مجله مطالعات حقوقی دانشگاه شیراز
دوره دهم، شماره اول، بهار ۱۳۹۷

بررسی مفهوم دفاع مشروع در پرتو حملات سایبری با تأکید بر حمله استاکس‌نت به تأسیسات هسته‌ای ایران

غلامعلی قاسمی* سعید نامدار**

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. 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

* دانشیار حقوق بین‌الملل دانشکده حقوق دانشگاه قم(نویسنده مسئول)
g.ghasemi43@gmail.com
** کارشناس ارشد حقوق بین‌الملل، دانشگاه قم saeednamdar.2014@gmail.com

تاریخ دریافت: ۱۳۹۵/۰۸/۰٤ تاریخ پذیرش: ۱۳۹٦/۰۵/۲٤

دفاع مشروع برخوردار خواهد بود. در خصوص حمله کرم رایانه‌ای استاکس‌نت در سال ۲۰۱۰ به تأسیسات هسته‌ای ایران، صرف‌نظر از مسئله انتساب آن به عنوان یک امر موضوعی، حق دفاع مشروع قابل اثبات است.

واژه‌های کلیدی: حملات سایبری، اصل عدم توسل به زور، حمله مسلحانه، دفاع مشروع، استاکس‌نت.

۱. مقدمه

فضای سایبری[۱۷]فضایی غیرمادی و ناملموس است که متشکل از صدها هزار رایانه، سرویس، روتر[۱۸]سویچ و کابل‌های فیبر نوری است که به هم متصل گشته و موجب عملکرد زیرساخت‌ها و نهادهای خصوصی و دولتی می‌گردد. در واقع این فضا شبکه به هم پیوسته زیرساخت‌های فناوری اطلاعات، اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای، کنترل‌کننده‌ها و پردازشگرها است (The White House, 2003: 1). منظور از حملات سایبری[۱۹]نیز هرگونه تلاش برای تغییر، قطع، تنزل یا تخریب سیستم‌ها، شبکه‌ها، اطلاعات یا برنامه‌های رایانه‌ها است(Owens, et.al, 2009: 2). اما باید حملات سایبری را معضل قرن بیست و یکم دانست، در این قرن کشورها به توسعه روزافزون برنامه‌های خود در زمینه مدیریت الکترونیک و دولت الکترونیک افتخار می‌کنند و سرمایه‌گذاری‌های سنگینی بر روی کارخانه‌های انرژی صورت گرفته که همگی به وسیله سیستم‌های رایانه‌ای کنترل می‌گردند. تمامی سیستم‌های سود و زیان بانکی از طریق رایانه‌های آنلاین محاسبه می‌گردد. همه این پیشرفت‌ها موجب شده است تأمین امنیت ساختارهای حیاتی یک دولت به فناوری اطلاعات متکی شود. در واقع در قرن حاضر شیوه‌های جدیدی

---

[1] Cyberspace
[1] Router
[1] Cyber Attack
[7]
[8]
[9]

برای آسیب‌رسانی به دولت‌ها ایجاد گردیده است(Kulesza, 2010: 2). و ویروس‌ها و کرم‌های رایانه‌ای می‌توانند پایه‌های اقتصادی یک کشور یعنی بهابازار اقتصادی آن را فلج نمایند، این‌ها می‌توانند باعث قطع کامل برق فرودگاه‌ها شده و از کنترل هواپیماها جلوگیری نمایند و تصادفات شدید هوایی را ایجاد کنند و یا با ارسال پیام‌های نادرست به راکتورهای هسته‌ای باعث انفجارهای سهمگین گردند و یا با ایجاد اختلال در سیستم کنترل سدها و آب‌بندها، می‌توانند موجب ایجاد سیل‌های عظیم و ویرانگر شده و هزاران نفر را به کام مرگ بکشند؛ و حال همه این‌ها تنها بخش کوچکی از ابعاد وسیع این دست حملات است.

حقوق بین‌الملل برای مقابله با این معضل جهانی- حملات سایبری- و تعیین حقوق و تکالیف اعضای جامعه بین‌المللی در برخورد با این پدیده با چالش‌های متعددی روبه روست. نه کنوانسیون خاصی در این زمینه وجود دارد و نه عرف بین‌المللی واحدی که دولت‌های قربانی بدانند در برابر آن‌ها به چه اقداماتی متوسل شوند؛ و آنچه مسلم است، حملات سایبری نیازمند قانونمند شدن و ایجاد رویه واحد در عرصه بین‌المللی است(Joyner & Lotrionte ,2001: 863-864) اما به طور کلی برای آنکه حوزه حملات سایبری خالی از قواعد حقوقی نباشد، باید بتوانیم قواعد فعلی حقوق بین‌الملل را بر این حملات حمل نماییم. البته این مطلب را با توجه به آن مطرح می‌کنیم که اختلالات سایبری با مشخصات ویژه خود همچنان یک حوزه چالش‌برانگیز است. یکی از مهم‌ترین اقداماتی که در چارچوب قواعد حقوق بین‌الملل می‌توان به آن در مقابل حملات سایبری متوسل شد، نهاد دفاع مشروع است.

حق دفاع مشروع هم بر اساس حق ذاتی دولت‌ها و به موجب حقوق بین‌الملل عرفی مورد شناسایی قرار گرفته است و هم به عنوان یک استثناء برای ممنوعیت استفاده از زور که در بند ٤ ماده ۲ منشور وضع شده در ماده ۵۱ منشور

لحاظ شده است. یکی از مسائلی که بند ٤ ماده ۲ منشور که بر می‌انگیزد، نسبت میان قاعده منع توسل به زور در این ماده با سایر قواعد آمره است. چرا که حقوقدانانی همچون آنتونیو کاسسه، بر این عقیده‌اند که دفاع مشروع در زمره قواعد امره قرار دارد؛ و در اینجاست که مسئله تعارض چند قاعده از نوع قواعد امره پیش می‌آید و از طرفی همواره بر این نکته تأکید شده که قواعد آمره از قواعد حقوق طبیعی نیست که نتوان آن را تغییر داد و یک‌بار برای همیشه و تا ابد تثبیت شده باشد؛ و برعکس، همواره قواعد جدیدی می‌تواند در زمره قواعد آمره درآید و این یک امر پذیرفته شده است؛ بنابراین هم باید حدود و قلمرو حقوق بین‌الملل روشن شود و هم حدود قواعد آمره در زمینه منع توسل به زور، آن هم در ارتباط با سایر قواعدی که می‌توانند در زمره این قواعد شناخته شوند.(وحید،۱۳۸۵: ۲٦۳-۲٦٤) بر این اساس ماده ۵۱ منشور ملل متحد، دفاع مشروع را این‌گونه تعریف نموده است: «در صورت وقوع حمله مسلحانه علیه یک عضو ملل متحد تا زمانی که شورای امنیت اقدامات لازم برای حفظ صلح و امنیت بین‌المللی را به عمل آورد، هیچ‌یک از مقررات این منشور به حق ذاتی دفاع از خود، خواه به طور فردی و خواه دسته‌جمعی لطمه‌ای وارد نخواهد کرد...» در سالیان اخیر و پس از مداخله امریکا در عراق در سال ۲۰۰۳ این پرسش همواره مطرح بوده که آیا قواعد حقوق بین‌الملل در مورد توسل به زور عوض شده است یا نه؟ (وحید، ۱۳۸۵، ۲۵٦). مسئله مورد بحث در این مقاله، این است که حق دفاع مشروع مندرج در ماده ۵۱ منشور در نتیجه حملات سایبری به‌طور عام و در برابر حمله استاکس‌نت به تأسیسات هسته‌ای ایران به‌طور خاص قابل استنباط است یا نه؟ زمینه و علت این سؤال نیز علاوه بر اینکه به نو پیدایی و فقدان هرگونه سابقه و رویه بین‌المللی در این خصوص، به مفهوم حمله مسلحانه و گستره آن بر می‌گردد؛ بدین معنی که باید مشخص شود که آیا حمله سایبری از لحاظ ماهیت و آثار آن در حدی است که

یک حمله مسلحانه مورد نظر ماده ۵۱ منشور تلقی گردد؟ پس با توجه به آنچه در ماده ۵۱ منشور ملل متحد آمده است، ضرورت دارد تا دیدگاه‌ها پیرامون مفهوم حمله مسلحانه به عنوان یک عنصر اساسی در بحث دفاع مشروع مورد تأمل و بررسی قرار گیرد. از این رو مقاله پیش رو تمرکز خود را بر روی درک این مفهوم قرار می‌دهد و ضمن تحلیل مبانی نظری این مفهوم به تقابل مفهوم حمله مسلحانه با پدیده نوظهور حملات سایبری پرداخته و در آخر با مطالعه پرونده حمله استاکس-نت به تأسیسات هسته‌ای نطنز به نتیجه‌گیری در خصوص اعمال حق دفاع مشروع در برابر حملات سایبری خواهد پرداخت.

۲. تبیین مفهوم حمله مسلحانه

از آنجایی که منشور ملل متحد در مورد تعریف حمله مسلحانه[2] ساکت است باید برای تعیین معنای آن به سراغ حقوق عرفی و منابع مکمل (دکترین و رویه قضایی) برویم و رویکردهای گوناگون تفسیری نسبت به این مفهوم را مورد ارزیابی قرار دهیم. بر اساس یک تعریف کلی حمله مسلحانه به استفاده از زوری تلقی می‌شود که از بیرون مرزهای تحت حاکمیت دولت هدف سرچشمه گرفته باشد و فراتر از یک حادثه با مقیاس کوچک مثل فعالیت‌های مجرمانه یا حوادث مسلحانه منفرد باشد. مثلاً هرگاه کشوری کشتی‌های نظامی و یا هواپیماهای خود را در آب‌های بین‌المللی و یا در فضای جو علیه حاکمیت یک کشور هدایت کند و یا به طور قانونی در سرزمین دیگری حضور یابد و یا اتباع یک کشور را در سرزمین دیگر مورد هدف قرار دهد، هیچ‌یک جزء حملات مسلحانه محسوب نمی‌شود (Ruys, 2010: 8)؛ بنابراین، یک حمله مسلحانه زمانی اتفاق می‌افتد که دولت متجاوز ماشه اسلحه را می‌چکاند یا مثلاً هواپیماهایش به پرواز در می‌آیند یا

---

[2] Armed Attack

موشک‌هایش برای شلیک هدایت می‌شوند، به بیان دیگر امکان تغییر اندیشه دولت متجاوز وجود ندارد (Alexandrov, 1996: 164). برخی از حقوقدانان، حمله مسلحانه را این‌گونه تعریف نموده‌اند؛ عمل یا دسته‌ای از اعمال نظامی که هم دارای شدت لازم و هم دارای نتایج تخریبی و نابودگر بوده که به زیرساخت‌ها و عناصر حیاتی دولت قربانی آسیب می‌رساند(Constantinou, 2007: 63-64).

