فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۵۰، شمارهٔ ۲، تابستان ۱۳۹۹: ۷۱۱-۷۳۶
DOI: 10.22059/jplsq.2019.230048.1499

حملات سایبری و نقض اصل عدم مداخله

پرستو اسمعیل‌زاده ملاباشی[۱]، محسن عبدالهی[۲*]

چکیده

پیشرفت فناوری موجب مواجههٔ روزافزون دولت‌ها با حملات سایبری شده است. بیشترین حملات سایبری که دولت‌ها با آن مواجه‌اند، از نوع حملات سایبری نفی یا محروم‌سازی از سرویس توزیع‌شدهٔ اینترنتی است. این‌گونه حملات آثار مخرب مستقیم و آنی ندارند، به همین دلیل ارزیابی آنها در قالب ممنوعیت توسل به زور و حملات مسلحانه قرار نمی‌گیرد و معمولا دولت‌ها نیز با توجه به شدت کمتر آنها در برخی موارد حتی از پیگیری و شناسایی عاملان حملات صرف‌نظر می‌کنند. با اینکه قواعد مستقیم و صریحی در مورد حملات سایبری و نظم بخشیدن به آنها وجود ندارد، نظر به تبعات چنین حملاتی حتی با شدت کم و اقتضای ارزیابی حقوقی این حملات، با بررسی مقررات فعلی حقوق بین‌الملل به این نتیجه می‌رسیم که بعضی از این‌گونه حملات غیرمخرب را می توان با اصل ممنوعیت مداخله به نظم درآورد و در صورت احراز عاملان و انتساب آن حملات به دولت، مسئولیت بین‌المللی دولت‌ها را در مراجع بین‌المللی مطرح کرد. به‌عبارت دیگر، در مقالهٔ حاضر سعی بر آن است تا نشان داده شود که صرفا حملات سایبری شدید ناقض مقررات حقوق بین‌الملل حاضر نیستند.

کلیدواژگان

اصل ممنوعیت مداخله، حاکمیت، حملات سایبری، مسئولیت بین‌المللی دولت، نقض تعهد.

---

۱. گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران. Email: Parastou.esmailzadeh@yahoo.com
۲. گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران، دانشیار دانشکدهٔ حقوق دانشگاه شهید بهشتی، تهران، ایران (نویسندهٔ مسئول). Email: Abdollahi75@hotmail.com
تاریخ دریافت: ۱۳۹۵/۱۲/۲۸، تاریخ پذیرش: ۱۳۹۶/۰۷/۱۰

مقدمه

پیشرفت فناوری در هر دورهٔ زمانی برای بشر مطلوب بوده است. امروزه پیشرفت فناوری از یک طرف سبب تسهیل در امور بشر و دسترسی به آرامش و آسایش بیشتر شده و از طرف دیگر آثار و تبعات مخربی نیز به‌همراه داشته است. به‌تبع به‌وجود آمدن فضای سایبر، مواجه شدن دولت‌ها با حملات سایبری در عصر حاضر اجتناب‌ناپذیر است. تعداد و آثار این حملات به‌گونه‌ای است که حملات سایبری می‌توانند به‌عنوان تهدیدی جدی‌تر از آنچه امروزه با آن مواجهیم، ارزیابی شوند، ازاین‌رو این موضوع نیاز به نظم‌دهی در این حوزهٔ جدید از حقوق بین‌الملل را بیش از پیش آشکار می‌کند. حقوقدانان بین‌المللی شدیدترین نوع این‌گونه حملات را مورد تجزیه‌وتحلیل بیشتری قرار داده‌اند که معمولا با توجه به آثاری که چنین حملاتی از خود به‌جا می‌گذارند، در چارچوب توسل به زور یا حملات مسلحانه بررسی و ارزیابی می‌شوند. با اینکه حملات سایبری با شدت کمتر که با حجمی به‌مراتب بالاتر به‌عنوان تهدید جدی برای دولت‌ها مطرح است، ولی چون در حال حاضر معاهده یا عرف بین‌المللی در مورد حملات سایبری وجود ندارد، قرار دادن و ارزیابی این‌گونه حملات سایبری نیز در چارچوب مقررات فعلی حقوق بین‌الملل ضروری به‌نظر می‌رسد، زیرا بیشترین حملاتی که دولت‌ها با آنها مواجه‌اند، حملات سایبری هستند که آثار و شدت زیادی ندارند. این‌گونه حملات که از جمله مهم‌ترین آنها حملات محروم‌کننده از سرویس توزیع‌شده[1] غیرمخرب‌اند و برخلاف حملات با شدت بالا، به‌دلیل اینکه آثار مخربی از خود به‌جا نمی‌گذارند، در چارچوب توسل به زور و حملات مسلحانه قابل بررسی و ارزیابی نیستند. در حقیقت حملات سایبری غیرمخرب حملاتی‌اند که به هیچ‌گونه خسارات فیزیکی همانند تخریب اموال یا صدمه به جان افراد منتهی نمی‌شوند. برای مثال از جمله حملات سایبری غیرمخرب حملاتی‌اند که صرفا دسترسی کاربران را به صفحه‌ای خاص در اینترنت با اخلال مواجه می‌کنند، ولی هیچ‌گونه تأثیرات مخرب فیزیکی در پی ندارند. با بررسی قواعد موجود در حقوق بین‌الملل و انطباق آن قواعد با خصوصیات و شرایط به‌وقوع پیوستن حملات سایبری غیرمخرب، این نتیجه حاصل می‌شود که می‌بایستی این‌گونه حملات را در وضعیت کنونی حقوق بین‌الملل به نظم درآورد. اصل ممنوعیت مداخلهٔ دولت در امور دولت‌های دیگر می‌تواند به‌عنوان چارچوبی برای مسئول قلمداد کردن دولت‌ها در حملات موردنظر قرار گیرد. در قسمت اول و دوم مقاله به تعریف حملات سایبری و انواع آن حملات می‌پردازیم و در قسمت‌های بعد، اصل عدم مداخله در حقوق بین‌الملل و سپس قابلیت اعمال این اصل در حملات سایبری غیرمخرب بررسی و ارزیابی می‌شود.

1. Distributed Denial of Service Attacks (DDoS)

تعریف حملات سایبری

امروزه پیشرفت فناوری سبب شده است که ما با شکل دیگری از حملات مواجه شویم که با حملات در عالم واقع متفاوت‌اند. این حملات که حملات سایبری نامیده می‌شوند، با به‌وجود آمدن فضای سایبر و پیشرفت فناوری و سوء استفاده از ضعف‌های این فضا به‌وقوع می‌پیوندند.

در مورد تعریف حملات سایبری هیچ‌گونه اتفاق‌نظری وجود ندارد و این موضوع همچنان بین دولت‌ها و سازمان‌های بین‌المللی مورد اختلاف است (اصلانی و رنجبریان، ۱۳۹۴: ۲۷۵). از جمله تعاریفی که از حملات سایبری ارائه شده، تعریفی است که در استراتژی نظامی ملی آمریکا برای عملیات سایبری[1] مطرح شده است. در تعریف مذکور حملات سایبری به‌عنوان عملیاتی که موجب مختل کردن[2]، انکار[3]، تنزل[4] یا تخریب[5] اطلاعات موجود در کامپیوتر یا اطلاعات موجود در شبکه‌ها و یا خود شبکه‌ها می‌شوند، تعریف می‌گردند (Roscini, 2014: 13). بیشتر حقوقدانان بر این عقیده‌اند که شدیدترین حملات سایبری که به تلفات یا خسارات انسانی منجر می‌شوند یا به اشیا خسارات وارد می‌کنند، می‌توانند حتی وضعیت مخاصمهٔ مسلحانه را نیز در عالم واقع به‌وجود آورند (خلف رضایی، ۱۳۹۲: ۱۲۹). تعریف دیگری نیز از حملهٔ سایبری در قاعدهٔ ۳۰ راهنمای تالین[6] مورد توجه قرار گرفته است. مطابق با راهنمای مذکور «حملهٔ سایبری عملیات سایبری تهاجمی یا تدافعی است که از آن به‌طور متعارف انتظار صدمه وارد شدن به اشخاص یا مرگ اشخاص یا وارد شدن خسارات به اشیا می‌رود» (Tallinn Manual, 2013: 106).

حملات سایبری می‌توانند ویرانگر یا غیرمخرب باشند و منشأ آنها هم می‌تواند از نوجوانان تا مجرمان اینترنتی یا نظامیان دولتی متغیر باشد. تاکنون شناسایی دقیق و قطعی حمله‌کنندگان تقریبا دشوار بوده است، به همین دلیل شناسایی مرتکبان حملات و در نهایت مسئول شناختن آنها از جمله اقداماتی پیچیده در حوزهٔ بررسی مسئولیت بین‌المللی دولت‌هاست[7] (Kesan &).

---

1. US National Military Strategy for Cyberspace Operations
2. Disrupt
3. Deny
4. Degrade
5. Destroy
6. Tallinn Manual on the International Law Applicable to Cyber Warfare

راهنمای تالین که «راهنمای تالین در خصوص حقوق بین الملل قابل اعمال در جنگ‌های سایبری» نام دارد، پژوهشی غیرالزام‌آور در مورد چگونگی اعمال حقوق جنگ و حقوق بشردوستانه در مورد حملات سایبری است که در سال ۲۰۱۳ با کتابی با همین عنوان به چاپ رسید.

۷. البته در مورد شناسایی شایان ذکر است که حتی درصورتی‌که مصدر حملهٔ سایبری شناسایی شود، این موضوع الزاما به معنی انتساب حملهٔ مذکور به دولتی که حملات از قلمرو آن دولت صورت پذیرفته است، نیست. به‌طور کلی انتساب در حملات سایبری موضوعی پیچیده است، زیرا دولت‌ها می توانند با توجه به خصوصیات فضای سایبر هویت خود را پنهان کنند.

(Hayes, 2012: 424) علت تنوع حمله‌کنندگان سایبری اغلب ارزان بودن تجهیزات لازم برای اقدام به حمله و در دسترس بودن این تجهیزات برای عموم است، درحالی‌که برای مثال اگر حملاتی را که با سلاح‌های سنتی به‌وقوع می‌پیوندند با حملات سایبری مقایسه کنیم، به این نکته پی می‌بریم که علاوه‌بر گران بودن تجهیزات و مواجه شدن با خطرهای استفاده از آنها، این‌گونه تجهیزات سنتی معمولا در اختیار نیروی نظامی دولت‌ها یا عده‌ای خاص هستند که به‌راحتی برای همگان قابل دسترس نیستند.

