط موضوعات حقوق بین‌الملل خود را تنظیم می‌کند. معمولاً رفتار شرکت‌ها یا افراد ICT (که معمولاً مشمول یک یا چند دستور قانونی داخلی هستند) هدایت نمی‌شود. بنابراین، برای اعمال قوانین بین‌المللی در فضای سایبری، شناخت هویت هر کسی که مسئولیت فعالیت مورد نظر را بر عهده دارد، ضروری است: آیا این یک دولت یا بازیگر تحت حمایت دولت است که مشمول حقوق بین‌الملل است یا یک فرد یا افراد درگیر رفتار است. خارج از محدوده حقوق بین‌الملل؟ با این حال، با توجه به چالش‌های شناخته شده در اسناد فنی، چنین شناسایی‌هایی در فضای سایبری دشوار است – شناسایی منشأ رفتار سایبری مخرب اغلب دشوار و زمان‌بر است. علاوه بر این، در جایی که دولت‌ها از پروکسی استفاده می‌کنند، انتساب به دلیل نیاز به نشان‌دادن شواهدی مبنی بر «کنترل» دولت بر بازیگر نیابتی پیچیده‌تر می‌شود (قوانین بین‌المللی هنوز به طور کامل تعیین نکرده است که چه مقدار کنترل موردنیاز است یا چه شواهدی باید برای اثبات آن

نشان داده شود).

اصول مسئولیت دولت بابت اعمال متخلفانه بین‌المللی ابتدا توسط دیوان دائمی دادگستری در قضیه لوتوس بیان شد[۱۶]. دیوان در این قضیه بیان داشت که حقوق بین‌الملل قاعده مسئولیت دولت برای نقض تعهدات وظایف بین‌المللی و جبران خسارت حاصله از آن را تأیید می‌نماید[۱۷]. در حال حاضر، طرح پیش‌نویس مسئولیت بین‌المللی دولت‌ها حاکم بر چارچوب حقوقی مسئولیت بین‌المللی دولت‌ها است [۱۸]. ماده ۳ طرح مسئولیت دولت‌ها به‌تفصیل در خصوص عناصر فعل متخلفانه بین‌المللی دولت صحبت کرده است.

یک رفتار زمانی می‌تواند متخلفانه محسوب شود که نقض یک تعهد بین‌المللی بوده و در عین حال به دولت قابل‌انتساب باشد. اصطلاح نقض تعهد بین‌المللی پیش از این در قضیه بارسلونا تراکشن توسط دیوان بین‌المللی دادگستری بیان شده بود[۱۹].

۲.۲.۳ قابلیت انتساب حمله سایبری به دولت

انتساب یک حمله سایبری به یک دولت، عنصر کلیدی در ساخت یک رژیم حقوق کارا در کاهش این نوع حملات است. در حوزه قواعد حاکم بر مسئولیت بین‌المللی دولت‌ها همیشه یکی از سؤالات بنیادی این است که افراد، گروه‌ها و مجموعه‌های حمله‌کننده به دولت وابسته‌اند و بایستی این وابستگی اثبات شود تا مسئولیت بین‌المللی نسبت به دولت‌ها شکل گیرد.

بی شک دولت‌ها برای تهاجم سایری مجبور به استفاده از گروه‌ها و افراد وابسته هستند و در این شرایط دولت‌های مهاجم تمام تلاش خود را برای پنهان نمودن خطوط و روابط خود با گروه‌های اجیر شده بکار خواهند بست و این امر، اثبات ارتباط حمله سایبری به دولت را دشوار خواهد کرد.

عمل متخلفانه در حقوق بین‌الملل نیز بایستی به دولت به هر طریقی نسبت داده شود وگرنه امر انتساب تخلف محقق نمی‌شود.

قاعده متداول انتساب تخلف به دولت بر اساس دکترین، عرف، رویه‌های قضایی و طرح کمیسیون حقوق بین‌الملل به افعال و اعمالی اطلاق می‌شود که توسط نهادها، اشخاص و سازمان‌های وابسته به دولت مهاجم یا انجام اعمال متخلفانه با هدایت، سازماندهی، تحریک، کنترل و ... آن دولت صورت‌گرفته و قابل‌انتساب باشد.

از این عبارت برمی‌آید که اصولاً حقوق حاکم بر مسئولیت دولت مبتنی بر نظریه نمایندگی است.

پس در راستای انتساب مسئولیت یک رفتار متخلفانه که بین‌المللی به دولت می‌بایست تعیین سازیم که آیا شخص در ارتکاب آن رفتار به نمایندگی از یک اعمال دولت محسوب می‌شود.

بنا بر موارد ذکر شده باید اذعان داشت که اصل بنیادین و حاکم بر مسئولیت بین‌المللی دولت‌ها، موید و اثبات‌کننده انتساب رفتار، اعمال و اقدامات خرابکارانه اشخاص، گروه‌ها و نهادها به دولت‌ها نیست مگر بر اساس ماده ۸ طرح مسئولیت بین‌المللی دولت‌ها و تفسیر دادگاه، افراد، اشخاص و گروه‌ها و ... به دستور، هدایت، یا تحت کنترل دولت مهاجم دست به اقدامات خصمانه زده باشند.