با توجه به ادبیات ماده ۵۱ منشور، می‌توان این‌گونه استنباط نمود که حملات منفرد و پراکنده مدنظر منشور ملل متحد نیست(Duffy, 2005: 152). این مسئله نیز یک مانع جدی برای اثبات مسلحانه بودن حملات سایبری است، چرا که عمدتاً این حملات پراکنده و منفرد هستند. دیوان بین‌المللی دادگستری نیز در قضیه نیکاراگوئه خاطرنشان می‌کند که اعمال نیروهای نامنظم می‌تواند در حد یک حمله مسلحانه باشد، در صورتی که از شدت یک حمله مسلحانه بالفعل نیروهای منظم برخوردار باشد. (قاسمی و بارین چهاربخش، ۱۳۹۰، ۱۷۹) مع‌الوصف، در ادامه با بررسی معیارهای تفسیری دفاع مشروع به این مورد نیز بیشتر می‌پردازیم؛ اما نکته‌ای که باید قبل از بررسی معیارها و مکاتب تفسیری مفهوم حمله مسلحانه مدنظر داشته باشیم، این است که حتی اگر همه دولت‌ها بهترین راهکارها را برای توافق بر سر معنای دفاع مشروع به موجب ماده ۵۱ به کار می‌بستند، باز هم در عمل موضوعاتی غیرقابل‌اجتناب مطرح می‌شود. از جمله این اختلافات، این است که در برخی موارد به سختی می‌توان دولت قربانی را از دولت مهاجم شناسایی کرد. چرا که محتمل است که هردو طرف درگیری به حق دفاع مشروع از خود استناد نمایند. مثلاً در جنگ ۲۰۰٦ رژیم صهیونیستی علیه حزب‌الله لبنان، دو طرف اظهار می‌کردند که در حال دفاع از خود و حفاظت از مردمشان هستند(Henderson, 2010: 223).

۲.۱. رویکرد مضیق به مفهوم حمله مسلحانه

طرفداران رویکرد مضیق به مفهوم حمله مسلحانه معتقدند که؛ اصطلاح حمله مسلحانه از لحاظ لغوی با سایر اصطلاحات مشابه آنکه در منشور ملل متحد به کار رفته است، متفاوت است؛ و ماهیتاً نیز مورد تفسیری به مراتب مضیق‌تر قرار می‌گیرد. به عنوان مثال امکان دارد اعمالی باشند که بر اساس بند ٤ ماده ۲ منشور به عنوان استفاده یا تهدید به زور قلمداد شوند؛ اما به آن سطح از حمله مسلحانه نرسد که بتوان در برابر آن‌ها به دفاع مشروع موضوع ماده ۵۱ منشور استناد نمود (Dinstein, 2002: 100-101). به بیان دیگر، این دسته از حقوقدانان معتقدند که انتخاب واژگان ماده ۵۱ به گونه‌ای عامدانه مضیق است؛ و به طور کلی سایر برداشت‌های موسع از دفاع مشروع، مثل دفاع پیش‌دستانه، دفاع در حمایت از اتباع و مداخله دموکراتیک هیچ‌گاه مورد پذیرش این دسته از حقوقدانان قرار نگرفته است؛ و این‌ها توجیه امریکا برای مداخله نظامی به گرانادا (در سال ۱۹۸۳) و پاناما (۱۹۸۹) را که بر پایه تفسیر موسع منشور استوار بود، نپذیرفتند(Gray, 2008: 127).در میان طرفداران این نوع رویکرد، دو معیار متفاوت برای حملات مسلحانه در نظر گرفته شده است، بر اساس معیار نخست: دفاع مشروع یک واکنش قانونی است که در برابر حمله مسلحانه صورت می‌پذیرد، منتها تجاوز مسلحانه سنگینی که بر علیه تمامیت ارضی و استقلال سیاسی یک کشور باشد و حیات آن دولت را به خطر اندازد(Cassese, 2005: 354)؛ اما در معیار دوم، برخلاف نخست که نتیجه حمله را مدنظر قرار می‌داد، آنچه اهمیت دارد میزان و نحوه خود حمله است. این معیار بیان می‌دارد که زمانی یک زور به سطح حمله مسلحانه می‌رسد که زور اعمال شده دارای شدت، استمرار و گستردگی کافی است. این معیار توسط سازمان جهانی صلیب سرخ برای شرح ماده ۲ کنوانسیون‌های ژنو ۱۹٤۹ برگزیده شده است (Sharp, 1999: 60). به نظر کاسسه شکل‌های با شدت کم توسل به زور نیز ممکن

است حمله مسلحانه تلقی نشوند. این موضوع در سال ۱۹۸٦ در رأی نیکاراگوئه توسط دیوان بین‌المللی دادگستری بیان شد و در قضیه سکوهای نفتی مورد تأیید دوباره قرار گرفت. ایشان علاوه بر این معتقدند که یک حمله باید به اندازه‌ای بزرگ باشد که به هیچ نحو دیگری نتوان آن را دفع نمود(Cassese, 2005: 354). دیوان در قضیه نیکاراگوئه برای اولین بار ضرورت وجود عنصر روانی قصد حمله مسلحانه را جهت وقوع حمله مسلحانه مطرح نمود (قاسمی و چهاربخش، ۱۳۹۰: ۱۹۲). همچنین دیوان در قضیه نیکاراگوئه اعلام کرد که تهاجم‌های بین مرزی که شدت و تأثیرشان کم است، می‌توانند به صرف درگیری‌های مرزی تلقی شوند و نه حمله مسلحانه (ICJ Reports, 1986, para.195). البته دیوان در قضیه سکوهای نفتی با استدلال امریکایی‌ها که شدت حملات ایران را به حدی می‌دانستند که حق دفاع مشروع را برای امریکا ایجاد کرده است، مخالفت نموده و با تأکید بر مواضع خود در پرونده نیکاراگوئه اجازه نمی‌دهد که معیار شدت (با این قرائت که حمله با هر میزان شدت، حق دفاع مشروع با همان شدت را می‌دهد.)، به معیاری برای تلقی نمودن حمله مسلحانه و در نتیجه تمسک به دفاع مشروع تبدیل شود و بیان می‌دارد که شدت حمله مربوط به رعایت اصل تناسب در واکنش به حمله است و ارتباطی به اینکه آیا حمله‌ای مسلحانه هست یا خیر، ندارد (Raab, 2004: 724-725)؛ اما در خصوص رویه دولت‌ها در مواجهه با این تئوری، باید به یکی از استدلال‌های امریکا برای حمله به افغانستان اشاره نمود. هرچند امریکا برای حمله به افغانستان در سال ۲۰۰۱ استدلال‌ها و دلایل زیادی را مطرح نمود، اما یکی از این دلایلی که توسط «درِک جینکز» مورد تأیید حقوقی واقع گردید، عبارت است از اینکه: «قلمرو، شدت و گستردگی حملات ۱۱ سپتامبر، موجب می‌شوند که این‌ها یک حمله مسلحانه محسوب شوند.» (موسوی، ۱۳۹۱: ۱۰۹). بر این اساس حملات مسلحانه باید از شدت لازم برای اینکه بتوان آن‌ها را به عنوان شدیدترین نوع توسل

به زور قلمداد نمود، برخوردار باشند. چرا که دیدیم دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه به شدت کافی حمله اشاره نموده بود.

۲.۲. رویکرد موسع به مفهوم حمله مسلحانه

در تشریح این رویکرد باید به سراغ نظریات حقوقدانان برویم. به نظر مالکوم شاو، این غیرمحتمل است، اگر کسی بخواهد مفهوم دفاع مشروع را محدود به وقوع یک حمله مسلحانه واقعی (فیزیکی) نماید(Shaw, 2008: 1137). بر اساس این رویکرد، ماده ۵۱ منشور با حمله توسط دولت ملازمه ندارد؛ و دفاع مشروع می‌تواند در پاسخ به یک حمله تروریستی که حتی توسط دولت محقق نشده باشد، مورد استفاده قرار گیرد. این مسئله پس از حملات تروریستی ۱۱ سپتامبر در امریکا، به موجب قطعنامه ۱۳٦۸ شورای امنیت (سال ۲۰۰۱) صراحتاً مورد شناسایی و پذیرش قرار گرفت (Aust, 2005: 227). در واقع حقوقدانانی که معتقد به این رویکرد می‌باشند، به دولت‌ها این حق را می‌دهند که در برابر هرگونه اعمال زور و فشار قهری دست به دفاع مشروع بزنند و در خصوص به خطر افتادن امنیت بین‌المللی با تفسیر موسع از ماده ۵۱ منشور، این‌گونه پاسخ می‌دهند که مفهوم موسع «حمله مسلحانه» می‌تواند با اعمال منطقی اصول ضرورت و تناسب که سنگ بنای مجوز توسل به زور در دفاع مشروع هستند، مرتفع گردد (نیاورانی، ۱۳۸٦: ٤٤۲). ولی به طور کلی، این رویکرد تا به امروز نتوانسته اقبال جامعه بین‌الملل را به خود جلب نماید؛ اما یکی از تئوری‌های قابل دفاع این مکتب، تئوری تجمیع وقایع[۲۱] است که ارتباط نزدیکی با پدیده حمله سایبری پیدا می‌کند. این تئوری از مباحث بحث برانگیز حقوق بین‌الملل در خصوص دفاع مشروع است و این پرسش را مطرح می‌کند که آیا تجمیع حملات با شدت کم یا تجمیع وقایع گوناگون امکان

---

[2] Accumulation of Events Theory[1]

حق دفاع مشروع را به قربانی می‌دهد یا خیر؟ (Blank, 2013: 417) به طور کلی یک حمله مسلحانه می‌تواند به روش‌های گوناگونی اتفاق بیفتد و طیف این‌گونه حملات از تاخت‌وتازهای با ابعاد وسیع آغاز می‌شود؛ در این حالت یعنی حملات شدید و گسترده چندان بحث و تردیدی در اینکه حمله مسلحانه است وجود ندارد؛ اما در مواردی ممکن است یک سری از عملیات نظامی با مقیاس کوچک توسط یک کشور علیه کشور هدف اعمال شود، به گونه‌ای که یک ارتباط منطقی چه از لحاظ جغرافیایی و چه از لحاظ دوره زمانی وجود داشته باشد، در این صورت این اعمال تشکیل حمله مسلحانه را می‌دهد. این بحث به تئوری تجمیع رخدادها برمی‌گردد(Gill & Ducheine, 2013: 445). بدین ترتیب که اگرچه با یک حمله مسلحانه شدید و گسترده روبرو نیستیم ولی وقوع حملات پراکنده و در ظاهر کوچک در یک دوره زمانی و مکانی مشخص نشان می‌دهد که این وقایع قابل تجمیع است و حمله مسلحانه واحدی را تشکیل می‌دهد.