برای شناخت بهتر حملات سایبری ابتدا باید انواع شبکه‌های کامپیوتری را شناسایی کنیم. دو نوع شبکهٔ کامپیوتری وجود دارد که عبارت‌اند از: شبکه‌های حاوی سیستم‌های اطلاعاتی[1] و شبکه‌های حاوی سیستم‌های کنترل زیرساخت‌ها[2]. سیستم‌های اطلاعاتی به پردازش اطلاعات می‌پردازند، ولی هیچ‌چیز ملموس دیگری را غیر از خودشان کنترل نمی‌کنند. این سیستم‌ها می‌توانند حاوی اسناد، پایگاه‌های داده‌ها و انواع دیگر اطلاعات باشند که از شبکه‌های محلی متعدد اداره‌شده توسط دولت‌ها، شرکت‌ها و سایر سازمان‌ها برای کمک به آنها در انجام کارهای خود تشکیل می‌شوند. حملات موفقیت‌آمیز به سیستم‌های اطلاعاتی سبب خسارات مستقیم فیزیکی نمی‌شوند، ولی در عین حال می‌توانند سبب ورود صدمات مهمی شوند (Heaton, 2005: 161). اهمیت اطلاعات و داده‌ها با توجه به پیشرفت روزافزون فناوری و وابستگی دولت‌ها به این‌گونه شبکه‌ها به‌حدی است که بعضا درصورتی‌که هیچ‌گونه نسخهٔ جداگانه‌ای از اطلاعات مذکور وجود نداشته باشد، با مختل شدن یا از بین رفتن اطلاعات موجود در شبکه‌ها، کلیهٔ اطلاعات ممکن است برای همیشه از بین بروند یا در صورت امکان بازگشت اطلاعات، این موضوع با فرایندی زمان‌بر و هزینه‌ای بالا صورت می‌پذیرد. به‌دلیل اهمیت بانک‌های اطلاعاتی دولت‌ها بر روی سیستم‌ها و شبکه‌های خود، حمله به چنین اطلاعاتی و از بین بردن آنها می‌تواند آثار مخرب و حتی با اهمیت بیشتری از یک حملهٔ نظامی سنتی برای دولت‌ها داشته باشد.

نوع دوم شبکه‌های کامپیوتری شبکه‌های حاوی سیستم‌های کنترل زیرساخت‌ها هستند که تجهیزات ملموسی را کنترل می‌کنند. رایج‌ترین نوع این سیستم‌ها کنترل نظارتی و سیستم جمع‌آوری اطلاعات[3] است. این سیستم‌ها برای کنترل حمل‌ونقل، آب، برق و تجهیزات تولیدی که در سراسر دنیا استفاده می‌شوند، هستند. این سیستم‌ها هدف نظامی جذاب و شایان توجهی برای حمله‌کنندگان سایبری هستند، زیرا این‌گونه زیرساخت‌های صنعتی که کنترل آنها از طریق سیستم‌ها و شبکه‌های کامپیوتری انجام می‌گیرد، می‌توانند بدون استفاده از سلاح‌های فیزیکی تخریب شوند (Heaton, 2005: 161- 162) . زیرساخت‌های ملی مهم که از چنین

1. Information Systems
2. Infrastructure Control Systems
3. Supervisory Control and Acquisition

حوزه‌های حیاتی همانند نیرو، حمل‌ونقل، ارتباطات و غیره حمایت می‌کنند، به‌طور فزاینده‌ای متکی بر برنامه‌های اینترنتی‌اند. سابقا این‌گونه زیرساخت‌های مهم و حیاتی اغلب به‌طور سنتی و به شکل دستی مدیریت می‌شد، ولی به‌تدریج این روش جای خود را به برنامه‌های ارزان و کارامد اینترنتی داد(Lipson, 2002: 3). امروزه با استفادهٔ کشورها از اینترنت در ادارهٔ زیرساخت‌های حیاتی، ضعف‌های این‌گونه سیستم‌ها و برنامه‌های کامپیوتری نیز مورد توجه حمله‌کنندگان سایبری برای هدف قرار دادن آنها قرار می‌گیرد.

در حال حاضر اغلب کشورها ارائهٔ خدمات اجتماعی را از طریق فضای سایبر آغاز کرده‌اند که کارامدی این روش با توجه به سطح پیشرفت فناوری و دانش کشورها متفاوت است. درجات کارامدی استفاده از این فضا توسط دولت‌ها به در دسترس بودن و اطمینان از در دسترس بودن این فضا توسط شهروندان و دانش کافی کاربران در استفاده از این فضا نیز بستگی دارد (Choucri & Clark, 2011: 24).

با توجه به انواع شبکه‌های کامپیوتری که در بالا به‌طور خلاصه بررسی شد، به همین ترتیب نیز حملات سایبری در دو بخش به‌وقوع می‌پیوندند. بخش اول حملاتی‌اند که اطلاعات موجود در شبکه‌ها و کامپیوترها را تخریب می‌کنند یا از بین می‌برند یا اینکه صرفا مانع دسترسی به آنها برای مدت زمانی مشخص می‌شوند. بخش دوم حملات سایبری حملاتی‌اند که به سیستم‌های کنترل‌کننده آسیب می‌رسانند. برای مثال حملات سایبری که به تأمین‌کننده‌های شبکه‌های برق، خطوط راه‌آهن یا تأمین‌کنندگان آب صورت پذیرد، آثار مخربی در مناطق جغرافیایی خاص با خود به‌همراه خواهد داشت. این‌گونه حملات می‌توانند با استفاده از اینترنت در ارسال برنامه‌های مخرب یا نفوذ به سیستم‌های امنیتی صورت پذیرند (Dogrul *et al.*, 2011: 34). آثار مخرب حملات سایبری بر زیرساخت‌های حیاتی حتی می‌تواند صدمات فیزیکی شدید و عمده‌ای هم با خود به‌همراه داشته باشند. البته هنوز همان‌طورکه تعریف واحدی برای حملات سایبری وجود ندارد، در مورد ارزیابی ماهیت حقوقی این حملات نیز هنوز معیار روشنی نیست (Theohary & Rollins, 2015: 4) و متخصصان امر با توجه به تفاسیر متعددی که از قواعد موجود حقوق بین‌الملل به‌عمل می‌آورند، نظرهای متفاوتی را ارائه می‌کنند.

از مباحثات مذکور این نتیجه حاصل می‌شود که حملات سایبری مفهومی گسترده دارند و با اینکه تعریف مشخص و یکسانی از این حملات ارائه نشده است، در هر حال این حملات می‌توانند از کم‌اهمیت‌ترین تا شدیدترین نوع متغیر باشند که شدیدترین آنها معمولا آثار مخرب فیزیکی بر جای می‌گذارند و با عنوان جنگ سایبری مورد شناسایی قرار می‌گیرند و کم‌اهمیت‌ترین حملات می‌تواند حملات سایبری باشد که دسترسی به اطلاعات و شبکه‌ها را برای مدت زمانی مختل می‌کنند.

انواع حملات سایبری

برای شناخت بیشتر حملات سایبری غیرمخرب، ابتدا باید انواع حملات سایبری را بررسی کنیم. حملات سایبری اغلب سه دسته‌اند که در این قسمت به‌اختصار بررسی می‌شوند:

۱. دستهٔ اول حملات سایبری شامل نشر نرم‌افزارهای مخرب[۱] همانند ویروس‌ها و کرم‌ها و تروجان‌ها می‌شود[۲]؛

۲. دستهٔ دوم حملات سایبری به شکل نفوذ غیرمجاز از راه دور[۳] به سیستم‌ها و شبکه‌هاست. چنین نفوذ غیرمجاز به سیستم‌ها به سرقت اطلاعات محرمانه و اختصاصی، تغییر یا تخریب داده‌ها، کنترل سیستم‌ها و شبکه‌ها و استفادهٔ نامناسب برای راه‌اندازی حملاتی بر روی سیستم‌های دیگر منجر می‌شود؛

۳. دستهٔ سوم از حملات سایبری را حملات محرومیت از سرویس اینترنتی تشکیل می‌دهند که خود به دو دستهٔ محرومیت از سرویس[۴] و محرومیت از سرویس توزیع‌شده[۵] تقسیم می‌شوند. نفی یا محرومیت از سرویس زمانی رخ می‌دهد که حمله‌کنندگان تلاش می‌کنند تا وب‌سایت‌ها، کامپیوترها و شبکه‌ها را از کار بیندازند یا مختل کنند. حملات محرومیت از سرویس از طریق غوطه‌ور ساختن و پر کردن سیستم کامپیوتری هدف حمله با اطلاعات و درخواست‌هایی که موجب توقف عملکرد آن سیستم می‌شود، انجام می‌گیرند. حملات نفی سرویس از جمله عملیات سایبری هستند که مستلزم چندین حمله در طی یک زمان می‌باشند، زیرا هر زمان که حملات متوقف شوند، سیستمی که به آن حمله شده است، به حالت قبل خود باز می‌گردد و بهبود می‌یابد. تیم آمادگی اضطراری کامپیوتر[۶و۷] در آمریکا حملات محروم‌سازی

---

1. Distribution of Malicious Software

۲. ویروس‌ها و کرم‌ها (Viruses and Worms) برنامه‌های کامپیوتری هستند که قطعات مربوط به ذخیره‌سازی اطلاعات یک کامپیوتر یا شبکه را تحت تأثیر قرار می‌دهند که در نتیجه اطلاعات سیستم کاربر را بدون آگاهی وی تکثیر می‌کنند. تروجان (Trojan) برنامه‌ای است که به‌نظر می‌رسد قانونی باشد، اما زمانی‌که اجرا می‌شود، اطلاعات رمز عبور را یافته و آسیب‌پذیری سیستم را برای ورود در آینده بیشتر می‌کند. یک تروجان قابلیت این را دارد که به‌سادگی برنامه‌ها یا اطلاعات داخل هارد دیسک‌ها را از بین ببرد. برای مطالعهٔ بیشتر ر.ک. Kirsch, 2012: 628

3. Unauthorized Remote Intrusions
4. Denial of Service
5. Distributed Denial of Service
6. Computer Emergency Readiness Team (CERT)

۷. در اوایل سال ۲۰۰۰ شبکه‌های دولت فدرال آمریکا حملات سایبری هشداردهنده‌ای را تجربه کرد. در پاسخ به حملات سایبری مذکور کنگرهٔ آمریکا مرکز پاسخ به حوادث کامپیوتری را تأسیس کرد و در سال ۲۰۰۲ با ایجاد وزارت امنیت داخلی، کنگره این مسئولیت را به وزارت جدید واگذار کرد و در سال ۲۰۰۳ نام این مرکز به تیم آمادگی اضطراری کامپیوتر تغییر یافت و مأموریت‌های آن هم گسترده‌تر شدند. برای مطالعهٔ بیشتر ر.ک: https://www.us-cert.gov/about-us

از سرویس را حملاتی تعریف می‌کند که قصدشان جلوگیری کاربران قانونی یک سرویس در استفاده از آن است. به‌دلیل اینکه تمایز بین حجم عظیمی از درخواست‌های قانونی و حملات نفی سرویس مشکل است، بعضی به این نکته اشاره می‌کنند که تحت تعقیب قرار دادن حمله‌کنندگان برای مقامات اجرایی دولت‌ها در این زمینه کار آسانی نیست، زیرا هر دو نوع کاربر در ظاهر شبیه به هم هستند و تنها تفاوت آنها، قصد و هدف آن افراد است. نکتهٔ شایان ذکر دیگر در مورد حملات محروم‌سازی از سرویس، این است که این‌گونه حملات برای اقدام و عملی کردن حملات به منابع زیادی نیاز دارند. یک هکر[1] به‌تنهایی نمی‌تواند تعداد زیادی درخواست از یک صفحه را انجام دهد یا به تعداد کافی نامهٔ الکترونیکی[2] برای از کار انداختن یک سرور[3] ارسال کند، به همین دلیل حملات نفی سرویس اغلب به حملات نفی یا محروم‌سازی از سرویس توزیع‌شده منتهی می‌شوند (Edwards, 2006: 24-25). در حملات نفی سرویس توزیع‌شده، شخص حمله‌کننده همزمان از کامپیوترهای مختلفی حملات را آغاز می‌کند و در نتیجه تهدیدات بیشتری را مطرح می‌کند. در این‌گونه حملات ممکن است هزاران کامپیوتر به‌کار گرفته شوند تا حمله‌ای صورت پذیرد. به همین دلیل دفاع در برابر آنان مشکل است (Kesan & Hayes, 2012: 430- 431). در این‌گونه حملات صرفا سیستم قربانی حملات از کار می‌افتد و حملات نفی سرویس توزیع‌شده به‌هیچ‌وجه اطلاعات را به سرقت نمی‌برند.[4]

