کاربرد اصل عدم مداخله در امور داخلی دولت‌ها در حملات سایبری

نازنین برادران[1]- دکتر همایون حبیبی[2]- دکتر سید قاسم زمانی[3]- دکتر سید علی هنجی[4]

تاریخ دریافت:۱۳۹۶/۴/۱۴- تاریخ پذیرش:۱۳۹۶/۵/۲

چکیده:

در عصر اطلاعات، حملات سایبری، نمایانگر نوع جدیدی از توسل به زور هستند و می-توانند باعث ایجاد آثاری از قبیل صدمات عظیم و وسیع به زیر ساخت‌های حیاتی یک دولت، تخریب اموال و کشته شدن انسانها شوند و به این ترتیب با نقض بند ۴ ماده ۲ منشور سازمان ملل متحد به عنوان توسل غیر قانونی به زور در نظر گرفته شوند. اما مسأله آن است که امروزه مشروعیت حملات سایبری از رویکرد عدم توسل به زور، ارزیابی می‌گردد و محققین این حوزه معتقدند که حملات سایبری صورت گرفته، زمانی به منزله مداخله غیر قانونی در امور داخلی دولتها محسوب می‌شوند که منجر به ایجاد صدمات فیزیکی شده باشند، اما این دیدگاه با این چالش مواجه است که بسیاری از حملات سایبری صورت گرفته در سال‌های اخیر، منجر به ایجاد صدمات فیزیکی نشده‌اند و در نتیجه در چارچوب ممنوعیت مقرر در بند ۴ ماده ۲ منشور قرار نمی‌گیرند، این مقاله درصدد آن است که نشان دهد، آن دسته از حملات سایبری که باعث اجبار دولتها به انجام اقداماتی می‌شوند که اصولا طبق اصل حاکمیت ملی، یک دولت حق دارد، خود آزادانه راجع به آنها تصمیم بگیرد، فی ذاته منجر به نقض اصل عدم مداخله در امور داخلی دولتها گردیده و در نتیجه برای دولت قربانی حق اتخاذ اقدامات متقابل در مقابل چنین تهدیداتی ایجاد می‌گردد.

واژگان کلیدی: حملات سایبری، توسل به زور، اصل عدم مداخله، اصل حاکمیت ملی

---

[1]- دانشجوی دکتری حقوق بین‌الملل عمومی،گروه حقوق عمومی و بین‌الملل، دانشکده حقوق و علوم سیاسی، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

na_baradaran@yahoo.com

[2]- استادیار و عضو هیات علمی، گروه حقوق عمومی و بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران (نویسنده مسئول)

homayuonhabibi@yahoo.com

[3]- استادیار و عضو هیات علمی، گروه حقوق عمومی و بین‌الملل، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبایی، تهران، ایران

[4]- دانشیار و عضو هیئت علمی،گروه حقوق بین الملل،دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران

مقدمه:

شناخت موضوع

امروزه اطلاعات، تکنولوژی و ارتباطات بخش مهمی از زندگی انسانها را در بر گرفته است و دولتها جهت انجام فعالیت‌های خود به تکنولوژی و استفاده از کامپیوتر به شدت، نیازمند هستند و فضای سایبر و ارتباطات دیجیتال، در عین اینکه آثار مفید بسیاری برای اشخاص خصوصی و دولتها به بار آورده است، اما همزمان منشا بسیاری از تهدیدات و آسیب‌ها نیز می‌باشد و بازیگران دولتی و غیر دولتی، با تشخیص این وابستگی، هنگامی که نیات خصمانه‌ای علیه سایر بازیگران داشته باشند، با اجرای حملاتی علیه سرورهای کامپیوتری و اطلاعات موجود در آنها، سعی در دستیابی به مقاصد خود می‌نمایند، به همین دلیل امروزه حفظ امنیت در فضای سایبر، به یکی از اولویت‌های دولتها تبدیل شده است و بنا به گزارش هیأت ۱۵ نفره متخصصان سازمان ملل که در ژانویه ۲۰۱۳ تهیه شده است[1] امروزه ۴۰ دولت در دنیا، خود را برای جنگ‌های سایبری تهاجمی تجهیز کرده‌اند. از نشانه‌های عملی این ادعا، آن است که در سال‌های اخیر، شاهد بروز موارد متعدد حملات سایبری، میان دولتها بوده‌ایم، برای مثال کشور آمریکا هدف حملات متعدد سایبری قرار گرفته است که ادعا می‌شود از طرف کشور چین صورت گرفته‌اند.(Shacketford,2009.204) مورد معروف دیگر حمله به کشور استونی در آوریل سال ۲۰۰۷ میلادی است که به مدت سه هفته، این کشور هدف حملات سایبری قرار گرفت که باعث از کارافتادن وب سایت‌های رسمی دولتی، ایستگاه‌های تلویزیونی، بانک‌ها و... گردید و دولت استونی مدعی است که این حملات از سوی فدراسیون روسیه صورت گرفته است. از دیگر موارد حملات سایبری، حملات صورت گرفته علیه کشور گرجستان در ژوئیه و آگوست سال ۲۰۰۸ میلادی است که قبل از درگیری و نیز در جریان مخاصمات مسلحانه این کشور با فدراسیون روسیه اتفاق افتاد و باعث شد که وب سایت‌های دولتی از شبکه خارج شده و تغییر شکل دهند و محتوای آنها با تبلیغات روسیه جایگزین

[1] . "On the Developments in the Field of Information and Telecommunications in the Context of International Security".

گردد. (Markoff,2008). سایر موارد حملات سایبری، علیه کشورهایی از جمله انگلستان، تایوان،کره جنوبی، قزاقستان، سویس و.. رخ داده اند. (Roscini,2010.89)

جمهوری اسلامی ایران نیز در سال ۲۰۱۰ میلادی از طریق کرم استاکس نت[1] هدف حملات سایبری با هدف ایجاد اختلال در فعالیت‌های هسته‌ای قرار گرفت و به تعدادی از سانتریفیوژهای فعال در مرکز هسته‌ای نطنز آسیب وارد گردید و آمریکا و اسراییل مظنونین اصلی اجرای حمله استاکس نت هستند.

موارد حملات سایبری بسیار متعدد بوده و اشاره به همه آنها در این مقال نمیگنجد، اما یکی از بحث برانگیزترین موارد اخیر، انتخابات ریاست جمهوری آمریکا در سال 2016 میلادی می-باشد که این کشور سرویس‌های اطلاعاتی روسیه را به هک کردن کامپیوترهای کمیته ملی دموکرات‌ها و مداخله در انتخابات، متهم نموده است. (tnews.ir/news/48d767754311.html)

حملات سایبری با پیچیدگی‌های فنی و تکنیکی خاصی همراه هستند که آنها را از حملات کلاسیک متمایز می‌سازد مانند گمنامی و مشخص نبودن هویت اجرا کنندگان حملات و نیز آثار مخرب مستقیم یا غیر مستقیم گسترده‌ای که اینگونه سلاح‌ها می‌توانند ایجاد کنند. به همین دلیل جهت درک بهتر ویژگی‌های فوق‌الذکر، توضیح برخی عبارات از جمله فضای سایبر و حملات سایبری ضروریست.

فضای سایبر، فضایی غیر مادی و ناملموس است که توسط رایانه‌ها و شبکه‌های رایانه‌ای به وجود آمده است و دنیایی مجازی را در کنار دنیای واقعی ایجاد نموده است. (فضلی،۱۷:۱۳۸۹)، این فضا فراتر از اینترنت توسعه یافته است و تمامی فعالیت‌های دیجیتال شبکه‌ای را در بر می‌گیرد. فضای مذکور دارای گستره‌ای جهانی و بدون مرز، پوشیده و پنهان بوده و ماهیتا برای آزادی گردش اطلاعات شکل گرفته و محدودیت در این فضا معنا ندارد.(پاکزاد،۲۱۶:۱۳۸۹)

در ارتباط با نحوه عملکرد حملات سایبری باید گفت که بطور سنتی، سه هدف، اهداف متعارف امنیت در محیط اطلاعاتی را تشکیل می‌دهند: محرمانه بودن[2]، یکپارچگی[3] و در

[1]. Stux net
[2] .Confidentiality
[3] .Integrity

دسترس بودن[1]. به این ترتیب بهترین روش جهت طبقه بندی حملات این است که ببینیم کدام یک از این اهداف، مورد تهدید واقع شده‌اند. حملاتی که در دسترس بودن را مورد هدف قرار می‌دهند، سعی می‌کنند که از دسترسی به شبکه (خواه با پیاده سازی حمله DoS[2]، خواه با آفلاین کردن یا خاموش کردن فیزیکی فرآیندهای مجازی و...) جلوگیری کنند.

