علوم اسلامی انسانی، شماره ۱۵، پاییز ۱۳۹۷، جلد دوم، ص ۸۰- ۷۰

ISSN: 2538-3671
http://www.johi.ir

مجله علمی علوم اسلامی انسانی (سال چهارم)
شماره ۱۵/ پاییز ۱۳۹۷ / ص ۸۰- ۷۰

مسئولیت بین المللی دولت ها در قبال اعمال بازیگران غیردولتی در فضای سایبر

مریم استوار[۱]

[۱] کارشناسی ارشد، حقوق بین الملل، دانشگاه آزاد اسلامی، واحد شیراز

نویسنده مسئول:
مریم استوار

چکیده

عملیات های سایبری چالش های جدیدی را در قبال چارچوب کلی و محافظه کارانه حقوق مسئولیت دولت ها مطرح می کند. یکی از این چالش ها، مساله قابلیت انتساب است که در نقطه تلاقی تکنولوژی و حقوق، قرار دارد. پیشرفت های جدیدی در قدرت تکنولوژیکی دولت ها بوجود آمده است تا بتوانند منشا حملات سایبری را از دیدگاه حقوق بین الملل شناسایی کنند. این پژوهش در مورد سه استاندارد مجزای قابلیت انتساب تحت عناوین دستورات، هدایت و کنترل بحث می کند و سپس مزایا و محدودیت های هریک را در قبال اعمال سایبری شرح می دهد. دولت ها طبق حقوق بین الملل عرفی ملزم می باشند تا مانع استفاده از زیر ساخت های سایبری شان جهت آسیب رساندن به حقوق قانونی و بین المللی دولت های دیگر شوند. این پژوهش به دنبال بررسی این مسئله است که در چه مواردی دولت ها ممکن است مسئول اعمال زیان بار بازیگران غیردولتی در فضای سایبر قلمداد شوند. به دلیل ویژگی های خاص فضای سایبر، انتساب مسئولیت ناشی از اعمال بازیگران غیردولتی در فضای سایبر سخت و دشوار است، ولی چنانچه دولت بر عملکرد آنها کنترل کلی داشته باشد، این اعمال قابل انتساب به دولت می باشند.

کلمات کلیدی: فضای سایبری، مسئولیت بین المللی، بازیگران غیردولتی، کنترل موثر، کنترل کلی.

علوم اسلامی انسانی، شماره ۱۵، پاییز ۱۳۹۷، جلد دوم، ص ۸۰- ۷۰

ISSN: 2538-3671
http://www.johi.ir

مقدمه

از سه دهه ی گذشته، فضای سایبر وارد زندگی انسانها شده و اکنون در سرتاسر جهان گسترش پیدا کرده است. اشکال جدید این فضا بیانگر آن است که در دسامبر سال ۲۰۱۷ میلادی،۵۴/۴٪ از جمعیت دنیا کاربران اینترنت هستند که از سال ۲۰۰۰ میلادی، ۱/۰۵۲٪ افزایش یافته است [۱]. فضای سایبر فضایی غیرمادی و ناملموس است که توسط رایانه ها و شبکه های رایانه ای بوجود آمده و دنیای مجازی را در کنار دنیای واقعی ایجاد کرده است. این فضا دارای گستره ای جهانی و بدون مرز، پوشیده و پنهان، ناهنجارمند و کنترل ناپذیر است و محدودیت در این فضا معنا ندارد [۲]. علیرغم مزیت ها و فرصت های موجود درفضای سایبر، این فضا منشا تهدیدات و حملاتی شده است که شامل هک کردن، جرایم سایبری و جاسوسی سایبری می باشد که برعلیه سیستم ها و شبکه های ارتباطی اینترنتی صورت می گیرد و منجر به تخریب و ازهم گسیختگی زیرساختهای ملی و حساس یک دولت می شود و خسارات قابل توجهی را به بار می آورد [۳]. در سال های اخیر حضور بازیگران غیردولتی در صحنه بین المللی افزایش یافته است. فضای سایبر محیطی وسیع برای بازیگران غیردولتی ایجاد کرده و به آنها قدرت می دهد تا مستقل از دولت ها در صحنه بین المللی اعمالی را انجام دهند. بهتر است که بگوییم هر عمل دولت، عمل اشخاصی است که طبق قانون به آن دولت نسبت داده می شود. این اعمال قابل انتساب، اعمالی هستند که یک دولت خواهان انجام آنها بطور مستقیم توسط ارگانهای رسمی خود نیست [۴]. به عبارت دیگر دولت ها تمایل دارند تا کارهای جزئی و کم اهمیت خود را به گروه ها و اشخاص خصوصی واگذار کنند و به راحتی از زیر بار مسئولیت شانه خالی کنند. در نتیجه نقض حقوق بین الملل توسط اشخاص خصوصی که به جای دولت اعمالی را انجام می دهند، ممکن است مسئولیت آن دولت را در پی داشته باشد. یکی از پایه های حقوق مسئولیت دولت ها، این اصل کلی می باشد که دولت ها طبیعتا مسئول اعمال بازیگران غیردولتی یا خصوصی که برای دولت های دیگر زیان بار می باشد، نیستند. سوالی که در اینجا قابل طرح می باشد این است که در چه مواردی دولتها می توانند مسئول اعمال زیان بار بازیگران غیردولتی در فضای سایبر شناخته شوند؟ در پاسخ می توان گفت که در صورتی که عمل آنها، یک عمل خلاف قواعد حقوق بین الملل و قابل انتساب به دولت باشد، دولت، مسئول چنین اقداماتی خواهد بود ؛ یعنی دولت می بایست کنترل موثر خود را بر یک عمل غیر قانونی ارتکابی از سوی بازیگران غیردولتی اعمال کند [۵]. اما استفاده از این دکترین در خصوص اعمال سایبری زیان بار ارتکابی از سوی بازیگران غیردولتی، مسئله ای پیچیده و غامض می باشد. به این دلیل که به منظور ایجاد یک رابطه واقعی میان دولت و بازیگر غیردولتی در فضای سایبر، می بایست آن عمل به لحاظ فنی و تکنیکی نیز قابل انتساب به دولت باشد. بازیگری که مرتکب یک عمل خلاف قواعد حقوق بین الملل شده می بایست به درستی شناسایی شود. ولی احراز این امر در فضای سایبر دشوار است. زیرا مرتکب می تواند با ارائه آدرسی اشتباه در سیستم آدرس دهی یا استفاده از شبکه های دستگاه خودکار، خود را مخفی نماید. به این ترتیب ما در این مقاله به دنبال بررسی این مسئله هستیم که تحت چه شرایطی اعمال خلاف قواعد حقوق بین الملل ارتکابی توسط یک بازیگر غیردولتی در فضای سایبر که به آستانه حمله مسلحانه نرسیده، می تواند قابل انتساب به دولت باشد. همچنین دولت زیان دیده تحت چه شرایطی می تواند در برابر این اعمال زیان بار به اقدامات متقابل متوسل شود. بدین منظور باید مسئله قابلیت انتساب و معیارهای آن مورد بررسی قرار گیرد. همچنین تعهداتی را که دولت ها می بایست در قبال این اعمال زیان باردر فضای سایبر انجام دهند، مورد تحلیل قرار خواهند گرفت.