بیشترین حملاتی را هم که دولت‌ها با آنها مواجه‌اند، حملات محروم‌سازی از سرویس توزیع‌شده تشکیل می‌دهد. این‌گونه حملات می‌توانند از نظر فیزیکی کاملا غیرمخرب باشند، ولی همچنان برای دولت‌های قربانی این‌گونه حملات مشکلاتی را به‌وجود آورند. حملات سایبری سال ۲۰۰۷ به استونی از جمله حملات محروم‌سازی یا نفی سرویس توزیع‌شده بود که این کشور را با مشکلاتی مواجه کرد. مطابق با نظریات موجود در مورد تطبیق فضای سایبر با قواعد حقوق بین‌الملل موجود، صرفا آن حملات سایبری را می‌توان در قالب توسل به زور و حملهٔ مسلحانه در نظر گرفت که از شدت زیادی برخوردار باشند و آثار آن حملات به صدمات جانی و مالی به اشخاص منتهی شود. سؤالی که همچنان در مورد حملات سایبری باقی می‌ماند، به‌خصوص حملات محروم‌سازی از سرویس غیرمخرب آن است که آیا با توجه به قواعد موجود در حقوق بین‌الملل می‌توان این‌گونه حملات را به‌عنوان نقض تعهدات دولتی که به این‌گونه حملات متوسل می‌شود در نظر گرفت یا خیر. یکی از قواعد عرفی موجود در حقوق بین‌الملل، اصل منع مداخلهٔ دولت‌ها در امور داخلی دولت‌های دیگر است که به‌نظر می‌رسد در

1. Hacker
2. e-mail
3. Server
4. Targeted cyber-attacks, The dangers faced by your corporate network, GFI White Paper, Microsoft Gold Certificate Paper, p. 8, Available at: http://www.gfi.com/whitepapers/cyber-attacks.pdf, Visited on 15 September 2016

حملات سایبری محروم‌سازی یا نفی سرویس توزیع‌شده که غیرمخرب‌انـد، حـداقل اصـل عـدم مداخله در حقوق بین‌الملل نقض می‌شود که در ذیل پس از بررسی کلیات در این زمینـه ابتـدا به بررسی مفهوم این اصل در حقوق بین‌الملل می‌پردازیم و در قسمت بعد حمـلات سـایبری را در قالب این اصل بررسی و تجزیه‌وتحلیل حقوقی می‌کنیم.

نقض اصل ممنوعیت دخالت دولت‌ها در امور داخلی دولت‌های دیگـر و حملات سایبری

همان‌گونه‌که اشاره شد، پیشرفت فناوری موجب ایجاد آرامش و آسایش در جوامع مـی‌شـود. از طرف دیگر موجب به‌وجود آمـدن اشـکال جدیـدی از تخلفـات در ابعـاد داخلـی و بـین‌المللـی می‌شود. از نظر ابعاد بین‌المللی متعاقب به‌وجود آمدن فضای سایبر توسل بـه حمـلات سـایبری ضرورت اقدامی را مطرح می‌کند و آن نظم بخشیدن به وضعیت‌هایی است که دولت‌هـا بـه‌طـور روزافزون با توجه به خصوصیات فضای سایبر با آنها مواجه می‌شوند. امروزه توسـل بـه حمـلات سایبری برای دولت‌ها در رسیدن به مقاصدشان به‌عنوان راه‌حل و جایگزین مناسبی برای توسل به جنگ واقعی درآمده است، زیرا ناشناس ماندن در فضای سایبر، کـم‌هزینـه بـودن، سـرعت و نبود قواعدی که مستقیما این‌گونه حملات را تحت شمول خود قرار دهد و دشوار بـودن اثبـات مسئولیت دولت‌ها در این‌گونه حملات به‌دلیل دشواری در انتساب حملات به دولتی خـاص کـه باز این امر به خصوصیات این فضا که از جملهٔ آنها ناشناس ماندن حمله‌کنندگان سایبری است، بازمی‌گردد، همگی موجب اهمیت این‌گونه حملات در عصر حاضر شـده اسـت. از طـرف دیگـر، وابستگی دولت‌ها به فناوری‌های روز، استفادهٔ دولت‌ها از این فضا بـرای ارتبـاط بـا شـهروندان و رسانیدن خدمات به آنان و همچنین ذخیـرهٔ اطلاعـات حیـاتی و ادارهٔ زیرسـاخت‌هـای حیـاتی دولت‌ها این فضا را به طعمه‌ای مناسب و جذاب برای حملات سایبری تبدیل کرده است.

اگرچه فضای سایبر بعضا در قالب کنوانسیون جـرائم سـایبری بوداپسـت در اروپـا و رویـه و استراتژی ملی مربوط به امنیت سایبری در بسیاری از کشورها تا حدی ساماندهی شده، ولی بـا عنایت به اینکه در مورد حملات سایبری هنوز هیچ‌گونه اجماع بین‌المللی در چارچوب معاهـده حاصل نشده است و با توجه به اینکه هنوز رویه و عرفی هم در این خصوص موجود نیست، باید حملات سایبری را در چارچوب قواعد موجود حقوق بین‌الملل ارزیابی کنیم و به نظم درآوریـم. اصولا در همهٔ موضوعات بیشترین کارایی را قواعدی خواهنـد داشـت کـه در مـورد موضـوعاتی خاص به‌وجود می‌آیند و آنها را به نظم درمی‌آورند، ولی با توجه به اینکه تاکنون دولت‌ها بنـا بـه دلایل گوناگون توافقی بر انعقاد معاهده‌ای که به این موضوع بپـردازد نداشـته‌انـد، تنهـا راه‌حـل موجود توسل به قواعد موجود در حقوق بین‌الملل است.

راه‌حلی که در حقوق بین‌الملل برای به نظم درآوردن این‌گونه حملات وجود دارد، در قالب مباحث مسئولیت بین‌المللی دولت‌ها مورد توجه قرار می‌گیرد. مطابق با مواد ۱ و ۲ پیش‌نویس مواد مربوط به مسئولیت دولت‌ها در اعمال متخلفانهٔ بین‌المللی، برای مسئول شناختن دولت‌ها در عرصهٔ بین‌المللی می‌بایستی رفتاری اعم از فعل یا ترک فعل به موجب حقوق بین‌الملل قابل انتساب به آن دولت باشد و دیگر اینکه رفتار دولت مذکور نقض تعهد بین‌المللی آن دولت تلقی شود. موضوع مقالهٔ حاضر از بحث مسائل مربوط به انتساب خارج است. آنچه در مقالهٔ حاضر بررسی و تبیین می‌شود، بررسی این موضوع است که آیا حملات سایبری غیرمخرب موجب نقض تعهد دولت‌ها در عدم دخالت در امور داخلی دولت‌های دیگر می‌شوند یا خیر.

اصل ممنوعیت مداخلهٔ دولت‌ها در امور داخلی دولت‌های دیگر در حقوق بین‌الملل

اصل عدم مداخلهٔ دولت‌ها در امور داخلی دولت‌های دیگر برگرفته از حاکمیت دولت‌ها و اصل برابری بین آنهاست که تأمین‌کنندهٔ حق تعیین سرنوشت[1] آنهاست (Orford, 2003: 128) . ممنوعیت مداخله، تلفیقی از حق دولت بر حاکمیت، تمامیت ارضی و استقلال سیاسی است (Wood, 2007: 2). با اینکه اصل منع مداخلهٔ دولت‌ها در امور دولت‌های دیگر اهمیت زیادی در حفظ و تحکیم صلح دارد، ولی هیچ مقرره‌ای در منشور ملل متحد به‌طور صریح به آن اشاره نمی‌کند (Watts, 2014: 5). اصل عدم مداخله قسمتی از عرف بین‌المللی است که دیوان بین‌المللی دادگستری در چندین قضیه در آرای خود نیز به آنها اشاره کرده است.[2] این اصل نشأت‌گرفته از حقوق عرفی در بسیاری از معاهدات هم منعکس شده است[3](Wood, 2007: 2) و به مرور اصل عدم مداخله به نماد انحصاری حاکمیت دولت‌ها در عرصهٔ روابط بین‌المللی تبدیل شد (کازرونی، ۱۳۹۳: ۴۰).

در مورد مداخله تعاریف مختلفی ارائه شده است، از جمله اینکه مداخله را دخالت آمرانهٔ کشور یا گروهی از کشورها در امور (خارجی یا داخلی) کشور یا کشورهای دیگر گویند و شامل تهدید یا استفاده از زور با هدف حفظ یا تغییر شرایط موجود است (تقی‌زاده انصاری، ۱۳۹۴: ۲۷۰). برای مداخلهٔ غیرقانونی در واقع دو عنصر مورد نیاز است؛ اول اینکه مداخله‌ای باید از جانب یک دولت در امور داخلی دولت دیگر صورت پذیرفته باشد؛ دوم اینکه مداخلهٔ انجام‌گرفته

1. The Right of Self-Determination
2. Armed Activities in D.R.C. judgment, para. 161-63; Nicaragua judgment, para. 202; Corfu Channel case, p. 35
۳. از جمله این معاهدات منشور سازمان کشورهای آفریقایی، قانون تشکیل‌دهندهٔ اتحادیهٔ آفریقایی‌اند.

باید از جمله موضوعاتی باشد که هر دولت مطابق با اصل حاکمیت مجاز به تصمیم‌گیری آزادانه در آن موارد است. آنچه مداخله قلمداد می‌شود، در هیچ سندی به‌طور مشخص تعیین نشده است (Jamnejad & Wood, 2009: 347). در حقیقت محتوای این اصل مدام در حال تغییر است، ازاین‌رو آنچه را که شامل امور داخلی دولت‌ها می‌شود، باید با توجه به موازین بین‌المللی سنجید (جاوید و محمدی، ۱۳۹۲: ۵۵ و۵۶).

اسناد بین‌المللی متعددی این اصل را مورد توجه قرار می‌دهند؛ از جمله مادهٔ ۸ کنوانسیون مونته ویدئو در خصوص حقوق و وظایف دولت‌ها که بیان می‌دارد: «هیچ دولتی حق دخالت در امور داخلی و خارجی دولت‌های دیگر را ندارد».[1] با وجود این، بیشترین انعکاس اصل عدم مداخله را می‌توان در قالب بند ۴ مادهٔ ۲ منشور ملل متحد در خصوص ممنوعیت توسل به زور یافت. سازمان ملل متحد با هدف برقراری صلح و امنیت بین‌المللی و توسعهٔ روابط دوستانه براساس برابری و احترام به حاکمیت دولت‌ها و رعایت آزادی‌های اساسی تشکیل شد. منشور ملل متحد با تأکید بر اصل حاکمیت که نتیجهٔ منطقی آن رسیدن به اصل عدم مداخله است، شکل گرفت و روابط دولت‌ها را براساس اصل کلیدی ممنوعیت توسل به زور قرار داد (صادقی حقیقی، ۱۳۹۰: ۹۸). البته با تفسیری رسمی از مقررات مربوطه در منشور می‌توان به این نتیجه رسید که دولت‌های عضو ممکن است علیه تمامیت ارضی یا استقلال سیاسی دولت دیگر اقدام کنند که در آن صورت با تهدید به زور یا استفاده از زور تلاقی پیدا می‌کنند. با در نظر گرفتن بند ۴ مادهٔ ۲ منشور در مورد ممنوعیت توسل به زور نیز می‌توان به‌طور غیرمستقیم به اصل منع مداخلهٔ دولت‌ها در امور داخلی دولت‌های دیگر رسید. از طرف دیگر، می‌توان گفت هرچند در منشور ملل متحد صرفا اشکال شدید مداخله همانند توسل به زور یا تهدید به زور مورد توجه قرار گرفته است، ولی حقوق بین‌الملل عرفی به‌طور جداگانه، هم تهدید و توسل به زور را ممنوع اعلام می‌کند و هم اشکال دیگر دخالت را که از اجبار کمتری برخوردارند، موردنظر قرار می‌دهد (Watts, 2014: 6). مادهٔ مذکور نیز به‌عنوان تعهدی معاهده‌ای در مقابل اعضای سازمان ملل در نظر گرفته می‌شود و در عین حال به‌عنوان قاعدهٔ عرفی مستقل تلقی می‌شود (Mattessich, 2016: 877).