حملاتی که محرمانه بودن را مورد هدف قرار می‌دهند، تلاش می‌کنند تا ورود به شبکه - های کامپیوتری را به منظور نظارت بر فعالیت‌ها و استخراج اطلاعات سیستم‌ها و داده‌های کاربران، بدست آورند. ارزیابی این نوع حمله، هم به اطلاعات استخراج شده و هم به مقیاس تلاش بستگی دارد. چالش واقعی این حملات هنگامی رخ می‌دهد که استخراج اطلاعات در یک روش سازمان یافته و عظیم اتفاق بیفتد.

در نهایت، حملاتی که یکپارچگی و صحت داده‌ها را مورد هدف قرار می‌دهند شامل ورود به سیستم برای تغییر اطلاعات به جای استخراج آن می‌باشند. این حملات، داده‌هایی را در دنیای مجازی دستکاری می‌کنند که افراد در دنیای واقعی به آن داده‌ها نیاز دارند. در بیشتر موارد، این حملات قصد دارند که یا ادراک کاربر را تغییر دهند یا شناخت وضعی از او داشته باشند یا دستگاه‌های فیزیکی، فرآیندهای هدایت شده یا سیستم‌های اطلاعاتی را خرابکاری یا براندازی کنند.

یکی از بحث برانگیزترین سوالاتی که راجع به اینگونه حملات مطرح می‌شود، نحوه واکنش در برابر این قبیل اقدامات است. اصل عدم توسل به زور به عنوان یکی از اصول مهم سازمان ملل متحد موضوع بند ۴ ماده ۲ منشور می‌باشد و ممنوعیت مطرح شده در آن هم، فقط شامل کاربرد آن نیست، بلکه تهدید به کاربرد آن را نیز در بر می‌گیرد. همچنین منظور از زور، توسل به زور نظامی است و بنابراین فشارهای سیاسی یا اقتصادی از حوزه آن خارج می- گردد. منشور ملل متحد محصول گفتمان حقوقی بیش از شصت سال پیش است. بنابراین آنچه که در بند ۴ ماده ۲ منشور به عنوان منع استفاده از زور نظامی مطرح شده، استفاده از زور به وسیله سلاح‌های کلاسیک و شناخته شده است. اما امروزه با روش‌های نوین توسل به

[1] .Availability.
[2]. Denial of Service .

زور یعنی حملات سایبری مواجه هستیم. حملات سایبری از این توانایی برخوردارند که آثار مخرب فراوانی به بار آورند، مثلا با حملات سایبری می‌توان تاسیسات و زیر ساخت‌های حیاتی یک کشور را از قبیل شبکه برق، تاسیسات آب آشامیدنی، راه آهن، خطوط لوله نفت، خطوط هوایی، سیستم‌های حمل ونقل، بازارهای مالی و.... از کار انداخت، به این ترتیب حملات سایبری که چنین آثاری به بار می‌آورند، با نقض بند ۴ ماده ۲ منشور، توسل به زور غیر قانونی محسوب می‌شوند و در صورتی که به آستانه لازم برای ایجاد یک حمله مسلحانه برسند، در مقابل برای دولت قربانی حق دفاع مشروع از خود، طبق چارچوب مقرر در ماده ۵۱ منشور به وجود می‌آید که بررسی این موارد از حوزه موضوعی این مقاله خارج است.

اما در مقابل در سال‌های اخیر شاهد وقوع موارد متعدد حملات سایبری بوده‌ایم که صدمات فیزیکی مستقیم به بار نیاورده‌اند، در مورد این قبیل حملات، این مساله قابل طرح است که آیا این ابزارهای جدید، از جمله استفاده از فضای سایبر جهت انجام حملات سایبری، در صورتی که منجر به ایجاد صدمات فیزیکی نشوند، می‌توانند به عنوان یک مداخله غیر قانونی که منجر به نقض حاکمیت یک دولت گردیده است، ارزیابی شده و در مقابل برای دولت قربانی، حق اتخاذ اقدامات متقابل ایجاد گردد؟

هر چند هنوز در حوزه حملات سایبری این مساله نزد مراجع قضایی مطرح نشده است، ولی می‌توان از آنچه دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه بیان کرده است نتیجه گرفت که توسل به زور «یک مثال واضح ویژه از مداخله غیر قانونی است». (Nicaragua Case,op.cit.205) بطور سنتی، ارزیابی حقوقی مساله مداخله در امور داخلی دولتها، از منظر استفاده از زور، مورد ارزیابی قرار می‌گیرد. (Damrosch,1989.3)

بنابراین، با وجود اینکه قواعد عرفی حقوق بین‌الملل مربوط به مداخله، اکنون به میزان قابل ملاحظه‌ای در کنار ممنوعیت عمومی توسل به زور قرار می‌گیرند، اما مداخله هنوز یک مفهوم متفاوت است.(Jennings and A watts,1999.429) در قضیه نیکاراگوئه قاضی جنینگز می-گوید: هیچ شکی وجود ندارد که اصل عدم مداخله یک اصل مستقل حقوقی عرفی است.
(Nicaragua Case, op. cit.534)

در این ارتباط، محققین حوزه حملات سایبری نیز از الگوی مشابهی پیروی کرده‌اند و جهت ارزیابی مشروعیت اینگونه حملات، بسیاری از مفسرین انحصاراً بر بند ۴ ماده۲ منشور، جهت ممنوعیت این قبیل حملات، تأکید کرده‌اند، بدون اینکه اصل عرفی و وسیعتر عدم مداخله را در نظر بگیرند. (Kodar, 2009) سایر نویسندگانی نیز که ظرفیت اجرای این اصل را شناخته‌اند، آن را به صورتی بسیار مضیق تفسیر کرده‌اند، مهمتر آنکه این نویسندگان به این مسئله نپرداخته‌اند که چگونه اصل عدم مداخله ممکن است در مورد حملات سایبری به کار رود که به آستانه لازم برای ایجاد حمله مسلحانه نرسیده‌اند. (Waxman,2011)

با توجه به موارد فوق الذکر هدف در این مقاله، توضیح این مطلب است که چگونه و تحت چه شرایطی اصل عدم مداخله، به عنوان یک وسیله قانونی مفید و در دسترس، می‌تواند از دولتها در مقابل حملات سایبری دفاع کند، که آسیب‌های فیزیکی به بار نیاورده‌اند، اما با این وجود، امنیت آنها را به خطر انداخته‌اند.

۱ . حاکمیت دولت و اصل عدم مداخله

در اینجا ابتدا به این مسئله پرداخته می‌شود که چرا تاکنون توجه اندکی به اصل عدم مداخله در پژوهش‌های مربوط به قواعد حقوق بین‌الملل قابل اعمال، در حوزه حملات سایبری شده است. توضیح این مسئله به نظر می‌رسد، متکی به تعریفی است که بطور سنتی از مفهوم حقوقی حاکمیت دولت ارایه می‌گردد. به خصوص اصطلاح حاکمیت دولت که بطور معمول با ارجاع به قلمرو فیزیکی یک دولت تعریف می‌شود. در این مفهوم، دولت‌ها اغلب با "حاکمیت سرزمینی"[1] خود در نظر گرفته می‌شوند. (Corfu Channel,1949) حاکمیتی که همیشه بوده بوده و اساس آن، بر تئوری سرزمین است. بر اساس این تعریف، محدوده حاکمیت معمولاً در چارچوب مرزهای جغرافیایی در نظر گرفته می‌شود. (wristion,1992.843)

بنا به دیدگاه دیوان بین‌المللی دادگستری: گستره حقوقی حاکمیت دولت در حقوق بین‌الملل عرفی... در چارچوب مرزهای مربوط به آبهای داخلی و دریایی سرزمینی و نیز قلمرو هوایی فراز سرزمین یک دولت اعمال می‌گردد. (Nicaragua,op .cit.212)

[1]. Territorial Sovereignty.

