حملات سایبری و ممنوعیت توسل به زور[1]

همایون حبیبی[2]
وحید بذّار[3]

چکیده

حملات سایبری به سبب مزایایی از جمله عدم نیاز به تدارکات گسترده و هزینه‌های گزاف و هم‌چنین حفظ نیروی انسانی که در مقایسه با مخاصمات مسلحانه‌ی رایج دارد، امروزه مورد توجه سران سیاسی و نظامی دولت‌ها و سایر بازیگران بین‌المللی قرار گرفته است. به‌رغم افزایش قابل ملاحظه‌ی حملات سایبری طی دو دهه‌ی اخیر، قواعد حاکم بر حق توسل به مخاصمات مسلحانه در حملات سایبری کاملاً روشن نیست. این مقاله در صدد است نشان دهد حمله‌ی سایبری در صورت دارا بودن برخی شرایط می‌تواند به عنوان حمله‌ی مسلحانه تلقی شود و اصل عدم توسل به زور را نقض نماید؛ بنابراین امکان دفاع مشروع دولت قربانی در واکنش به این حملات متصور خواهد بود. در عین حال، با وجود این که اغلب قواعد حاکم بر حق توسل به مخاصمات مسلحانه به حملات سایبری نیز تعمیم داده می‌شود، به دلیل وضعیت خاص این حملات، برخی از این قواعد، محلی برای اجرا نمی‌یابد.

واژگان کلیدی: حمله‌ی سایبری، توسل به زور، عدم مداخله، دفاع مشروع، اقدام متقابل.

---

۱. تاریخ دریافت مقاله ۱۳۹۶/۲/۱۴، تاریخ پذیرش مقاله ۱۳۹۶/۶/۶.

۲. استادیار دانشکده‌ی حقوق و علوم سیاسی دانشگاه علامه طباطبایی.

۳. دانشجوی دکتری حقوق بین‌الملل عمومی دانشگاه علامه طباطبایی؛ نویسنده‌ی مسؤول:
vahidbazzar@gmail.com

درآمد

«حملات سایبری»[1] به خلاف استفاده از نیروی متداول نظامی، غالباً نیاز به تدارکات گسترده و صرف هزینه‌های گزاف ندارد و تنها با یک رایانه و توان برنامه‌نویسی و اتصال به اینترنت[2] می‌توان دست به حملات سایبری زد (Roscini, 2010: 97)؛ ولی استفاده از همین وسایل ساده نیز می‌تواند خسارات قابل ملاحظه‌ای را بر قربانی وارد نماید. به عنوان مثال، «انجمن جهانی اقتصاد»[3] برآورد کرده است که اگر ایالات متحده آمریکا در اتخاذ تدابیر مؤثر ایمنی در مقابل تهدیدهای سایبری کوتاهی نماید، در سال‌های ۲۰۱۴ تا ۲۰۲۰ بیش از سه هزار میلیارد دلار به این کشور خسارت وارد خواهد شد (Gross, 2015: 106). «حمله‌ی سایبری»[4] غالباً خسارت جانی یا فیزیکی به همراه ندارد. به عنوان مثال، حمله‌ی سایبری به کشور استونی در سال ۲۰۰۷ که بانک‌ها، ارتباطات، سایت‌ها و پایگاه‌های داده[5] را در مقیاس بزرگی مورد حمله قرار داد و هم‌چنین حملات سایبری گسترده منتسب به روسیه در جریان جنگ گرجستان مربوط به سال ۲۰۰۸، هیچ یک خسارت فیزیکی یا جانی به همراه نداشتند (Kilovaty, 2014: 91-92). افزون بر این، «گمنامی»[6] از بزرگ‌ترین مزایای این نوع اقدامات است و این ویژگی باعث می‌شود حمله کننده‌ی سایبری بتواند خود را به گونه‌ای مخفی کند که نتوان به راحتی کشور مبداء حمله را مشخص کرد و یا حتی نتوان به طور قطع از مشارکت مالکان رایانه‌هایی که ظاهراً مسؤول حمله هستند سخن گفت (Eichensehr, 2015: 374). به عنوان مثال، حمله‌ی سایبری «طلوع خورشید»[7] علیه سیستم وزارت دفاع ایالات متحده آمریکا

---

1. Cyber War

۲. البته تمامی حملات سایبری به وسیله‌ی اینترنت انجام نمی‌گیرد. در سال ۲۰۱۰ ویروس استاکس نت از طریق شبکه‌ی اینترنت به نیروگاه هسته‌ای نطنز منتقل نشد؛ چون این نیروگاه به دلیل مسایل امنیتی به شبکه‌ی اینترنت متصل نبود.