«آلبرتوکول»[1] از حقوق‌دانان بین‌المللی در سال ۱۹۹۵ این‌گونه به تئوری تجمیع وقایع پرداخت که جنگ‌های سنتی که از آغاز قرن بیستم به طور فزاینده‌ای رشد پیدا کرده، به دلیل خطرات و خسارات گسترده اقتصادی، نظامی و سیاسی، بسیاری از دولت‌ها و نهادهای غیردولتی را به سمت تغییر شیوه‌های ابراز خشونت برده و این شیوه‌های نوین را به بخشی از سیاست خارجی آن‌ها مبدل نمود. در واقع بنابراین نظر سناریوی جنگ‌های با شدت کم از آن جهت مورد استقبال و انتخاب واقع شد که یک ادعای مشروعیت ساختگی را با خود به همراه داشت(Coll, 1995:6- 7). دیوان در بخشی از رأی پرونده سکوهای نفتی به این تئوری اشاره کرده، اما تحلیل دقیقی در این زمینه ارائه نمی‌نماید. دیوان به اظهارات نماینده دائم امریکا در سازمان ملل متحد اشاره می‌کند که بیان کرده بود: «حمله به

[1] Coll, Alberto

کشتی «شهر جزیره دریایی»[1] آخرین حمله از سری حملات موشکی علیه کشتی‌های دارای پرچم امریکا و سایر کشتی‌های غیرمتخاصم بوده (منظور کشتی‌های غیر عراقی است، چرا که در زمان رخداد این حوادث، ایران درگیر جنگ با کشور عراق بود) که برای اهداف تجاری در آب‌های کویت فعالیت می‌کردند.» دیوان در پاسخ به این اظهارات بیان می‌دارد که با در نظر گرفتن جمیع رخدادها و با محفوظ نگه داشتن مسئله مسئولیت ایران، به نظر دیوان نمی‌رسد که این رخدادها بتوانند حمله مسلحانه علیه امریکا تلقی شوند (ICJ Reports, 2003, paras.46-64). با وجود آنکه دیوان به طور صریح تئوری تجمیع وقایع را نه تحلیل و نه تأیید نمود و با وجود آنکه در هنگام مطرح شدن این تئوری در شورای امنیت، شورا نیز از تأیید این تئوری خودداری کرده و همچون گذشته، در مورد پرونده‌های مربوط به دفاع مشروع، سعی کرده با بررسی دقیق واقعه بدان پاسخ دهد و رسیدگی موردی به پرونده‌ها را بر هر دکترین دیگری در این زمینه ترجیح دهد(Gray, 2008: 155). (اما برخی از حقوقدانان بر این باورند که دیوان این تئوری را پذیرفته و وقوع حمله مسلحانه به صورت مجموعه‌ای از چند حمله کوچک را امکان‌پذیر دانسته است. دیوان بین‌المللی دادگستری در دسامبر سال ۲۰۰۵، در خصوص شکایت جمهوری دموکراتیک کنگو علیه اوگاندا، رأی خود را در خصوص حقوق توسل به زور مرتبط با فعالیت‌های نظامی اوگاندا صادر نمود. دیوان در بند ١٤٦ این رأی حکم می‌کند: «اگر مجموعه حملات صورت گرفته را بتوان یکجا در نظر گرفت و حمله مسلحانه قلمداد نمود، بازهم قابل استناد برای کنگو نیستند.» (ICJ Reports 2005.The Armed Activities on the Territory of the Congo Case,para,146)

این اظهارنظر دیوان موجب گردیده است که برخی حقوقدانان به این نتیجه برسند که دیوان مجدداً احتمال اینکه انباشتی از حملات با مقیاس کوچک را بتوان

[1] Sea Isle City

یک حمله مسلحانه محسوب و علیه آن اقدام به دفاع مشروع نموده، رد نکرده است (Gray, 2008: 156). در واقع اگر مجموع حملات انجام‌شده فاصله زمانی بیش از اندازه نداشته باشد و عرفا بتوان آن‌ها را یک حمله در نظر گرفت اعمال دفاع مشروع در برابر آن‌ها می‌تواند از نظر حقوقی توجیه گردد. این تئوری در سال‌های آینده بر اثر گسترش احتمالی حملات سایبری بیش‌تر از گذشته مورد استناد قرار خواهد گرفت.

۳. تقابل مفهوم حملات مسلحانه با حملات سایبری

با وجود اینکه اصطلاح جنگ سایبری در ادبیات متداول رسانه‌ای و حقوقی زیاد به کار می‌رود؛ اما بخش اندکی از فعالیت‌ها و حملات سایبری که صورت می‌گیرد، به گونه‌ای هستند که حقوق جنگ بر آن‌ها حاکم باشد (Hathaway, et.al, 2012: 839). در واقع تمامی موقعیت‌هایی که به عنوان حمله سایبری قلمداد می‌شود، آن حمله مسلحانه‌ای که به موجب دفاع مشروع در حقوق بین‌الملل مدنظر است، نیست. اکثر وقایع و رخدادهایی که حمله سایبری نامیده می‌شود تشکیل استفاده از زور نمی‌دهد و پایین‌تر از حد یک حمله مسلحانه است. حمله سال ۲۰۰۷ به استونی که موجب یک اختلال چندساعته و آسیب جزئی شد از این دست مثال‌هاست که واقعه به حد یک حمله مسلحانه نمی‌رسد. مثال‌های بی‌شماری می‌توان عنوان کرد که صرفاً یک هک رایانه‌ای یا جاسوسی یا خرابکاری و سرقت اطلاعات و یا سرقت اموال معنوی محسوب می‌شوند و تشکیل یک حمله مسلحانه را نمی‌دهند (Rid, 2013: 4-5). در واقع باید حملات سایبری را از تهدیدات امنیتی سایبری[1] تفکیک نماییم؛ و بدانیم که فعالیت‌های مجرمانه سایبری[2] جاسوسی

[1] Cyber security threats
[2] Cyber-criminal activities

سایبری[1] و انواع گوناگون نفوذ به سیستم‌های رایانه‌ای از جمله سرقت اطلاعات و خرابکاری عمدی در سیستم‌های رایانه‌ای متعلق به بخش عمومی یا خصوصی و با وجود جدی بودن این تهدیدات برای امنیت اقتصادی و ملی دولت، داخل در تعریف حمله سایبری قرار نمی‌گیرد و تابع قواعد دفاع مشروع نیز نمی‌شوند؛ اما چنین اقداماتی ممکن است یک مداخله غیرقانونی تلقی شوند یا بتوان آن‌ها را به اقسام دیگری از نقض حقوق ملی یا حقوق بین‌الملل مرتبط ساخت؛ اما نکته قابل توجه این است که هیچ وفاق عامی میان دولت‌های گوناگون و میان سازمان‌های بین‌المللی یا منطقه‌ای برای تعریف مشترک از حمله سایبری وجود ندارد(اصلانی و رنجبریان، ۱۳۹٤، ۲۷۵). مع‌الوصف مفهوم حمله سایبری دارای دو مفهوم عام و خاص است، در مفهوم عام هرگونه مخاطره سایبری را می‌توان یک حمله سایبری نامید. در خصوص مفهوم خاص حمله سایبری – که توأم با تخریب و آسیب گسترده به زیرساخت‌های حیاتی یک کشور است– اتفاق‌نظر وجود ندارد. با این حال باید توجه داشت در حالتی که یک دولت قصد جنگیدن با دولت دیگر را داشته باشد، سعی می‌کند برای انجام یک حمله همه جانبه از تمامی روش‌های نظامی ممکن استفاده نماید؛ بنابراین در این موارد که حمله سایبری در کنار سایر جنگ‌افزارهای متداول استفاده می‌شود، شکی در مسلحانه بودن حمله سایبری نداریم. به طور کلی این نوع حملات متداول‌ترین نوع حملات سایبری است و کمتر رخ می‌دهد که کشوری برای جنگ و عملیات نظامی تنها از حمله سایبری بهره گیرد(Gill & Ducheine, 2013: 436-440). حمله اسرائیل به تأسیسات هسته‌ای «الکیبر»[2] در شمال سوریه در سپتامبر ۲۰۰۷ از آن نمونه‌هایی است که به وضوح حملات سایبری، به عنوان حمله مسلحانه تلقی می‌شود، چرا که این حملات در کنار

[1] Cyber espionage
[2] Al-Kibar

حملات فیزیکی متداول (سنتی) رخ داده و موجب آماده‌سازی بستر جنگی و میدان نبرد شده است. در واقع از طریق حملات سایبری شرایط مساعدی برای انجام یک عملیات موفقیت‌آمیز همه جانبه فراهم شده است (Gill & Ducheine, 2013: 462). البته صرف همراهی حملات سایبری با حملات فیزیکی موجب نمی‌شود که این حملات، مسلحانه تلقی شوند. در واقع حملات سایبری در این موارد یا باید به آماده سازی فضا برای حملات فیزیکی کمک نماید یا اینکه دوش به دوش حملات فیزیکی هرچند با شدت کم به پیکار با مواضع دشمن بپردازد.