تعریف حاکمیت دولت در چارچوب قلمرو فیزیکی سرزمین آن دولت، مفاهیم مهمی برای توصیف دامنه شمول اصل عدم مداخله، ارایه می‌نماید که به عنوان نتیجه اصل حاکمیت دولت در نظر گرفته می‌شود. (Ibid.202)

به این ترتیب، نتیجه چنین تعریفی آن است که مداخله غیر قانونی فقط جایی اتفاق می - افتد که قلمرو فیزیکی یک دولت، مورد تجاوز قرار گرفته باشد. (Lotus Case,1927) با توجه به این تعریف، فضاهای سایبری اغلب بعنوان یک قلمرو مجازی در نظر گرفته می‌شوند که در محدوده آنها هیچ دولتی قادر به اجرای کنترل سرزمینی خود نمی‌باشد. بر اساس نظر مؤسسه بین‌المللی حقوق بشردوستانه[1]: یکی از ویژگی‌های متفاوت فضای سایبر آن است که یک محیط مجازی که ورای صلاحیت هر دولتی است را ایجاد می‌نماید. (Handbook ,2009.15)

در این ارتباط، این دیدگاه قابل طرح است که فضای سایبر قسمتی از "قلمرو مشترک جهانی"[2] است. جهت تایید این دیدگاه می‌توان به نظر وزارت دفاع آمریکا نیز استناد نمود که اعلام نموده است: "قلمرو مشترک جهانی" از آبهای بین‌المللی و قلمروی هوا فضای بین‌المللی و نیز فضای سایبر تشکیل می‌گردد"[3]

با توجه به موارد ذکر شده، این مسئله قابل طرح است که آیا مداخله غیر قانونی در قلمرو مجازی دولت دیگر، می‌تواند بعنوان مداخله غیر قانونی در قلمرو دولت دیگر در نظر گرفته شود؟ برای مثال، در زمینه اینگونه حملات گفته شده است که: "این به سختی قابل قبول به نظر می‌رسد که مداخله یک دولت با یک حادثه‌ی نامحسوس مانند تابش [4] یا الکتریسیته، فی نفسه نقض مقررات قانونی علیه دولت خاصی محسوب گردد" (Kanuck,op. cit.288)

در پاسخ باید گفت که گستره حقوقی حاکمیت دولت، فقط محدود به قلمرو مادی یک دولت نیست، در واقع مفهوم حقوقی حاکمیت، مافوق مفاهیم کنترل سرزمینی است و حقوق بین‌الملل عرفی تعریفی وسیع‌تر از اصطلاح حاکمیت دولت، ارایه می‌دهد. بطور کلی حاکمیت دولت عبارت است از ظرفیت تصمیم‌گیری یک دولت، برای تدوین سیاست‌های

1. International Humanitarian law Institute.
2. Global Common.
3. US Department of Defense, The Strategy for Home Land Defense and Civil Support (June 2005).
4. Radiation.

خود در رابطه با موضوعات داخلی و خارجی که از این دولت در مقابل مداخلات خارجی، حمایت می‌نماید. (R Buchnan,op.cit:223) این برداشت از حاکمیت دولت در رویه دیوان بین‌المللی دادگستری هم دیده می‌شود و دیوان در تعیین وضعیت عرفی اصل عدم مداخله و دامنه آن در قضیه نیکاراگوئه اعلام می‌کند که:

"مداخله غیر قانونی در موضوعاتی قابل طرح است که در رابطه با آن موضوعات، هر دولتی مجاز است طبق اصل حاکمیت ملی، خود آزادانه راجع به آنها تصمیم گیری نماید. از جمله این موضوعات انتخاب یک سیستم سیاسی، اقتصادی، اجتماعی، فرهنگی خاص و نیز تدوین سیاست خارجی کشور می‌باشد. (Kanuck,op.cit:288) مداخله زمانی غیر قانونی است که از این روش‌ها برای اعمال اجبار در جهت این انتخاب‌ها استفاده شود، انتخاب‌هایی که باید آزادانه صورت بگیرند... عنصر اجبار... شرط ایجاد یک مداخله غیر قانونی است. (Nicaragua Case, op. cit.205) بنابراین جوهره مداخله، اجبار است. (Jamnejad and Wood, 2009. 348)

به این ترتیب، مداخله زمانی صورت می‌گیرد که واجد شرایط اجبار شود و معمولاً به منظور ایجاد تغییر در سیاست‌های دولت هدف، اعمال می‌گردد. به هر حال توجه به این مسئله مهم است که اجبار به تنهایی برای ایجاد یک مداخله غیر قانونی کافی نیست. این اجبار باید در رابطه با موضوعی صورت گرفته باشد که دولت قربانی به طور آزادانه حق دارد، خود راجع به آن موضوع تصمیم‌گیری نماید، بنا به دیدگاه دیوان بین‌المللی دادگستری" انتخاب‌ها، باید آزاد باقی بمانند" به طور کلی رویه دولت‌ها می‌تواند حوزه اصل عدم مداخله را تعیین کند. در حقیقت، تغییراتی که در حوزه اصل عدم مداخله به وجود آمده به وسیله دیوان در قضیه‌ی نیکاراگوئه توسعه داده شده‌اند. در این قضیه دیوان باید تعیین می‌کرد که آیا نشانه‌هایی در رویه دولتها دیده شده که گویای آن باشد که یک حق کلی برای دولتها، محفوظ است که به طور مستقیم یا غیر مستقیم، چه در قالب اقدامات نظامی و چه بصورت غیر نظامی جهت حمایت از مخالفان داخلی، در امور داخلی دولت دیگر مداخله کنند؟ گروه-هایی که به دلیل ارزش‌های اخلاقی یا سیاسی، حمایت از آنها مهم تلقی می‌شود. (Nicaragua Case ,op.cit.206)

النهایه در این قضیه دیوان اعلام نمود که حتی در موارد محدود که دولتها از گروه‌های مخالف داخلی حمایت کرده بودند، رفتار خود را به عنوان یک حق مداخله جدید یا استثنایی بر اصل عدم مداخله توجیه نکرده‌اند. (Ibid.207)

بنابراین دیوان نتیجه گیری نمود که هیچ حق کلی برای مداخله جهت حمایت از مخالفان در دولت دیگر در حقوق بین‌الملل معاصر وجود ندارد. (Ibid.2.9) با وجود این نتیجه گیری، اهمیت این حکم در آن است که دیوان بین‌المللی دادگستری به شناسایی این مسئله کمک نمود که قلمرو اصل عدم مداخله می‌تواند در جایی که با رویه کافی از دولت ها همراه شده باشد، تحول یابد.

به این ترتیب، در ارتباط با مساله حملات سایبری و نقض اصل عدم مداخله و در نتیجه وقوع یک مداخله غیر قانونی، باید به دو سوال مهم پاسخ داده شود. اولاً اینکه آیا اجرای این قبیل حملات و در نتیجه مداخله صورت گرفته، با قصد اجبار دولت قربانی به تغییر یک سیاست انجام شده است؟ این به کارگیری عمدی اعمال زور در مقابل صرف نفوذ است که اصل عدم مداخله آن را نهی می‌کند و نیازمند ارزیابی اثر مداخله بر دولت قربانی است. ثانیاً اینکه اگر قصد تحمیل و اجبار وجود دارد، پس از آن باید پرسیده شود که آیا اجرای اجبار از طریق حملات صورت گرفته، در مورد موضوعاتی بوده است که یک دولت محق است طبق اصل حاکمیت ملی، خود آزادانه در ارتباط با آنها تصمیم گیری نماید؟ پاسخ به این سوال نیز نیازمند شناسایی آن هدفی است که اجبار بخاطر آن صورت گرفته است. اگر بررسی حقوق بین‌الملل عرفی ورویه دولت‌ها نشان دهد که اجرای چنین اجباری مجاز است، در این صورت نمی‌توان گفت که مداخله صورت گرفته، غیر قانونی بوده است.

۲. ضابطه میزان و شدت خسارات و صدمات ثانویه حملات سایبری

در قسمت قبلی در ارتباط مفهوم حاکمیت، اصل عدم مداخله و ارتباط آن با حملات سایبری که منجر به نقض اصل عدم مداخله می‌شوند، توضیحاتی ارایه گردید. در این قسمت به لحاظ ضرورت تبیین دقیقتر آثار حملات سایبری، این موضوع با تفصیل بیشتری مورد بررسی قرار می‌گیرد.

حوزه شمول اصل عدم مداخله به حدی وسیع و گسترده است که می‌توان هر فعل متخلفانه‌ای را که دولتها علیه یکدیگر مرتکب می‌شوند، در قالب این اصل قرار داد مشروط بر اینکه افعال متخلفانه ارتکابی، مشمول دیگر تعاریف و عناوین موجود در حقوق بین الملل نگردند. در عمل اکثر حملات سایبری صورت گرفته در سال‌های اخیر به آستانه لازم برای ایجاد یک حمله مسلحانه نرسیده‌اند و می‌توان گفت جز حمله سایبری ویروس استاکس نت در سال ۲۰۱۰ میلادی به تاسیسات هسته‌ای نطنز، سایر موارد حملات سایبری تاکنون به عنوان حمله مسلحانه ارزیابی نشده‌اند. [۱]

به این ترتیب توسل به اصل عدم مداخله وسیله مناسبی جهت ممنوعیت این قبیل اقدامات می‌باشد.