3. World Economic Forum (WEF)

4. Cyber Attack

5. Databases

6. Anonymity

7. Solar Sunrise

از ســـوی یک نوجوان اسراییلی و چند دانش‌آموز کالیفرنیایی از طریق یک رایانه در امـــارات متحده عربی و بدون اطلاع صاحـــب آن رایانه یا دولت امارات، انجام گرفته اســـت (Shackelford, 2009: 204-231). به دلیل همین ویژگی‌ها و کوتاه بودن نســـبی زمان عملیات ســـایبری[1] و حفظ منابع انسانی، جنگ سایبری برای رهبران نظامی بسیار جذاب شده است. برخی آمارها نشان می‌دهد که در حال حاضر یکصد و چهل کشـــور جهان قابلیت توسل به جنگ ســـایبری را دارند و یا در حال ایجاد چنین قابلیت‌هایی می‌باشند (Brenner and Clarke, 2010: 1012-2014) و در این راســـتا، دول صنعتی به دلیل وابســـتگی زیاد به شبکه‌های رایانه‌ای، بیش‌تر در معرض خطر چنین حملاتی قرار دارند (آهنی امینه و فتح اللهی، ۱۳۹۳: ۱۳۰). در نقطه‌ی مقابل، تاثیر بازدارنده‌ی توانایی سایبری و استفاده‌های دفاعی از آن می‌تواند توسل به مخاصمات مسلحانه را کاهش دهد.

حملات ســـایبری در ابتدا تنها محدود به خرابکاری در شبکه‌های رایانه‌ای بود، اما امروزه از «عملیات جنگی سایبری»[2] و ساخت «سلاح سایبری»[3] نیز سخن گفته می‌شـــود. «کرم استاکس‌نت»[4] که به عنوان نخســـتین سلاح سایبری از آن یاد می‌شـــود (Kilovaty, 2014: 91)، در ســـال ۲۰۱۰ میلادی به منظور تخریب سانتریفوژهای موجود در مرکز هسته‌ای نظنز ساخته شد و بر اساس اطلاعات تایید نشده، توانسته است هزار سانتریفوژ نسل اول این نیروگاه را دچار خودتخریبی کرده و از رده خارج سازد (Shakarian, 2011: 5).

نگرانی از شدت آســـیب‌های سایبری برخی دولـت‌ها را وادار ســاخته است تا برای کاهـــش این آسیـب‌ها با یکـدیگر قراردادهـای دفـاعی مـشترک سایـبری

---

۱. به عنوان مثال، حمله‌ی ســـایبری علیه دولت استونی در سال ۲۰۰۷ و حمله‌ی سایبری علیه دولت گرجستان در سال ۲۰۰۸، تنها سه هفته به طول انجامید (Shrivastava 2013: 13,16).

2. Cyberwarfare

3. Cyberweapon

4. Stuxnet Malware (Stuxnet Worm)

دستورالعمل تالین، استفاده از ویروس استاکس نت را صریحاً استفاده از زور تلقی می‌نماید.
(Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rule.10, Commentary 9)