در درگیری میان روسیه و گرجستان در سال ۲۰۰۸، تأثیرات حمله سایبری بسیار محدود بوده و حتی از لحاظ زمانی نیز این حملات به اندازه‌ای طول نکشیدند که بخواهند تشکیل یک حمله مسلحانه بدهند. با وجود این اگر این حملات فراتر از محو نمودن وب سایت دولتی و آسیب‌رسانی به بخش‌های عمومی بودند. مثلاً اگر با خنثی نمودن سلاح‌ها و یا سیستم‌های ارتباط نظامی، از عملیات نظامی حمایت می‌کردند، قطعاً تشکیل حمله مسلحانه می‌دادند. در واقع اگر از حملات سایبری بدین روش استفاده می‌نمودند، می‌توانستیم بگوییم که حملات سایبری بخشی از آن حمله مسلحانه همه‌جانبه است که علاوه بر حملات نظامی متداول از حملات سایبری هم استفاده شده است؛ و یا حملات سایبری به آماده سازی فضا برای حمله فیزیکی کمک نموده است(Gill & Ducheine, 2013: 461). و به طور کلی در جایی که حمله سایبری به تنهایی صورت می‌پذیرد (بدون اینکه همراه با حمله فیزیکی باشد). در اکثر موارد تشکیل حمله مسلحانه نمی‌دهد. البته این بدین دلیل است که اکثر این‌گونه حملات پتانسیل لازم برای ایجاد تلفات فیزیکی و یا ایجاد بحران‌های بنیادی در ساختارهای حیاتی یک دولت را ندارند. وگرنه یک حمله خرابکارانه سایبری علیه مرکز کنترل و فناوری اطلاعات کارخانه‌های شیمیایی که توانایی ایجاد خسارتی همچون نشت گازهای سمی را

دارد، بالاخص در زمانی که این کارخانه‌ها نزدیک به مراکز پرجمعیت واقع شده باشند (مانند کشور هلند که تأسیسات شیمیایی شل نزدیک به بندر و شهر روتردام واقع شده است.) قطعاً یک حمله مسلحانه تلقی می‌شوند(Schmitt, et.al, 2013: 460).

برای درک اینکه کدام‌یک از حملات سایبری تشکیل حمله مسلحانه می‌دهد، باید به سراغ دکترین حقوقی برویم، چرا که در این زمینه نه معاهده‌ای وجود دارد و نه تابه‌حال هیچ دولتی در پاسخ به یک حمله سایبری متوسل به حمله مسلحانه شده است تا به بررسی رویه دولت‌ها و عرف‌های احتمالی بپردازیم. دکترین نقش مؤثری در تشخیص و تصریح قواعد نانوشته حقوق بین‌الملل (عرف و اصول کلی) دارد. دکترین اگرچه ایجادکننده این قواعد نبوده ولی می‌تواند با کمک به شناسایی موجودیت آن‌ها به تدوین برخی قواعد نانوشته حقوق بین‌الملل پرداخته و کمک به شکل‌گیری قواعد در زمینه‌های جدید حقوق بین‌الملل یا قواعد در حال تغییر سریع، نماید؛ مانند حقوق فضا که بخش مهمی از آن مرهون دکترین بوده است. در دکترین حقوق بین‌الملل سه دیدگاه یا سه معیار متفاوت برای مسلحانه انگاشتن حملات سایبری وجود دارد که عبارت‌اند از: دیدگاه ابزارمحور، دیدگاه هدف‌محور و دیدگاه نتیجه‌محور(Hathaway, et.al, 2012: 845-846) . البته معیارهای مطرح شده مختص زمانی است که یک حمله سایبری تنها بکار گرفته شود و همان‌طور که گفته شد اگر حملات سایبری به همراه سایر حملات یا مقدمه‌ای برای حملات سنتی و یا تسهیل‌کننده این‌گونه حملات باشد؛ در مسلحانه بودن آن تردیدی وجود ندارد.

۳.۱. دیدگاه ابزارمحور[1]

شیوه ابزارمحور نامی است که برای شیوه سنتی تحقیق در زمینه حملات مسلحانه انتخاب گردیده است. بر اساس این دیدگاه تقریباً هیچ‌گاه حملات سایبری تشکیل حمله مسلحانه مدنظر ماده ۵۱ منشور ملل متحد را نمی‌دهد. علت این امر این است که حملات سایبری، مشخصه‌های فیزیکی که باید به طور متداول با حملات نظامی همراه باشند را دربر ندارد. به بیان دیگر به طور کلی حملات سایبری سلاح‌های نظامی سنتی محسوب نمی‌شوند. این دیدگاه حملات سایبری را تنها زمانی به عنوان یک حمله مسلحانه قلمداد می‌نماید که اگر آن‌ها مانند سلاح‌های نظامی بکار گرفته شوند. به طور مثال: اگر از آن‌ها برای بمباران سرورهای رایانه یا کابل‌های اینترنتی استفاده شود و از شدت کافی برخوردار باشند، می‌توان آن‌ها را حمله مسلحانه قلمداد نمود(Hollis, 2007: 1041).

طرفداران این دیدگاه به دو سند مهم اشاره می‌کنند که در آن‌ها برای تمیز حملات مسلحانه از سایر حملات، از معیار ابزارمحور استفاده شده است. نخست ماده ٤١ منشور ملل متحد است(Hathaway, et.al, 2012: 846) که اقداماتی همچون قطع ارتباط تلگرافی و رادیویی را در دسته اقداماتی که متضمن استعمال نیروهای مسلح نیست، قرار می‌دهد. در پاسخ باید گفت حتی اگر فرض نماییم که منشور رویه ابزارمحور را اتخاذ نموده است؛ نمی‌توانیم این ماده را به حملات سایبری توسعه دهیم و این‌گونه استنباط نماییم که حملات سایبری نیز از شمول حملات مسلحانه خارج است، چرا که در تفسیر این ماده باید از یکی از دو روش عینی یا ذهنی استفاده شود. بر اساس روش ذهنی قصد و نیت طرف‌های معاهده ملاک تفسیر قرار می‌گیرد. پس بر اساس این روش، حملات سایبری که در زمان انعقاد این معاهده بروز خارجی نداشته است، هیچ‌گاه نمی‌توانسته در قلمرو قصد و نیت واضعین

---

[1] Instrument-based approach

منشور قرار گیرد. ترجیح قصد و یقین متعاهدین بَر سَنَد، مطابق با اصل انصاف است. دیوان دائمی دادگستری بین‌المللی در بسیاری از آراء خود، از جمله در قضیه امتیازات ماورو ماتیس[۲] (۱۹۲۵) قصد واقعی متعاهدین را بر متن معاهده ترجیح داده است؛ و روش دوم، روش عینی است که بر اساس آن تفسیر معاهده با توجه به اوضاع و احوال زمان انعقاد معاهده صورت می‌پذیرد؛ به بیان دیگر از آنجایی که معاهده تجلی قاعده حقوقی است که هدفش حکومت بر مناسبات اجتماعی است. در نتیجه، این قاعده نمی‌تواند جدا و مستقل از اوضاع و احوال مربوط به ایجادش باشد (ضیایی بیگدلی، ۱۳۸۸: ۱۷۳-۱۷۱). از آنجایی که حملات سایبری در بازه سال‌های ۱۹٤۳ تا ۱۹٤٥ (سال‌های تصویب منشور ملل متحد) نه‌تنها رخ نداده است، بلکه تصور آن هم بر اساس اوضاع و احوال حاکم غیرممکن بوده است، پس بر اساس تفسیر عینی نیز می‌توان این‌گونه استنباط نمود که موارد مذکور در ماده ٤۱ منشور شامل حملات سایبری نمی‌شود. تفسیر عینی به صراحت در ماده ۳۲ کنوانسیون حقوق معاهدات وین مورد اشاره قرار گرفته است.

سند دومی که طرفداران مکتب ابزارمحور بدان اشاره می‌کنند؛ اعلامیه سال ۱۹۷٤ مجمع عمومی سازمان ملل در مورد تعریف تجاوز (UN.Doc. A/RES/29/3314) است؛ که معتقدند این سند به طور ضمنی از دیدگاه ابزارمحور حمایت نموده است. ماده ۳ این اعلامیه به تشریح تعدادی از اعمال که تشکیل تجاوز (تجاوز مدنظر در ماده ۳۹ منشور) می‌دهند، پرداخته است. ماده ۳ در بیان تمامی مصادیق تنها در صورتی اعمال را تجاوز قلمداد می‌نمایند که به شکل «زور یا سلاح نظامی» استفاده شوند(Hathaway, et.al, 2012: 846). درست است که هیچ‌کدام از مصادیق ماده ۳ نمی‌توانند دربردارنده حملات سایبری باشد، اما لازم به ذکر است که انتهای ماده اشاره شده است که این لیست اعمال، حصری نیست؛ و

[2] THE MAVROMMATIS JERUSALEM CONCESSIONS, series A, No. 5, march 26th 1925.

به طور کلی در پاسخ به این استدلال باید گفته شود که تجاوز مدنظر این قطعنامه فراتر از حمله مسلحانه مذکور در ماده ۵۱ منشور ملل متحد است و نمی‌توان به راحتی از آن وحدت ملاک گرفت.

سهولت در به‌کارگیری و اعمال، مزیت مهم و عمده نگرش ابزارمحور است؛ چرا که استفاده از سلاح‌های نظامی نسبتاً به آسانی قابل‌شناسایی است. مع‌ذلک از آنجایی که حملات سایبری پتانسیل ایجاد خسارت‌های فاجعه‌بار بدون به‌کارگیری از سلاح‌های نظامی سنتی و متداول را دارند تقریباً تمامی حقوقدانان نظریه ابزارمحور را رد کرده و به‌کارگیری این دیدگاه را خطرناک و منسوخ اعلام کرده‌اند. به طور کلی اگر در خصوص حملات سایبری و ماده ۵۱ منشور تمرکز را بر روی ابزار استفاده شده قرار دهیم، ممکن است به این نتیجه برسیم که سیگنال‌های الکترونیکی که حواس انسانی آن‌ها را درک نمی‌کند شبیه هیچ بمب، گلوله و سربازی نیستند اما به نظر می‌رسد که منفعت جامعه جهانی در این است که حملات سایبری را مسلحانه فرض نماییم (Department of Defense & Office of General Counsel, 1999: 22). این منفعت در پرتو اهداف و اصول حقوق بین‌الملل قابل درک و تحلیل است. حفظ و تقویت صلح و امنیت بین‌المللی مهم‌ترین هدف نظم حقوقی بین‌المللی مبتنی بر منشور ملل متحد است که باید در چارچوب و از طریق اصول حقوق بین‌الملل به دست آید. ممنوعیت کاربرد زور و تهدید به آن در روابط بین دولت‌ها سرآمد این اصول برای تأمین صلح و امنیت است. از این رو، مسلحانه تلقی کردن حملات سایبری و در نتیجه ممنوعیت آن، زمینه اجرای بهتر این اصل و حاکمیت آن در روابط بین دولت‌ها را فراهم می‌کند.