بدون شک هر حمله سایبری، آثار و تبعات سوء و مخربی را از خود به جای می‌گذارد. این آثار و تبعات منفی بعضا به صورت مستقیم و غالبا به صورت غیر مستقیم و ثانویه به هدف مورد نظر (قربانی) آسیب رسانده و خسارت وارد می‌کنند. بعنوان مثال وقتی که حمله سایبری بر روی سیستم کنترل ترافیک هوایی یا راکتورهای اتمی صورت بگیرد و آسیب‌های انسانی و مالی وسیعی به بار آورد، به مثابه یک حمله مسلحانه محسوب می‌شود و آثار مخرب حمله سایبری به صورت مستقیم ایجاد می‌گردد اما خسارات و صدمات ناشی از حملات سایبری در غالب موارد تبعی و ثانویه می‌باشند، در نتیجه مبنای قضاوت را می‌توان بر اساس میزان و شدت خسارات و صدمات وارده، مورد ارزیابی قرار داد، به این نحو که اگر خسارات وارده باعث تخریب و ورود آسیب‌های جدی به زیر ساخت‌های حیاتی کشور قربانی نشود، به گونه‌ای که نتوان آن را حمله مسلحانه به مفهوم کلاسیک تلقی کرد، می‌توان حمله سایبری صورت گرفته را مصداق مداخله در امور داخلی دولتها از نوع خصمانه قلمداد نمود که طبیعتا موجبات طرح مسئولیت بین‌المللی مرتکب یا مرتکبین آن حملات را فراهم خواهد نمود. به عنوان مثال اگر به موجب یک حمله سایبری نظام اقتصادی یک کشور دچار اختلال گردد به نحوی که

[1] - Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," Prepared by the the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence,General Editor:Michael N.Schmitt,Cambridge University Press, New York, 2017.Rule 1.at 26

خدمت رسانی به اشخاص حقیقی و حقوقی در کشور مورد نظر مختل گردد و یا مثلا بازار بورس و سهام کشور قربانی به گونه‌ای بهم بریزد که انجام معاملات در بازار بورس را برای یک بازه زمانی مختل بسازد، در چنین وضعیتی تلقی حمله مزبور به عنوان مصداقی از مداخله در امور داخلی دولتها امری منطقی به نظر می‌رسد، هر چند که در مقابل، عده‌ای نیز معتقدند که حملات سایبری که علیه زیر ساخت‌های حیاتی یک دولت اجرا می شوند و دستگاه‌های دولتی را فلج نموده و عملکرد آنها را مختل می‌سازند، باید به عنوان حمله مسلحانه در نظر گرفته شوند، حتی اگر فوراً منجر به خسارات مادی یا کشته شدن انسانها نگردند. (Jensen,2008.221-229) این گروه از حقوقدانان مثلا همان مورد حمله بر روی سیستم مالی دولت را که با تغییر دادن یا تخریب اطلاعات باعث به خطر افتادن حیات اقتصادی دولت می‌شود، بعنوان حمله مسلحانه در نظر می‌گیرند و این نه به دلیل ایجاد تخریب‌های مادی، بلکه به این دلیل است که اینگونه حملات باعث می‌شوند که چنین زیر ساخت‌های دولتی از انجام هدفی که بخاطر آن به وجود آمده‌اند، ناتوان شوند.

به این ترتیب تعیین معیار و ضابطه در بر شمردن مصادیقی از حملات سایبری به عنوان نقض اصل عدم مداخله در حال حاضر امری مورد اختلاف می‌باشد اما تا زمان تعیین قطعی چنین ضابطه و معیاری از سوی جامعه بین‌المللی، نمی‌توان وضعیت حقوقی چنین حملاتی را در هاله‌ای از ابهام قرار داد و از این رو به نظر می‌رسد که در حال حاضر چاره‌ای جز توسل به رویکرد بررسی موردی آثار و تبعات ثانویه حملات سایبری وجود ندارد و اتخاذ این موضع منجر به این خواهد شد که از این پس جامعه بین‌المللی موضعی منفعل و خنثی در قبال حملات سایبری نداشته باشد. (اصلانی،۱۳۹۵: ۲۰۱-۲۰۰)

۳. بررسی موردی برخی از حملات سایبری

جهت تبیین دقیقتر مفاهیمی که در قسمت‌های قبل ذکر گردید، در این قسمت به بررسی دو مورد مهم از حملات سایبری که در سال‌های اخیر صورت گرفته، یعنی حمله سایبری به کشور استونی در سال ۲۰۰۷ میلادی و حمله سایبری به کشور آمریکا در سال ۲۰۱۶ میلادی، پرداخته می‌شود و قابلیت اعمال مفاهیم ذکر شده در این موارد خاص از حملات سایبری، مورد ارزیابی قرار می‌گیرند. در واقع هدف تحلیل این مسئله است که آیا

حملات سایبری صورت گرفته علیه کشورهای ذکر شده، می‌تواند به عنوان مداخله غیر قانونی در امور داخلی کشورهای مورد هدف، در نظر گرفته شوند؟ پاسخ به این سوال نیازمند بررسی این مسئله است که اولا آیا حملات سایبری منجر به اجرای اجبار علیه این کشورها شده است؟ و ثانیا اینکه حملات سایبری اجرا شده، به عمد و جهت اجبار این کشورها به تغییر یک سیاست خاص، صورت گرفته است؟

۳-۱ - حمله سایبری به استونی در سال ۲۰۰۷ میلادی

در اوایل بهار سال ۲۰۰۷ میلادی، دولت استونی اعلام کرد که یک مجسمه سرباز روسی (معروف به سرباز برنزی) را به یک محل جدید در حومه پایتخت، به نام تالین[1] منتقل می‌کند. می‌کند. دلیل این اقدام نیز آن بود که مجسمه برای یادآوری سربازان اتحاد شوروی که در نبرد علیه آلمان نازی در طول جنگ جهانی دوم جان خود را از دست داده بودند، بنا شده بود و با توجه به تعداد زیاد جمعیت روس تبار که در استونی زندگی می‌کردند، این اعلام (جابجایی مجسمه) اهانت آمیز تلقی شده و منجر به چندین روز بلوا و غارت، در شهر تالین گردید. علاوه بر آن، این اعتراضات خشونت آمیز با حملات سایبری علیه آژانس‌های دولتی و کمپانی‌های خصوصی (مانند ایستگاه‌های رسانه‌ای و بانک‌ها) همراه گردید. اساساً این حملات به شکل حملات(DDOS) [2] بودند که به زبان ساده یعنی سرازیر کردن تقاضاهای زیاد به یک یک سرور و استفاده بیش از حد از منابع (پردازنده، پایگاه داده، پهنای باند، حافظه و...)، به طوری که سرویس دهی عادی به کاربران، دچار اختلال شده یا سرور از دسترس خارج گردد. (به دلیل حجم بالای پردازش یا به اصطلاح overload شدن عملیات‌های سرور)، در این نوع از حملات، در یک لحظه یا در طی یک زمان، به صورت مداوم از طریق کامپیوترهای مختلف که ممکن است خواسته یا حتی ناخواسته مورد استفاده قرار گرفته باشند، به یک سرور (با آی پی مشخص) درخواست دریافت اطلاعات ارسال می‌شود و موجب می‌شود که سرور، از دسترس خارج شده یا به اصطلاح Down شود. در این حالت، صفحه‌های وب‌سایت‌های

[1].Tallina.

[2]. In Computing , a Denial- of Service (Dos) or Distributed Denial- of- Service (DDOS) Attack is an Attempt to Make a Machine or Network Resource Unavailable to its Intended Users.

اینترنتی، موضوع درخواست‌های دریافت اطلاعات بسیار زیادی قرار می‌گیرند و این امر باعث می‌شود که عملکرد این وب سایتها به شدت کنده شده یا حتی کاملاً متوقف گردد و در نتیجه، کاربران امکان دسترسی به آن صفحه‌ها را از دست می‌دهند. در مورد استونی، ابتدا حملات DDOS ساده و بطور نامناسبی ترکیب شده و به سادگی قابل دفع بودند. (Tikk et al., 2008.19) اما به سرعت سازمان یافته شده و پیچیده گردیدند. به خصوص، بات نت‌های[1] بزرگی مورد استفاده قرار گرفتند. یک بات نت ترکیبی از کامپیوترهای به خطر افتاده است که بعداً ممکن است بدون اطلاع کاربر اصلی هم استفاده شوند. در مورد کشور استونی این مسئله منجر به این شد که تقریباً از ۸۵۰۰۰ کامپیوتر مورد سرقت، تقاضاهایی برای دریافت اطلاعات به وب سایت‌های اینترنتی این کشور فرستاده می‌شد و چون وب سایت‌های مورد هدف، قادر نبودند که از پس این تقاضاها برآیند، صفحه‌های وب مورد هدف، خراب شده و از سرویس خارج شدند[2]. در نهایت این حملات تقریباً سه هفته طول کشیدند. (از ۲۶ آپریل تا ۱۹ ژوئن). هر چند که دولت روسیه دخالت خود را در ارتکاب این حملات انکار کرد و هرگز انتساب قطعی این مسئله به فدراسیون روسیه محرز نشد، اما دولت استونی اعلام نمود که دولت روسیه مسئول اصلی این حملات است[3].