مـــنعقد نمـــایند. به عنوان مثال، آمـریکا و اســـترالیا یک معـاهده‌ی دفـاعی در زمینـــه‌ی همکاری امنیتی ســـایبری امضاء کرده‌اند که بر اســـاس آن، حمـــله‌ی ســـایبری به هر یک از این کشـــورها به منزله‌ی حمله به هر دو کشور خواهد بود (Theohary and Rollins, 2015: 9). تعداد حملات ســـایبری روز به روز در حال افزایش اســـت. در سال ۱۹۹۸ سه هزار هکر چینی به ســـایت‌های دولتی اندونزی حمله کردند (Shrivastava, 2013: 3). در سال ۲۰۰۷ حملات سایبری که منشا آن کشـــور چین بود، هزار و پانصد رایانه‌ی پنتاگون را در واشینگتن دی‌سی از کار انداخت. این حملات در سال ۲۰۰۷ علیه استونی، در سال ۲۰۰۸ علیه گرجستان، در ســـال ۲۰۰۹ علیه قرقیزســـتان و در ســـال ۲۰۱۰ علیه ایران نیز انجام گرفت (Hayes and Kesan, 2014: 6-7). در ســـال ۲۰۱۲ ورود ویروس شارون[1] به سی هزار رایانه‌ی شرکت نفتی دولتی آرامکو[2] در عربستان که بزرگترین تولید کننده‌ی نفت و گاز جهان اســـت، موجب اخلال در فعالیت‌های این شـــرکت بزرگ نفتی به مدت دو هفته شـــد (Bronk and Tikk-Ringas, 2013: 3). لذا این پرسش‌ها که آیا می‌توان حملات سایبری را مشـــابه حملات فیزیکی نظامی تلقی کرد؛ و این‌که آیا قواعد حقوق بین‌الملل ناظر به توسل به زور بر آن حاکم است یا خیر، به عنوان مباحثی قابل تامل و مهم، موضوع این مقاله اســـت و در این راستا ابتدا چهارچوب حقوقی ناظر به حملات سایبری بررسی می‌شود تا تلقی حمله‌ی سایبری به عنوان توسل به زورِ منع شده در منشور ملل متحد ممکن گردد. سپس به مساله‌ی انتساب حمله به یک دولت و پیچیدگی‌های آن خواهیم پرداخت و در انتها، پیچیدگی‌های امکان توسل به دفاع مشروع و اتخاذ اقدامات متقابل در واکنش به حملات سایبری مورد بحث قرار می‌گیرد.

1. Sharoon Virus
2. Aramco

۱. چارچوب حقوقی موجود ناظر به حملات ســـایبری از منظر«حق توسل به مخاصمات مسلحانه»[۱]

خلاء اســـناد معاهداتی و حقوق بین‌المللی عرفی در عرصه‌ی حق توســـل به زور در فضای ســـایبر بسیار مشهود است. به اســـتثنای کنوانسیون سال ۲۰۰۱ بوداپست موضوع جرایم سایبری که در چارچوب «شورای اروپا»[۲] منعقد گردید؛[۳] و پروتکل الحاقی به آن[۴] که صرفاً به جرایم افراد مربوط می‌شود، سند بین‌المللی مهم دیگری در حوزه‌ی حملات سایبری موجود نیست و شاید تنها بتوان به دستورالعمل تالین اشـــاره کرد که در ســـال ۲۰۱۳ توســـط جمعی از کارشناسان بین‌المللی در چارچوب سازمان ناتو[۵] تهیه گردید؛[۶] سندی که خود به غیر الزام‌آور بودن قواعدش تصریح نموده است[۷]. مجمع عمومی سازمان ملل متحد نیز با صدور چند قطع‌نامه به موضوع حملات سایبری پرداخته است و در این قطع‌نامه‌ها از دولت‌ها تقاضا می‌کند حملات ســـایبری را در حقوق داخلی خود جرم‌انگاری کنند؛[۸] از ایجاد پناهگاه‌های امن برای انجام حملات ســـایبری پیش‌گیری نمایند و در تحقیق و تعقیب حملات

---

1. jus ad bellum

2. The Council of Europe

3. The 2001 Budapest Convention on Cybercrime, Entered into Force on 1 July 2004

۴. این پروتکل در خصوص «لزوم جرم‌انگاری اقدامات نژادپرســـتانه و بیگانه هراسی که با استفاده از رایانه ارتکاب می‌یابند» می‌باشد.

(Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer System (2003), Entered into Force on 1 March 2006)

5. The North Atlantic Treaty Organization (NATO)

۶. از ترکیب بیست و سه نفری این کارشناسان، نه نفر از ایالات متحده آمریکا بودند و کشورهای دارای قابلیت‌های ســـایبری یا کشورهای قربانی حملات سایبری مانند روسیه، ایران و چین نماینده‌ای در این مجموعه نداشتند که این امر انتقادات شدیدی را برانگیخت (Liivoja and McCormack, 2013: 4-12).

7. Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rule. 48, Commentary 9

این دســـتورالعمل که در مرکز دفاع سایبری ناتو در تالین پایتخت کشـــور استونی نگاشته شده، به نام این شهر نام‌گذاری شده است.