۱. فضای سایبرو ویژگیهای آن

فضای سایبر به عنوان مجموعه تعامل های انسان ها از طریق رایانه و فن آوری های نوین ارتباطات، بدون درنظر گرفتن «زمان» و «مکان» توسط ویلیام گیبسون[۱] نویسنده داستان علمی تخیلی در کتاب «نورومونسر»[۲] در سال ۱۹۸۴ به کار برده شد. وی فضای سایبر را بازنمایی گرافیکی از داده ها از نظام های رایانه ای می داند. مفهومی که مورد نظر گیبسون بود، شاید به نوعی به هوش مصنوعی و روبوتیک نزدیک تر است تا آنچه اکنون به نام فضای سایبر شناخته می شود [۶]. یک سیستم آنلاین نمونه ای از فضای سایبر است که کاربران آن می توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند. مفهوم فضای سایبر، معطوف به فضای ساختگی و خیالی واقعیت مجازی و اینترنت است که انسان از طریق آن به فضای واقعیت مجازی وارد می شود. درواقع اینترنت دروازه فضای سایبر است، اما فضای سایبر با ویژگی هایی چون میزان و چگونگی دسترسی، راهبری، فعالیت اطلاع یابی، بالندگی و اعتماد شناخته می شود [۶]. امروزه فضای سایبر یک دنیای مجازی را در کنار دنیای واقعی

[2]-William Gibson
[3]-Neuromoncer

ISSN: 2538-3671
http://www.johi.ir

ایجاد کرده است. دنیای واقعی با خصایصی مانند جغرافیا داشتن، دارای نظام سیاسی خاص بودن، محبوس بودن، طبیعی بودن و غیره از دنیای مجازی متمایز می شود و دنیای مجازی نیز در مقابل، با ویژگی هایی مثل جهانی و فرامرزی بودن، فرا زمان بودن، غیرقابل کنترل بودن، قابل دسترس بودن همزمان و نهانی و پوشیده بودن از دنیای واقعی به طور نسبی جدا می شود. هر فردی در هر نقطه از جهان می تواند از طریق این فضا به آسانی، به جدیدترین اطلاعات دست یابد. اینترنت که بر اساس استاندارد های جهانی بوجود آمده است به هیچ فرد یا نهاد خاصی تعلق ندارد، بنابراین هیچ فرد، دولت یا موسسه تجاری مالک آن نیست. از اینرو هرکس قادر است تا از پروتکلهای شبکه ای که اینترنت روی آن قرار گرفته است، بدون محدودیت استفاده کند [۷]. نهانی بودن فضای سایبر ذهن افراد را در انتشار عقاید و اهداف خود آزاد گذاشته و فارغ از هرگونه ترس از نقض هنجارها و قوانین جاری، آنان را در به فعل رساندن خواسته های خود کاملا آزاد و اغلب غیر قابل تعقیب و شناسایی گذاشته است [۷]. همچنین غیرقابل کنترل بودن این فضا تا حدی است که حتی کوچکترین واحد گروهی اجتماع یعنی خانواده نیز توانایی کامل کنترل فرزندان خود که در این فضا مشغول فعالیت هستند را ندارد [۷]. بنابراین فضای سایبر دارای یک نظام طولی و سلسله مراتبی نیست تا بتوان از بالا بر آن اعمال نظارت نمود، بلکه در آن از نظام قدرت و کنترل، تمرکز زدایی شده و هیچ نهاد بالادستی بر آن حاکمیت ندارد که امر کنترل و ایجاد نظم را در آنجا عهده دار باشد [۷].

۲. تعریف حملات سایبری

حملات سایبری در چارچوب طیف گسترده تری از آن چه «عملیات اطلاعاتی» نامیده می شود، قرار می گیرند. عملیات اطلاعاتی که «جنگ اطلاعاتی» زیرمجموعه ای از آن است و هنگام مخاصمات مسلحانه مورد استفاده قرار می گیرد. به کارگیری منسجم توانمندی های جنگ الکترونیکی، عملیات شبکه ای رایانه ای، عملیات روانی، حیله های نظامی و عملیات هماهنگ با قابلیتهای پشتیبانی است که به منظور تاثیرگذاری، متوقف نمودن، تخریب یا سرقت اطلاعات دشمن و در عین حال پشتیبانی از فرایندهای تصمیم گیری نهادهای ملی صورت می گیرد[۸]. تاثیر حملات سایبری در زندگی واقعی در سال ۲۰۰۷ آشکار شد. در این سال هکرهای روسی با به راه انداختن یک هجوم سایبری بین المللی باعث شدند که کامپیوترهای دولتی کشور استونی به طور موقت از کار بیفتد. این کار به دلیل حرکت توهین آمیز کشور استونی در جابجایی بنای یادبود یک سرباز روسی جنگ جهانی دوم بود [۹]. در سال ۲۰۰۸ روسیه دوباره از حملات سایبری برای تکمیل نبرد فیزیکی علیه گرجستان استفاده نمود که این بار تعداد زیادی از وب سایتهای دولتی این کشور را ازکار انداخت [۱۰]. همچنین در سال ۲۰۱۰ بدافزاراستاکس نت برای اولین بار تاسیسات هسته ای نطنز را مورد حمله قرار داد و برخی احتمال می دهند که این بدافزار از لپ تاپ های کارشناسان روسی وارد سیستم های رایانه ای تاسیسات هسته ای نطنز شده باشد. اگرچه دولتی مسئولیت تهیه یا ارسال این بدافزار را به عهده نگرفته است، اما با توجه به قرائن و گمانه زنی ها بیشتر متوجه دولت آمریکاست؛ زیرا دولت و رئیس جمهور این کشور، حملات سایبری علیه جمهوری اسلامی ایران را به طور رسمی در دستور کار خود قرار داده است [۱۱].

۳. مساله قابلیت انتساب و معیارهای آن

در گذشته دولت ها در خصوص مسئولیت طرفهای مقابل در فضای سایبر هیچگونه اظهارنظری نمی کردند. در اواخر سال ۲۰۰۲ میلادی مشاور امنیتی سایبر در کاخ سفید ایالات متحده امریکا، ریچاردکلارک[۳] اعلام کرد که «ایالات متحده هنوز هیچ گونه مدرکی در خصوص دیگر دولت ها درباره یک حمله سایبری ویژه در دست ندارد» [۴]. تا مدت ها حتی در مهمترین حملات، تعیین تقصیر یک دولت از اهمیت چندانی برخوردار نبود. اگرچه ایران هزینه گزافی در رابطه با ویروس استاکس نت متحمل شده بود، که منجر به تخریب ۲۰ درصد از سانتریفیوژهای هسته ای ایران گردید، ولی دولتمردان ایران هرگز یک بیانیه رسمی در ارتباط با این رویداد صادر نکردند. در وقایع بعدی و مستقیم حملات سایبری در سال ۲۰۰۷ میلادی بر علیه دولت استونی، وزیر امورخارجه دولت استونی بیان کرد: «اتحادیه اروپا در معرض چنین حملاتی است، زیرا روسیه در شرف حمله به دولت استونی می باشد. اما این بیانیه جسورانه توسط یک عضو دیگر دولت استونی بدین صورت اصلاح گردید: دولت استونی در واقع دلایل کافی در رابطه با حملات صورت گرفته از جانب دولتمردان دولت روسیه در دست ندارد» [۴]. در گذشته، در صورتی دولت ها به صورت رسمی عملیات های سایبری را به دیگر دولت ها قابل انتساب می دانستند که منشأ حملات به طور چشمگیری قابل پیگیری بود. به عنوان مثال در اواخر سال ۱۹۹۰ میلادی دولت آمریکا از یک حمله گسترده

[4]-Richard Clarke

ISSN: 2538-3671
http://www.johi.ir

شبکه ای رایانه ای دچار ضرر و زیان شد که منجر به سرقت دهها هزار فایل اطلاعاتی گردید. وزارت دفاع آمریکا از طریق منابع جاسوسی و یک سری اطلاعات دیجیتالی خود، اینگونه نتیجه گیری کرد که حملات گسترده به داده های اطلاعاتی ایالات متحده آمریکا از جانب دولت روسیه صورت گرفته است. البته روسیه اتهامات وارده از سوی آمریکا را رد و انکار نمود. بدون شک مساله قابلیت انتساب در فضای سایبر هنوز مملو از مشکلات و چالش های آشکاری است که حتی از جانب ایالات متحده در ژوئن ۲۰۱۵ میلادی به تازگی پذیرفته شده است.