اصل عدم مداخلهٔ دولت‌ها در امور داخلی دولت‌های دیگر علاوه‌بر مادهٔ مذکور در بند ۷ مادهٔ ۲ منشور نیز به‌طور غیرمستقیم مورد تأکید قرار گرفته است. این بند مقرر می‌دارد که «هیچ‌یک از مقررات مندرج در این منشور، ملل متحد را مجاز نمی‌دارد در اموری که ذاتا جزو صلاحیت داخلی هر کشوری است دخالت نماید و اعضا را نیز ملزم نمی‌کند که چنین موضوعاتی را تابع مقررات این منشور قرار دهند، لیکن این اصل به اعمال اقدامات قهری

1. Montevideo Convention on the Rights and Duties of States, 1933, Available at: https://www.ilsa.org/jessup/jessup15/Montevideo%20Convention.pdf, Visited on 1 November 2016

پیش‌بینی‌شده در فصل هفتم لطمه وارد نخواهد آورد». تعیین اینکه چه اقداماتی دخالت در امور داخلی دولت‌ها محسوب می‌شود، در این ماده مورد توجه قرار نگرفته است. به‌عبارت دیگر، با توجه به رویکرد موسع منشور، سازمان ملل به‌طور مطلق از مداخله در امور داخلی کشورها فارغ از اینکه این مداخله همراه با اقدامات قهری و نظامی باشد یا بدون آن منع شده است، مگر در مورد اقداماتی که برای حفظ صلح و امنیت بین‌المللی براساس فصل هفتم منشور صورت پذیرد (کمالی‌نژاد، ۱۳۹۱: ۲۴۶).

مطابق با مفاد صریح این بند، سازمان ملل نمی‌تواند در امور داخلی دولت‌ها دخالت کند، ولی بعضی اوقات این بند به‌عنوان بندی که دربرگیرندهٔ اصل کلی منع مداخله[1] است، هم تفسیر می‌شود (Simma & others, 2012: 284). بی‌شک این اصل یک اصل مربوط به حقوق بین‌الملل عرفی محسوب می‌شود، ولی آنچه را که این اصل در برمی‌گیرد، همان‌طورکه اشاره شد، به‌طور کامل مشخص نیست (Wood, 2007: 6). با اینکه حدود و ثغور اصل عدم دخالت دولت‌ها در امور داخلی دولت‌های دیگر مطابق با حقوق بین‌الملل تعیین نشده، لیکن می‌توان این اصل را به‌عنوان اصلی که ممنوعیت دخالت از روی اجبار دولت‌ها را در امور دولت‌های دیگر که تصمیم‌گیری در مورد این امور کاملا تحت اختیار دولت هدف قرار گرفته است، تعریف کرد. تعریف مذکور می‌تواند شامل اشکال مختلفی از اقدامات از روی اجبار شود که رضایت دولت‌های قربانی این‌گونه مداخلات در آن نقشی نداشته است.

اگرچه در طول تاریخ سازمان ملل اغلب به بند ۷ مادهٔ ۲ منشور ملل متحد استناد نشده و حتی بعضا ادعای متروک ماندن و بلااستفاده شدن آن مطرح می‌شود (Simma *et al*., 2012: 282) با وجود این به نظر دبیر کل وقت سازمان ملل که این بند همچنان که در زمان شکل‌گیری سازمان ملل مناسب بوده است، به همین نحو در زمان حاضر هم این خصوصیت خود را حفظ کرده و نقض حاکمیت دولت‌ها همچنان نقض نظم جهانی است.[2] این بند در حقیقت منعکس‌کنندهٔ یکی از اصول اصلی سازمان ملل متحد است که سازمان ملل براساس و مبنای آن تشکیل شده است. در مقدمهٔ منشور سازمان ملل متحد نیز به برابری ملت‌های کوچک و بزرگ اشاره شده است که باز می‌توان این موضوع را تأکیدی بر ممنوعیت مداخلهٔ دولت‌ها در امور داخلی دیگر کشورها دانست و همین‌طور دولت‌های بزرگ و قدرتمند نباید در امور دولت‌های حتی ضعیف‌تر دخالت کنند. کنوانسیون‌های سال‌های ۱۹۶۹[3] و ۱۹۸۶[4] وین در

1. General Principle of Non-Intervention
2. Press Release, SG/SM/6613, Secretary-General Reflects on "Intervention" in Thirty-Fifth Annual Ditchley Foundation Lecture, 26 June 1998, Available at: http://www.un.org/press/en/1998/19980626.sgsm6613.html , Visited on August 2016
3. Vienna Convention on the law of treaties
4. Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations

خصوص حقوق معاهدات هم در مقدمهٔ خود به اصل ممنوعیت مداخله در امور داخلی دولت‌های دیگر اشاره می‌کنند.

اعلامیهٔ مجمع عمومی سازمان ملل در مورد اصول حقوق بین‌الملل حاکم بر روابط دوستانه و همکاری میان دولت‌ها مطابق با منشور ملل متحد نیز به‌کرات در متن خود به وظیفهٔ دولت‌ها در عدم مداخله در امور داخلی دولت‌های دیگر اشاره کرده است.[1] از جمله در بخشی از اعلامیهٔ مذکور به وظیفهٔ دولت‌ها به خودداری از اجبار نظامی، سیاسی و اقتصادی یا هر نوع دیگری از اجبار که علیه استقلال سیاسی یا تمامیت ارضی هر دولتی پرداخته و مداخله را مغایر با جوهرهٔ منشور و ایجادکنندهٔ وضعیت‌هایی می‌داند که می‌تواند صلح و امنیت را به خطر بیندازد. در حقیقت می‌توان گفت ماهیت مداخله اجبار است. این موضوع در اعلامیهٔ مذکور نیز مورد تأکید قرار گرفته است. قسمت دیگری از اعلامیهٔ مذکور بیان می‌دارد که «هیچ دولتی نمی‌تواند به‌منظور به‌دست آوردن تبعیت سایر دولت‌ها از اعمال حقوق مربوط به حاکمیتش برای به‌دست آوردن هر گونه مزایا از اقدامات اقتصادی، سیاسی یا هر اقدام دیگری برای اجبار دولت دیگر استفاده کند و یا توسل به آن اقدامات را برای به‌دست آوردن تبعیت از اعمال حقوق مربوط به حاکمیتش و به‌دست آوردن هر گونه مزایا سوق دهد».

اعلامیهٔ مجمع عمومی سازمان ملل متحد در مورد عدم پذیرش مداخله در امور داخلی دولت‌ها[2] به سال ۱۹۸۱ نیز بر ممنوعیت مذکور تأکید کرده است.[3] در فصل یک منشور حقوق اقتصادی و وظایف دولت‌ها نیز از اصل عدم مداخله به‌عنوان یکی از اصولی که باید در روابط اقتصادی و همین‌طور سیاسی و دیگر روابط بین دولت‌ها حاکم باشد، نام برده شده است.[4] در حقیقت اسناد بین‌المللی که موضوع عدم مداخله را مطرح می‌کنند، هم به مداخلاتی اشاره دارند که با استفاده از توسل به زور صورت می‌پذیرند و هم مداخلاتی را در نظر می‌گیرند که با تحمیل و بدون توسل به زور انجام می‌گیرند (Mattessich, 2016: 880). دیوان بین‌المللی دادگستری نیز به سهم خود مداخلات ممنوعه در امور داخلی دولت‌ها در قضیهٔ نیکاراگوئه را به‌عنوان «موضوعاتی که هر دولت مجاز است که مطابق با اصل حاکمیت دولت‌ها به‌طور آزادانه در موردش تصمیم‌گیری کند» در نظر گرفته است. دیوان در ادامه بیان می‌کند درصورتی‌که در مداخله از روش‌های تحمیل در خصوص چنین انتخاب‌هایی که می‌بایستی به‌طور آزادانه باقی بمانند استفاده شود، این‌گونه مداخلات غیرقانونی تلقی می‌شوند. دیوان در قضیهٔ مذکور توسل به زور را به‌عنوان نمونه‌ای بارز از مداخلات غیرقانونی

1. Declaration on Principles of International Law Concerning Friendly Relations among States in accordance with Charter of the United Nations, A/RES/25/2625, 24 October 1970
2. Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States
3. A/RES/36/103, 9 December 1981
4. Charter of Economic Rights and Duties of States, A/RES/29/3281, 12 December 1974

تلقی می‌کند (Nicaragua V. United States of America, 1986: para 205). بنابراین با آنکه قواعد عرفی حقوق بین‌الملل در خصوص مداخله تا حد زیادی در کنار ممنوعیت کلی‌تر استفاده از زور در نظر گرفته می‌شوند، ولی هنوز مداخلهٔ مفهومی مجزایی دارد. به عقیدهٔ بعضی حقوقدانان هیچ ابهامی در مورد اینکه اصل عدم مداخله یک اصل مستقل عرفی است، وجود ندارد (Buchan, 2012: 221). البته بعضی حقوقدانان برای این اصل ماهیت آمره در نظر می‌گیرند. برای مثال در قضیهٔ نیکاراگوئه در دیوان بین‌المللی دادگستری، قاضی سیت کامارا[1] در نظریهٔ جداگانهٔ خود بیان کرد درصورتی‌که معیار مندرج در مادهٔ ۵۳ کنوانسیون وین[2] در خصوص معاهدات را به‌کار گیریم، اصل عدم مداخله به‌عنوان قاعده‌ای آمره تلقی می‌شود. از نظر وی درصورتی‌که معاهده‌ای متضمن مقرراتی باشد که دولت‌ها به‌طور مستقیم و غیرمستقیم در مورد مداخله در امور داخلی دولت‌های دیگر موافقت کنند، این موضوع بی‌شک داخل در مادهٔ ۵۳ کنوانسیون مذکور قرار می‌گیرد و باید به‌دلیل اینکه با قواعد آمرهٔ حقوق بین‌الملل در تعارض است، باطل و بلااثر تلقی شود.[3] البته به‌نظر می‌رسد با اینکه موضوع ممنوعیت عدم مداخلهٔ دولت‌ها در امور داخلی دولت‌های دیگر اهمیت بسیاری دارد، ولی حداقل در حال حاضر نمی‌توان مدعی آمره بودن این قاعده شد و آن را در زمرهٔ قواعد آمرهٔ حقوق بین‌الملل تلقی کرد.