[16] PCIJ, 1927, PCIJ Reports, Series A, No. 10
[17] PCIJ, 1927, PCIJ Reports, Series
[18] http://www.ilsa.org/jessup/jessup06/basicmats2/DASR.pdf
[19] Belgium v. Spain, 1970, ICJ, Reports, para 174

بدیهی است که تفسیر و صدور این حکم به دادگاه‌ها واگذار شده است. به طور خلاصه باید اشاره داشت که تاکنون دو ضابطه در خصوص نحوه انتساب رفتار ارگان‌های غیردولتی به دولت‌ها توسط رویه قضایی بین‌المللی مورد شناسایی واقع شده است. این دو مورد عبارت‌اند از: کنترل مؤثر و کنترل کلی.

از سوی دیگر جدای از مباحث پیرامون کنترل دولت، در باب مسئولیت دولت از بابت اعمال افراد خصوصی عنوان شده که مسئولیت دولت نه‌تنها می‌تواند برخاسته از فعل او باشد، بلکه ناشی از ترک فعلش هم می‌تواند باشد؛ بنابراین، دولتی که از وظیفه پیشگیری از این که فعالیت‌های انجام شده در سرزمینش موجب ورود صدمه به دولت دیگر نشود، تخلف کرده و مسئول نقض تعهدات خویش است.

۳.۳ ضرورت اجماع برای اِعمال حقوق بین‌الملل در حوزه سایبری

تا به امروز، قوی‌ترین مجامع برای رسیدگی به کاربرد حقوق بین‌الملل، غیردولتی هستند. حاکمیت اینترنت شامل یک فرایند چندجانبه است و بازیگران غیردولتی مانند گروه‌های مستقل کارشناسان که کتاب‌های راهنمای تالین را تهیه کردند، بر گفتمان در مورد چگونگی تنظیم قوانین بین‌المللی عملیات سایبری دولت تسلط دارند. مانند سه بیانیه اخیر آکسفورد که توسط وکلای بین‌المللی در مورد ممنوعیت‌ها و حمایت‌های قانون در قبال بخش مراقبت‌های بهداشتی و تحقیقات واکسن در بحبوحه همه‌گیری کووید-۱۹ و همچنین مداخله خارجی در انتخابات ریاست‌جمهوری ۲۰۲۰ آمریکا پیش از این ارائه شده است، چنین تلاش‌هایی ممکن است همچنان ادامه داشته باشد.

در عین حال، تلاش‌های کشورهای عضو سازمان ملل متحد برای رسیدگی به قوانین بین‌الملل که در مورد مسائل مربوط به سایبری ICT اعمال می‌شود، چند برابر شده است.

فراتر از ساختار اصلی گروه کارشناسان دولتی سازمان ملل، فرایندهای سازمان ملل اکنون شامل یک گروه کاری با پایان باز در کمیته اول مجمع‌عمومی سازمان ملل و همچنین یک فرایند کمیته سوم در مورد کنوانسیون جرایم سایبری سازمان ملل است. با این حال، این یک نتیجه قطعی نیست که سازمان ملل متحد تنها محل فرود برای شکل دادن به بحث‌ها در مورد چگونگی اعمال قوانین بین‌المللی باشد.

سازمان‌های منطقه‌ای (مانند اتحادیه اروپا) ممکن است جایگزینی ارائه دهند که در برخی موارد می‌تواند از جنبه‌های خاصی از ژئوپلیتیک که بر گفتمان سازمان ملل تسلط دارد، اجتناب کند. سایر فرایندهای چند ذی‌نفعی موجود یا آتی نیز ممکن است این کار را به خود اختصاص دهند. به طور خلاصه، حتی زمانی که دولت‌ها از محدودیت اولیه خود برای رسیدگی به کاربرد قوانین بین‌الملل در (و به) رفتارهای بازیگران مختلف در فضای سایبری عبور می‌کنند، پیامدهای صداهای جدید در اشکال و مجامع مختلف توجه را افزایش می‌دهد. کشورها و سایر ذی‌نفعان باید با دقت مسائل و بازیگران مختلف درگیر را با نگاهی به تصویر کلان ردیابی کنند و ببینند آیا قوانین بین‌المللی می‌تواند بیش از اعمال ساده در زمینه‌های سایبری انجام دهد. سؤال اصلی این است که آیا می‌تواند این کار را به روش‌هایی انجام دهد که در تنظیم رفتار دولت‌ها و سایر بازیگران بین‌المللی مؤثر باشد؟

۴ مسئولیت دولت‌ها برای نقض تعهدات بین‌المللی از رهگذر حملات سایبری

مسئله مسئولیت دولت یکی از قدیمی‌ترین مسائل حقوق بین‌الملل است که ابتدائاً برای حمایت از بیگانگان مدنظر قرار گرفت و توسعه یافت و سپس در رابطه دولت با دولت مطرح شد. خاستگاه این اصل در رویه قضایی به رأی دیوان دائمی دادگستری در قضیه کارخانه کروزوف برمی‌گردد. دیوان در این قضیه اعلام کرد: یک تعهد کلی برای دولت‌ها وجود دارد که در برابر هر نقض تعهد جبران خسارت داشته باشند. از نظر دیوان، مسئله جبران خسارت یک جزء لاینفک ناشی از رفتار خلاف یک دولت است و لذا نیازی به ذکر آن در کنوانسیون نیست[۲۰].