8. G.A. Res. 45/121, para. 3 (Dec. 14, 1990)

سایبری بین‌المللی مشارکت کنند.[۱] افزون بر این، نمی‌توان به آسانی از وجود قواعد عرفی در حوزه‌ی حملات سایبری سخن گفت؛ زیرا این حملات و چگونگی پاسخ به آن‌ها پیشـــینه‌ی چندانی ندارد تا بتوان رویه‌ی دولت‌ها در این خصوص را استخراج کرد[۲].

فقدان قواعد خاص به این معنا نیست که دولت‌ها می‌توانند بدون محدودیت اقـــدام به حملات ســـایبری نمایند و هر چند حقوق عرفـــی و معاهداتی موجود به صراحت در خصوص حملات ســـایبری قاعده‌ای ندارد، اما به کمک ابزارهای تفسیر می‌توان قواعد موجود را به عملیات سایبری نیز تعمیم داد؛ سازمان‌های بین‌المللی مانند سازمان ملل متحد، اتحادیه‌ی اروپا و دولت‌های متعدد از جمله ایالات متحده آمریکا، ایران، بریتانیا، روســـیه، ایتالیا، استرالیا، چین، هلند، قطر، کوبا، مجارستان و مالـــی این نظریـــه را پذیرفته‌انـــد (Roscini, 2014: 19-22). اظهار نظر دیوان بین‌المللی دادگســـتری در قضیه‌ی اختلافات ناوبری و حقوق مرتبط (کاســـتاریکا علیه نیکاراگوئه در سال ۲۰۰۹ میلادی) این رویکرد را تایید می‌نماید که به عبارات منـــدرج در معاهدات قدیمی می‌توان معنای امروزی بخشـــید. دیوان در این قضیه تصریح می‌نماید «هنگامی که طرفین یک معاهده از واژه‌های کلی استفاده می‌کنند، می‌داننـــد که معنای این اصطلاحات در طـــول زمان تکامل می‌یابد و به عنوان یک قاعده‌ی عام، زمانی که یک معاهده برای یک دوره‌ی بسیار طولانی منعقد می‌شود، باید این گونه فرض شـــود که طرف‌های معاهده قصد داشته‌اند اصطلاحات مذکور در آن یک معنای در حال تکامل داشـــته باشـــد».[۳] در این جا با همین رویکرد، به ممنوعیت توسل به زور و مفهوم حمله‌ی مسلحانه مندرج در منشور می‌پردازیم.

---

1. G.A. Res. 55/63, para. 1 (Jan. 22, 2001)

۲. دولـــت روســـیه پیشـــنهاد داده است کـه یـک معـاهـده بـر اســـاس کنوانسیـون سـلاح‌هـای شیـمیایـی The Chemical Weapons Convention (CWC) در خصـــوص فضای ســـایبر تنظیم گردد. هم‌چنین آقای شرس تیوک (Vladislav P. Sherstyuk) معاون نماینده‌ی روسیه در شورای امنیت سازمان ملل متحد، در ســـخنرانی هجدهم مارس ۲۰۱۲، پیشنهادهای اساسی دولت روسیه را در خصوص خلع سلاح سایبری تشریح نمود (O'Connell, 2012: 9).

3. Dispute Regarding Navigational and Related Rights (Costa Rica v Nicaragua), ICJ Reports 2009, para. 66

۲. حمله‌ی سایبری و نقض اصل منع توسل به زور

«اصل ممنوعیت اســـتفاده از زور»[1]، به عنوان یکی از اصول ســـازمان ملل متحد در منشـــور آن سازمان آمده است[2] و از آن جا که منشور واژه‌های استفاده از زور و «حمله‌ی مسلحانه»[3] را تعریف نکرده است، باید مشخص کرد که آیا حمله‌ی سایبری نقض اصل منع توسل به زور تلقی می‌شود یا خیر. در واقع باید تعیین شود که آیا حمله‌ی ســـایبری مصداق توســـل به زور تلقی می‌شود یا خیر. هم‌چنین اگر بپذیریم که اقدامات سایبری توسل به زور و ممنوع تلقی می‌شود، تهدید به ارتکاب این اقدامات نیز مشمول همان ممنوعیت خواهد بود (قاسمی و چهاربخش، ۱۳۹۱: ۱۲۵-۱۲۴).