دولت‌ها هم به‌طور منظم در اظهارات حقوقی، دادخواست‌ها و لوایح خود در دیوان‌های بین‌المللی، به اصل منع مداخله استناد می‌کنند. محققان حقوق بین‌الملل نیز به مدت طولانی است که اصل منع مداخله را به‌عنوان نمادی از اصول حاکمیت و برابری دولت‌ها در نظر گرفته‌اند (Watts, 2014: 2- 3).

لغت مداخله در معنای موسع و همچنین در معنای مضیق آن تفسیر شده است. پیش‌نویسان منشور ملل متحد مداخله را به معنای وسیعی در نظر گرفته بودند، به‌نحوی که حتی شامل توصیه‌ها و پیشنهادهای مربوط به مسائل داخلی دولت‌ها نیز می‌شد. به‌نظر می‌رسد قصد دولت‌ها از در نظر گرفتن چنین مفهوم موسعی از مداخله، حصول اطمینان از این موضوع بوده است که سازمان ملل فراتر از اختیارات خود به‌خصوص در مورد موضوعات اقتصادی، اجتماعی و فرهنگی دولت‌های عضو دخالت نکند. در مقابل، مطابق با حقوق بین‌الملل کلاسیک واژهٔ «مداخله» به

---

1. Judge Sette-Camara

۲. مطابق با مادهٔ ۵۳ کنوانسیون وین، معاهدات متعارض با قاعدهٔ آمرهٔ حقوق بین‌الملل عام در زمان انعقاد باطل هستند. معیاری که مادهٔ مذکور برآمره بودن قاعده در نظر می‌گیرد، قاعده‌ای است که به‌وسیلهٔ اجماع جامعهٔ بین‌المللی کشورها به‌عنوان قاعده‌ای تخلف‌ناپذیر که تنها توسط یک قاعدهٔ بعدی حقوق بین‌الملل عام با همان ویژگی قابل تعدیل است، پذیرفته و به رسمیت شناخته شده است.

3. Separate Opinion of Judge Sette-Camara, pp. 199, 200, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)

معنی مداخلهٔ دیکتاتورانه[1] تعریف شده است، یعنی در صورتی عملی مداخله تلقی می‌شود که توسل به زور یا فشاری آمرانه[2] در آن وجود داشته باشد (Simma *et al*., 2012: 285).

در حقیقت اصل عدم مداخله در امور داخلی دولت‌های دیگر نه‌تنها در مورد اقداماتی که به‌صورت مستقیم و غیرمستقیم از زور استفاده می‌شوند قابلیت اعمال دارد، بلکه در مورد اقدامات دیگری هم که تابع ارادهٔ مطلق دولت‌هاست، در شرایطی قابل اعمال است (Mattessich, 2016: 880). در قسمت بعد به این موضوع می‌پردازیم که آیا حملات سایبری از نوع محروم‌سازی از سرویس توزیع‌شدهٔ غیرمخرب که دولت‌ها بیشتر با آن مواجه‌اند، می‌تواند ناقض اصل منع مداخله در حقوق بین‌الملل تلقی شود؟

حملات سایبری به‌عنوان ناقض اصل ممنوعیت مداخلهٔ دولت‌ها در امور داخلی دولت‌های دیگر

با بررسی سوابق حملات سایبری که دولت‌ها به‌خصوص طی چند سال اخیر با آن مواجه شده‌اند، به این نتیجه می‌رسیم که حملات سایبری همیشه از شدت زیادی برخوردار نیستند و آثار و آسیب‌های زیادی از خود به‌جا نمی‌گذارند. برعکس بیشترین تعداد حملات سایبری، حملاتی‌اند که از شدت پایینی برخوردارند. این‌گونه حملات نه‌تنها در چارچوب حملهٔ مسلحانه قرار نمی‌گیرند، بلکه از موارد توسل به زور هم به‌شمار نمی‌روند. سؤالی که در چنین وضعیت‌هایی باید بررسی شود و پاسخ مناسب به آن داده شود، این است که درصورتی‌که بخواهیم دولتی را مسئول این‌گونه حملات بدانیم، چنین حملاتی چه تعهدی از تعهدات دولت‌ها را نقض می‌کنند؟ همان‌طورکه اشاره شد، با توجه به اینکه مقررات مستقیمی در مورد نظم‌دهی به حملات سایبری وجود ندارد، باید حملات سایبری را در قالب مقررات موجود حقوق بین‌الملل به نظم درآوریم و بررسی و ارزیابی کنیم. از جمله تعهداتی که دولت‌ها می‌توانند در مورد حملات سایبری به‌خصوص حملات سایبری با شدت کمتر نقض کنند، اصل ممنوعیت مداخله در امور داخلی دولت‌های دیگر است.

همان‌طور که ذکر شد، حملات سایبری با شدت کمتر به تعداد بیشتری از حملات با شدت زیاد رخ می‌دهند، به همین دلیل وضعیت حقوقی این حملات باید مورد توجه بیشتری قرار گیرد. سؤالی که در مورد این‌گونه حملات سایبری مطرح می‌شود این است که آیا آنها اصل عدم مداخلهٔ دولت‌ها در امور داخلی دولت‌های دیگر را نقض می‌کنند؟

در ادبیات حقوق بین‌الملل در مورد فضای سایبر و حملات سایبری متأسفانه به مباحث

1. Dictatorial Interference
2. Imperative Pressure

مربوط به ممنوعیت مداخله در امور داخلی کشورها و حملات سایبری کمتر پرداخته شده است. شاید دلیل این موضوع به مفهوم سنتی حاکمیت بازمی‌گردد. بدین شرح که اغلب دولت‌ها حاکمیت را به معنا و مفهوم حاکمیت سرزمینی به‌طور فیزیکی تلقی می‌کرده‌اند. این موضوع در حالی است که فضای سایبر اغلب به قلمرویی مجازی تلقی می‌شود که دولت‌ها نمی‌توانند کنترل حاکمیتی خود را اعمال کنند (Buchan, 2012: 221). البته دولت‌ها به‌طور مداوم بر حق خود بر اعمال کنترل بر زیرساخت‌های سایبری واقع در سرزمینشان و محافظت از آنها در قبال هر گونه مداخلهٔ دولت‌ها یا اشخاص خارجی تأکید می‌کنند (Heinegg, 2012: 10).

با وجود این به‌نظر می‌رسد حاکمیت دولت‌ها دیگر صرفا محدود به قلمرو فیزیکی آنها نمی‌شود و مفهوم حاکمیت فراتر از مفهوم سنتی حاکمیت ارضی است.[۱] مفاهیمی که در مورد حاکمیت به‌طور سنتی شکل گرفته است به زمانی قبل از به‌وجود آمدن فضای سایبر بازمی‌گردد. همان‌طور که قوانین با پیشرفت فناوری باید تغییر کنند و تکمیل شوند، مفاهیم موجود در حقوق داخلی و حقوق بین‌الملل نیز می‌بایستی به همین ترتیب تغییر کنند، به‌نحوی که پاسخگوی تغییرات امروزی هم باشند. در فضای سایبر اصل حاکمیت به دولت حق تنظیم و کنترل فعالیت‌های سایبری و زیرساخت‌های داخل سرزمینش را می‌دهد. حاکمیت سرزمینی دولت در واقع از زیرساخت‌های سایبری واقع در سرزمین آن دولت فارغ از اینکه دولت موردنظر چه ویژگی‌هایی دارد، حمایت می‌کند (Schmitt, 2014: 704- 705).

در موضوع حملات سایبری هم به‌نظر می‌رسد برخی از این‌گونه حملات اصل عدم مداخلهٔ دولت‌ها در امور داخلی یکدیگر را نقض می‌کنند و در صورتی هم که حملات قابلیت انتساب[۲] به دولتی خاص را داشته باشند، مسئولیت بین‌المللی دولت حمله‌کننده متصور خواهد بود. از اعلامیهٔ سال ۱۹۸۱ مجمع عمومی سازمان ملل در مورد ممنوعیت مداخله در امور داخلی

---

۱. برای دیدن نظر موافق ر.ک. Buchan, 2012: 223

۲. با این توضیح که دولت‌ها معمولا به‌طور آشکار اقدام به انجام حملات سایبری علیه دولت‌های دیگر نمی‌کنند، بلکه سعی می‌کنند هویت خود را پشت ابزارها و عوامل تکنیکی که با توجه به ماهیت فضای سایبر به‌راحتی امکان‌پذیر است، مخفی کنند. مضافا اینکه دولت‌ها سعی دارند از بازیگران غیردولتی برای این‌گونه حملات استفاده کنند تا بتوانند بحث انتساب را در مورد این‌گونه حملات به چالش بکشند و این موضوع را بسیار دشوار سازند. به‌عبارت دیگر، دولت‌ها به دو شکل سبب به‌وجود آمدن موانع و دشواری‌هایی در خصوص به چالش کشیده شدن مسئولیت خود در قبال حملات سایبری می‌شوند؛ اول اینکه تا جایی که ممکن است با عوامل تکنیکی و انتخاب نوع حملهٔ سایبری سعی بر استتار هر گونه رد پا از خود کرده و در ثانی در صورتی هم که دولتی موفق به ردیابی آن حملات سایبری شود، چون معمولا دولت‌ها برای این‌گونه حملات خود مستقیما اقدام نمی‌کنند، چالش دیگری که دولت قربانی با آن مواجه می‌شود. بحث ارتباط آن بازیگران غیردولتی با دولتی است که در پشت پرده تمامی حملات را اداره کرده و دستور آنها را صادر کرده است که البته از موضوع بحث مقالهٔ حاضر خارج است.

دولت‌ها می‌توان چنین برداشت کرد که حملات سایبری نیز می‌تواند در شمول اعلامیهٔ مذکور قرار گیرد. اعلامیهٔ مذکور حق دولت‌ها بر دسترسی آزاد به اطلاعات، ترقی کامل بدون دخالت در سیستم اطلاعاتی و رسانه‌های جمعی، استفاده از رسانه‌های اطلاعاتی‌شان به‌منظور ترویج منافع و آرمان‌های سیاسی، اجتماعی و فرهنگی‌شان، از جمله مواد مربوط به اعلامیهٔ جهانی حقوق بشر و اصول نظم اطلاعاتی بین‌المللی جدید را مورد تأکید و توجه قرار داده است.[۱] همان‌طورکه ملاحظه می‌شود، اگرچه در زمان اعلامیهٔ مذکور فضای سایبر به‌وجود نیامده بود، ولی متن اعلامیه حکایت از هر گونه ممنوعیت دخالت در مختل کردن سیستم‌های اطلاعاتی کشورها دارد. بنابراین با توجه به اعلامیهٔ مذکور حملات سایبری نیز می‌توانند مختل‌کنندهٔ سیستم‌های اطلاعاتی کشورها و موجب عدم دسترسی آنها به اطلاعات شوند. به‌علاوه مطابق با همان اعلامیه وظیفهٔ دولت‌ها در پرهیز از هر گونه مبارزات انتخاباتی توهین‌آمیز و تبلیغات خصمانه به‌منظور مداخله در امور داخلی دولت‌های دیگر مورد تأکید قرار گرفته است.[۲] ازاین‌رو با توجه به حملات سایبری اخیری که در انتخابات آمریکا رخ داد، در صورت انتساب آن حملات به کشور روسیه، حملات سایبری در انتخابات ریاست جمهوری آمریکا را می‌توان به‌منزلهٔ دخالت در امور داخلی دولت آمریکا تلقی کرد. به گفتهٔ مقامات اطلاعاتی آمریکا، هکرهای روسی تلاش‌های مکرری را قبل از انتخابات آمریکا در سال ۲۰۱۶ به‌منظور ورود به مؤسسات بزرگ آمریکایی از جمله کاخ سفید و وزارت امور خارجهٔ آمریکا انجام دادند. حملات سایبری صورت‌پذیرفته حملات ساده‌ای بودند. این حملات شامل ارسال ایمیل‌هایی از صفحات جعلی[۳] بودند، با این قصد که افراد وارد صفحات مذکور شوند و مجددا اطلاعات شخصی خود را وارد آن کنند تا هکرها و حمله‌کنندگان سایبری بتوانند به آنها دسترسی یابند. متخصصان امنیت آمریکا بر این عقیده بودند که دو گروه مرتبط با کرملین پشت این حملات بوده‌اند[۴] و دولت روسیه هزاران ایمیل محرمانه را که طی انجام این حملات از کمیتهٔ ملی حزب دموکرات[۵] به سرقت برده شده بود، به ویکی لیکس[۶] داده است. البته مؤسس ویکی لیکس اعلام کرد که