در ارتباط با حملات صورت گرفته سوالی که هم در رسانه‌ها و هم تفاسیر آکادمیک مطرح شد، آن بود که آیا این نوع از حملات سایبری (به خصوص حملات DDOS) می‌توانند به عنوان توسل به زور غیر قانونی در نظر گرفته شوند؟ این مسئله قابل انکار نیست که تخریب گسترده‌ای در تشکیلات کامپیوتری کشور استونی رخ داد. به زبان سخنگوی پارلمان استونی: "من وقتی که به یک انفجار هسته‌ای نگاه می‌کنم و انفجاری که در کشور ما در ماه می، اتفاق

[1]. Botnet.

[2]. برای بازبینی حملات سایبری علیه استونی مراجعه شود به:
NATO's Documentary Entitled 'Six Colours: War in Cyberspace' an http://www. nato. int/ebookshop/video/six-colours/sixcolours. Html-accessed 19 June 2012.

[3]. 'Russia Accused of Unleashing Cyberwar to Disable Estonia' The Guardian (London, 17 May 2007) at http://www.guardion. co.ulc/world/2007/May/17/topstories3-russia accessed at 8 April 2012.

افتاد، یک چیز مشابه را می‌بینیم... مانند تشعشعات هسته‌ای، جنگ سایبری باعث خونریزی نمی‌شود اما می‌تواند همه چیز را تخریب کند[۱] ".

به هرحال نکته‌ای که در این نقل قول باید مورد توجه قرار بگیرد آن است که بر خلاف یک انفجار هسته‌ای، حملات سایبری ارتکاب یافته علیه استونی منجر به ایجاد صدمه فیزیکی نگردیدند ،[۲] هر چند که آثار مخرب، قابل مقایسه با چنان حمله‌ای باشند. این نکته بسیار حایز اهمیت است زیرا نقض بند ۴ ماده ۲ منشور فقط وقتی اتفاق می‌افتد که یک سلاح باعث ایجاد صدمات فیزیکی شده باشد. به این ترتیب، با فقدان صدمات فیزیکی، حملات سایبری ارتکاب یافته علیه استونی نمی‌توانند بعنوان توسل به زور غیر قانونی برابر مقاصد بند ۴ ماده ۲ منشور در نظر گرفته شوند. برای پاسخ به این پرسش باید میزان اختلال ایجاد شده به وسیله حملات DDoS [۳] صورت گرفته در استونی مشخص شود. در این زمینه باید به این مسئله توجه شود که استونی در سال۲۰۰۷ میلادی کشوری بوده که در آن تعداد کاربران اینترنت در این کشور، نسبت به سایر کشورهای اروپایی بیشتر بوده است (Davis,2007) و در آن زمان کشور استونی یک جامعه اطلاعاتی محسوب می‌شده است.(Tikk et al., op. cit.16) بنابراین وقتی که حملات اتفاق افتاد، بخش دولتی، بخش خصوصی، افراد و شهروندان به شدت به سرویس‌های اینترنتی برای اجرای امور خود نیازمند بودند. بعنوان مثال، در سال ۲۰۰۷ میلادی حدود ۹۵ درصد عملیات‌های بانکی در این کشور بصورت الکترونیکی انجام می‌شده است، (Ibid.17) و در نتیجه این حملات باعث ایجاد اختلال در کار بسیاری از بزرگترین بانک‌های استونی شد و آثار نامطلوب فراوانی بر اقتصاد کشور استونی تحمیل گردید. ایستگاه‌های رسانه‌ای هم هدف این حملات قرار گرفتند و از آنجایی که دسترسی به رسانه‌ها در کشور استونی اساسا از طریق اینترنت صورت می‌گیرد، این حملات مشکلات زیادی ایجاد نمودند. بنابراین با از کار انداختن وب سایت خبری اصلی، استفاده از اینترنت جهت ارتباط و

---

1. E Ergrna, Speaker of the Estonian Parliament, quoted in J Davis, 'the Most Wired Country in Europe' Wired Magazine (21 August, 2007).

2. 'No Lives were Lost, no Troops Deployed across Borders, and no Guns were Fired…[in conclusion] the Cyber – Assault on Estonia failed to Generate Physical Damage': k Hinkle, 'Countermeasures in the Cyber Content :One More thing to Worry About'(2011) 37 Yale J Intl L online 11, 13-14.

Distributed Denial of Service..3

دریافت اطلاعات از کار افتاد و با احراز این مسئله که منشا حملات DDoS صورت گرفته خارج از کشور استونی بوده، برای کاهش حملات، سایر سردبیران خبر هم ارتباط‌های بین-المللی خود را از طریق شبکه قطع کردند و در نتیجه تمام ارتباطات از طریق سایت‌ها مسدود گردید و در عمل کشور استونی از سایر نقاط دنیا جدا شد.

اثر حملات DDoS در بخش عمومی هم بسیار شدید بود زیرا وب سایت‌های دولتی هم هدف این حملات قرار گرفته بودند. از همه مهمتر اینکه این حملات، وب سایت‌های مربوط به دفتر نخست وزیر و گروه سیاسی مربوطه، دفتر رئیس جمهور، پارلمان و ... را نیز هدف قرار داده بودند. علاوه بر آن، وب سایت‌های متعلق به پلیس و وزارتخانه‌های دولتی هم هدف حملات قرار گرفتند. در واقع این حملات به حدی مخرب بودند که باعث از کار افتادن این وب سایت‌ها هم شده و در نتیجه مقامات دولتی و شهروندان نیز از دسترسی و به روزرسانی اطلاعات از طریق وب‌سایت‌ها و حفظ تماس‌های اینترنتی باز ماندند. (Woltag, op.cit.5)

به این ترتیب و با توجه به شدت حملات سایبری صورت گرفته می‌توان گفت که این حملات از آستانه صرف اعمال نفوذ فراتر رفته و منجر به اجرای عمدی اجبار علیه دولت استونی گردیده‌اند، با این هدف که دولت استونی از تصمیم خود برای جابجایی مجسمه سرباز برنزی یادگار دوران اتحاد جماهیر شوروی صرف نظر کند.

اگر به سوال دوم باز گردیم، آیا این اجبار در موضوعی صورت گرفته است که دولت حق داشت خود بطور آزادانه راجع به آن تصمیم بگیرد؟ که در این زمینه نیز پاسخ مثبت است، زیرا بدیهی است که اتخاذ تصمیم در مواردی چون جابجایی مکان یادبودهای تاریخی، از جمله مواردی است که هر دولتی حق دارد آزادانه راجع به آنها تصمیم بگیرد. به عبارت دیگر، این یک تصمیم در حوزه قلمرو حاکمیتی دولتها می‌باشد و به وسیله اصل عدم مداخله مورد حمایت قرار می‌گیرد، لذا با توجه به مراتب فوق می‌توان گفت که حملات سایبری علیه استونی، منجر به نقض حاکمیت دولت استونی گردیده و یک مداخله غیر قانونی محسوب می-شود.