همین موضوع در قضیه کانال کورفو نیز مورد تأیید قرار گرفت.

۱.۴ حمله سایبری و منع اصل توسل به زور

ممنوعیت توسل به زور مندرج در بند چهارم ماده ۲ منشور سازمان ملل متحد عنوان شده است: کشورهای عضو سازمان ملل متحد در روابط با کشورهای دیگر حق استفاده از تهدید و توسل زور با هدف خدشه به تمامیت ارضی / سرزمینی، استقلال سیاسی و هرگونه رفتار خلاف مشی منشور را ندارند.

به اذعان دیوان بین‌المللی دادگستری در قضیه فعالیت‌های مسلحانه در قلمرو کنگو سنگ بنای منشور ملل متحد است. بااین‌وجود تعریف دقیق توسل به زور و این که چه اعمالی توسل به زور تلقی می‌شوند، مشخص نیست[۲۱]. منشور و هیچ یک از اسناد بین‌المللی دیگر به این مسئله نپرداخته است که این خود باعث نوعی سردرگمی می‌شود و ما به دنبال تسری ممنوعیت توسل به زور به فضای سایبر و حملات طراحی شده از این فضا هستیم. در این راستا، دیدگاه‌های پیرامون معنای زور و هدف و مفهوم متداول طرح چنین ممنوعیتی در منشور مورد بررسی قرار می‌گیرد. معنای زور در بند ۴ ماده ۲ منشور ملل متحد مبنای حقوقی نوین ممنوعیت ۲ منشور آغاز می‌شود (میثاق جامعه ملل و پیمان ۱۹۲۸ بریان کلوگ بین وزرای امور خارجه ایالات متحده انگلستان و آمریکا).

توسل به زور با ماده (۴ هم متضمن اصل منع توسل به زور بودند، اما با وقوع جنگ دوم جهانی دولت‌ها به این نتیجه رسیدند که این اسناد برای جلوگیری از توسل به زور کافی نبوده است.) ممنوعیت توسل به زور همان‌گونه که دیوان دادگستری بین‌المللی در قضیه فعالیت‌های نظامی و شبه‌نظامی در نیکاراگوئه بیان داشته، برای اعضای سازمان ملل متحد به دلیل آمره بودن این اصل و ویژگی معاهداتی منشور الزام‌آور است و در عین حال برای کشورهای غیر عضو هم بر این مبنا که بیانگر قاعده عرفی حقوق بین‌الملل است، لازم‌الاجرا است.ل منع توسل به زور بودند، اما با وقوع جنگ دوم جهانی دولت‌ها به این نتیجه رسیدند که این اسناد برای جلوگیری از توسل به زور کافی نبوده است.) ممنوعیت توسل به زور همان‌گونه که دیوان دادگستری بین‌المللی در قضیه فعالیت‌های نظامی و شبه‌نظامی در نیکاراگوئه بیان داشته، برای اعضای سازمان ملل

[20] http://www.worldcourts.com/pcij/eng/decisions/1928.09.13Corfo Channel Case,UK V. Albania
[21] (Congo v.Oganda), 2005, I.C.J. Reports 2005, p. 82, para 14

متحد به دلیل آمره بودن این اصل و ویژگی معاهداتی منشور الزام‌آور است و در عین حال برای کشورهای غیر عضو هم بر این مبنا که بیانگر قاعده عرفی حقوق بین‌الملل است، لازم‌الاجرا است[۲۲].

۲.۴ حمله سایبری به‌عنوان تجاوز یا حمله مسلحانه

حقوق بین‌الملل معاصر توسل به زور بین دولت‌ها را جز در مورد مجوز شورای امنیت و دفاع مشروع منع می‌کند[۲۳]. بنابراین، نقض بند ۴ ماده ۲ عملی غیرقانونی است. این که چه اعمالی نقض بند ۴ ماده ۲ محسوب می‌شود، مشخص نیست و عبارت حمله مسلحانه و تجاوز که در منشور بیان شده، قطعاً ناقض منشور محسوب می‌شوند.

در منشور ملل به عمل تجاوز[۲۴] رویکرد غیرکیفری نگریسته شده و احراز و تشخیص تجاوز به‌موجب ماده ۳۹، در صورت وقوع واقعه نظامی میان دو کشور یا بیشتر به عهده شورای امنیت گذاشته شده است. در سال ۱۹۷۴، مجمع‌عمومی قطعنامه ۳۳۱۴ را با اجماع و به‌منظور رفع خلأ حقوقی موجود در تعریف تجاوز تصویب نمود که هر چند فاقد ضمانت اجرایی بوده، ولی به‌عنوان راهنما برای شورای امنیت قابل استفاده می‌باشد.