1. A/RES/36/103, 9 December 1981, Section 1, Para C
2. A/RES/36/103, 9 December 1981, Section 2, Para J

۳. صفحات جعلی به‌طور تخصصی با عنوان Phishing مورد خطاب قرار می‌گیرند. نامه‌های الکترونیکی صفحات جعلی نامه‌های الکترونیکی‌اند که کاربر را به سمت بازدید از یک وب‌سایت هدایت می‌کند که طی آن از کاربر تقاضا می‌شود اطلاعات شخصی خود را مجدد وارد کند، درصورتی‌که اطلاعات قبلا در سازمان یا نهاد قانونی مربوطه موجود است. برای مطالعهٔ بیشتر ر.ک. استالینگز، ۱۳۹۳: ۳۳۴.

4. What we know about Russia's interference in the US election, Available at: https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election , Visited on 5 January 2017
5. Democratic National Committee (DNC)

۶. ویکی لیکس (WikiLeaks) یک سازمان رسانه‌ای چندملیتی است که در سال ۲۰۰۶ تأسیس شد. ویکی لیکس کتابخانه‌ای بزرگ از اسناد است که به گفتهٔ متصدیان این سازمان اسناد و مدارک تجزیه‌و تحلیل و منتشر

روسیه در این قضایا نقشی نداشته است.[۱] روسیه نیز هر گونه دخالت از طریق حملات سایبری را نفی کرد.[۲] مطابق با ارزیابی‌های انجام‌گرفتهٔ متخصصان آمریکایی، هدف روسیه اقدام به نفع یکی از نامزدهای انتخاباتی آمریکا یعنی یاری رساندن به ترامپ برای پیروزی در انتخابات بود. ایمیل‌های مورد بحث به‌طور پیوسته چند ماه قبل از انتخابات به بیرون درز پیدا کرد که در آنها کلینتون مورد هدف و انتقاد واقع شده بود.[۳] متعاقبا اوباما از خط تلفن قرمز[۴] برای تماس با ولادیمیر پورتین استفاده کرد و اهمیت حملات سایبری را گوشزد کرد. سازمان‌های اطلاعاتی آمریکا یقین داشتند که روسیه به نفع ترامپ در انتخابات ریاست جمهوری آمریکا عمل کرده و شخص پوتین کنترل‌کنندهٔ حملات بوده است. از محتوای مکالمهٔ اوباما با پوتین اطلاعات زیادی در دست نیست، ولی اوباما در کنفرانسی خبری این مکالمه را مکالمه‌ای موفقیت‌آمیز خواند و تأکید کرد که طی تماس مذکور به روسیه هشدار داده که در صورت عدم توقف حملات، این اقدامات عواقب جدی در پی خواهند داشت.[۵]

قاعدهٔ ۱۰ راهنمای تالین حملات سایبری را که به سطح توسل به زور نمی‌رسند نیز مطابق با حقوق بین‌الملل الزاما قانونی نمی‌شناسد. راهنمای مذکور بیان می‌دارد که یک حملهٔ سایبری می‌تواند به نقض ممنوعیت مداخله منجر شود. راهنمای تالین با اینکه اذعان می‌دارد که منشور ملل متحد به‌طور صریح اصل ممنوعیت مداخله را مورد توجه قرار نمی‌دهد، ولی اصل مذکور تلویحا در بند ۱ مادهٔ ۲ منشور ملل متحد در قالب اصل برابری دولت‌ها آورده شده است. سپس راهنمای مذکور به اعلامیه‌ها، معاهدات و رأی مشورتی دیوان بین‌المللی دادگستری اشاره می‌کند و در ادامه بیان می‌دارد که این اصل به‌عنوان قسمتی از حقوق بین‌الملل عرفی درآمده است.

می‌شوند. برای مطالعهٔ بیشتر ر.ک.

What is WikiLeaks, Available at: https://wikileaks.org/What-is-Wikileaks.html , Visited on 5 January 2017

1. WikiLeaks' Assange Denies Russia Behind Podesta Hack. Available at: http://www.politico.com/story/2016/11/julian-assange-russia-john-podesta-wikileaks-230676, Visited on 12 January 2017
2. Moscow Denies Russian Involvement in us dnc Hacking, Available at: http://www.reuters.com/article/us-usa-election-hack-russia-idUSKCN0Z02EK, Visited on 15 January 2017
3. CIA concludes Russia interfered to help Trump win election, say reports, Available at: https://www.theguardian.com/us-news/2016/dec/10/cia-concludes-russia-interfered-to-help-trump-win-election-report., Visited on 5 January 2017

۴. خط تلفن قرمز (Red Telephone Line) خط اختصاصی بین مسکو و واشنگتن است. این سیستم ارتباط مستقیمی را بین سران دولت آمریکا با فدراسیون روسیه برقرار می‌کند. این خط اختصاصی در سال ۱۹۶۳ بین پنتاگن و کرملین به‌وجود آمد. برای مطالعهٔ بیشتر ر. ک.

Hotline Established Between Washington and Moscow, Available at: http://www.history.com/this-day-in-history/hotline-established-between-washington-and-moscow , Visited on 15 January 2017

5. What Obama Said to Putin on the Red Phone about the Election Hack, Available at: http://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116 , Visited on 15 January 2017

راهنمای تالین با اشاره به قضیهٔ نیکاراگوئه در دیوان بین‌المللی دادگستری که مداخلهٔ اجبارکننده را غیرقانونی تلقی می‌کند، بر این عقیده است که مداخله‌ای ساده به‌عنوان نقض اصل ممنوعیت مداخله تلقی نمی‌شود. مطابق با راهنمای تالین تشخیص اینکه اجباری در مداخله وجود داشته است یا خیر، به شرایط و اوضاع و احوال هر حملهٔ سایبری بستگی دارد. راهنمای تالین به‌عنوان نمونه ویروس استاکسنت را که به توسل به زور منجر می‌شود، به‌وضوح نقض اصل عدم مداخله نیز تلقی می‌کند، ولی راهنمای مذکور بررسی حملات سایبری را که پایین‌تر از حد توسل به زور هستند، در چارچوب اصل عدم مداخله دشوار می‌داند (Tallinn Manual, 2013: 44- 45).

مطابق با حقوق بین‌الملل حاضر، حملات محروم‌سازی از سرویس توزیع‌شده غیرمخرب که بیشترین نوع حملات سایبری را در حال حاضر در برمی‌گیرند، به‌شرطی که آن حملات خشونت‌آمیز نباشند و به خسارت منتهی نشوند، مطابق با مقررات حقوق بین‌الملل در مورد توسل به زور مجاز شمرده می‌شوند. استناد به ممنوعیت توسل به زور یا تهدید به استفاده از زور در خصوص این‌گونه حملات که آثار فیزیکی فوری از خود به‌جا نمی‌گذارند، به‌عنوان نقض حقوق بین‌الملل کافی و امکان‌پذیر نیست. لیکن در مورد این‌گونه حملات توسل به اصل عدم مداخلهٔ دولت‌ها در امور دولت‌های دیگر می‌تواند برای به نظم درآوردن آن حملات راهگشا باشد. این‌گونه حملات می‌توانند تخریب گستردهٔ سیستم ارتباطاتی و کارکرد شبکه‌های دیجیتالی را ایجاد کنند که می‌تواند نقض حقوق بین‌الملل محسوب شود (Mattessich, 2016: 890) و می‌توان آن را در زمرهٔ دخالت در امور داخلی دولت‌های دیگر تلقی کرد. در نتیجه حتی درصورتی‌که حملات سایبری به سطح توسل به زور که مطابق با بند ۴ مادهٔ ۲ منشور ممنوع اعلام‌شده است نرسند، با این وجود این‌گونه حملات می‌توانند همچنان در مغایرت با منشور ملل متحد باشند (Gervais, 2012: 536).

این موضوع نیز کاملا واضح است که تمام نقض‌های مربوط به تمامیت ارضی و حاکمیت دولت‌ها بلافاصله مربوط به اصل عدم مداخله نمی‌شوند. مداخله شامل تلاش دولت‌ها با اجبار برای اثر گذاشتن و رسیدن به هدفی خاص در برابر دولت قربانی است. به‌نظر می‌رسد این موضوع در فضای سایبر نیز کاربرد داشته باشد. در چارچوب فضای سایبر به‌طور یقین صرف نفوذ به شبکه‌های دولت‌های دیگر به نقض حاکمیت آن دولت منجر می‌شود، ولی بدون وجود مدرک و شواهدی که نشان دهد تلاش برای به‌دست آوردن اطلاعات با اجبار موجب نتیجه یا عملکردی خاص از دولت قربانی شده است، آن نفوذ و حمله را نمی‌توان مداخله تلقی کرد. ولی درصورتی‌که حملهٔ سایبری با قصد کمک به جنبش مخالفان با قصد و هدف تأثیر گذاشتن بر مسائل سیاسی دولت قربانی صورت پذیرد، آن حمله را هم می‌توان مداخله دانست (Watts, 2014: 8). رویکرد مذکور در تعریف ارائه‌شده از حملات سایبری در سازمان همکاری شانگهای نیز وجود دارد. سازمان ذکرشده با توسل به تعریفی موسع، حملات

سایبری را هر گونه استفاده از فناوری سایبری با قصد تضعیف سیاسی دولت در نظر می‌گیرد (Hathaway & Crootof, 2012: 865) .