۳-۱. معیار دستورات

معیار دستورات، اولین معیار قابلیت انتساب می باشد که براساس آن دولت ها دستوراتی را برای بازیگران غیردولتی صادر می کنند و آنها را وادار به انجام اعمالی می نمایند. این واژه بر این امر دلالت دارد که یک دولت مصمم می باشد تا انجام عمل خاصی را به یک شخص غیردولتی واگذار کند و به او دستور می دهد تا آن عمل را از طرف او انجام دهد. طبق حقوق داخلی چنین شخصی قادر خواهد بود تا عناصری از اقتدارات دولتی را اعمال کند. بنابراین عمل چنین شخصی در ماده ۵ از مواد مسئولیت بین المللی دولت ها قرار می گیرد. در دنیای فیزیکی نمونه هایی وجود دارند که طبق ماده ۸ طرح مسئولیت بین المللی دولت ها، شامل اشخاصی می گردند که خارج از ساختارهای رسمی دولت عمل می کنند و از جانب دولت به عنوان نیروی کمکی استخدام و یا به عنوان داوطلب به کشورهای ثالث فرستاده می شوند تا وظایف خاصی را انجام دهند [۱۲]. در خصوص عملیات های سایبری، اگر دولت به یک بخش فناوری اطلاعات در دانشگاهی دستور دهد تا یک حمله DDOS[۴] علیه یک هدف طراحی شده انجام دهد، آثار و نتایج این عملیات به آن دولت قابل انتساب است. به عنوان مثال در خصوص وقایع استونی در سال ۲۰۰۷ میلادی، تفکرات ایجاد شده حاکی از این بود که دولتمردان دولت روسیه از چت رومهای (اتاقهای گفت و گو) مختلف و دیگر شبکه های آنلاین جهت تحریک هکرهای وطن پرست روسی خود استفاده می کردند تا به شبکه های ارتباطی دولت استونی حمله کنند. هدف پایمال کردن روحیه وطن پرستی مردم و ارزش های آنها بود که آشکارا در دکترین امنیت اطلاعاتی روسیه[۵] که در آن زمان معتبر بود، ذکر شده و ظاهرا از صحت این گزارشات حمایت می کرد. اما حتی اگر دولت روسیه مسئول اعمال هکرهای خصوصی نباشد ولی می تواند با این گروه آنلاین ارتباط داشته باشد. البته روسیه در قبال اعمال ماموران خودش به عنوان ارگان های دولتی مسئول می باشد. اگر دولت عمدا دستورات مبهم صادر کند، این ریسک برای او وجود خواهد داشت که در خصوص آثار و نتایج آن عمل مسئول شناخته شود. جهت اهداف قابلیت انتساب طبق دستورات اولیه می بایست مشخص شود که آیا قصد دولت تایید آن عمل غیرقانونی بوده است یا خیر. به عنوان مثال، در مورد انقلاب ایرانیان در سال ۱۹۷۹ میلادی، آیت الله خمینی جوانان ایرانی را فراخواند تا با تمام قدرت خویش حملاتشان را علیه ایالات متحده و اسرائیل که مقدمات بازگشت شاه را فراهم می کردند، گسترش دهند. دیوان بین المللی دادگستری در قضیه گروگان گیری در تهران اعلام کرد که «این اقتدارو اختیار دولتی است که عملیات خاص حمله و تصرف سفارت ایالت متحده را برعهده گرفته است» [۱۳]. بیانیه اولیه آیت الله در بر گیرنده تمایل آشکار دولت ایران به اشغال سفارت نمی شد ولی اعمال بعدی دولت ایران باعث انتساب اعمال بازیگران غیردولتی به دولت گردید. به علاوه دولت ها در قبال سرپیچی اشخاص خصوصی از دستورات صادره و همچنین در قبال اعمالی که فراتر از حدود اختیارات قانونی انجام داده اند، مسئول نخواهند بود [۱۲]. به عنوان مثال اگر دولتی یک شرکت خصوصی را جهت مقابله با حملات سایبری به کار گمارد، در صورتی که کارمندان این شرکت فراتر از اختیارات قانونی و دسترسی آنها به شبکه های ارتباطی، یک حمله سایبری را علیه دولت های دیگر آغاز کنند، دولت دستوردهنده، مسئول حملات صورت گرفته نخواهد بود.

۳-۲. معیار هدایت

از میان سه معیار استاندارد قابلیت انتساب، معیار هدایت کمتر مورد بررسی قرار گرفته است. این معیار، معنی و مفهوم مستقلی دارد. اینکه دقیقا این معیار چه مفاهیمی را دربر می گیرد در حقوق بین الملل و در ادبیات بی پاسخ مانده است. یکی از قضیه های بین المللی نادر که در آن طرفین به مفهوم «هدایت» در مفاد ماده ۸ توجه کرده اند، قضیه نسل کشی است که دیوان بین المللی دادگستری قابلیت انتساب اعمال بازیگران غیردولتی را به عنوان یکی از موضوعات اصلی مورد توجه قرار داده است. پرفسور الن پیه[۶] در دادخواست شفاهی خود برای بوسنی و هرزگوین، واژه «هدایت» را این گونه توصیف کرد که «

---

[5]-Distributed Denial of Service
سرازیر کردن تقاضاهای زیاد به یک سرور و استفاده بیش از حد از منابع به طوری که سرویس دهی آن به کاربرانش دچار اختلال شده یا از دسترس خارج شود.

[6]-Russian Information Security

[7]- Professir Alain Pellet

ISSN: 2538-3671
http://www.johi.ir

شدت واژه «هدایت» از واژه «دستورات» کمتر است» [۴]. دیوان سرانجام در خصوص معیار هدایت اظهار کرد که «یک ارگان دولتی قادر است تحت هدایت یک دولت مرتکب اعمال خلاف قواعد حقوق بین الملل شود» [۴]. بنابراین بر اساس اظهارات دیوان، به طور ضمنی می بایست یک رابطه مستمر میان دولت و بازیگر غیردولتی وجود داشته باشد. این موضوع فراتر از صدور یک دستور ساده از جانب یک دولت می باشد. پرفسور کراوفورد [۷]واژه هدایت را یک دوره مستمری از دستورات یا رابطه ای فیمابین دولت و یک بازیگر غیردولتی می شناسد که ممکن است منجر به ایجاد مسئولیت گردد. اگر شخص یا گروهی از اشخاص که خارج از ساختارهای رسمی دولت عمل می کنند، از دولت تبعیت کنند و دولت اعمال چنین بازیگران خصوصی را هدایت کند [۴]، این احتمال وجود دارد که او مسئولیت اعمال آنها را حتی در صورت فقدان دستورات صریح جهت ارتکاب آن اعمال متحمل شود. در زمینه فضای سایبر، استفاده از کرم استاکس نت در این رابطه قابل طرح می باشد، ساخت این ویروس مشهور هنوز به طور رسمی مشخص نشده است اما طبق گزارشات، انتخاب اهداف و ساختار پیچیده این ویروس همگی گویای این واقعیت است که حملات توسط دولت های متخاصم مانند ایالات متحده و اسرائیل آغاز و طراحی شده است [۴]. همچنین هدایت و مدیریت تیم هایی که در چنین پروژه های طولانی مدتی مشارکت داشتند، بسیار پیوسته و مستمر می باشد و نشان از حمایت دولتی و پشتیبانی مالی شدید از این پروژه ها دارد. این امر منجر به ایجاد یک رابطه مستمر تبعی تحت نظریه «هدایت» می شود.