این قطعنامه اولاً تجاوز را محدود به توسل به زور سنتی استفاده کرده و در نهایت بر مفاهیم سنتی تمامیت سرزمینی تکیه دارد. ماده ۱ قطعنامه ۳۳۱۴ در تعریف تجاوز آورده است: به‌کارگیری نیروهای نظامی وابسته به کشورها علیه آن حکومت، تمامیت سرزمینی یا ثبات سیاسی کشور هدف و یا به‌کارگیری سایر راه‌های مغایر اهداف ملل متحد است.

قسمت آخر ماده ۱ اشاره به اشکال نظامی توسل به زور در ماده ۳ قطعنامه کرده و تمامی آنها را تجاوز محسوب می‌نماید.

ماده ۳ قطعنامه هم با ذکر مصادیق، تعریف ماده ۱ را تکمیل می‌کند. آن مصادیق عبارت‌اند از: تهاجم با ورود نیروهای ارتشی و اشغال پس از آن که خود تا هر زمان ادامه یابد، نیز ضمیمه کردن خاک یک کشور حتی بدون درگیری نظامی، بمباران و فرو فرستادن موشک (بدون حضور نیروی انسانی)، محاصره دریایی، حمله در خارج از سرزمین، مثلاً به نیروهای نظامی یا ناوگان غیرنظامی دریایی و هوایی در دریا یا هوا، بیرون نرفتن نیروهای نظامی پس از ختم قرارداد از خاک یک کشور یا تعهدات آنها در مدت قرارداد، معاونت دولت ثالث برای عبور از سرزمین او و بالاخره تجاوز غیرمستقیم از طریق اعزام نیروهای نامنظم نظامی به خاک کشور دیگر.

ماده ۴ قطعنامه از تمثیلی بودن فهرست بالا صحبت کرده و اختیار تعیین سایر اعمال تجاوزکارانه را به عهده شورای امنیت نهاده است. با توجه به این که مثال‌های بیان شده در قطعنامه همه حکایت از اقدامات نظامی مسلحانه سنتی دارد، جای دادن حملات سایبری در بین این دسته دشوار است، تأکیدات بالا، من جمله تأکید بر مفاهیم سنتی تمامیت ارضی و نمونه آوردن جنگ‌های تجاوزی سنتی، حاکی از آن است که قطعنامه، حمله به ساختارهای کلیدی یک دولت از طریق شبکه الکترونیکی آن را به‌عنوان تجاوز نمی‌شناسد؛

[22] Judgment of 27 June 1986 merits, para 174 & 188
[23] U.N Charter art. 2, para. 4; Arts.39 & 51
[24] http://daccess-ddsny.un.org/doc/resolution/GEN/NRO/739/16/NRO73916.pdf

زیرا که این حملات تجاوز فیزیکی به تمامیت ارضی یک دولت با توسل به ابزارهای سنتی مسلحانه محسوب نمی‌شود.

چنین برداشتی هماهنگ با کارهای مقدماتی در تصویب قطعنامه است که به روشنی حاکی از آن است که سایر عملیات خارج از محدوده تعریف شده، من جمله آن‌هایی که نتایج اقتصادی در پی دارد، نمی‌تواند به‌عنوان عمل بین‌المللی تجاوز شناخته شود. نتایج زیان‌بار توسل به سلاح‌های سنتی را در پی داشته باشد، می‌تواند دلیل قانع‌کننده‌ای برای شورای امنیت به منظور جای دادن این حملات در ماده ۳۹ منشور باشد.

۱.۲.۴ حمله سایبری به‌عنوان حمله مسلحانه

ماده ۵۱ منشور سازمان ملل مقرر می‌دارد: در صورت وقوع حمله مسلحانه علیه یکی از اعضا و کشورهای عضو سازمان ملل، هیچ یک از مقررات این منشور به حق ذاتی دفاع از خود، خواه به طور فردی و یا دسته‌جمعی و اجتماعی برای حفظ صلح و امنیت بین‌المللی، لطمه‌ای وارد نخواهد کرد تا زمانی که شورای امنیت اقدامات لازم را به عمل آورد. البته این امر بایستی با اطلاع و در میان گذاشت شورای امنیت صورت پذیرد.

بنابراین پیش‌شرط توسل به دفاع از خود مطابق ماده ۵۱ منشور، وقوع حمله مسلحانه است[۲۵]. بنابراین توسل به زورهایی که حمله مسلحانه محسوب نشوند، نمی‌توانند موجبی برای اقدام یک‌جانبه دولت در راستای دفاع مشروع مطابق ماده ۵۱ منشور باشد.