۳.۲. دیدگاه هدف محور[3]

بر این اساس تنها زمانی یک حمله سایبری، حمله مسلحانه تلقی می‌شود که سیستم رایانه‌ای مورد حمله از اهمیت کافی و حیاتی برخوردار باشد (Hathaway, et.al, 2012: 847). به بیان دیگر طرفداران این تئوری معتقدند که حملات سایبری اگر در یک زیرساخت ملی حیاتی نفوذ کند، فارغ از آنکه آیا هنوز موجب خسارات فیزیکی یا تلفات شده است، حمله مسلحانه قلمداد خواهد شد و به کشور هدف این حق را می‌دهد که به دفاع مشروع تمسک جوید(Sharp, 1999: 129-130).

در حملات سنتی، تفاوتی نمی‌کند که مواضع مورد حمله نظامی باشد یا غیرنظامی، مواضع حساس باشد یا غیرحساس، مواضعی باشد که با منافع ملی دولت قربانی ارتباط دارد یا ندارد؛ اما در حملات سایبری که موجب تخریب و ویرانی در حد یک حمله نظامی سنتی نشده باشد؛ زمانی حمله سایبری، یک حمله مسلحانه قلمداد می‌شود که موضع مورد حمله، از زیرساخت‌های حیاتی دولت قربانی باشد(Dinstein, 2005: 105). پس بر اساس این تئوری می‌توانیم نتیجه بگیریم که حتی در غیاب صدمات فیزیکی هم یک حمله می‌تواند حمله مسلحانه تلقی شود؛ و فقط کافی است که به زیرساخت‌های حیاتی و ملی نفوذ کرده و پتانسیل ایجاد اختلال در عملکردهای اساسی یک دولت را داشته باشد و بتواند ثبات یک کشور را مورد تهدید قرار دهد؛ و یا اینکه حمله‌ای بتواند در یک دوره طولانی مدت موجب ناتوانی دولت قربانی گشته به گونه‌ای که در یک دوره زمانی معقول نتواند به حالت اولیه بازگردد؛ در این صورت نیز حمله سایبری یک حمله مسلحانه قلمداد می‌گردد.

---

[3] Target-based approach

تعدادی از دولت‌ها از جمله امریکا، روسیه و کانادا این موضع‌گیری را در راهبردهای امنیت ملی فضای سایبری خود مورد پذیرش قرار دادند؛ و بسیاری از کارشناسان به این توافق رسیده‌اند که حملات با این سطح از توانایی هرچند که در فضای سایبری صورت می‌گیرند؛ اما به سطح یک حمله مسلحانه رسیده‌اند (Gill & Ducheine, 2013: 444-445). به طور کلی مثال‌هایی که برای حملات سایبری و عواقب آن‌ها بیان می‌شود، معمولاً عبارت است از: حمله به کارخانه‌های انرژی هسته‌ای با هدف از کار انداختن سیستم خنک‌کننده آن‌ها و ایجاد فاجعه‌ای فوکوشیما گونه، یا ایجاد اختلال در سیستم کنترل حمل‌ونقل هوایی با هدف ایجاد تصادفات هوایی و ایجاد اختلال در سیستم کنترل سدهای آبی و ایجاد سیل‌های مخرب و فاجعه‌آمیز است. این دست اقدامات قطعاً و بدون شک به حد یک حمله مسلحانه می‌رسند فارغ از اینکه تئوری هدف‌محور مدنظر باشد و بدون آنکه نیاز باشد که این حملات همراه با حملات گسترده فیزیکی همراه باشند. پس بر اساس این تئوری، علاوه بر حمله به زیرساخت‌ها یا پتانسیل تخریب آن‌ها، فاکتور دیگری که در مسلحانه بودن حملات سایبری نقش اساسی دارد، قصد نهانی از این حملات است(Clarke & Knake, 2010: 65-66). بر این اساس از کار انداختن سیستم راداری یا موشکی یک کشور که مزیت نظامی غیرقابل‌انکاری دارد را به صرف اینکه موجب تلفات جانی یا تخریب نشده است را به سختی می‌توان حمله‌ای مسلحانه تلقی نکرد (خلف رضایی، ۱۳۹۲، ۱۳۵)

هدف مقدماتی از نگرش هدف‌محور این است که مواقعی را که یک حمله سایبری در بر دارنده یک آسیب کافی و قریب‌الوقوع است را تعیین نماید تا بتوان از این طریق پاسخ به شیوه دفاع پیش‌دستانه را توجیه نمود(Hollis, 2007: 1041)؛ اما مزیت دیدگاه هدف‌محور این است که حمایت از زیرساخت‌های حیاتی را تضمین می‌کند، اما به دلیل آنکه استناد به دفاع مشروع را تسهیل می‌نماید و موجب افزایش

احتمال منازعات سایبری و حتی افزایش جنگ‌های مسلحانه ویرانگر سنتی می‌شود، مورد نقد قرار گرفته است(Sklerov, 2009: 54). به بیان دیگر طبق تئوری هدف‌محور تنها کافی است که یک حمله سایبری به سیستم‌ها و زیرساخت‌های حیاتی نفوذ کند تا دولت مورد حمله، به پاسخ نظامی به شیوه یک جنگ فیزیکی کلاسیک متوسل شود. به نظر می‌رسد که این تئوری امنیت جامعه بین‌المللی را به خطر انداخته و افزایش جنگ را در پی داشته باشد(Hathaway, et.al, 2012: 847). شاید مهم‌ترین زنگ خطر برای کشورهایی مثل ایران در این مورد به صدا درآید. چرا که کشور ما هم قربانی حملات سایبری قرار گرفته و هم در مواردی متهم به اعمال حمله سایبری علیه دشمنان خود شده است. هیچ بعید به نظر نمی‌رسد که کشورهای ابرقدرت، هنگام تحلیل حملات سایبری که ایران را متهم به آن کرده‌اند از این تئوری پیروی نمایند. در حالی که در طرف مقابل در مورد حملات سایبری خود علیه ایران با استناد به تئوری‌های ضعیفی مثل تئوری ابزارمحور، ایران را از حق دفاع مشروع خود محروم نمایند؛ اما خوشبختانه رویه دولت‌ها و بیانیه‌های سیاسی و رسمی آن‌ها به اندازه‌ای نیست که بخواهیم نتیجه بگیریم که حملاتی که پتانسیل از بین بردن انسان‌ها و وارد آوردن خسارت به اموال و ایجاد صدمات فیزیکی را ندارند یک حمله مسلحانه تلقی شوند؛ و تئوری هدف محور از مقبولیت کافی برخوردار نیست. (Gill & Ducheine, 2013: 445).

۳.۳. دیدگاه نتیجه محور (اثر محور)[4]

این دیدگاه برای دسته‌بندی حملات سایبری به عنوان حمله مسلحانه معیار شدت تأثیرات و نتایج آن‌ها را مدنظر قرار می‌دهد. اگر طیفی را در نظر بگیریم که ۲ تئوری (دیدگاه) قبلی در دو سر این طیف قرار بگیرند، این دیدگاه سوم در میانه

[4] Effects-based approach

طیف و بین دو دیدگاه قرار می‌گیرد. تئوری اثر محور مورد پذیرش گسترده حقوقدانان بین‌المللی و جامعه جهانی قرار گرفته است. البته برای اندازه‌گیری شدت تأثیر، تفسیرهای گوناگونی از تئوری اثرمحور صورت گرفته و عوامل گوناگونی را برای اتخاذ مسلحانه بودن حمله سایبری ملاک قرار داده‌اند؛ و طیف وسیعی ایجاد شده که در یک سر آن محض شدت صدمه را ملاک قرار داده و در سر دیگر طیف کشف رابطه علّی بین حمله سایبری و خسارت‌ها را مدنظر قرار داده‌اند؛ اما تمامی تفسیرهای مکتب اثرمحور یک جهت‌گیری مشترک در زمینه ارجاع به نهادی برای تحقیق دارند(Hathaway, et.al, 2012: 848). نام دیگر این تئوری، دکترین توازن سایبری[5]است. این دکترین توسط برخی از حقوقدانان به منظور ایجاد یک دکترین دفاعی برای امریکا در برابر حملات سایبری طرح‌ریزی شده است. ریچارد کلرک[6] یکی از این حقوقدانانی است که دکترین توازن سایبری را ارائه می‌دهد. دکترین او اشاره دارد که حملات سایبری باید با توجه به اثراتشان قضاوت شوند و نه با توجه به ابزارهای سایبری بکار رفته در حملات. به بیان دیگر این دکترین بیان می‌کند که در هر مورد که حمله سایبری به وقوع پیوسته است، باید این‌گونه فرض نماییم که اگر به جای این حمله یک حمله نظامی فیزیکی با همان آثار و نتایج به وقوع پیوسته بود، آنگاه در پاسخ به آن، چه حمله فیزیکی یا روش دیگری می‌تواند اتخاذ شود؟(Clarke & Knake, 2010: 178)

با این حال درک این مسئله که کدام دسته از آثار حملات توجیه‌کننده دفاع مشروع هستند، از مشکلات این تئوری است. برای درک بهتر این مسئله باید به مثال‌های زیر توجه نمود: ۱) حمله سایبری به سیستم کنترل حمل‌ونقل هوایی، ۲) حمله به نیروگاه‌های برق منطقه‌ای، ۳) حمله سایبری به بازار سهام نیویورک (یا حمله به هر

---

[5] Doctrine of cyber equivalency
[6] Richard Clarke

شبکه مالی دیگر)، ٤) حمله سایبری به وب‌سایت‌های مهم استونی در سال ۲۰۰۷. حال سؤال این است که کدام‌یک از این حملات باید یک حمله مسلحانه تلقی شود؟ و در پاسخ به کدام‌یک از آن‌ها می‌توان به دفاع مشروع استناد نمود؟ همه این مثال‌ها ممکن است در سطح گسترده یا حتی بسیار پایین موجب مرگ انسان‌ها شوند و موجب خسارت به زیرساخت‌های حیاتی کشور شوند؛ اما پیش‌بینی نتایج حمله برای کشور متجاوز بسیار دشوار خواهد بود؛ و متأسفانه تفسیرهای مختلف تئوری اثرمحور در خصوص مثال‌های مطروحه، نتایج متفاوتی را ارائه می‌دهند(Hathaway, et.al, 2012: 848). اولین طرفدار مکتب اثرمحور پرفسور مایکل اشمیت است که برای مسلحانه بودن حمله سایبری بر اساس این مکتب ٦ معیار را مطرح نموده است: ۱) شدت: منظور نوع و میزان صدمه است؛ ۲) فوریت: در اینجا فاصله زمانی میان خسارت و حمله سایبری مدنظر است که باید خسارت به سرعت بعد از حمله به وقوع پیوسته باشد؛ ۳) مستقیم و بی‌واسطه بودن: بر این اساس باید بین خسارت ایجاد شده و حمله یک زنجیره روابط علی وجود داشته باشد؛ ٤) خاصیت تهاجمی: منظور آن است که حمله سایبری باید به اندازه کافی در قلمرو حاکمیت دولت قربانی نفوذ کرده باشد؛ ۵) قابلیت اندازه‌گیری: حمله سایبری باید به اندازه‌ای باشد که بتوان خسارت حاصله را اندازه‌گیری نمود؛ ٦) غیرقانونی بودن حمله: حملات سایبری زمانی به عنوان یک حمله مسلحانه تلقی می‌شوند و می‌توان در مقابل آن‌ها به دفاع مشروع استناد نمود که به طور غیرقانونی آغاز شده باشند(Schmitt, 1999: 914-915).