۳-۲- حمله سایبری به آمریکا در انتخابات ریاست جمهوری سال ۲۰۱۶ میلادی

از میان بحث برانگیزترین حملات سایبری که در سال‌های اخیر صورت گرفته‌اند، حمله سایبری به آمریکا در جریان انتخابات ریاست جمهوری این کشور در سال ۲۰۱۶ میلادی است. بر اساس گزارش‌های جامعه اطلاعاتی ایالات متحده آمریکا[1]، ماموران روسیه در انتخابات سال ۲۰۱۶ آمریکا مداخله کرده‌اند. در اکتبر همان سال دولت آمریکا اعلام نمود، که اطلاعات موثقی دارد، مبنی بر اینکه دولت روسیه در هک شدن کامپیوترهای کمیته ملی دموکراتیک[2] و سایر سازمان‌های سیاسی حزب دموکرات دخالت دارد. در این روند هکرها به حدود ده هزار ایمیل این حزب دست پیدا کردند و آنها را برای وب سایت ویکی لیکس فرستادند و این وب سایت نیز کلیه اسناد را منتشر نمود و در زمان رقابت‌های انتخابات ریاست جمهوری آمریکا در دسترس عموم قرار داد. در ۲۹ دسامبر همان سال کاخ سفید اعلام نمود که فعالیت‌های سایبری دولت روسیه به منظور اثرگذاری بر انتخابات امریکا صورت گرفته است و اعتماد مردم به نهادهای دموکراتیک آمریکا را خدشه دار نموده و تمامیت و امنیت سیستم انتخاباتی این کشور را زیر سوال برده است و اینگونه اقدامات قابل قبول نبوده و تحمل نمی‌شود و در همان روز نیز رییس جمهور، یک فرمان اجرایی صادر کرد که بر اساس آن مقرر گردید که علیه دو سرویس اطلاعاتی روسیه، یعنی آژانس اطلاعات اصلی[3] و خدمات امنیتی فدرال [4] و افسران آژانس اطلاعات اصلی و نیز شرکت‌هایی که به این نهادها جهت پیشبرد مقاصدشان، کمک نموده اند، تحریم‌هایی اعمال گردد. در شش ژانویه ۲۰۱۷ نیز دبیر سرویس اطلاعات ملی، گزارشی را منتشر نمود که در آن گزارش جزییات اقدامات دولت روسیه در این زمینه بیان شده است.

با توجه به اطلاعات منتشر شده و با این پیش فرض که اطلاعات مورد استناد سرویس‌های امنیتی آمریکا موثق بوده و انتساب هک صورت گرفته نسبت به ایمیل‌های کمیته ملی

[1] .U.S. Intelligence Community.
[2] .Democratic National Committee.(DNC).
[3] . Main Intelligence.
[3] . Federal Security Service. Agency.
[4] . Federal Security Service.

دموکرات‌ها نیز به دولت روسیه محرز است[1]، اکنون این سوال قابل طرح است که آیا دخالت سایبری دولت روسیه در انتخابات آمریکا، منجر به نقض اصل عدم مداخله، در امور داخلی امریکا شده است؟ جهت پاسخ به این پرسش این مسئله باید مورد ارزیابی قرار گیرد که آیا دخالت سایبری روسیه در انتخابات آمریکا منجر به اعمال عمدی اجبار علیه این کشور گردیده است؟

همان طور که در قسمت‌های قبلی توضیح داده شد، حاکمیت یعنی قدرت انحصاری در تصمیم گیری در امور داخلی بدون هرگونه دخالت خارجی. دستورالعمل تالین نیز در این زمینه می‌گوید: هرگونه مداخله در در انتخاب‌های سیاسی یک دولت بعنوان مداخله در حاکمیت آن دولت تلقی می‌گردد، اگر آن مداخله، همراه با اجبار باشد. به این ترتیب تهیه کنندگان دستور العمل تالین نیز ، مواردی چون صرف انتشار تبلیغات را به خودی خود، نشان دهنده مداخله غیرقانونی علیه حوزه صلاحیتی و حاکمیت دولت دیگر ارزیابی نمی کنند.[2]

در سایر موارد تعارضات بین‌المللی نیز، هم دولت آمریکا و هم سایر کشورها، اسنادی علیه دیگرکشورها منتشر نموده‌اند تا مردم آن دولتها را قانع کنند که بر دولت خودشان جهت اتخاذ سیاستی خاص، اعمال فشار کنند. دولت آمریکا، از طریق رسانه صدای آمریکا، صدای خود را در سراسر جهان به گوش مخاطبان خود می‌رساند. دولت کره جنوبی نیز بلندگوهایی را نزدیک مرزهای خود با کره شمالی قرار داده تا اخبار و اطلاعات را به گوش مردم کره شمالی که در حالت انزوای بین‌المللی به سر می‌برند، برساند. در جریان انتخابات ریاست جمهوری آمریکا نیز با وجود اینکه محرز است که رییس جمهور فدراسیون روسیه، آقای پوتین، حمایت خود را از آقای ترامپ، از طریق رسانه‌های طرفدار خود اعلام نمود و از رای دهندگان آمریکایی خواست، که به او رای بدهند اما اینگونه اقدامات را نمی‌توان به منزله نقض حاکمیت دولت آمریکا تلقی نمود.

---

۵. هر چند که دولت روسیه تاکنون هر گونه دخالت خود را در این امر را انکار نموده و در هیچ نهاد بین المللی نیز دخالت دولت روسیه در این زمینه به اثبات نرسیده است ، اما بررسی این موارد از حوزه ی موضوعی این مقاله خارج است.

[2] - Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence , General Editor: Michael N.Schmitt, Cambridge University Press, New York , 2017.Rule 1.at 26

جهت نقض اصل عدم مداخله، دستورالعمل تالین وجود عنصر اجبار را ضروری می‌داند و لیستی از اعمالی را بر می‌شمرد که انجام آنها مصداق دخالت در اموری می‌باشند که در روند یک انتخابات آزاد، جز صلاحیت‌های ذاتی دولت مجری آن انتخابات است مانند مانع ایجاد کردن در عملکرد نهادهای دولتی در روند برگزاری انتخابات از طریق اقداماتی چون تغییر یا حذف اطلاعات و یا ایجاد اختلال از طریق حملات سایبری در روند شمارش آرا.

در انتخابات ۲۰۱۶ آمریکا، دولت روسیه فقط اطلاعات خصوصی برخی از شخصیت‌های سیاسی را منتشر و در اختیار عموم قرارداد که مصداق اعمالی چون تغییر دادن یا پاک کردن اطلاعات نمی‌باشد. در نتیجه اگر دولت روسیه در امور مربوط به صندوق‌های رای و یا روند رای گیری الکترونیک دخالت نموده بود، از آن جایی که این قبیل اعمال، جز صلاحیت‌های ذاتی هر دولتی می‌باشد، نقض اصل عدم مداخله محسوب می‌گردید، اما در انتخابات ۲۰۱۶ امریکا چنین اتفاق‌هایی رخ نداده است.

با توجه به موارد فوق الذکر، مداخله دولت روسیه شامل افشای اطلاعات خصوصی و یا انتشار برخی اخبار غیر واقعی در روند انتخابات بوده است که اینگونه اقدامات زیر چتر تبلیغات و نقض حق بر حریم خصوصی قرار می‌گیرند و با توجه به اینکه آثار اقدامات صورت گرفته تا امروز چندان روشن نیست، نمی‌توان گفت اینگونه اقدامات منجر به اعمال اجبار علیه دولت آمریکا و یا رای دهندگان آمریکایی شده است و در نتیجه نقض اصل عدم مداخله در امور داخلی دولت آمریکا محسوب نمی‌شود. (Ohlin,2017.15-17) عده‌ای نیز قائل به این هستند که اقدامات صورت گرفته توسط دولت روسیه در روند انتخابات آمریکا مصداق جاسوسی در روابط بین‌المللی می‌باشد که اگر قائل به این امر هم باشیم واقعیت این است که جاسوسی کشورها در امور یکدیگر در روابط بین‌المللی آنقدر گسترش یافته است که حقوق بین‌الملل عرفی آن را ممنوع نکرده است، البته این امر مانع از این نیست که بتوان اینگونه اقدامات دولت روسیه را به دلیل نقض حق اشخاص بر حریم خصوصی خود و یا نقض حق مردم آمریکا در تعیین سرنوشت خود، خلاف مقررات حقوق بین‌الملل ارزیابی نمود اما آن چه که در این مقاله مورد نظر است، آن است که به توجه به داده‌های ذکر شده، نمی‌توان در این مورد خاص، دولت روسیه را متهم به نقض اصل عدم مداخله در امور داخلی دولت آمریکا نمود.