این عبارت بیانگر تمایل منشور به پاسخ‌های جمعی در مقابل اقدامات فردی است[۲۶]. در خصوص حملات سایبری هم به واسطه مشکلاتی که دولت‌ها در تعیین منشأ حملات خواهند داشت، این رویکرد محتاطانه‌تر است و برای ارتباط این امر در ادامه توضیح خواهیم داد.

۳.۴ حمله سایبری دولتی

همان‌گونه که در تعریف و اهداف حملات سایبری در بخش ابتدایی پژوهش آمده است، حملات سایبری توسط افراد و گروه‌های مختلف با اهداف مختلف صورت می‌گیرد. مواد کمیسیون حقوق بین‌الملل در خصوص مسئولیت دولت بر این اصل حقوقی استوار شده که برای انتساب مسئولیت به دولت، ارگانی که عمل متخلفانه را انجام می‌دهد، باید یک نهاد دولتی باشد؛ بنابراین قبل از آن که دولت بابت اعمال انجام شده از داخل قلمرواش مسئول تلقی شود، باید مسئولیت نیابتی‌اش ثابت شود.

۵ آیا امکان اثبات متهم و مهاجم در حملات سایبری وجود دارد؟

یکی از موضوعات مهم در حملات سایبری، اثبات منشأ حمله و فاعل حمله است. بررسی اینکه آیا این حمله از سوی دشمن یا کشور خاصی بوده یا عامل آن ویروسی رها شده در فضای سایبر باشد، چندان راحت نیست. در واقع، اثبات منشأ حمله و فاعل حمله کار سختی است؛ زیرا نیاز به همکاری بین‌المللی دارد و این همکاری

[25] American Journal of International Law, 1985, p. 405
[26] Schachter, Oscar, op. cit., p. 127

در دنیا تعریف نشده است. از همین رو، بیشتر در چنین حوادثی، بحث احتمال و گمان مطرح است[۲۷].

سال ۲۰۲۲ از نظر امنیت سایبری رکوردشکنی بود؛ زیرا جهان شاهد اولین «جنگ سایبری تمام‌عیار» به‌عنوان بخشی از درگیری روسیه و اوکراین بود. در درگیری سنتی، مهاجم مرتکب شناسایی می‌شود، جرم ثابت یا رد می‌شود و حکم صادر می‌شود که منجر به اقدامات انضباطی می‌شود. اما در فضای مجازی معمولاً مراحل اولیه است که بیشترین دردسر را ایجاد می‌کند؛ یعنی شناسایی مهاجم و اثبات اینکه حمله توسط متهم انجام شده است. در حوزه سایبری، این فرایند اولیه «اسناد» یا «انتساب سایبری» نامیده می‌شود [۱۹].

امروزه انتساب دقیق حملات سایبری یکی از بحث‌انگیزترین پیچیدگی‌ها برای پیشرفت در حکمرانی جهانی و صلح در فضای سایبری است. سؤالات و معضلات با چندین جنبه از اسناد مرتبط هستند، از حقوقی تا استراتژیک. برای بسیاری از ایالت‌ها، انتساب سایبری یک قابلیت گریزان باقی مانده است. برای دیگران، به مکانیزمی برای پیگیری بازدارندگی در برابر دشمنان تبدیل شده است. انتساب سایبری دارای پیچیدگی‌های متعددی است که موضوع را به یک ابزار ژئوپلیتیکی و راهی برای دیپلماسی بین کشورها تبدیل می‌کند. انتساب سایبری اکنون یک فرایند چندلایه است که در آن ملاحظات استراتژیک، عملیاتی، دیپلماتیک و سیاسی داخلی همپوشانی دارند. وقتی علناً توسط دولت – ملت‌ها انجام شود، انتساب «انتساب عمومی» تلقی می‌شود. در حال حاضر به طور فزاینده‌ای به‌عنوان راهی برای دولت‌ها برای ترسیم خطوط قرمز در مورد آنچه که رفتار قابل قبول در فضای مجازی است، تلقی می‌شود [۱۹].

پژوهشگر در این تحقیق با بررسی رویکرد کشورهای مختلف در دفاع و پدافند سایبری به دو مورد از اقدامات سازمان ملل و کشور امریکا پرداخته است. در سازمان ملل، حکمرانی فضای سایبری یک دستور کار مهم در دو دهه اخیر بوده است. اسناد سایبری نیز بسیار مورد توجه قرار گرفته است. در گزارش ۲۰۱۴–۲۰۱۵ گروه کارشناسان دولتی (GGE) – یک گروه بیست و پنج‌نفره در مورد پیشبرد رفتار مسئولانه دولت در فضای سایبری در زمینه امنیت بین‌المللی – همه دولت‌ها توافق کردند که در مورد حوادث سایبری، همه موارد مرتبط، اطلاعات و زمینه بزرگ‌تر رویداد، همراه با چالش‌های انتساب در محیط فناوری اطلاعات و ارتباطات (ICT) باید در نظر گرفته شود. در مارس ۲۰۲۰، کمیسیون سولاریوم فضای سایبری ایالات متحده امریکا، گزارش خود را منتشر کرد که رویکرد «بازدارندگی سایبری لایه‌ای» را برای امنیت سایبری ارائه می‌کرد. این از یک رویکرد سه‌جانبه برای دستیابی به بازدارندگی سایبری حمایت می‌کند [۱۸]:

۱. با همکاری با متحدان و هم‌پیمانان، رفتاری شکل دهید تا بر نحوه عملکرد احزاب در فضای مجازی تأثیر بگذارد (تولید هنجار، حقوق بین‌الملل، موافقت‌نامه‌ها، معاهدات و غیره).