برخی دیگر از حقوقدانان که ظاهراً طرفدار همین تئوری اثرمحور هم هستند، معیار خاصی را برای مسلحانه بودن حملات سایبری ارائه نداده‌اند. بلکه بیشتر بر شدت خسارات و نوع آن‌ها اشاره دارند؛ و بیان می‌کنند که اگر نتایج قابل پیش‌بینی از یک حمله سایبری منجر به تلفات جانی و خسارت مادی به اموال گردد. یا حتی

اگر شدت نتایج قابل پیش‌بینی از حمله شبیه به نتایج یک حمله و جنگ مسلحانه باشد، می‌توان آن حمله سایبری را یک حمله مسلحانه قلمداد نمود(Silver, 2002: 90-91). البته معیاری که این دست از حقوقدانان تعریف کرده‌اند، نیز خالی از ابهام نیست. چرا که به سختی می‌توان نتایج حاصل از حمله سایبری را پیش‌بینی نمود. البته شاید در مورد یک سری وقایع مانند حمله به سیستم کنترل حمل‌ونقل هوایی و یا اختلال در نیروگاه‌های برقی و اتمی بتوان با قطعیت بیان نمود که خسارات مادی و تلفات جانی منتج از آن قابل پیش‌بینی بوده اما در مورد حمله به وب‌سایت‌های سیستم‌های مالی و بانکی قدری ابهام وجود دارد. در همین راستا پرفسور داینشتین بیان می‌کند که حملات سایبری می‌تواند داخل در معنای حمله مسلحانه قرار گیرد، اگر موجب ایجاد تلفات شود. به طور مثال، در جایی که سیستم کنترل رایانه مربوط به یک آب‌بند یا سد مورد حمله قرار گیرد. به عقیده ایشان حملات «سیستم توزیع انکار سرویس»[۷] موقتی اگر موجب ایراد خسارات جانی یا مالی نشود، حمله مسلحانه تلقی نمی‌گردد؛ اما یک توسل به زور محسوب می‌شود(Dinstein, 2005: 105). با توجه به استدلال‌هایی که توسط قائلین به رویکرد سوم مطرح گردید، این دیدگاه از منطق و مقبولیت بیش‌تری برخوردار است. چرا که فلسفه اصلی دفاع مشروع جلوگیری از ورود خسارت‌های مالی و جانی به یک کشور است. این نوع نگاه حتی می‌تواند به حفظ صلح جهانی نیز کمک بیش‌تری نماید چرا که صرف نفوذ به تأسیسات حیاتی یک کشور را دلیلی برای اعمال حق دفاع مشروع نمی‌داند.

---

[۷] در حملات توزیع انکار سرویس (DDOS) تعداد بیشماری پیام‌های درخواست به سمت سرورها هجوم می‌آورند، سرورها نمی‌توانند به این همه پیام پاسخ دهند، چرا که پیام‌ها از موقعیت‌های متعددی در اینترنت به سرورها ارسال می‌شوند و در برخی موارد خسارات مالی جدی و قابل ملاحظه‌ای را به دنبال داشته‌اند. در اکثر حملات سایبری این شیوه مدنظر قرار گرفته است از جمله در حمله ۲۰۰۷ به استونی.

٤. بررسی حق دفاع مشروع ایران در برابر حمله سایبری استاکس‌نت

کرم رایانه‌ای استاکس‌نت[8] که در سال ۲۰۱۰ علیه سیستم‌های «اسکادا»[9] تأسیسات هسته‌ای ایران بکار گرفته شد، موجب گردید تا سانتریفیوژهای برنامه تولید سوخت هسته‌ای به طور فیزیکی آسیب ببینند؛ و همین امر باعث شد که تردید برای مسلحانه بودن این حمله قوت بگیرد. البته قبل از هر چیز شاید لازم باشد که قدری با استاکس‌نت و نحوه عملکرد آن آشنا شویم و بدانیم که برخلاف آنچه به اشتباه مصطلح و متداول گردیده است، استاکس‌نت یک کرم رایانه‌ای است و نه ویروس. کرم یک بدافزاری است که می‌تواند به‌تنهایی از یک کامپیوتر به یک کامپیوتر دیگر کپی شود. برخلاف ویروس‌ها که نیاز دارند تا در یک برنامه رایانه‌ای جاگذاری شوند. کرم‌ها به‌تنهایی خود از کامپیوتری به کامپیوتر دیگر تکثیر می‌شوند. استاکس‌نت برای تجهیزات و نرم‌افزارهایی طراحی شده است که سیستم اسکادای آن‌ها توسط شرکت زیمنس ساخته شده است. پیلود[10] استاکس‌نت شامل یک منطق قابل برنامه‌ریزی است که «روتکیت»[11] کنترل‌کننده دارد. استاکس‌نت بعد از حمله به تأسیسات هسته‌ای ایران بر سر زبان‌ها افتاد(Schmitt, et.al, 2013: 214-215).

پایگاه اینترنتی سیمانتیک در خصوص عملکرد کرم استاکس نت تشریح نموده است که این کرم از طریق ایمیل و حافظه‌های جانبی انتشار یافته و پس از آن‌که سیستم را آلوده نمود فایل‌هایی را در خود سیستم کپی می‌نماید و در حافظه سیستم ثبت می‌شود این کرم از این طریق اطلاعات مربوط به شبکه‌ها را جمع‌آوری می‌نماید(symantec,14/7/2010, "security response") به روایت سایت جام

---

[8] Stuxnet

[9] سیستم اسکادا برای کنترل سانتریفیوژهای غنی سازی اورانیم به کار رفته است. (SCADA)

[10] منظور بخش ویرانگر و تخریبی یک بدافزار است. (Payload)

[11] Rootkit

جم آنلاین یکی از کارشناسان و مدیران صنعتی ایرانی درباره چگونگی عملکرد این کرم رایانه‌ای می‌گوید: «با فعال شدن این بدافزار، سیستم‌های اتوماسیون صنعتی، اطلاعات خط تولید را به مرکز اصلی مشخص شده توسط بدافزار منتقل می‌کنند و این اطلاعات توسط طراحان استاکس‌نت مورد پردازش قرار می‌گیرند و به این ترتیب برای ضربه زدن به کشور برنامه‌ریزی می‌شوند.» هم‌زمان که ایشان این بدافزار را یک کرم جاسوسی معرفی می‌نماید؛ خبرگزاری فرانسه نیز در تشریح این کرم جاسوس می‌نویسد: استاکس نت قادر به تخریب لوله‌های گاز، ایجاد خلل در فعالیت‌های تأسیسات هسته‌ای و حتی انفجار دیگ‌های بخار کارخانه‌های مختلف است(

http://188.75.89.1/papertext.aspx?newsnum=100888862821jame .(jamonline.ir

اما فارغ از جمع‌آوری اطلاعات، آنچه بیش‌تر در خصوص استاکس‌نت مطرح است حمله ویرانگری است که این کرم به سانتریفیوژهای تأسیسات هسته‌ای نمود و موجب تخریب آن‌ها گردید. به طور کلی به استناد سایت اصلی سیمانتیک استاکس نت برای رسیدن به این مقصود به سیستم‌هایی حمله‌ور می‌شود که دارای یک مبدل فرکانس هستند؛ و پس از شناسایی دستگاه مبدل، فرکانسی که سیستم قربانی با آن کار می‌کند را به دست می‌آورد. دستگاه مبدل فرکانس غالباً در تأسیسات غنی‌سازی اورانیوم به کار می‌رود؛ و در ایران فقط مرکز غنی‌سازی نطنز است که از این دستگاه‌های مبدل فرکانس استفاده می‌نماید. استاکس نت با بالا و پایین بردن میزان فرکانس دستگاه موجب اختلال در تنظیم میزان فرکانس شده و در پی این اختلال وقوع هر حادثه‌ای امکان‌پذیر است.(symantec,14/7/2010, .(“security response”

کارشناسان حقوق بین‌الملل که مأمور تدوین اصول راهنما برای سازمان ناتو بودند، در این زمینه به دو گروه تقسیم شده‌اند. عده‌ای صرف خسارت را معیاری برای مسلحانه بودن قلمداد نموده و عده‌ای دیگر در این خصوص تردیدهایی را مطرح نمودند(Schmitt, et.al, 2013: 75). البته از آنجایی که گروه کارشناسان حقوق بین‌الملل منتخب ناتو بوده و به منظور تهیه پیش‌نویسی برای این سازمان فعالیت می‌کردند و با توجه به این مطلب که کرم استاکس نت علی‌الظاهر توسط یکی از اعضای مهم این سازمان یعنی ایالات‌متحده امریکا بکار گرفته شده ذکر مطلب فوق امری دور از ذهن نیست. و طبیعی است که این‌گونه با جانب احتیاط در خصوص مسلحانه بودن حمله به تأسیسات ایران سخن بگویند. البته در جای دیگری از این پیش‌نویس اظهارات متناقضی مطرح شده که در ادامه مباحث بدان می‌پردازیم. مع‌الوصف حمله به تأسیسات هسته‌ای ایران علاوه بر خسارت‌های مالی بالفعلی که ایجاد نمود، می‌توانست خسارات بسیار گسترده‌تری ایجاد نماید که کارکنان این تأسیسات و حتی مردم شهر نطنز نیز از گزند آسیب در امان نمانند.