۳-۳. معیار کنترل

استاندارد نهایی قابلیت انتساب در ماده ۸ طرح مسئولیت بین المللی دولت ها مربوط به وضعیتی می شود که درآن، بازیگران غیردولتی تحت کنترل یک دولت عمل می کنند. صحیح نیست که معیار مستقل کنترل را با دو معیار قبلی برابر بدانیم. تفسیر واژه «کنترل» درکنار تفسیر«دستورات» و «هدایت» نامناسب است. موضوع اساسی، نوع و درجه کنترلی است که دولت می بایست اعمال کند تا آن عمل قابل انتساب به او باشد. اینکه هر دولتی ممکن است قدرت خود را صرف کنترل اعمال اشخاص خصوصی کند که در سرزمینش مرتکب می شوند، نشانگر اقتدار حاکمیتی آن دولت بر قلمرو خویش است؛ اما در واقع بدین معنا نیست که او باید از هرگونه عمل خلاف قواعد حقوق بین الملل ارتکابی در قلمروش آگاه باشد. این کنترل بالقوه از یک مکان یا محدوده جغرافیایی نشات می گیرد که برای اهداف قابلیت انتساب کافی نمی باشد. بنابراین کنترل واقعی در رابطه بین دولت و بازیگر غیردولتی مساله ای اساسی است. دیوان بین المللی دادگستری در قضیه نسل کشی بوسنیایی ها اعلام کرد (درصورتیکه درجه کنترل شدید باشد) [5] «اگر اشخاص غیردولتی به عنوان ارگان یا مامور عملی دولت تلقی شوند، طبق ماده ۴ دولت، مسئول اعمال چنین اشخاصی می باشد» [5]. به عنوان مثال، وقتی که دولت، تعدادی از موسسات و شرکت های خصوصی امنیتی سایبری را گردهم می آورد تا در برابر یک حمله سایبری اضطراری واکنش نشان دهند، می بایست بر عملکردهای این گروه کنترل کلی داشته باشد. موضوع درجه بالای کنترل که رابطه بین دولت و بازیگر غیر دولتی را به یک رابطه ناشی از وابستگی تام تبدیل می کند، از لحاظ منطقی درست است. اما اینکه چه میزان کنترل برای قابلیت انتساب ضروری می باشد مسئله ای غامض و پیچیده است. معیار های عملی و مناسب کنترل در رویه قضایی بین المللی در سه دهه اخیر بوجود آمده است. ابتدا دیوان بین المللی دادگستری معیار «کنترل موثر» را در قضیه نیکاراگوئه بکار برد همچنین آن را در قضیه نسل کشی بوسنیایی ها نیز مورد استفاده قرار داد. دوم در دادخواست تجدیدنظر دادگاه کیفری بین المللی برای یوگسلاوی سابق، معیار کنترل کلی در قضیه تادیچ استفاده شد [۱۴]. گاهی اوقات از آنها به عنوان «معیار نیکاراگوئه» و «معیار تادیچ» نیز تعبیر می شود. در اینجا لازم است تا عناصر هر دو معیار را مورد بررسی قرار دهیم. از یک طرف برای معیار کنترل موثر، دولت می بایست اساسا از حمایت کردن یک بازیگر غیردولتی فراتر رود وآن بازیگر را تامین مالی، سازماندهی، آموزش و تجهیز کند. همچنین او باید در طراحی عملیات ها، انتخاب اهداف و در پشتیبانی کردن عملیات ها مشارکت مستقیم داشته باشد [۱۵]. بطور کلی دولت باید توانایی کنترل شروع و پایان عملیات را داشته باشد، ولی لازم نیست که دولت هر عمل خلاف قواعد حقوق بین الملل ارتکابی را کنترل کند بلکه باید دامنه وسیعی از آن اعمال را تحت کنترل داشته باشد. در زمینه فضای سایبر، به دلیل اینکه ادله اثبات به سختی قابل جمع آوری می باشد، استفاده از معیار کنترل ممکن است در بسیاری از قضایا منجر به نتایج مشابهی گردد. به عنوان مثال، گروه جرایم سایبری و هکرهای شبکه ارتباطی تجاری روسیه از حمایت طولانی مدت دولت روسیه که به شکل قیمومت و براساس عملکرد خاص دولتمردان آن می باشد، برخوردار بوده اند. همچنین دولت چین سرمایه و آموزش های دولتی را برای دانشگاهیانی که در برابر مخالفان خود، حملات سایبری انجام می دادند، فراهم کرده است. از طرفی دیگر معیار کنترل کلی توسط دادگاه کیفری بین المللی برای یوگسلاوی سابق در قضیه

[8]- Professor Crawford

ISSN: 2538-3671
http://www.johi.ir

تادیچ پیشنهاد شده بود که صراحتا این معیار واجد درجه پایینی از کنترل بود [۱۴]. براساس این معیار، دولت ملزم است تا کمک و مساعدت مالی و آموزشی، تجهیزات نظامی و پشتیبانی عملیاتی را برای بازیگران غیر دولتی فراهم کند ولی نیازی نیست درانجام عملیات ها مشارکت داشته باشد. به عنوان مثال، اگر دولت بدافزار پیشرفته ای را برای گروهی از هکرهای غیردولتی فراهم کند، آن دولت می بایست کنترل کلی بر عملکرد آن گروه داشته باشد. دادگاه کیفری بین المللی برای یوگسلاوی سابق صراحتا استفاده از معیار کنترل کلی را تنها به گروه های مسلح سازمان یافته اختصاص داده ولی معیار کنترل موثر را در مورد اشخاص یا گروههایی که به صورت ساختارهای نظامی سازماندهی نشده اند، بکار برده است. در زمینه عملیات های سایبری، حتی اگر گاهی اوقات هکرها به صورت گروهی عمل کنند، عملیات آنها از گروه های مسلح سازمان یافته متمایز می باشد. گروه های مسلح سازمان یافته طبیعتا بوسیله «یک ساختار»، زنجیره ای از دستورات و یک سری اصول و قواعد و سمبل های خارجی حاکمیتی مشخص می شوند، درحالیکه در دنیای آنلاین کاربرانی افسارگسیخته و کمترسازماندهی شده وجود دارند [۴]، مانند گروه فعالان چینی گمنام [۸] و نیروی ویژه پلیس سایبر [۹].

۴. انتساب اعمال بازیگران غیردولتی به دولت ها در فضای سایبر

اصولا رفتار یا اعمال اشخاص خصوصی – اعم از حقیقی یا حقوقی- را نمی توان به عنوان عمل خلاف بین المللی محسوب و به دولت ها منتسب نمود و آنها را مسئول شناخت. با این حال، ممکن است در مواردی اعمال و رفتار اشخاص خصوصی در قلمرو یک دولت، موجبات مسئولیت بین المللی آن دولت را فراهم نماید. از جمله اینکه اگر رفتار اشخاص ناشی از عدم پیش بینی و پیشگیری از وقوع تخلف و یا عدم کفایت کنترل یا کوتاهی یا عدم مراقبت لازم در این امر از سوی ارکان دولتی باشد.در مجموع بازیگران غیردولتی یا اشخاص خصوصی را می توان به اشخاص حقیقی و اشخاص حقوقی تفکیک نمود. مسئله قابل طرح آن است که آیا ارتکاب اعمال سایبری زیان بار توسط این اشخاص قابل انتساب به دولت می باشد یا خیر؟ بنابراین باید در ابتدا مشخص شود که اشخاص حقیقی و حقوقی چه کسانی هستند؟