۲. ایجاد انعطاف‌پذیری و ایمن‌سازی شبکه‌های حیاتی در فضای مجازی (دفاع سایبری).

۳. تحمیل هزینه به مجرمین با انتقام از بازیگران مخربی که از فضای مجازی برای آسیب رساندن به ایالات متحده استفاده می‌کنند (به‌عنوان مثال، انتساب سایبری، کیفرخواست، تحریم).

[۲۷] سردار جلالی. June ۳۰، ۲۰۲۰

۶ دفاع مشروع در مقابل حمله سایبری

با توجه به نوپدید بودن موضوع حملات و جنگ سایبری، هنوز در حوزه تقنینی و حقوقی خلأهایی وجود دارد. یکی از این چالش‌ها، حق دفاع مشروع کشورها در برابر حملات سایبری کشور مهاجم است. در اینجا سؤال مطرح می‌شود که آیا حمله سایبری علیه زیرساخت‌های هسته‌ای، بانکی، انرژی و... یک کشور که موجب ایجاد خسارت گسترده می‌شود را می‌توان به‌مثابه حمله مسلحانه قلمداد کرد؟

بی شک این سؤال جای تأمل و بررسی بیشتری دارد.

یک کشور ممکن است به یک عملیات سایبری که واجد شرایط «حمله مسلحانه» است، مطابق با حق مرسوم دفاع از خود، همان‌طور که در ماده ۵۱ منشور سازمان ملل متحد تدوین شده است، با قدرت پاسخ دهد. بیشتر مفسران تنها استفاده‌های شدید از زور را – معمولاً مواردی که باعث کشتن یا زخمی شدن افراد یا آسیب یا تخریب اموال می‌شود – به‌عنوان حملات مسلحانه در نظر می‌گیرند [۱۷].

ایالات متحده امریکا نیز به استناد ماده ۵۱ منشور، در اسناد حقوق بین‌الملل خود اعلام کرده است در شرایط خاصی، فعالیت‌های سایبری می‌تواند با یک حمله مسلحانه واقعی یا قریب‌الوقوع قیاس شود که در این صورت، حق ذاتی یک دولت برای دفاع از خود ایجاد می‌شود. این در حالی است که تفاوتی بین دولتی و غیردولتی بودن مهاجم وجود ندارد. حق ذاتی یک دولت برای دفاع از خود که در ماده ۵۱ منشور ملل متحد به رسمیت شناخته شده است، ممکن است در شرایط خاصی توسط فعالیت‌های سایبری که به یک حمله مسلحانه واقعی یا قریب‌الوقوع می‌رسد، ایجاد شود [۲۴].

حقوق‌دانان معتقدند هرگونه تفسیری در دفاع مشروع در حملات سایبری باید به منشور سازمان ملل و هدف آن که جلوگیری از تشدید فعالیت‌های مسلحانه است، احترام بگذارند. این بدان معنا است که تمایز بین حمله مسلحانه به‌عنوان نقض جدی منشور، از یک سو، و هرگونه استفاده کمتر از زور، از سوی دیگر، حفظ می‌شود.

به همین ترتیب، شرایط اعمال حق دفاع مشروع در فضای سایبری مانند استفاده از سلاح‌های مسلحانه اعمال می‌شود. اگر حمله سایبری قابل مقایسه با یک حمله مسلحانه باشد و بتوان آن را به یک کشور خاص نسبت داد، حق دفاع از خود به وجود می‌آید. در عین حال، استفاده از زور باید با حمله صورت گرفته تناسب داشته باشد [۱۳].

ماده ۵۱ منشور سازمان ملل متحد [۲۸] مقرر می‌دارد: در صورت حمله مسلحانه علیه یک عضو سازمان ملل متحد، تا زمانی که شورای امنیت اقدامات لازم را برای حفظ صلح و امنیت بین‌المللی به عمل آورد، هیچ یک از این منشور به حق دفاع مشروع انفرادی یا دسته‌جمعی اعضا لطمه‌ای وارد نخواهد کرد. اعضا باید اقداماتی را که در اعمال این حق دفاع از خود به عمل می‌آورند، فوری به شورای امنیت گزارش دهند.