۴. اقدامات دولت قربانی در مقابل نقض اصل عدم مداخله

از آنجایی که غالب حملات سایبری صورت گرفته با در نظر گرفتن معیار مضیق مندرج در منشور، به آستانه یک حمله مسلحانه نمی‌رسند، لذا می‌توان تحقق چنین حملاتی را در فضای سایبر علیه سایر کشورها نوعی اقدام متخلفانه غیر از توسل به زور و حمله مسلحانه تلقی نمود و در نتیجه با در نظر گرفتن حملات مذکور به عنوان اقدامی خلاف قواعد حقوق بین‌الملل، دولت قربانی قادر خواهد بود که علیه دولت خطاکار، تحت عنوان خود حمایتی به اقدامات متقابل متوسل گردد. (Noortman,2005,36-37)

هر چند اقدام متقابل رفتار غیر دوستانه‌ای است که با تعهدات بین‌المللی دولتی که به آن مبادرت می‌ورزد مغایر نیست، اما مقابله به مثل[1]، رفتار دولت در مغایرت با تعهدات بین‌المللی آن دولت است که در پاسخ به یک فعل متخلفانه بین‌المللی صورت می‌گیرد و همانطور که دیوان بین‌المللی دادگستری در قضیه گابچیکوو – ناگی ماروس اعلام نموده است، چنین اقداماتی اگر چه به خودی خود غیر قانونی است اما چنانچه در پاسخ به یک عمل متخلفانه دولت دیگر صورت گیرد، جایز شمرده می‌شود.[2]

بنابراین دولت قربانی حملات سایبری زمانی می‌تواند به این اقدامات متوسل گردد که عملیات و حملات سایبری انجام گرفته علیه او، طبق حقوق بین‌الملل غیر قانونی محسوب شود، در نتیجه حملات سایبری صورت گرفته با هدف اجبار دولت قربانی به تغییر رفتار در باب موضوعی که محق است خود به طور آزادانه راجع به آن تصمیم بگیرد، به دلیل مغایرت با اصل عدم مداخله در امور داخلی دولت دیگر، غیر قانونی محسوب شده و به دولت قربانی حق اعمال اقدام متقابل متناسب مطابق با شروط و محدودیت‌های بیان شده درمواد ۵۱ و ۵۰ و ۵۲ طرح مسئولیت دولتها مورخ ۱۲ دسامبر ۲۰۰۱ را می‌دهد. (Roscini, Marco, op. cit.114)

این نوع اقدامات استثنایی بر این قاعده عمومی است که دولتها می‌بایست اختلافات خود را به طرق مسالمت آمیز حل و فصل نمایند و به دولتها این اجازه را می‌دهد که در

[1] - Reprisal.
[2] - Gabcikovo-Nagymaros (Hungary/Slovakia), Merits, ICY Report 1997:55-56

مقابل دولتی که تعهدات بین‌المللی خود را در مقابل آن دولت نقض می‌کند، به اقدامات غیر مشروع متوسل گردند.

این نوع اقدامات باید مطابق سه ضابطه صورت پذیرند:

۱- در وهله اول این اقدامات می‌بایست در پاسخ به اقدام متخلفانه بین‌المللی دولت دیگر صورت گرفته و علیه دولت خاطی هدایت شود.

۲- دولت متضرر می‌بایست ابتدا از دولت خاطی بخواهد که اقدام متخلفانه‌اش را قطع یا در صورت وقوع درصدد جبران آن برآید.

۳- اثرات چنین اقداماتی می بایست متناسب با آسیب و ضرر متحمله باشد. (Gabcikovo-Nagymaros, op.cit.127)

مهم‌ترین شرط از میان شرایط ذکر شده، تعیین نوع اقدام متقابل در قبال حمله سایبری است و آنچه که به لحاظ ماهوی در این حوزه حایز اهمیت است، مسئله تناسب نوع اقدام متقابل با حمله سایبری صورت گرفته است، موضوعی که در ماده۵۱ طرح مسئولیت بین-المللی نیز مورد تاکید قرار گرفته است. تناسب یک شرط پذیرفته شده در اتخاذ اقدامات متقابل است که به صورت گسترده‌ای در رویه دولت‌ها، دکترین و رویه قضایی بین‌المللی مورد اشاره قرار گرفته است. مسئله مهم در رعایت اصل تناسب در اقدام متقابل در برابر حملات سایبری به موضوع تعیین نوع و یا جنس اقدام متقابل باز می‌گردد و در این زمینه باید اذعان داشت که کشور قربانی در حال حاضر در باب تصمیم گیری در خصوص جنس و یا نوع اقدام متقابل کاملا مختار است، گویا و مثبت چنین ادعایی نوع واکنش رسمی کشورهایی همانند ایالات متحده آمریکاست که در برابر حملات سایبری که به زعم آنها حمله مسلحانه تلقی شود، حق توسل به زور از نوع کلاسیک برای خود قایل هستند.(اصلانی، پیشین: ۲۷۵)

البته باید متذکر شد که دیدگاه و موضع رسمی آمریکا به این صورت بیشتر در قالب واکنش وفق ماده۵۱ منشور ملل متحد و در قالب دفاع مشروع اعلام شده است و نه اقدام متقابل، ولی از آنجایی که در دفاع مشروع نیز شرط تناسب مورد نظر است و جهت رعایت تناسب هیچ ضرورتی وجود ندارد که اقدام دفاعی از لحاظ ماهیت مانند اقدامی باشد که حمله مسلحانه را تشکیل داده است، لذا اشاره به موضع ایالات متحده آمریکا در این رابطه می-

تواند وحدت ملاک خوبی برای توضیح و تبیین حقوقی مقوله اقدامات متقابل و رعایت شرط تناسب باشد.

به این ترتیب و با توجه به موارد فوق الذکر در خصوص حمله سایبری که بحد حمله مسلحانه می‌رسد، مسلم است که دولت قربانی هم حق پاسخ سایبری هم مسلحانه را دارد، اما در جایی که حمله سایبری به آستانه حمله مسلحانه نمی‌رسد، دولت تنها حق توسل به اقدامات متقابل غیر قهر آمیز را دارد.

اقدام متقابل در برابر حملات سایبری می‌تواند در قالب حملات سایبری صورت بگیرد و قاعدتا و به طور عموم به نظر می‌رسد که اکثر کشورها تمایل داشته باشند تا حمله سایبری را با حمله سایبری پاسخ دهند و از این جهت اقدام متقابل در برابر حملات سایبری بیشتر به نظر از جنس سایبر و در فضای سایبر خواهد بود اما گاهی اوقات ممکن است دولتی که به اقدام متقابل متوسل می‌گردد از تکنولوژی و توان علمی و فنی لازم جهت اجرای حملات سایبری متقابل برخوردار نباشد و یا دولت آغازگر حملات سایبری به لحاظ توانایی سایبری از چنان قدرتی برخوردار است که دولت قربانی قادر به اجرای حملات سایبری در قالب اقدامات متقابل علیه دولت مورد نظر نمی‌باشد، در چنین حالتی، از آن جایی که دولتها در قبال عمل متخلفانه بین‌المللی دولت دیگر من جمله حمله سایبری، مادامی که به آستانه حمله مسلحانه نرسیده باشد، حق استعمال زور به گونه‌ای که مغایر منشور باشد را ندارند، می‌توانند از دیگر انواع اقدامات متقابل از جمله اجبارهای اقتصادی و سیاسی که شامل اقداماتی از قبیل فشارها و تحریم‌های اقتصادی، قطع روابط دیپلماتیک، مسدود کردن دارایی‌ها و اموال دولت خاطی، استفاده کنند که نمونه‌ای از اقدامات متقابلی هستند که هیچ مسئولیتی برای دولت ایجاد نمی‌کنند و ممنوعیتی هم ندارند.

بنابراین هر دولتی حق دارد وضعیت حقوقی خود را نسبت به سایر دولتها ارزیابی نموده و در برابر وضعیتی که به نظرش نقض تعهد بین‌المللی، توسط دولت دیگر است، حق خود را از طریق اقدام متقابل غیر نظامی استیفا نماید،[1] در نتیجه اگر چه توسل به دفاع مشروع در

[1]- رای داوری تفسیر توافق نامه میان فرانسه و ایالات متحده در مورد حمل و نقل هوایی،۱۹۸۷، مجموعه آرای داوری، جلد ۲، صفحه۴۱۷

در مقابل همه انواع حملات سایبری مجادله انگیز است، اقدام متقابل راهکار مناسبی برای دولت به دور از چالش دفاع مشروع می‌باشد و به طور کلی می‌توان گفت که اصل عدم مداخله یک چارچوب قانونی ایجاد می‌کند که می‌تواند دولتها را در مقابل حملات سایبری حفاظت نماید که هر چند باعث ایجاد خسارات فیزیکی نشده‌اند و در نتیجه به دلیل نرسیدن به آستانه لازم برای ایجاد یک حمله مسلحانه، تهدید یا توسل به زور محسوب نمی‌شوند، اما مداخله غیر قانونی در امور داخلی دولت محسوب می شوند.

نتیجه گیری:

مسئله مشروعیت حملات سایبری بیشتر در پرتو بند ۴ ماده ۲ منشور، مورد ارزیابی قرار می‌گیرد و در نتیجه حملات سایبری که منجر به ایجاد آثار فیزیکی گردیده‌اند، با نقض بند ۴ ماده ۲ منشور، توسل به زور غیرقانونی محسوب شده و در صورتی که به آستانه لازم برای یک حمله مسلحانه رسیده باشند، در مقابل، برای دولت قربانی حق دفاع مشروع از خود، طبق ماده ی ۵۱ منشور ایجاد می‌گردد.