۴-۱. فعل اشخاص حقیقی

اشخاص حقیقی در واقع همه انسان ها می باشند که موضوع حق و تکلیف اند. آنها در زندگی اجتماعی خود به تنهایی مسئولیت اعمال خود را به عهده دارند [۱۶]. حال اگر این اشخاص از طرف دولت اعمالی را انجام دهند آیا این اعمال قابل انتساب به دولت است؟ طبق ماده ۸ طرح کمیسیون حقوق بین الملل در خصوص مسئولیت بین المللی دولت ها مورخ ۲۰۰۱ میلادی رفتارهای متخلفانه اشخاص خصوصی تحت هدایت یا کنترل دولت نیز به دولت منتسب می شود. کمیسیون حقوق بین الملل در تفسیر شماره ۹ ماده ۸ بیان می دارد که «این ماده ناظر به «شخص یا گروهی از اشخاص» است و دولت می تواند اقدامی را از طریق مجموعه ای از اشخاص یا گروه هایی انجام دهد که فاقد شخصیت حقوقی هستند اما با این وجود به صورت جمعی عمل می کنند» [۱۷]. هکرهای خصوصی نمونه بارز اشخاص حقیقی می باشند. چنانچه دولت برای حمله سایبری خود به هکرهای خصوصی رهنمود داده یا آن ها را برای این حملات تحریک و ترغیب نموده باشد، حمله ی سایبری فعل دولت تلقی می شود. در موارد دیگر ممکن است رفتاری به دولت منتسب شود که در زمان ارتکاب به او قابل انتساب نبوده یا ممکن نبوده که قابل انتساب باشد اما متعاقبا دولت مزبور آن را تایید کرده و آن را به عنوان عمل خویش تلقی کرده است. این امر در ماده ۱۱ طرح مسئولیت بین المللی دولت ها مورد اشاره قرار گرفته است. بنابراین می توان حالتی را فرض نمود که در آن اقدام اولیه افراد خصوصی به یک حمله سایبری با تحریک دولت نبوده است، ولی بعد از صورت گرفتن حمله، دولت نه تنها تلاش معقول براب پیشگیری و کنترل آن انجام نمی دهد بلکه از آن حمله حمایت می کند، که در این صورت می تواند برای دولت مسئولیت آور باشد [۱۸]. باید توجه داشت چنانچه افراد خصوصی ابتدائا اقدام به حمله سایبری کرده باشند و دولت صرفا به آنها کمک کرده باشد این اقدام منتسب به دولت نخواهد بود و دولت صرفا از جهت کمک به یک عمل متخلفانه بین المللی مسئولیت خواهد داشت [۱۸].

[9]-Anonymous Honker Group
[10]-CyberBerkut

ISSN: 2538-3671
http://www.johi.ir

۴-۲. فعل اشخاص حقوقی

اشخاص حقوقی به اجتماع منافع و هدف هایی گفته می شود که قدرت عمومی آن را به عنوان واحدی مستقل از عناصر تشکیل دهنده اش مورد شناسایی و حمایت قرار می دهد [۱۶]. بدین ترتیب شرکت های تجاری، موسسات غیر تجاری و سازمان ها که دارای حقوق و تکالیف هستند و موجودیتی مستقل از تشکیل دهندگان خود می باشند، می توان اشخاص حقوقی به شمار آورد. موسسات غیر تجاری خود شامل انجمن ها و اتحادیه های صنفی نیز می شوند. این شرکت ها و موسسات توسط اشخاص حقیقی ایجاد می شوند و به منظور دست یابی به اهداف و منافعی مشترک اقدام به تشکیل یک شخص حقوق خصوصی می کنند [۱۶]. حال اگر دولت اعمالی را به این شرکت ها یا موسسات واگذار کند آیا اعمال آنها قابل انتساب به دولت خواهد بود؟ طبق ماده ۵ طرح مسئولیت بین المللی دولت ها «رفتار شخص یا نهادی که ارگان دولتی محسوب نمی شود اما به موجب قانون آن دولت مجاز به اعمال اقتدارات دولتی است به موجب حقوق بین الملل فعل آن دولت محسوب می شود مشروط بر آنکه شخص یا نهاد مزبور در قضیه ذیربط در این سمت عمل کرده باشد» [۱۷]. هدف از این ماده آن بوده که پدیده رو به افزایش نهاد های شبه دولتی که در مواقعی به جای ارگان های دولتی به اعمال اقتدارات دولتی می پردازند و همچنین وضعیت شرکت های دولتی سابق که خصوصی شده اند اما همچنان برخی اشتغالات عمومی یا تنظیمی را انجام می دهند را در بر گیرد [۱۸]. به عنوان مثال در برخی کشورها ممکن است با موسسات و شرکت های امنیتی خصوصی، قراردادی منعقد شود تا به عنوان نگهبانان زندان فعالیت کنند. همچنین ممکن است به خطوط هوایی دولتی یا خصوصی اختیاراتی در زمینه کنترل های مهاجرتی یا قرنطینه تفویض شود [۱۷]. بنابراین با توجه به ماده ۵ طرح مسئولیت بین المللی دولت چون این شرکت ها در مقام اعمال اقتدار عمومی هستند، مشارکت عامدانه آنها در حملات سایبری منتسب به دولت خواهد بود مگر آنکه دولت تلاش مقتضی برای جلوگیری از آن را به عمل آورد [۱۸].

۵. رویه های قضایی بین المللی

۵-۱. قضیه کارکنان دیپلماتیک و کنسولی ایالات متحده در ایران

در این قضیه اشغال سفارت آمریکا و به تبع آن بازداشت ماموران و کارکنان دیپلماتیک و کنسولی این کشور از سوی مقامات ایرانی مورد تایید دولت ایران قرار گرفت. دیوان بین المللی دادگستری حکم نمود: « هرچند حمله اولیه به سفارت ایالات متحده آمریکا در تهران قابل انتساب به دولت ایران نبوده است اما پشتیبانی بعدی مقامات ایران و تصمیم به دائمی کردن اشغال سفارت، این اقدام را به اعمال دولت بدل نموده است» [۱۳]. همچنین ماده ۱۱ طرح مسئولیت دولت مقرر داشته است: «چنانچه اقدام صورت گرفته قابل انتساب به یک دولت نباشد، با این وجود به موجب حقوق بین الملل فعل آن دولت تلقی می شود در صورتی که و تا حدی که آن دولت آن رفتار را تایید نموده و آن را همچون رفتار خویش تلقی می کند طبق حقوق بین الملل عمل آن دولت محسوب می شود» [۱۷]. بنابراین با وجود اینکه دیوان ادله کافی برای انتساب افعال و اقدامات دانشجویان در اشغال سفارت به دولت ایران پیدا نکرد، ولی اعلام داشت که دولت ایران در قبال این وضعیت مسئولیت دارد چرا که نسبت به تعهدات خود وفق کنوانسیون ۱۹۶۱ وین در خصوص روابط دیپلماتیک و کنوانسیون ۱۹۶۳ در خصوص روابط کنسولی دال بر حمایت از سفارت آمریکا و کارکنانش آگاه بوده ولی از اجرای تعهدات حقوقی خود قصور کرده است [۷].