[۲۸] ماده ۵۱ منشور سازمان ملل متحد: اگر یک عضو ملل متحد مورد تجاوز مسلحانه واقع شود، هیچ یک از مقررات این منشور به حق طبیعی دفاع مشروع انفرادی یا اجتماعی تا موقعی که شورای امنیت اقدام لازم برای حفظ صلح و امنیت بین‌المللی به عمل آورد، لطمه وارد نخواهد آورد. اقداماتی را که اعضاء برای اجرای حق دفاع مشروع به عمل می‌آورند، باید فوراً به شورای امنیت اطلاع دهند، ولی این اقدامات به هیچ وجه در اختیارات و وظایفی که شورا بر طبق‌این منشور دارد و به موجب آنها در هر موقع روشی را که برای حفظ و یا اعاده صلح و امنیت بین‌المللی لازم می‌داند می‌توانند اتخاذ کند تأثیری نخواهد داشت.

حقوق بین‌الملل و قوانین مرتبط با آن، اجازه حمله به دیگر کشورها را سلب می‌کند و این یک قانون کلی است و کشورهایی که منشور سازمان ملل را امضا کرده‌اند، به این امر متعهد خواهند بود و خود را ملزم به رعایت این امر می‌دانند. در صورتی که کشوری علیه یک کشور حمله سایبری انجام داده باشد، شرایط استثنایی به وجود می‌آید.

در این شرایط کشور مورد تهاجم بایستی بر اساس فناوری‌های پیچیده فنی، با ردیابی محل و مکان مدیریت، فرماندهی حمله و... بتواند مسئولیت حمله را به کشور ثالث منتسب کند و سپس با توجیه فنی و حقوقی، موضوع دفاع مشروع خود را از طریق حمله سایبری توجیه نماید.

در این شرایط کشور آغازکننده وضعیت متفاوتی نسبت به کشور صدمه‌دیده دارد. برای مثال، کشور آغازکننده آمادگی دفاع در سطح حمله سایبری ابتدایی را دارا است و احتمال از پای درآمدن در برابر حمله سایبری در همان سطح بعید به نظر می‌رسد. از سوی دیگر، با توجه به محتمل دانستن دریافت پاسخ، سعی می‌کنند تا سیستم‌های خود را از طرق مختلف امن کنند. این وضعیت می‌تواند از طریق ارتقای دیواره آتش، نرم‌افزارهای امنیتی، قطع ارتباط با شبکه جهانی و ... باشد؛ لذا ضد حمله در قوانین حقوق بین‌الملل شرایط سختی دارد[۲۹] و ضد حمله‌ای که از معیارهای حقوقی تجاوز نماید، در حقوق بین‌الملل، قانونی و اخلاقی نیست[۳۰].

۷ ایران و دفاع مشروع در برابر حمله سایبری

بر اساس اعلام رسمی پایگاه وابسته به دبیرخانه شورای امنیت ملی ج.ا.ایران، نیروهای مسلح جمهوری اسلامی ایران بر این باورند که یقیناً آن دسته از عملیات سایبری که منجر به خسارات مادی به اموال و یا اشخاص به‌صورت گسترده و شدید شود و یا منطقاً چنین پیامدهایی را در پی داشته باشد، به منزله استفاده از زور است.

اگر چنین عملیاتی بر زیرساخت‌های حیاتی ملی، از جمله زیرساخت‌های دفاعی – اعم از متعلق به بخش دولتی یا خصوصی – تأثیر بگذارد، باید اصل عدم استفاده از زور را نقض کند.

نیروهای مسلح جمهوری اسلامی ایران نیز بر این باورند که در صورت رسیدن به شدت عملیات سایبری علیه زیرساخت‌های حیاتی کشور در آستانه حمله مسلحانه متعارف، حق دفاع مشروع محفوظ خواهد بود [۱۰].

۸ نتیجه‌گیری

در برهه کنونی در شرایط تخاصم بین دولت‌ها، عموماً کشورها بجای لشکرکشی و حملات نظامی متداول، تلاش می‌کنند از اقداماتی علیه کشور هدف استفاده کنند تا ضمن ایجاد خسارت، افکار عمومی را از خود دور کرده و تبعات حقوقی را علیه خود تا حد امکان کاهش دهند.

[29] Gardam, 2004
[30] Fotion and Elfstrom, 1986

حملات سایبری یکی از جذاب‌ترین ابزارها برای ایجاد خسارت علیه کشورهای هدف به شمار می‌رود که در این پژوهش تلاش شد برخی از حملات سایبری در جهان و در ایران برای مخاطب ارائه گردد.

در این زمینه، کشور مهاجم پس از ضربه زدن به کشور هدف، تلاش خود را برای نفی انتساب و عمل متخلفانه می‌کند و برعکس، کشوری که مورد ضربه واقع شده است بایستی اسناد خود را برای اثبات عمل متخلفانه و انتساب آن به دولت خاص به مجامع حقوقی بین‌المللی ارائه نماید تا بتواند مسئولیت بین‌المللی دولت در قبال حملات سایبری را مشخص نماید که با توجه به روند فعلی دادرسی و همچنین سطح فناوری آشکارساز در این زمینه، بی‌شک اثبات آن کاری سخت است.