معنای نقض اصل عدم مداخله در حملات سایبری در صورتی است که آن حملات اجبارکننده باشند. برای اینکه حملات سایبری اصل عدم مداخله را نقض کنند، این حملات باید با حق دولت‌ها در انجام امور داخلی و خارجی‌شان در تعارض باشند. اصل عدم مداخله تا حدی به ممنوعیت توسل به زور شباهت دارد، با این تفاوت که نقض اصل عدم مداخله شامل اعمالی که شدت کمتری دارند و به آستانهٔ توسل به زور هم نمی‌رسند، می‌شود (Kilovaty, 2014: 107)، یعنی اگر حمله‌ای سایبری را نتوان مصداقی از توسل به زور در نظر گرفت، ولی حملهٔ مذکور می‌تواند اصل ممنوعیت مداخله را نقض کند (خلیل‌زاده، ۱۳۹۳: ۵۸). با این تفاسیر همهٔ حملات سایبری در زمرهٔ ناقضان اصل عدم مداخله قرار نمی‌گیرند، زیرا همهٔ حملات سایبری اجبارکننده نیستند. برای مثال جاسوسی سایبری به‌دلیل اینکه انتخاب‌های آزادانهٔ دولت را در زمینه‌ای سیاسی، اقتصادی، اجتماعی یا فرهنگی خود اجبار نمی‌کند، بنابراین مداخله محسوب نمی‌شود (Kilovaty, 2014: 10). طیفی که اجبار را در حملات سایبری در برمی‌گیرد، می‌تواند از کمترین آن که نقض حاکمیت است تا شدیدترین آن که حمله‌ای مسلحانه است، در تغییر باشد. در حقیقت توسل به زور و مداخله، حد وسط بین نقض حاکمیت و حملهٔ مسلحانه‌اند. همانند دنیای فیزیکی، ارزیابی قانونی بودن عملیات سایبری که اجبارکننده یا تحمیلی‌اند، ولی شدت آنها کمتر از حد توسل به زور هستند و مطابق با اصل منع مداخله قانونی نیستند امکان‌پذیر است، ولی معمولا ارزیابی قانونی بودن یا نبودن این‌گونه حملات با دشواری صورت می‌پذیرد (Lotrionte, 2015: 501- 502). در واقع حقوق بین‌الملل عرفی دو نوع از اقدامات دولت‌ها را ناقض اصل عدم مداخله تلقی می‌کند. نوع اول اقداماتی هستند که توسل به زور محسوب می‌شوند و نوع دوم هم به‌کارگیری اقداماتی که توسل به زور نیستند، ولی مداخله از روی اجبار محسوب می‌شوند (Stockburger, 2016: 567). در هر حال برای نقض اصل عدم مداخله نیز باید صدمه‌ای به دولت وارد شده باشد، ولی صدمهٔ مذکور به‌طور یقین صدمه‌ای همانند صدمات حملات مسلحانه نیست. در عین حال مداخله می‌تواند اقداماتی باشد که با اینکه غیرقانونی‌اند، ولی شدت آن برای رسیدن به توسل به زور کافی نیست. به‌عبارت دیگر، می‌توان گفت همهٔ اقداماتی که به توسل به زور منتهی می‌شوند، مداخله محسوب می‌شوند، ولی همهٔ مداخلات الزاما توسل به زور نیستند و می‌توانند درجاتی پایین‌تر از توسل به زور را داشته باشند. دربارهٔ اینکه آن اقدامات چه خصوصیاتی می‌تواند داشته باشد تا به‌عنوان مداخله تلقی شود، می‌توان از معیار مقیاس و اثرات[1] استفاده کرد. با این شرح که عوامل متعددی در اینکه بتوانیم اقدامی را مداخله تلقی کنیم، دخیل‌اند. اینکه ماهیت منافع

1. Scale and Effects

دولتی که متأثر از حملات بوده چیست و دیگر اینکه میزان تأثیراتی که اقدام سایبری بر روی دولت قربانی گذاشته و تعداد افرادی را که حملهٔ مذکور درگیر خود کرده است به چه میزان بوده است، می‌تواند برای تشخیص مداخله بودن یا نبودن اقدامات سایبری یاری رساند (Lotriionte, 2015: 505- 506). البته شایان ذکر است که هر حملهٔ سایبری را باید با توجه به خصوصیات، شرایط وقوع و تأثیراتی که بر جا می‌گذارد، در قالب اصل ممنوعیت مداخله مورد توجه و ارزیابی قرار داد.

واضح است اصل عدم مداخله که به‌عنوان قاعدهٔ عرفی پذیرفته شده، حتی به اقدامات دولت‌ها در فضای سایبر نیز تعمیم‌پذیر است. در حقیقت فضای سایبر فرصت‌هایی را برای مداخلهٔ بیشتر دولت‌ها در امور دولت‌های دیگر فراهم آورده است، ولی ماهیت این فضا موجب به‌وجود آمدن بهانه‌ای برای نقض اصل عدم مداخله نخواهد شد (Watts, 2014: 5). مطابق با حقوق بین‌الملل حملات محروم‌سازی از سرویس توزیع‌شدهٔ غیرمخرب درصورتی‌که با اجبار همراه شوند، غیرقانونی شناخته می‌شوند. در حقیقت حملات محروم‌سازی از سرویس توزیع‌شده که سبب تخریب فراگیر ارتباطات و عملکردهای دیجیتالی شود، حقوق بین‌الملل را نقض می‌کند. اجبار می‌تواند در امور اقتصادی[1] یا سیاسی وجود داشته باشد، حتی درصورتی‌که اجبار هیچ خسارت فیزیکی از خود به‌جا نگذارد. حملات محروم‌سازی از سرویس توزیع‌شده نیز می‌توانند تأثیرات گسترده در توانایی شهروندان دولت در برقراری ارتباط و همین‌طور ممانعت از دسترسی به اطلاعاتی خاص در مدت زمان خاص داشته باشند. این نوع از صدمات مشابه صدماتی هستند که از اجبار اقتصادی ناشی می‌شود. تنها تفاوتی که این دو موضوع می‌توانند داشته باشند این است که حملات محروم‌سازی از سرویس توزیع‌شده به‌عنوان نقض اصل منع مداخله قوی‌تر از فشار اقتصادی است، زیرا در حملات محروم‌سازی از سرویس توزیع‌شده قصد حمله‌کننده کاملا مشخص است، درصورتی‌که در مورد اجبار اقتصادی ممکن است مقاصد قانونی[2] مطرح باشد (Mattessich, 2016: 890-892)، درصورتی‌که بخواهیم حملات سایبری را که در قالب نقض اصل عدم مداخله با خصوصیت اجبار بررسی کنیم، می‌توانیم برای نمونه به حملات سایبری به استونی در سال ۲۰۰۷ اشاره کنیم. در آوریل ۲۰۰۷ مجموعه‌ای از حملات

---

۱. بین اجبار اقتصادی و حملات محروم‌سازی از سرویس توزیع‌شده نیز شباهت وجود دارد، با این توضیح که هر دو می‌توانند مخرب باشند، ولی در عین حال خسارات فیزیکی مستقیمی را در بر نداشته باشند. تأثیرات حملات محروم‌سازی از سرویس توزیع‌شده با اجبار و فشار اقتصادی هم شباهت دارند. خسارات در این‌گونه حملات به دولت قربانی ناشی از ناتوانی کاربران قانونی در دسترسی به منابع دیجیتالی است که خود می‌تواند سلامت اقتصادی و سیاسی دولت قربانی را تحت تأثیر قرار دهد. فشارهای اقتصادی نیز به‌نحو مشابهی بر روی دولت قربانی به‌طور غیرآنی تأثیر می‌گذارند. Mattessich, 2016: 889- 890

۲. برای مثال ممکن است ایجاد فشار اقتصادی بر روی دولتی خاص با هدف اجبار آن دولت به انجام تعهدات بین‌المللی خود صورت پذیرفته باشد.

سایبری سیستم‌های اطلاعاتی و شبکه‌های ارتباط از راه دور استونی را مورد هدف قرار دادند. این حملات دقیقا پس از جابه‌جایی نمادی از جنگ جهانی دوم که «سرباز برنز»[1] نام دارد، از مرکز شهر تالین به یک آرامگاه نظامی صورت پذیرفت. حملات سایبری مذکور تا ۲۲ روز ادامه داشتند و حملات تعدادی از سرورها را مورد هدف خود قرار دادند. از جمله مهم‌ترین اهدافی که مورد حملات سایبری قرار گرفته بود، وب‌سایت‌های نهادهای سیاسی همانند ریاست جمهوری، پارلمان و احزاب سیاسی بودند، ولی در بین تمام قربانیان ذکرشده دو بانک مهم استونی، تأمین‌کنندگان خدمات اینترنتی[2] و کمپانی‌های ارتباط از راه دور[3] هم مورد هدف حملات سایبری مذکور قرار گرفتند. بیشترین حملات سایبری که کشور استونی را مورد هدف قرار داده بود، از نوع حملات نفی سرویس توزیع‌شده بود (Joubert, 2012: 1) و همان‌طورکه قبلا هم به آن پرداخته شد، این کار با استفادهٔ حمله‌کنندگان از تعداد بسیاری کامپیوتر برای ایجاد ترافیک و حجم بالا برای سیستم‌ها و سرورهای مورد حمله با قصد از کار انداختن آنها صورت می‌پذیرد. کشور استونی از کوچک‌ترین اعضای پیمان ناتو است که به میزان زیادی به اینترنت وابسته است.[4] تقریبا تمام کشور استونی تحت پوشش اینترنت است و تمام خدمات دولتی به‌صورت آنلاین انجام می‌گیرد و ۸۶ درصد مردم این کشور نیز کارهای بانکی خود را از طریق اینترنت انجام می‌دهند (Kozlowski, 2014: 238).

اگرچه حملات سایبری به کشور استونی آثار تخریبی مستقیم و آنی از خود به‌جا نگذاشت و شدت زیادی هم نداشت که آن حملات به‌عنوان توسل به زور در نظر گرفته شوند، ولی آثار آن حملات مشابه با فعالیت‌ها و اقداماتی بود که به‌عنوان نقض ممنوعیت مداخله تلقی شود، زیرا آن حملات شبکهٔ دیجیتالی یک دولت را مختل کردند و امکان برقراری ارتباط، خدمات بانکی و خدمات دولتی را برای مدتی در آن کشور مختل کرد (William, 2016: 894). با بررسی تحلیل‌های انجام‌گرفته توسط نظریه‌پردازان چنین استنباط می‌شود که مختل کردن شبکه‌های دیجیتالی و کامپیوتری دولت‌ها در سطح گسترده با حملات سایبری نتایجی همانند اعمال اجبار متوجه دولت قربانی می‌کند، ازاین‌رو از این دیدگاه نیز حملات سایبری موردنظر می‌توانند در شمول نقض اصل عدم مداخله قرار گیرند. بنابراین ملاحظه می‌شود در مورد حملات سایبری محروم‌سازی از سرویس توزیع‌شده شبیه آنچه در استونی اتفاق افتاد، اگرچه شدت کم و چگونگی آثار حملات مانع از قرار دادن آن حملات در قالب توسل به زور یا حملات مسلحانه

---

1. Bronze Soldier
2. Internet Service Providers
3. Telecommunications Companies
۴. وابستگی این کشور به اینترنت و استفاده از آن در امور ادارهٔ کشور استونی به‌اندازه‌ای است که دولت آن به‌عنوان دولت الکترونیک (Egovernment) شناخته می‌شود. برای مطالعهٔ بیشتر ر.ک:
http://ec.europa.eu/idabc/servlets/Docd7a7.pdf?id=32608 , Visited on 15 September 2016

می‌شود، ولی در صورت انتساب آن حملات به یک دولت می‌توان دولت مذکور را ناقض تعهد دولت‌ها در ممنوعیت مداخله در امور داخلی دولت‌های دیگر قلمداد کرد.