۵-۲. حملات ۱۱ سپتامبر به ایالات متحده آمریکا

در ۱۱ سپتامبر ۲۰۰۱، چهار هواپیمای بوئینگ ۷۵۷ و ۷۶۷ خطوط هوایی آمریکا که قرار بود مطابق برنامه پرواز از شمال شرق آمریکا (بوستون) به جنوب غرب (کالیفرنیا) پرواز کنند، ربوده شدند. هواپیماهای خطوط ۷۶۷ راس ساعت ۸:۴۵ دقیقه با برج شمالی و هواپیمای دیگر در ساعت ۹:۳۰ دقیقه با برج جنوبی برخورد کردند. بعد از مدت کوتاهی به ترتیب هر دو برج در ساعت ۱۰:۰۵. ۱۰:۳۰ دقیقه فرو ریختند. در اثر ریزش چندین ساختمان مجاور نیز تخریب شدند. علاوه بر برج های دوقلوی مرکز تجارت جهانی، دو حادثه همزمان دیگر نیز رخ داد. اول پس از ربوده شدن هواپیمای خطوط ۷۵۷ آمریکا، این هواپیما در ساعت ۱۰:۱۰ صبح به مرکز پنتاگون اصابت کرد و هواپیمای چهارم نیز که به قصر یکی از مراکز کمپ دیوید، کاخ سفید یا پایتخت هدایت می شد، در میانه راه در سامرست پنسیلوانیا سقوط کرد. مطابق بررسی های انجام شده ۲۸۹۳ نفر در سقوط برج ها، ۶۴ نفر در پنتاگون، ۱۲۵ نفر در سه هواپیمای ربوده شده و در نهایت ۴۴ نفر در هواپیمای چهارم کشته شدند [۱۹]. در زمان حمله القاعده به برج های دوقلو مرکز تجارت جهانی، این سازمان، جزو ارگان دولت طالبان نبود، از این رو نمی توان گفت که حادثه ۱۱ سپتامبر بر اساس ماده ۴ طرح کمیسیون حقوق بین الملل به رژیم طالبان به عنوان دولتی که القاعده در استخدام آن است، منتسب می شود. همچنین روابط القاعده با رژیم طالبان آنقدر نزدیک نبود که تصور شود آنها ارگان عملی

ISSN: 2538-3671
http://www.johi.ir

دولت مذکورند و در نتیجه حمله مزبور به دولت افغانستان منتسب شود. در همین زمینه یکی از حقوقدانان نیز اساسا میزان مشارکت طالبان را بسیار کمتر از آن دانسته که بتواند انتساب و در نتیجه حمله مسلحانه علیه آن را توجیه کند [۲۰]. همچنین اگر رژیم طالبان به القاعده اجازه داد که مستقل عمل کند و حتی در ارتباط با موضوعات مشخص تا حدودی مثل یک حکومت اقدام کند، اما اسناد و مدارک معتبر کمی وجود دارد تا اثبات کند که این گروه از سوی دولت طالبان مجاز به اعمال برخی اقتدارات دولتی *در آن زمان بود [20]*. از این رو حادثه ۱۱ سپتامبر را از طریق سه فاکتور مذکور نمی توان به دولت طالبان منسوب کرد.

۵-۳. مسئولیت دولت در پناه دادن به تروریست ها

معیار حمایت و پناه دادن به تروریست ها در قطعنامه های ۱۳۶۸ (۲۰۰۱) و ۱۳۷۳ (۲۰۰۶) شورای امنیت آمده است. حال سوالی که قابل طرح است آن است که آیا پناه دادن به یک گروه تروریستی موجب انتساب عمل آنها به دولت حامی و در نتیجه تحقق مسئولیت خواهد شد؟متعاقب حملات تروریستی ۱۱ سپتامبر ۲۰۰۱، قاعده انتساب جدیدی پا به عرصه وجود گذاشت مبنی بر اینکه دولتی که به تروریست ها پناه می دهد، به خاطر تمامی اقدامات گروه های تروریستی ذی ربط مسئول خواهد بود. بوش رئیس جمهور اسبق ایالات متحده، پس از این حملات، اعلامیه ای صادر کرد و این دکترین نوظهور را تحت لوای تعابیر و عبارات مختلف مطرح نمود. وی پس از حملات ۱۱ سپتامبر خطاب به مردم آمریکا گفت: « ما میان تروریست هایی که مبادرت به انجام چنین اقداماتی نموده اند و افرادی که به آن ها مأوا می دهند، تمایزی قائل نمی شویم» [۲۱]. حقوقدانان آمریکایی در مقام توجیه مشروعیت حمله نظامی به آن کشور، قاعده انتساب جدیدی را مطرح نمودند که مطابق آن، صرف پناه دادن به گروه های تروریستی برای انتساب مسئولیت اقدامات آن ها به دولت پناه دهنده کفایت می کرد [۲۱]. بنابراین پناه دادن و حمایت از گروه های تروریستی که نقض قواعد اولیه حقوق بین الملل محسوب می شود، موجبات مسئولیت بین المللی دولت های حامی را ایجاد می کند در صورتی که ارتباط دولت با این گروه ها به نحوی باشد که زمینه انتساب اعمال آنها به دولت را فراهم کند. این ارتباط و دخالت دولت می تواند به صورت هدایت، کنترل، حمایت، مدارا و مماشات، تایید و پذیرش باشد [۲۰].

۶. تعهد دولت ها به پیشگیری از ضرر و زیان های فرامرزی بازیگران غیردولتی

این تعهد دولت ها را ملزم می نماید تا مانع استفاده از قلمرو خود جهت انجام اعمال متخلفانه در قبال دولت های دیگر شوند. مهمترین مبنای این تعهد عرفی در قضیه کانال کورفو در سال ۱۹۴۹ میلادی می باشد.در این قضیه، دو کشتی جنگی بریتانیایی هنگام عبور از تنگه بین المللی کورفو در آبهای ساحلی کشور آلبانی، با مین برخورد کردند و انفجار مین موجب وارد آمدن خسارت به کشتی ها و کشته شدن چند تن از افسران و دریانوردان انگلیسی شد. در حالیکه دیوان بین المللی دادگستری قادر نبود تا کارگذاشتن مین ها بوسیله دولت آلبانی را به اثبات برساند، در نهایت دیوان اینگونه اظهار کرد که «دولت آلبانی وظیفه داشته است که کشتی های انگلیسی را که از این تنگه عبور می کردند از خطر انفجار مین که عبور بی ضرر کشتی های کلیه کشورها را در تنگه کورفو تهدید می کرد، مطلع سازد. همچنین دیوان طبق اصول کلی اینگونه نتیجه گیری کرد که هر دولتی متعهد است آگاهانه مانع استفاده از قلمرو خود جهت انجام اعمال خلاف حقوق بین الملل درقبال دولت های دیگر شود» [۲۲].در این خصوص، اعمالی که در قبال دولت های دیگر انجام می شود اعمال بازیگران غیردولتی می باشد که منجر به اعمال متخلفانه بین المللی می شوند. فضای سایبر یک محیط سرزمینی است که هیچ یک از دولت ها نمی توانند در آن ادعای حاکمیت داشته باشند [۲۳]. اگر این دیدگاه درست باشد پس تعهد دولت ها به پیشگیری از ضرر و زیان های فرامرزی برای اعمال متخلفانه موجود در فضای سایبر غیرقابل اجراست. ولی رویه عملی دولت ها بدین صورت است که آنها حقیقتا حاکمیت سرزمینی خود را از طریق زیر ساخت های فیزیکی مستقر در قلمرو خویش بر بخش هایی از فضای سایبر اعمال می کنند. در نتیجه دولت ها می بایست به تعهدات خود در خصوص پیشگیری از ضرر و زیان های فرامرزی که زیرساختهای سایبری شان را تهدید می کند، عمل نمایند. به عنوان مثال، دولت ها موظفند تا از زیرساختهای اطلاعاتی خود محافظت کنند و سیستم های ملی خود را از خسارات یا استعمال بی جا دور نگه دارند. برای مثال در قضیه نیکاراگوئه، دیوان اعلام کرد که « دولت نیکاراگوئه طبق اصل تعهد به پیشگیری نباید اجازه دهد که از سرزمینش به عنوان راهی برای قاچاق تجهیزات نظامی که برای شورشیان السالوادور درنظر گرفته شده بود، استفاده شود» [۱۵]. در جائیکه حقوق بین الملل دولت ها را به انجام اقدامات ایجابی در این زمینه متعهد می کند، لازم است که این وظیفه بین المللی به صورت تعهد به نتیجه یا تعهد به وسیله طبقه بندی شود [۲۳].تعهد به نتیجه یک تعهد مطلق را بر دولت ها تحمیل می کند تا آنها بتوانند طبق این تعهد به نتایج مشخصی دست یابند. همچنین اثبات کوتاهی و غفلت دولت در نقض این تعهد و اینکه آیا او مقصر بوده یا خیر،