متخصصان فناوری اطلاعات نیز در این زمینه راهکارهایی دارند تا بتوانند این اثبات را در حدی انجام دهند که در این مسیر، پس از اثبات انتساب حمله سایبری به گروه یا کشور، می‌توان از مسیر سازوکارهای حقوق بین‌الملل این امر را پیگیری نمود؛ هرچند برخی کشورها ازجمله ایران به‌صورت رسمی اعلام کرده‌اند که حق دفاع مشروع در این زمینه را برای خود قائل هستند.

بر اساس بررسی پژوهشگر، مبرهن است که در خصوص دفاع و پدافند سایبری کشورهای مختلف اقدامات متعددی انجام داده‌اند؛ اما در حوزه انتساب این جرم هنوز با چالش‌هایی مواجه هستند که در تلاش‌اند با استفاده از فناوری اطلاعات بتوانند بر این چالش امنیت ملی خود فائق آیند.

سپاس‌گزاری

این مقاله تقدیم به: سربازان و جهادگران جنگ سایبری (رایانیکی) ایران عزیز و حقوق‌دانان عرصه بین‌الملل که در این عرصه به همت آنها برای مطالبه حقوق مردم ایران در برابر حملات دشمن نیاز داریم.

مراجع

[۱] فرجزاده، ح. حقوق بین‌الملل، امنیت سایبری. بازیابی از انجمن ایرانی مطالعات سازمان ملل متحد. (۱۴۰۱، ۰۶): https://unstudies.ir/iauns-forum

[۲] جلالی فراهانی، امیرحسین، تروریسم سایبری، نشریه فقه و حقوق، شماره ۱۰، ۱۳۸۵.

[۳] ضیایی، یاسر، حمایت از حقوق بشر در فضای سایبر، مجله پژوهش‌های حقوقی، شماره ۲۱، ۱۳۹۲.

[۴] زمانی، سید قاسم و ضیایی، سید یاسر، تعمیم نظام مسئولیت بین‌المللی به بازیگران غیردولتی؛ با تأکید بر مسئولیت بین‌المللی جدایی‌طلبان، مجله حقوقی بین‌المللی، ۱۳۹۱، شماره ۴۵.

[۵] سازمان ملل، نشریه بین‌المللی سیاست جنائی، ترجمه دبیرخانه شورای‌عالی انفورماتیک، سازمان برنامه و بودجه کشور، ۱۳۷۶.

[۶] علیرضا ابراهیم گل، متن و شرح مواد کمیسیون حقوق بین‌الملل در خصوص مسئولیت بین‌المللی دولت، نشر شهر دانش، ۱۳۸۸.

[۷] خبر آنلاین. (۲۰۲۱، ۱۰). بازیابی از https://www.khabaronline.ir/news/۱۵۶۷۷۴۴

[۸] فارس. (۱۴۰۱، ۱۰). www.farsnews.i. بازیابی از https://www.farsnews.ir/news/۱۴۰۱۱۰۰۷۰۰۰۴۹۶

[۹] فرجزاده، ح. (۱۴۰۱، ۰۶). حقوق بین‌الملل، امنیت سایبری. بازیابی از انجمن ایرانی مطالعات سازمان ملل متحد: https://unstudies.ir/iauns-forum

[۱۰] نور نیوز. (۲۰۲۰، ۰۸). .nournews.ir بازیابی از https://nournews.ir/En/News/۵۳۱۴۴/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat

[۱۱] کاشی نهنجی، وحیده. (۱۳۹۴). اصول اخلاقی سلاح‌های سایبری در نبرد. ره‌آورد نور، (هشت صفحه - از ۱۸ تا ۲۵).

[12] CENTER, C. S. (2015). csrc. Retrieved from https://csrc.nist.gov/glossary/term/Cyber-Attack

[13] cyberspace, I. l. (2020). Finland's national position.

[14] foxnews. (2015, 12). Retrieved from https://www.foxnews.com/politics/obama-continued-accelerated-use-of-bush-era-stuxnet-computer-attacks-on-iran

[15] Gibney, A. (Director). (2016). Zero Days [Motion Picture].

[16] ibm. (n.d.). International Business Machines. Retrieved from www.ibm.com/topics/cyber-attack

[17] ((1986)). ICJ. (Merits) [1986] ICJ Rep 14, para 95. Retrieved from https://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

[18] Jaikaran, C. (2022). Cybersecurity: Deterrence Policy. Congressional Research Service. Retrieved from https://crsreports.congress.gov/product/pdf/R/R47011

[19] Jindal, D. (2023). Geopolitics of Cyber Attribution.: vifindia.

[20] Rosencrance, Linda. (2017, October). tech target. Retrieved from https://www.techtarget.com/searchsecurity/definition/cyber-attribution

[21] spiegel. (2013, 07). Retrieved from https://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html

[22] Szoldra, P. (2016, 7). businessinsider.

[23] Testing, I. S. (2019, 3). astqb. Retrieved from https://astqb.org/assets/documents/Glossary-of-Software-Testing-Terms-v3.pdf

[24] US Department of Defense. ((June 2015)). Office of the General Counsel, Law of War Manual.