نتیجه‌گیری

امروزه دولت‌ها در سطح گسترده‌ای با حملات سایبری مواجه‌اند. این‌گونه حملات از شدت و همین‌طور تأثیر یکسانی برخوردار نیستند. با اینکه حملات سایبری با به‌جا گذاردن شدیدترین تأثیرات در قالب توسل به زور و حملات مسلحانه بیشترین جذابیت را در بررسی برای حقوقدانان داشته است، ولی بیشتر حملاتی که دولت‌ها با آن مواجه می‌شوند، حملات سایبری به‌خصوص از نوع حملات محروم‌سازی یا نفی سرویس توزیع‌شده‌ای هستند که آثار تخریبی از خود به‌جا نمی‌گذارند. از جمله دلایلی که دولت‌ها تمایل بیشتری به این‌گونه حملات دارند، علاوه‌بر دشوار بودن مباحث مربوط به انتساب و معیارهای قابل اعمال در مورد انتساب که از بحث فعلی خارج است، شدید نبودن این‌گونه حملات است، با این توضیح که معمولا با توجه به آثار غیرمخرب این حملات و با عنایت به اینکه این‌گونه حملات در قالب توسل به زور و حملات مسلحانه قرار نمی‌گیرند و رژیم حقوقی قابل اعمال در مورد این‌گونه حملات در مقایسه با حملات شدیدتر از ابهام بیشتری برخوردار است، دولت‌ها ترجیح می‌دهند برای رسیدن به مقاصد خود به حملات مذکور متوسل شوند. به هر حال با توجه به ممنوعیت مداخلهٔ دولت‌ها در امور دولت‌های دیگر که هم به‌عنوان تعهدی معاهده‌ای و هم تعهدی عرفی در نظر گرفته می‌شود، حداقل می‌توان حملات محروم‌سازی از سرویس توزیع‌شدهٔ توأم با اجبار را نقض تعهد دولت حمله‌کننده تلقی کرد. علاوه‌بر این حداقل تا انعقاد معاهدات مرتبط یا تا زمانی‌که عرف بین‌المللی در مورد چگونگی نظم‌دهی به این فضا و این‌گونه حملات شکل بگیرد، استفاده از اصل عدم مداخله در مورد حملات سایبری چه در شدیدترین وضعیت و چه در وضعیت‌هایی که حملات آسیب‌های فیزیکی از خود باقی نمی‌گذارند، می‌تواند راه‌حل مناسبی برای جبران کمبودهای فعلی حقوق بین‌الملل و نبودن تعریفی یکسان از توسل به زور و حملات مسلحانه و چگونگی اعمال آنها در مورد حملات سایبری باشد.

منابع

۱. فارسی

الف) کتاب‌ها

۱. تقی‌زاده انصاری، مصطفی (۱۳۹۴)، *ترمینولوژی حقوق بین‌المللی*، چ اول، تهران: خرسندی.

۲. خلیل‌زاده، مونا (۱۳۹۳)، *مسئولیت بین‌المللی دولت ها در قبال حملات سایبری*: تهران: مجمع علمی و فرهنگی مجد.
۳. کازرونی، سید مصطفی (۱۳۹۳)، *مسئولیت حمایت در حقوق بین‌الملل*، چ اول، تهران: نگاه بینه.

ب) مقالات

۴. اصلانی، جبار؛ رنجبریان، امیرحسین (۱۳۹۴)، «بررسی تطبیقی و تحلیل تعریف حملهٔ سایبری از منظر دکترین، رویهٔ کشورها و سازمان‌های بین‌المللی در حقوق بین‌الملل»، *فصلنامهٔ تحقیقات حقوقی دانشگاه شهید بهشتی*، ش ۷۱، ص ۲۷۸-۲۵۷.
۵. جاوید، محمدجواد؛ محمدی، عقیل (۱۳۹۲)، «نسبت اصل عدم مداخله در حقوق بین‌الملل معاصر و اصل حاکمیت از مستضعفین در حقوق اسلامی»، *مجلهٔ مطالعات حقوقی دانشگاه شیراز*، دورهٔ پنجم، ش ۱، ص ۸۸-۴۹.
۶. خلف رضایی، حسین (۱۳۹۲)، «حملات سایبری از منظر حقوق بین‌الملل (مطالعهٔ موردی استاکس نت)»، *فصلنامهٔ مجلس و راهبرد*، سال بیستم، ش ۷۳، ص ۱۵۳-۱۲۵.
۷. صادقی حقیقی، دیدخت (۱۳۹۰)، «تحول در مفهوم اصل عدم مداخله»، *فصلنامهٔ مطالعات روابط بین‌الملل*، دورهٔ ۴، ش ۱۶، ص ۱۲۸-۹۳.
۸. کمالی‌نژاد، حسن (۱۳۹۱)، «بند ۷ مادهٔ ۲ منشور ملل متحد: رویکرد های نوین مجمع عمومی ملل متحد»، *مجموعه مقالات همایش نقش مجمع عمومی سازمان ملل متحد در تدوین و توسعهٔ تدریجی حقوق بین‌الملل*، انجمن ایرانی مطالعات سازمان ملل متحد، ص ۲۴۴-۲۸۲.

۲. انگلیسی

A) Books

9. Oxford, Anne (2003), *Reading Humanitarian Intervention, Human Rights and the Use of Force in International Law*, Cambridge University Press.
10. Simma, Bruno and Daniel Erasmus Khan and George Nolte and Andreas Paulus, (2012), *The Charter of the United Nations, A Commentary*, Third Edition, Vol. 1, Oxford University Press.

B) Articles

11. Buchan, Russell, (2012), "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions", Journal of Conflict & Security Law, Vol. 17, No. 2, pp. 211-227.
112. Choucri, Nazli & Clark, David, (2011), "Cyberspace and International Relations Towards an Integrated System", Version 8-25 for internal ECIR

review, Available at: http://web.mit.edu/chintanv/www/Publications/CESUN_2012_Cyber_International_Relations_as_an_Integrated_System_Vaishnav_Choucri_Clark.pdf , Visited on 10 September 2016, pp. 1-10

13. Gervais, Michael, (2012), "Cyber Attacks and the Laws of War", Berkeley Journal of International Law, Vol. 30, Issue 2, pp. 525-579.
14. Hathaway, Oona A., & Rebecca Crootof, (2012), "The Law of Cyber-Attack", *California Law Review*, Vol. 100, pp. 817-886.
15. Heaton, Major J. Ricou, (2005), "Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces", *The Air Force Law Review*, Vol. 57, pp. 155-209.
16. Jamnejad, Maziar & Michael Wood, (2009), "The Principle of Non-intervention", *Leiden Journal of International Law*, Vol. 22, Issue 2, pp. 345-381.
17. Kesan, Jay P. & Carol M. Hayes, (2012), "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", *Harvard Journal of Law and Technology*, Vol. 25, NO. 2, pp. 429-543.
18. Kilovaty, Ido (2014), "Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare", *American University National Security Law Brief*, Vol. 5, Issue 1, pp. 91-124.
19. Kirsch, Cassandra M., (2012), "Science Fiction No More: Cyber Warfare and the United States", *Denver Journal of International Law and Policy*, Vol. 40:4, pp. 620-647.
20. Kozlowski, Andrzej (2014), "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan", *European Scientific Journal /SPECIAL/ edition*, Vol.3, pp. 237-245.
21. Lotrionte, Catherine (2015), "Countering State-Sponsored Cyber Economic Espionage under International Law", *North Carolina Journal of International Law and Commercial Regulation*, Vol. XL, pp. 443-541.
22. Mattessich, William (2016), "Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage", *Columbia Journal of Transnational Law*, Vol. 54, pp. 873-896.
23. Schmitt, Michael N., (2014), "Below the threshold" Cyber Operations: The Countermeasures Responses Option and International Law", *Virginia Journal of International Law*, Vol. 54:3, pp. 697-732.
24. Stockburger, Peter Z., (2016), "Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum", American University International Law Review, Vol. 31, Issue 4, pp. 545-591.
25. Watts, Sean, (2014), "Low-intensity Cyber Operations and the Principle of Non-intervention", Baltic Yearbook of International Law Online, Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479609, Visited on 10

August 2016, pp. 137-161

C) Documents

26. Charter of Economic Rights and Duties of States, A/RES/29/3281, 12 December 1974
27. Declaration on Principles of International Law Concerning Friendly Relations among States in accordance with Charter of the United Nations, A/RES/25/2625, 24 October 1970
28. Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, A/RES/36/103, 9 December 1981
29. Dogrul, Murat and Adil Aslan, Eyyup Celik, (2011), *Developing an International Cooperation on Cyber Defense and Deterrence Against Cyber Terrorism*, 2011, 3rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011 © CCD COE Publications, p. 34, Available at: https://ccdcoe.org/ICCC/materials/proceedings/dogrul_aslan_celik.pdf
30. Heinegg, Wolff Heintschel von, (2012), *Legal Implications of Territorial Sovereignty in Cyberspace*, 2012 4th International Conference on Cyber Conflict, NATO Publications, Tallinn, pp. 7-19
31. Joubert, Vincent, (2012), *Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO*?, Research Paper, Research Division, NATO Defense College, Rome, No. 76, , Available at: https://www.files.ethz.ch/isn/143191/rp_76.pdf, Visited on 10 August 2016
32. Lipson, Howard F, (2002), *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, Carnegie Mellon Software Engineering Institute, Special Report CMU/sei-2002-sr-009
33. Press Release, SG/SM/6613, Secretary-General Reflects on "Intervention" in Thirty-Fifth Annual Ditchley Foundation Lecture, 26 June 1998, Available at: http://www.un.org/press/en/1998/19980626.sgsm6613.html , Visited on August 2016
34. Roscini, Marco, (2014), *State Responsibility for Cyber Operation: International Law Issues*, Event Report, 9th October 2014, British Institute of International and Comparative Law, Available at: http://www.biicl.org/documents/380_biicl_report_-_state_responsibility_for_cyber_operations_-_9_october_2014.pdf, Visited on 6 February 2016
35. Tallinn Manual on the International Law Applicable to Cyber Warfare, (2013), Prepared by International Group of Experts at the Invitation of NATO Cooperative Cyber Defence Centre of Excellence (edited by M. N. Schmitt), Cambridge University Press
36. Targeted cyber-attacks, The dangers faced by your corporate network, GFI White Paper, Microsoft Gold Certificate Paper, p. 8, Available at: http://www.gfi.com/whitepapers/cyber-attacks.pdf, Visited on September 2016

37. Theohary, Catherin A. and John W. Rollins, (2015), *Cyber warfare and Cyberterrorism: In Brief*, Congressional Research Service, Available at: https://www.fas.org/sgp/crs/natsec/R43955.pdf, Visited on 10 January 2016
38. Vienna Convention on the law of treaties (1969)
39. Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations (1986)
40. Wood, Sir Michael, (2007), *The Principle of Non-Intervention Contemporary International Law: Non-Interference in a State's Internal Affairs Used to be a Rule of International Law: Is it still?*, A summary of the Chatham House International Law discussion group meeting held on 28 February 2007, Available at: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/il280207.pdf , Visited on August 2016

D) Cases

41. Case concerning Military and Paramilitary Activities in and against Nicaragua, (1986), Judgement of International Court of Justice
42. Separate Opinion of Judge Sette-Camara, pp. 199, 200, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)

E) Websites

43. http://ec.europa.eu/idabc/servlets/Docd7a7.pdf?id=32608 , Visited on 15 September 2016
44. http://www.history.com/this-day-in-history/hotline-established-between-washington-and-moscow , Visited on 15 January 2017
45. http://www.nbcnews.com/news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116 , Visited on 15 January 2017
46. http://www.politico.com/story/2016/11/julian-assange-russia-john-podesta-wikileaks-230676 , Visited on 12 January 2017
47. http://www.reuters.com/article/us-usa-election-hack-russia-idUSKCN0Z02EK , Visited on 15 January 2017
48. https://wikileaks.org/What-is-Wikileaks.html , Visited on 5 January 2017
49. https://www.theguardian.com/us-news/2016/dec/10/cia-concludes-russia-interfered-to-help-trump-win-election-report. , Visited on 5 January 2017
50. https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election , Visited on 5 January 2017
51. https://www.us-cert.gov/about-us , Visited on 15 September 2016