اما گروهی که معتقدند حمله سایبری به تأسیسات هسته‌ای ایران صرف یک خرابکاری بوده و به سرحد حمله سایبری مسلحانه نرسیده است؛ علت آن را این‌گونه بیان می‌کنند که این حملات نه موجب مرگ اشخاص و نه موجب ایراد خسارات فیزیکی شده است. همچنین اینان معتقدند که این حملات، در آن حد خسارت ایجاد نکرده است تا موجب شود که ساختارهای حیاتی دولت ایران دچار اختلال شده و یک بحران بنیادین در ایران ایجاد شود؛ و تنها اثر ثانوی و جدی که این حمله ایجاد کرده است، ایجاد تأخیر و تعلل در برنامه هسته‌ای ایران آن هم برای چند ماه است. همچنین این گروه معتقدند که خیلی سخت است که بخواهیم تصور کنیم که حمله به تأسیسات هسته‌ای ایران موجب اختلال در ثبات جامعه ایران شود، چرا که بر اساس گزارش‌های مرکز تحقیقات جهانی سازمان سیا ۸۶/۱٪

از انرژی برق در ایران از سوخت‌های فسیلی تولید می‌شوند و ۱۳/۷٪ از کارخانه‌های برق‌آبی تولید می‌گردد(Gill & Ducheine, 2013: 459). البته این گروه از مفسران با بیان این دست آمارها قصد دارند که صلح‌آمیز بودن برنامه هسته‌ای ایران را زیر سؤال برده و منفعت اقتصادی آن برای جامعه ایران را منتفی دانسته و آن را یک برنامه نظامی معرفی نمایند. در خصوص ماهیت برنامه هسته‌ای ایران باید این مطلب را مدنظر داشت که تصور نظامی بودن فعالیت‌های هسته‌ای ایران بر پایه یک پیش فرض کاملاً نادرست و ادعایی اثبات نشده است. به بیان دیگر هیچ مدرک مثبِت بین‌المللی وجود ندارد که نشان دهد برنامه صلح‌آمیز هسته‌ای ایران، برنامه‌ای برای ساخت سلاح اتمی است تا از این رهگذر مجوز تخریب و از بین بردن تأسیسات هسته‌ای ایران صادر شود. علاوه بر این، نکته دیگر که باید بدان توجه شود، این است که زمانی حق دفاع مشروع برای یک دولت ایجاد می‌شود که یک حمله مسلحانه علیه آن کشور به وقوع پیوسته باشد. حمله‌ای که امکان ایجاد خسارات بالقوه را داشته باشد. در خصوص حمله سایبری به تأسیسات هسته‌ای ایران، اگر کارشناسان هسته‌ای ایران به موقع جلوی اختلال‌های ایجاد شده در سانتریفیوژها را نمی‌گرفتند، یک فاجعه انسانی در سطح بسیار گسترده به وقوع می‌پیوست. حال چگونه می‌توان این اثر بالقوه را نادیده گرفت. با توجه به این مطلب، از نظر بسیاری از نویسندگان حمله استاکس نت که با رمز عملیات بازی‌های المپیک(مرتیوس)[۱۲]انجام شده است تنها مورد حملات سایبری منفرد[۱۳]است که می‌تواند به عنوان حمله مسلحانه تلقی شود، چرا که این کرم رایانه‌ای در طی سال‌های ۲۰۱۰-۲۰۰۸ موجب خسارات فیزیکی گسترده به سانتریفیوژهای تأسیسات هسته‌ای ایران گردید(Fidler, 2011: 57-58). آثار بدافزار

---

[1] Operation Olympic Games(Myrtus)

[۱۳] منظور حملات سایبری که همراه حملات فیزیکی نیستند.

استاکس نت به گونه‌ای بوده است که نگاه کارشناسان را به فراتر از یک حمله سایبری سوق داده و بسیاری از جمله کارشناسان امنیت ملی امریکا را بر آن داشته تا استاکس نت را زمینه‌ساز جنگ‌های سایبری مورد ارزیابی قرار دهند و حتی عده‌ای از آن به عنوان سلاحی با آثار گسترده یاد کرده‌اند به طوری که برخی با استناد به گفته مایکل هایدن، رئیس سابق سیا و آژانس اطلاعات ملی امریکا اظهار داشته‌اند که استاکس‌نت ازجمله ابزارهای سایبری است که باعث آثار فیزیکی می‌شود و همانند یک جنگ سایبری مرزها را طی کرده است، از این رو می‌تواند به عنوان حمله‌ای مسلحانه ارزیابی شود (خلف رضایی:۱۳۹۲،۱٤۱). همان‌طور که پیش از این بیان شد، جمعی از کارشناسان حقوق بین‌الملل در جای دیگری از پیش‌نویس مربوط به ناتو به توافق رسیده‌اند که حمله کرم استاکس نت به مرحله حمله مسلحانه رسیده است و جالب است که جمع دیگر کارشناسان که عقیده به مسلحانه بودن این حمله نداشتند، اما بر این باور بودند که حداقل حق دفاع پیش‌دستانه برای ایران محفوظ است (Schmitt, et.al, 2013: 56). با این حال، برای اظهار نظر در این خصوص باید یک دولت به عنوان مسئول قلمداد و این اقدام به عنوان یک حمله مسلحانه مندرج در ماده ۵۱ منشور تلقی گردد. با توجه به دیدگاه‌های تفسیری که پیش از این تبیین گردید و با در نظر گرفتن دیدگاه ابزار محور و توجه صرف به نوع سلاح بکار رفته در یک حمله نمی‌توان حمله سایبری را یک حمله مسلحانه تلقی کرد لکن ارزیابی موضوع از دیدگاه هدف محور و نتیجه محور وضعیت متفاوت است؛ بدین ترتیب که هدف قرار دادن تأسیسات هسته‌ای ایران که با امنیت ملی کشور در ارتباط است و از سوی دیگر با لحاظ اینکه این حمله ظرفیت بالقوه برای ایجاد تخریب و تلفات جانی و مالی را داشته است، این امکان را فراهم می‌نماید تا به عنوان حمله‌ای مسلحانه تلقی شود؛ اما انتساب استاکس نت به دولتی خاص و اثبات آن، یک امر موضوعی است و از

ظرفیت این مقاله خارج است. بااین‌وجود، انتساب این اقدام به گروه‌های غیردولتی مطلب دیگری است که در این صورت موضوع مسئولیت دولت میزبان در برابر بازیگران غیردولتی مطرح خواهد بود. در این حالت، دولت برای پیشگیری از حملات سایبری علیه دولت دیگر مسئولیت دارد. البته بحث از مسئولیت بین‌المللی دولت و انتساب اعمال مسئولیت آور به آن موضوع این نوشته نیست و فرصت دیگری را می‌طلبد.«در هر حال اقدام به دفاع مشروع منوط به احراز حمله مسلحانه است و در غیر این صورت (عدم احراز حمله مسلحانه و امکان دفاع مشروع) بنابر یک اصل کلی مسئولیت بین‌المللی، دولت‌ها در مواجهه با اعمال متخلفانه بین‌المللی می‌توانند با رعایت شرایطی خاص به اقدامات متقابل روی آورند و از این راه مانع تجری طرف متخلف و جلوگیری از تداوم عمل متخلفانه شوند»(خلف رضایی:۱۳۹۲،۱٤۷)

۵. نتیجه‌گیری

حملات سایبری یک پدیده نوظهور است که هنوز قاعده حقوقی معتبری در قالب معاهدات یا عرف بین‌المللی در خصوص آن شکل نگرفته است؛ از این رو موضوع باید در چارچوب قواعد موجود حقوق بین‌الملل تحلیل شود؛ و از طرفی به اذعان کارشناسان و داده‌های موجود ایجاد اختلال و آسیب در شبکه‌های اطلاعاتی و سیستم‌های الکترونیکی نیروگاه‌های برق و تولید انرژی، سیستم‌های حمل‌ونقل هوایی و مانند آن آثار زیانباری در تخریب زیرساخت‌های حساس داشته و حتی قابلیت تلفات جانی دارد و در سطوح بالاتر ممکن است منافع ملی و حیاتی دولت را در معرض خطر جدی قرار دهد. در این صورت این پرسش مطرح است که آیا دولت‌ها می‌توانند با تمسک به نهاد سنتی دفاع مشروع به عنوان یک قاعده قراردادی مندرج در ماده ۵۱ منشور ملل متحد ونیز قاعده عرفی حقوق بین‌الملل از

خود دفاع نمایند یا نه؟ قبل از پاسخ به این پرسش باید متذکر شد که اغلب حملات سایبری در حد یک خرابکاری، سرقت اطلاعات یا جاسوسی بوده و نمی‌تواند یک حمله مسلحانه قلمداد شود؛ و از سوی دیگر چنانچه حملات سایبری در کنار حملات فیزیکی در صحنه نبرد بکار گرفته شود قطعاً یک حمله مسلحانه است؛ اما سؤالات مطرح شده مربوط به حملات سایبری منفرد بوده که برای پاسخ به آن، نخست از مفهوم حمله مسلحانه به عنوان پیش‌شرط دفاع مشروع بحث شد زیرا ضرورت داشت تا امکان اطلاق «حمله مسلحانه» بر حملات سایبری ارزیابی و تبیین گردد. در مقام بررسی مفهوم حمله مسلحانه به دکترین و رویه قضایی مراجعه و دیدگاه حقوقدانان در این باره شامل دو رویکرد مضیق و موسع به مفهوم حمله مسلحانه مطرح و تحلیل گشت. در رویکرد مضیق، اولاً حمله باید علیه تمامیت ارضی و استقلال سیاسی یک کشور بوده و ثانیاً دارای شدت، استمرار و گستردگی کافی باشد تا بتوان بدان اطلاق حمله مسلحانه نمود. بدین نحو در این رویکرد به هرگونه استعمال زور نمی‌توان حمله مسلحانه اطلاق کرد اما در رویکرد موسع، حمله مسلحانه محدود به دولت‌ها نیست و هر نوع حمله‌ای حتی توسط گروه‌های غیردولتی هم می‌تواند یک حمله مسلحانه تلقی شود. علاوه بر این، در رویکرد موسع تئوری تحت عنوان تئوری تجمیع وقایع مطرح است؛ که بر اساس آن، حملات با شدت کم ولی پراکنده و متعدد یک حمله مسلحانه واحدی را تشکیل می‌دهد و به دولت قربانی حق توسل به دفاع مشروع می‌دهد. در خصوص اعتبار این تئوری و کاربرد آن در موضوع بحث، به آرای دیوان بین‌المللی دادگستری مراجعه شد؛ دیوان در قضیه سکوهای نفتی اشاره‌ای به این تئوری دارد ولی صراحتاً تأیید نمی‌کند، اگرچه برخی، اظهار نظر دیوان در قضیه کنگو علیه اوگاندا را نوعی صحه گذاشتن به این تئوری تلقی کرده‌اند. به‌هرحال این تئوری قابل اعتنا و تأمل است لکن همچنان در حد دکترین باقی مانده است. با این اوصاف می‌توان گفت که