اما در مقابل در سال‌های اخیر حملات سایبری رخ داده‌اند که ویژگی‌های فوق الذکر را ندارند، اما این به آن معنی نیست که چنین حملاتی قانونی محسوب می‌شوند. در واقع حملات سایبری که خسارات فیزیکی ایجاد نمی‌کنند، اما آثاری به بار می‌آورند که باعث می-شود یک دولت، مجبور به اتخاذ تصمیم در ارتباط با موضوعاتی شود که در چارچوب اعمال حاکمیت خود، حق دارد آزادانه در ارتباط با آنها تصمیم بگیرد، ناقض اصل عدم مداخله محسوب و بر اساس حقوق بین‌الملل عرفی مداخله غیر قانونی محسوب می‌شوند و در مقابل برای دولت قربانی، حق توسل به اقدامات متقابل ایجاد می‌گردد.

به این ترتیب اصل عدم مداخله، نمایانگر یک وسیله قانونی بین‌المللی است که می‌تواند از دولتها در مقابل حملات سایبری حمایت کند که با هدف اجبار یک دولت، به اتخاذ سیاستی خاص، اجرا می‌شوند. این دیدگاه، مخالف دیدگاه‌های موجود در ارتباط با توسعه مفهوم بند ۴ ماده ۲ منشور و تفسیر موسع از مفهوم توسل به زور و یا لزوم تصویب یک معاهده بین-المللی خاص در ارتباط با حملات سایبری نیست، اما هدف از این مقاله آن است که نشان دهد، در غیاب چنین چارچوب‌هایی که حداقل به نظر می‌رسد، در آینده‌ای نزدیک محقق

نخواهند شد و با رد این ادعا که قواعد موجود حقوق بین‌الملل جهت دفاع از دول قربانی حملات سایبری کافی نیستند، اصل عدم مداخله می‌تواند، ابزار حقوقی موثری، جهت حفاظت از امنیت سایبری دولتها ارایه نماید.

منابع فارسی

کتب

- جعفری لاری، علی اصغر (۱۳۹۴)، **امنیت سایبری و جنگ سایبری**، چاپ اول، تهران: انتشارات پندار پارس

- دی آنجلیز، جینا (۱۳۸۳)، **جرایم سایبر**، مترجم: سعید حافظی و عبدالصمد خرم آبادی، چاپ اول، تهران: دبیرخانه شورای عالی اطلاع رسانی

مقالات

- پاکزاد، بتول (۱۳۹۰)، **تروریسم سایبری**، مجله تحقیقات حقوقی، دانشگاه شهید بهشتی، ویژه نامه شماره ۴

- دولت شاهی، شاهپور (۱۳۸۳)، **صلاحیت قضایی در محیط مجازی**، مجموعه مقالات همایش بررسی جنبه‌های حقوقی فناوری اطلاعات و معاونت توسعه قضایی قوه قضائیه

- مجید عباسی و حسین مرادی (۱۳۹۳)، **جنگ سایبری از منظر حقوق بین‌الملل بشر دوستانه**، مجلس و راهبرد، سال ۲۲، شماره ۸۱

پایان نامه

- اصلانی، جبار(شهریور۱۳۹۵)، **حملات سایبری در چارچوب نظام مسئولیت بین‌المللی**، رساله دکتری، دانشگاه تهران

Ressources

BOOKS

-Boothby,William H.(2009),**Weapons and the Law of Armed Conflict**, Oxford University Press

-Bothe,M., et al.,(1982), **New Rules for Victims of Armed Conflicts**,Leiden, Martinus Nijhoff Publishers

-Bowett,D.W.,(1958),**Self-Defence in International Law**.New York, Praeger

-Dinstein,Yoram,(2010**),The Conduct of Hostilities Under the Law of International Armed Conflict**.2nd edn ,cup

-Dinstein ,Yoram,(2011), **War Aggression and Self Defence**.5th ed

-Jennings, Robert and Arthur watts,(1992), **Oppenheim's International Law**, Longman

Articles

-Benetar,Marco,(2009)**The Use of Cyber Force: Need for Legal Justification**, Goettingen Journal of International Law

-Boebert,W.Ealr,(2002), **A Servey of Challenges in Attribution, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy**, National Research Council, National Academies press

-Condron,S.M.,(2007),**Getting it Right: Protecting American Critical Infrastructure in Cyberspace**, 20, Har V.J.L. Tech

-Crawford, James,(2001),**The International Law Commission's Articles on State Responsibility**, Cup

-Creekman, Daniel M.,(2002), **A Helpless America? An Examination of the Legal Options Available to the united States in Response to Varying Types of Cyber-Attacks from China**, American University International Law Review 17, no.3

-Damrosch, Lori Fisler (1989),**Politics Across Borders: Non intervention and Non forcible Influence of Domestic Affairs**, 83 AJIL.1

-Davis, Joshua,(2007), **Hackers Take Down the Most Wired Country in Europe ?**, Wired Magazine

-Falliere,Nicolas, Liam O Murchu, and Eric, (2011), **W32.Stuxnet Dossier**, Symantec

-Gill,T.D.,(2006), **The Temporal Dimension of Self- Defence: Anticipation, Pre- Emption, Prevention and Immediacy**. IIJ. Conflict & Security Law

-Hinkle, Katharine C., (2011), **Countermeasures in the Cyber Content :One More thing to Worry about** ,The Yale Journal of International Law Online

-Jamnejad ,M., and M wood, (2009), **The Principle of Non- Interventionl, Leiden Journal of International Law**, Volume 22, Number 2,Netherlands.

-Jensen, E.T .(2002), **Computer Attacks on Critical State Infrastructure: A Use of force Invoking the Right of self – Defence**, 38 Stanford J Intl L 207

-Joyner, Christopher C. and Catherine Lotriaonte,(2001),**Information Warfare as International Coercion: Elements of a Legal Framework**, EJIL ,Vol.12, No.5

- Markoff, John,(2008), **Before the Gunfire, Cyber Attacks**, the New York Times

-Roscini, Marco, (2010),**World Wide Warfare- Jus ad Bellum and Use of Cyber Force**, Max Plank Yearbook of United Nations Law, Vol.14
- Ohlin, Jens David,(2017), **Did Russian Cyber Interference in the 2016 Election Violate International Law?**,Texas Law Review, Cornell Law School Research Paper No .17-15
-Schmitt, Michael N. (1998),**Computer Network Attack and the Use of Force in International Law**, **Thoughts on a Normative Framework** ,Colum.J. Transnat'IL.,No.37
-Schmitt, Michael N.,(2005). **CNA and the Jus in Bello: An Introduction**, in Bystorm (ed.), International Expert Humanitarian Law ,Swedish National Defence College
-Shacketford, Scott J. (2009), **From Nuclear war to Net war: Analogizing cyber Attacks in Interactional Law** ,Berkley Journal of International Law ,192 et seq
-Silver, Daniel B.,(2002),C**omputer Network Attack as a Use of Force under** Article 2 (4),76 Int1 Studies
-Tikk,E.,K Kaska, K Rünnimeri,M Kert, AM Talihärm and L Vihul,(2008), **Cyber Attacks against Georgia: Legal Lessons Identified**,Analysis Document by Co-Operative Cyber Deffence Center of Exellence (CCDCOE)
-Waxman, Matthew C., (2011), ***Cyber*-Attacks and the Use of Force: Back to the Future of Article** 2 (4), 36 the yale J Int1 L
-Woltag , J-C., (2011**), Computer Network Operations below the Level of Armed Force**, European Society of International Law Conference Paper Series 1, Tartu, Extonia
-wristion,Walter B, (1992),**The Twilight of Sovereignty: How the Information Revolution is Transforming our World**,Scribner

CASES

- Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA) (Merits)[1986] ICJ
-Corfu Channel (United Kingdom V. Albania) (Merits) [1949] ICJ
-Lotus Case (France v Turkey) (1927) PCIJ

INTERNET SITES

-https://ccdcoe.org/tallinn-manual.html.(last visited on 2017-06-22)
-http://www.nato.int/cps/en/natohq/topics_78170.htm. (last visited on 2017-06-22)

-https://www.theguardian.com/world/2007/may/17/topstories3.russia. (last visited on 2017-06-22)
-http://www.cyberpolice.ir/geography.net. (last visited on 2017-06-22)
-http://tnews.ir/news/48d767754311.html. (last visited on 2017-06-22)