ISSN: 2538-3671
http://www.johi.ir

ضروری نمی باشد. درمقابل، تعهد به وسیله تعهدی غیر مطلق و مقید به استاندارد تلاش معقول می باشد [۲۳] و لازم نیست که دولت ها به نتایج خاصی برسند. نقض تعهد به وسیله تنها در صورتی رخ می دهد که تقصیر دولت ثابت شده باشد. قصور دولت در اعمال نظارت و انجام تلاش معقول منجر به مسئولیت بین المللی می گردد. در قضیه نسل کشی، دیوان بین المللی دادگستری ماهیت تعهد به وسیله را اینگونه شرح می دهد: « واضح و مبرهن است که این تعهد، یک تعهد به وسیله است و نه یک تعهد به نتیجه، بدین صورت که دولت ها نمی توانند براساس تعهدات خود و تحت هر شرایطی از ارتکاب نسل کشی جلوگیری نمایند : طرفین متعهد می باشند تا معقولانه از تمام امکانات موجود جهت پیشگیری از نسل کشی استفاده کنند» [۵]. در جائی که یک دولت به طور معقول در پیشگیری از عمل خلاف حقوق بین الملل کوتاهی کرده باشد و تعهد به وسیله را نقض نماید، آن دولت به خاطر این کوتاهی مسئول شناخته می شود و نه به خاطر آن عمل متخلفانه ای که منجر به نتایج زیان بار شده است [۲۳].

۷. اقدام متقابل دولت زیان دیده در برابرحمله سایبری

طرح مسئولیت دولت ها در قبال اعمال متخلفانه بین المللی مصوب ۲۰۰۱ میلادی در ماده ۵۲ شرایط حاکم بر اقدامات متقابل را بیان کرده است[۱۰].حال باید این شروط و امکان اعمال آنها در قبال حمله سایبری مورد تجزیه و تحلیل قرار گیرند. ماده مذکور دولت زیان دیده را ملزم می کند - تا با توجه به تعهداتی که در ماده ۴۳[۱۱] طرح مسئولیت برای وی وجود دارد- که از دولت مسئول و متخلف بخواهد تعهدات خود را به موجب بخش دوم این مواد رعایت نماید. در این رابطه مساله اطلاع رسانی دولت زیان دیده قابل طرح است؛ به این صورت که دولت زیان دیده ملزم است به دولت مسئول اطلاع دهد که وی قصد دارد به اقدامات متقابل متوسل گردد. پیش بینی این التزام از آن جهات است که اگر دولت متخلف فعل متخلفانه را متوقف نمود و اختلاف را به دیوان و یا محکمه صالح ارجاع داد، دیگر نمی توان به اقدامات متقابل در برابر وی دست یازید [۷]. بنابراین، به نظر می رسد که دولت قربانی حمله سایبری نیز نمی تواند از این شرط مستثنی باشد و باید جهت توسل به اقدامات متقابل نسبت به اطلاع رسانی قبلی به دولت مسئول اقدام نماید. اما نکته قابل تامل در این رابطه طرز تلقی دولت قربانی از حمله سایبری است؛ به این مفهوم که دولت یاد شده حمله سایبری را در حکم یک حمله مسلحانه علیه خود تلقی نماید یا اینکه آن را صرفا یک خرابکاری و فعل متخلفانه بین المللی محسوب نماید. در حال حاضر معیار و استاندارد واحد و مشخصی برای تلقی یک حمله سایبری به عنوان یک حمله مسلحانه یا یک اقدام متخلفانه وجود ندارد، از این رو در مقوله حملات سایبری نمی توان دولت قربانی را متهم به عدم رعایت شرط الزام به اطلاع رسانی قبلی نمود [۷]. در بند دوم آمده است که دولت زیان دیده می تواند برای حفظ و پاسداری از حقوق خود اقدامات متقابل فوری را که ضروری می داند انجام دهد. در فضای سایبر وجود چنین شرط حقوقی برای توسل به اقدامات متقابل از سوی دولت قربانی به طریق اولی از جایگاه منطقی برخوردار بوده و ضروری می نماید. تفسیر قید فوریت در توسل به اقدام متقابل در فضای سایبر، یک پدیده عینی، محسوس و قابل اندازه گیری نیست و صرفا باید رویه ملی کشورها را مد نظر قرار داد. به عبارتی باید گفت که این مساله نسبی تابعی از نحوه استنباط و طرز تلقی دولت ها از مفهوم امنیت ملی و منافع ملی و تصمیم و اراده سیاسی آنهاست که ترجمان آن در فضای سایبر به مراتب سخت تر و پیچیده تر از دنیای واقعی می باشد [۷].

---

[۱۱]- ماده ۵۲ طرح مسئولیت بین المللی دولت ها مورخ ۲۰۰۱ میلادی:۱-دولت زیاندیده پیش از مبادرت به اقدامات متقابل باید:الف- مطابق ماده ۴۳ از دولت مسئول بخواهد که تعهداتش را به موجب بخش دوم ایفا کند (توقف فعل متخلفانه و جبران خسارت).ب- هرگونه تصمیم راجع به اتخاذ اقدامات متقابل را به دولت مسئول اطلاع داده و به او پیشنهاد مذاکره کند.

۲-با وجود مفاد قسمت ب بند ۱، دولت زیاندیده ممکن است برای حراست از حقوقش چنان اقدامات متقابل فوری را که ضروری است اتخاذ کند.

۳-در موارد زیر نمی توان به اقدامات متقابل متوسل شد و در صورتیکه چنین اقداماتی از پیش آغاز شده اند باید بدون تاخیر غیرموجه متوقف شوند: الف-فعل متخلفانه بین المللی متوقف شده است؛ب- اختلاف نزد دادگاه یا دیوانی مطرح شده که برای اتخاذ تصمیمات لازم الاجرا برای هر دو طرف صلاحیت دارد.

۴-در صورتیکه دولت مسئول در اجرای مکانیسم حل و فصل اختلافات حسن نیت نداشته و قصور کند، بند ۳ فوق اعمال نمی شود.

[۱۲]- ماده ۴۳ طرح مسئولیت: الف- دولت زیان دیده ای که به مسئولیت دولت دیگر استناد می نماید باید دعوایش را به آن دولت ابلاغ کند. ب- دولت زیان دیده می تواند به ویژه به موارد ذیل تصریح کند: الف- در صورت تداوم فعل متخلفانه، رفتاری که دولت مسئول باید به منظور توقف فعل مزبور انجام دهد؛ ب- شیوه جبران خسارت مطابق مقررات بخش دوم.