حملات پراکنده و حوادث مرزی یک حمله مسلحانه تلقی نمی‌شود بلکه شدت این حملات و آثار تخریبی آن اهمیت دارد. نظریات حقوقدانان در مقام بررسی و تطبیق حملات سایبری و تطبیق آن با مفهوم حمله مسلحانه در قالب سه رویکرد ابزار محور، هدف محور و نتیجه محور بیان شده است. در رویکرد ابزار محور، حملات سایبری در مقایسه با سلاح‌های سنتی نظامی ارزیابی شده است و ازآنجاکه حملات سایبری از جنس این سلاح‌ها نیستند امکان اینکه حمله نظامی تلقی شوند وجود ندارد. در تئوری هدف محور، صرف هدف قرار دادن تأسیسات مهم مطرح است و هرگونه نفوذ و آسیب به این تأسیسات راه را برای طرح مسئله دفاع مشروع باز می‌نماید و در نتیجه زمینه منازعات و جنگ‌ها را فراهم می‌کند. این در حالی است که بر اساس دیدگاه نتیجه محور، یک حمله سایبری با توجه به نتایج و آثار آن یعنی شدت آسیب و تخریب ایجاد شده و البته وجود رابطه علت و معلولی بین حمله سایبری و خسارات به وجود آمده ارزیابی می‌گردد و در این چارچوب می‌تواند حمله مسلحانه تلقی شده و حق دفاع مشروع را در پی داشته باشد. این دیدگاه، راه حل میانه‌ای نسبت به دو دیدگاه دیگر ارائه می‌نماید زیرا نه همچون دیدگاه ابزار محور حملات سایبری را به‌طور کلی خارج از حمله مسلحانه لحاظ کرده و نه مانند دیدگاه هدف محور، صرف نفوذ و هدف قرار دادن تأسیسات مهم را معیار قرار داده است بلکه آثار و نتایج حمله سایبری را معیار اصلی می‌داند. با توجه به دیدگاه‌ها و رویکردهای گوناگون در خصوص مسلحانه بودن حملات سایبری، در خصوص حملات سایبری به تأسیسات هسته‌ای ایران می‌توان این‌گونه نتیجه گرفت که حمله کرم رایانه‌ای استاکس نت هم بر اساس دیدگاه هدف‌محور و هم بر اساس دیدگاه پرطرفدار نتیجه‌محور (اثرمحور) یک حمله مسلحانه محسوب می‌گردد. حمله استاکس نت علاوه بر خسارات مالی که به سانتریفیوژها و تأسیسات هسته‌ای که برای تولید انرژی فعال هستند، وارد نمود در صورتی که به

درستی کنترل و خنثی نمی‌گردید، امکان ایجاد تلفات انسانی به شهروندان عادی ساکن در شهر نطنز و مناطق مسکونی اطراف را نیز داشت. چرا که از جمله شاخصه‌های حملات سایبری گسترش غیرقابل پیش‌بینی و غیرقابل‌کنترل نتایج و خسارات است. در نتیجه ایران حق دفاع مشروع در برابر حمله استاکس نت داشته و می‌توانست متناسب با حمله صورت گرفته از حق خود مبنی بر دفاع مشروع در برابر مرتکبان آن استفاده نماید. این برداشت صرف‌نظر از اثبات انتساب این حمله به یک دولت خاص است؛ چه اینکه مسئله انتساب یک امر موضوعی است و برای نویسندگان امکان اظهار نظر قطعی وجود نداشته اگرچه قرائنی نیز وجود دارد. در صورتی که احراز حمله مسلحانه و در پی آن امکان دفاع مشروع متعذر باشد، توسل به اقدامات متقابل برای پیشگیری از تکرار اعمال متخلفانه نیز قابل طرح خواهد بود.

منابع

الف. فارسی

اصلانی، جابر؛ رنجبریان، امیرحسین (۱۳۹٤)، «بررسی تطبیقی و تحلیل تعریف حمله سایبری از منظر دکترین، رویه کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل»، تهران، فصلنامه تحقیقات حقوقی، شماره ۷۱، ۲۵۷-۲۷۸.

خلف رضایی، حسین(۱۳۹۲)، «حملات سایبری از منظر حقوق بین‌الملل(مطالعه موردی استاکس‌نت)»، تهران، فصلنامه مجلس و راهبرد، سال بیستم، شماره ۷۳، ۱۲۵- ۱۵٤.

ضیایی بیگدلی، محمدرضا(۱۳۸۸)، حقوق معاهدات بین‌المللی، تهران: انتشارات گنج دانش.

قاسمی علی ,چهاربخش ویکتور بارین(۱۳۹۰)، «رویه قضایی دیوان بین‌المللی دادگستری در خصوص دفاع مشروع پس از رویداد یازدهم سپتامبر ۲۰۰۱» ، تهران، مجله حقوقی بین‌المللی، شماره ٤۵; ۱۷۵ – ۱۹٤.

قاسمی علی، چهاربخش ویکتور بارین(۱۳۹۱)، «حملات سایبری و حقوق بین‌الملل»، تهران: مجله حقوقی دادگستری ، دوره۷٦، شماره۷۸؛ ۱۱۵ – ۱٤٦.

موسوی، سید فضل‌اله(۱۳۹۱)، اندیشه‌های حقوقی ۷ (حقوق بین‌الملل)، تهران: انتشارات مجد.

نیاورانی، صابر(۱۳۸٦)، تحول قاعده دفاع مشروع در حقوق بین‌الملل، تهران: دانشگاه شهید بهشتی، دانشکده حقوق.

وحید، هادی(۱۳۸۵)، «مسئله مشروعیت توسل به زور علیه عراق توسط ایالات‌متحده امریکا»، تهران، مجله حقوقی، شماره ۳۵؛ ۲۵۱ – ۲٦٦.

ب. انگلیسی

Alexandrov, A. Stanimir, (1996), **Self-Defense against the Use of Force in International Law**, The Hague, Kluwer Law International Publication.

Aust, Anthony, (2005), **Handbook of International Law**, New York, Cambridge University Press.

Blank, R. Laurie, (2013), "International Law and Cyber Threats from Non-State Actors". **International Law Studies, U.S. Naval War College**, Vol.89.

Cassese, Antonio, (2005), **International Law**, New York, Oxford University Press.

Clarke, A. Richard, Knake, K. Robert, (2010), **Cyber War**, New York, Harper Collins Publisher.

ColI, R. Alberto, (1995), "Unconventional Warfare, liberal Democracies, and International Order", **International Law Studies, U.S. Naval War College**, Vol.67.

Constantinou, Avra, (2007), **The Right of Self-defense under Customary International Law and Article 51 of the United Nations Charter**, University of Nottingham press.

Conway W. Henderson, (2010), **Understanding International Law**, West Sussex, a john Wiley & sons ltd. Publication.

Department of Defense & Office of General Counsel, (MAY 1999), an Assessment of International Legal Issues in Information Operations, available at **http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.**

Dinstein, Yoram, (2002)," Computer Network Attacks and Self-Defense", **International Law Studies, U.S. Naval War College**, Vol.76.

Dinstein, Yoram, (2005), **War, Aggression and Self-Defence**, New York, Cambridge University Press.

Duffy, Helen, (2005), **the 'War on Terror' and the Framework of International Law**, New York, Cambridge University Press.

Fidler, P. David, (2011)," Was Stuxnet an Act of War? Decoding a Cyberattack", **IEEE Security & Privacy**, vol. 9.

Gill, D. Terry, Ducheine, A. L. Paul, (2013), "Anticipatory Self-Defense in the Cyber Context", **International Law Studies, U.S. Naval War College**, Vol.89.

Gray, Christine, (2008), **International Law and the Use of Force**, New York, Oxford University Press.

Hathaway, A. Oona et al., (2012), "The Law of Cyber-Attack", **California Law Review**, Vol. 100,

Hollis, B. Duncan, (2007), "Why states need an international law for information operation", Lewis & Clark Law Review, Vol. 11.

http://188.75.89.1/papertext.aspx?newsnum=100888862821(jamejamonline.ir)

http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

ICJ Reports (2005), **The Armed Activities on the Territory of the Congo Case** (Democratic Republic of the Congo v. Uganda)

ICJ Reports, (1986), **Case concerning the military and paramilitary activities in and against Nicaragua** (Nicaragua v. United States of America).

ICJ Reports, (2003), **Case concerning Oil Platforms** (Islamic Republic of Iran v. United States of America).

Joyner, C. Christopher, Lotrionte, Catherine, (2001), "Information warfare as international coercion: Elements of a legal framework?" **European Journal of international law**, Vol.12.

Kulesza, Joanna, (13 September 2010), "State responsibility for acts of cyber-terrorism", University of Lodz, available at **http://www.wpia.uni.lodz.pl**

Owens, A. William et al., (2009), Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber-attack Capabilities, Washington, D.C., The National Academies Press, available at **http://www.3.nd.edu/~cpence/eewt/owens2009.pdf.**

Raab, Dominic, (December 2004)," 'Armed Attack' after the Oil Platforms Case", **Leiden Journal of International Law**, Volume 17.

Rid, Thomas, (2013), **Cyber War Will Not Take Place**, New York, Oxford university press.

Ruys, Tom, (2010)**, "Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice**, New York, Cambridge University Press.

Schmitt, N. Michael et al., (2013)**, Tallinn Manual on the International Law Applicable to Cyber Warfare**, New York, Cambridge university press.

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

Sharp, G. Walter, (1999)**, Cyberspace and Use of Force**, Virginia, Aegis Research Corporation.

Shaw N. Malcolm, **International Law**, Sixth edition, (New York: Cambridge University Press, 2008) Shaw, N. Malcolm, (2008), **International Law**, New York, Cambridge University Press.

Silver, B. Daniel, (2002),"Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter", **International Law Studies, U.S. Naval War College**, Vol.76.

Sklerov, J. Matthew, (April 2009), **Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active**

Defenses Against State who Neglect their to Prevent, United States Army,

The White House, (February 2003), the National Strategy to Secure Cyberspace, available at: **www.us-cert.gov/site/default/files/publications/cyberspace_strategy.pdf.**

UN General Assembly Resolution, (14 December 1974), Definition of Aggression, A/RES/29/3314, available at **http://www.un-documents.net/a29r3314.htm**