ISSN: 2538-3671
http://www.johi.ir

نتیجه گیری

اصل کلی در حقوق بین الملل آن است که دولت ها مسئول اعمال اشخاص خصوصی نیستند. با این حال از نظر کمیسیون حقوق بین الملل استثنائاتی بر این اصل وجود دارد. چنانچه دولت برای حملات سایبری خود به هکرهای خصوصی رهنمود داده یا آن ها را برای این حملات تحریک و ترغیب نماید، حملات سایبری فعل دولت تلقی می شوند. همچنین بر اساس ماده ۵ طرح کمیسیون حقوق بین الملل راجع به مسئولیت بین المللی دولت ها، همکاری یک شرکت خصوصی در حملات سایبری موجب انتساب آن عمل به دولت می شود مگر آنکه دولت تلاش مقتضی برای جلوگیری از آن را به عمل آورد. با توجه به ماهیت خاص حملات سایبری در فضای سایبر پیدا کردن ریشه نقض در اثر حملات سایبری و عامل آن در شبکه عنکبوتی اینترنت به سختی قابل ردیابی است و تشخیص دولت مسئول واقعی به ندرت امکان پذیر است و در صورتی که دولت بر اعمال اشخاص خصوصی کنترل کلی داشته باشد اعمال این اشخاص قابل انتساب به دولت خواهد بود. همچنین دولت ها بر مبنای حقوق بین الملل عرفی موظفند تا به سایر دولت ها اجازه ندهند که از زیرساخت های سایبری شان جهت لطمه زدن به حقوق قانونی و بین المللی آنها استفاده کنند. آنها می بایست اقدامات مقتضی جهت پیشگیری از خطرات احتمالی انجام دهند. در حقوق بین الملل ضمانت اجراهای چندی مورد پذیرش قرار گرفته است. از جمله چنین ضمانت هایی، اقدام متقابل است. اقدام متقابل دربرگیرنده اقدامات غیرخصمانه ای است که به خودی خود غیرقانونی است، اما زمانی که دولت زیان دیده در پاسخ به فعل متخلفانه دولت مسئول به این اقدامات مبادرت می ورزد، جنبه غیرقانونی آن زایل می شود.شرایط اقدام متقابل در ماده ۵۲ طرح مسئولیت بین المللی دولت ها، ذکر شده است. طبق این ماده، دولت قربانی حملات سایبری می تواند جهت توسل به اقدامات متقابل نسبت به اطلاع رسانی قبلی به دولت مسئول اقدام نماید. اما به دلیل این که در این رابطه معیار مشخصی برای تلقی یک حمله سایبری به عنوان یک حمله مسلحانه یا یک اقدام متخلفانه وجود ندارد، بنابراین نمی توان دولت قربانی حملات سایبری را متهم به عدم رعایت شرط الزام به اطلاع رسانی قبلی نمود. در بند دوم این ماده آمده است که دولت زیان دیده می تواند برای حفظ و پاسداری از حقوق خود اقدامات متقابل فوری را که ضروری می داند، انجام دهد. در فضای سایبر وجود چنین شرطی برای توسل به اقدامات متقابل از سوی دولت قربانی ضروری است. از آنجایی که قید فوریت در توسل به اقدامات متقابل در فضای سایبر، یک پدیده عینی و محسوس نمی باشد لذا باید رویه ملی کشورها را در نظر گرفت.

منابع و مراجع

منابع فارسی:

الف: کتب

[۱۷]ابراهیم گل، ع.، ۱۳۸۸، مسئولیت بین المللی دولت : متن و شرح مواد کمیسیون حقوق بین الملل، تهران: موسسه مطالعات و پژوهشهای حقوقی شهر دانش.

[۱۹]عبداللهی، م.،1388،تروریسم حقوق بشر و حقوق بشردوستانه، چاپ اول،تهران: شهر دانش.

[۱۶]موسی زاده، ر.، ۱۳۸۶، حقوق اداری (کلیات و ایران)، چاپ هشتم. تهران: نشر میزان.

ب: مقالات

[۱۰]اسمعیل زاده ملاباشی، پ.،عبداللهی، م.، سید قاسم زمانی،۱۳۹۶،"حملات سایبری و اصول حقوق بین الملل بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)"، فصلنامه مطالعات حقوق عمومی، دوره ۴۷، شماره ۲،صفحات ۵۵۹-۵۳۷.

[۸]اصلانی، ج.، ۱۳۹۴،"بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان های بین المللی در حقوق بین الملل"، مجله تحقیقات حقوقی، دوره ۱۸، شماره ۶۷۵، صفحات ۲۷۸-۲۵۷.

[۲]پاکزاد، ب.، ۱۳۹۰،"ماهیت تروریسم سایبری" مجله تحقیقات حقوقی دانشگاه شهید بهشتی، شماره۴، صفحات ۲۱۵-۲۴۹.

[۶]خانیکی، ه.، بابائی، م.، ۱۳۹۰، "فضای سایبر و شبکه های اجتماعی (مفهوم و کارکردها)"، فصلنامه انجمن ایرانی مطالعات جامعه اطلاعاتی، شماره ۱، صفحات ۹۶-۷۱.

[۱۱]خلف رضایی، ح.، ۱۳۹۲،"حملات سایبری از منظر حقوق بین الملل (مطالعه موردی: استاکس نت)"، فصلنامه مجلس و راهبرد، دوره ۲۰، شماره ۷۳، صفحات ۱۵۳-۱۲۵.

ISSN: 2538-3671
http://www.johi.ir

[۲۱]زمانی، ق.، میرزاده، م.، ۱۳۹۳،" انتساب اعمال متخلفانه اشخاص خصوصی به دولت بر اساس معیار کنترل: رویه دیوان داوری دعاوی ایران- آمریکا"، فصلنامه پژوهش حقوق عمومی، سال شانزدهم، شماره ۴۳، صفحات ۱۰۷-۸۲.

[۱۸]مومنی راد، ا.، فامیل زوار جلالی، ا.، ۱۳۹۵،"مسئولیت بین المللی دولت ها در حملات سایبری"، سومین کنفرانس بین المللی علوم انسانی، روانشناسی و علوم اجتماعی، صفحات ۱۶-۱.

[۲۰]میرعباسی، ب.، فامیل زوار جلالی، ا، ۱۳۹۵،" مسئولیت بین المللی دولت ها ناشی از مدارا و مماشات با گروه های دهشت افکن؛ با تاکید بر قضیه افغانستان"، فصلنامه مطالعات حقوق عمومی، دوره ۴۶، شماره ۲، صفحات۲۷۱-۲۴۷.

ج: پایان نامه

[۷]اصلانی، ج.، ۱۳۹۴،"حملات سایبری در چارچوب نظام مسئولیت بین المللی"، رساله دکترا، تهران، دانشکده حقوق و علوم سیاسی.

منابع انگلیسی:

A:Articles

[23]Buchan, R. 2016, "*Cyberspace,Non-State Actors and the Obligation to Prevent uuuuuuuuuuum mmmm*, Journal of Conflict & Security Law21.pp.430-453.

[4]Macak, K,. 2016, "*Decoding Article 8 of the International Law Commissions Articles on State Responsibility: Attribution of Cyber Operations by Non- State Actors*". Journal of Conflict & Security Law 21.pp.405-28.

[3]Sagourias,N.T and Buchan , R, 2012, *Cyber War and International Law*". Journal of conflict and security Law 17.pp.183-86.

C:Cases

[15]Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), I.C.J., reports 1986.

[5]Case concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Merits, I.C.J. reports 2007.

[22]Corfu channel case, (United Kingdom of Great Britain and Northern Ireland v. Albania), I.C.J reports 1949.

[14]Prosecutor v. Tadic, I.C.T.Y, 15 July 1999.

[13]US Diplomatic and Consular Staff in Tehran case, I.C.J. reports 1980.

D:Document

[12]The International Law Commission Articles on State Responsibility, 2001.

E:website

[1]Internet World Stats: Usage and Population Statistics (June 2016) 5 www.internet _wolrdstats.Com/stats.htm last accessed at 31 December 2017.

[9]forsatnet.ir/managers/gate last accessed 25 April 2018.