اصطلاح توســـل به زور در ادبیات منشور جانشین اصطلاح جنگ شده است تا ابهام در تعریف حقوقی جنگ بهانه‌ای برای دور زدن این قاعده نشـــود و در عین حال نویسندگان منشور اصرار داشته‌اند که این اصطلاح در معنی مضیق آن تفسیر شود و برای مثال، پیشنهادهای توسعه‌ی مفهوم توسل به زور به مواردی چون جنگ اقتصادی و جنگ سیاسی مورد موافقت قرار نگرفته است[4] و تفسیر مختار آن است که زور ممنوعه در بند ۴ ماده‌ی ۲ منشور، محدود به استفاده از نیروی نظامی است. با این حال از این تفسیر نمی‌توان نتیجه گرفت که منع استفاده از زور تنها شامل استفاده از تسلیحاتی با قدرت آتشین و انفجاری است؛ زیرا در سطح جهانی پذیرفته شده است که اگر حملات شـــیمیایی، بیولوژی یا رادیولوژی با تاثیر و مقیاس لازم واقع شـــود، حمله‌ی مسلحانه تلقی می‌شـــود هر چند که در چنین حملاتی نیروی مخرب به کار گرفته نشده باشـــد.[5] بنابراین حملات سایبری را نیز می‌توان با تاثیر

---

1. The prohibition of the use of force

2. U.N. Charter, art. 2, para. 4

دیوان بین‌المللی دادگســـتری در قضیه‌ی نیکاراگوئه (۱۹۸۶)، اصل عدم توســـل به زور را به عنوان یکی از قواعد حقوق بین‌الملل عرفی شناســـایی نمـــوده اســـت (Nicaragua v. United States of America, I.C.J. Reports 1986. paras. 188-190).

3. Armed Attack

4. Doc. 784, I/1/27, 6 U.N.C.I.O Docs. 331, 334, 609 (1945)

5. Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rule. 13, Commentary 3

و مقیاس لازم، حمله‌ی مسلحانه تلقی نمود. کنار گذاشتن یک حمله‌ی سایبری ویران‌گر که مراکز مهم و زیرساخت‌های یک کشور را مورد هدف قرار می‌دهد، از قلمرو توسل به زور، در تناقض با اهداف و روح منشور سازمان ملل متحد و ارزش‌های جامعه‌ی بین‌المللی است (Kilovaty, 2014: 124). دستورالعمل تالین اعلام می‌کند که برای صدق واژه‌ی مسلحانه در عبارت «حمله‌ی مسلحانه» لزومی به استفاده از سلاح نیست.[1] با این حال هنگامی که در سال ۲۰۰۷ تارنمای ریاست جمهوری، مجلس، وزارتخانه‌ها، احزاب سیاسی و دو بانک مهم کشور استونی مورد حمله‌ی سایبری قرار گرفت، سازمان ناتو در پاسخ به درخواست استونی اعلام کرد که در این برهه‌ی زمانی، حملات سایبری را یک اقدام مسلم نظامی نمی‌شناسد تا استفاده از ماده‌ی ۵ اساس‌نامه‌ی ناتو درباره‌ی دفاع مشروع دسته جمعی را ایجاب نماید (خلف رضایی، ۱۳۹۲: ۱۳۶).

معیار مورد استفاده در تلقی حمله‌ی سایبری به عنوان یک حمله‌ی نظامی از اهمیت بالایی برخوردار است.[2] به طور کلی برای ارزیابی یک حمله به عنوان حملات بزرگ و مهم، سه معیار شامل «معیار ابزار محور»[3]، «معیار هدف محور»[4] و «معیار مبتنی بر آثار ایجاد شده»[5] ارائه شده است. دیوان در نظریه‌ی مشورتی مشروعیت تهدید یا استفاده از سلاح‌های هسته‌ای (۱۹۹۶) با اعلام این که قواعد حاکم بر توسل به زور، بر تمامی موارد استفاده از زور بدون توجه به سلاحِ به کار گرفته شده اعمال می‌شود،[6] معیار ابزار محور را شیوه‌ای متداول برای

---

1. Ibid., Commentary 4

۲. اقداماتی مانند حمله‌ی هوایی و بمباران مراکز سایبری یا حملات نظامی الکترونیکی سنتی چون ارسال پارازیت، مشمول حمله‌ی سایبری نمی‌شود (صلاحی و کشفی، ۱۳۹۵: ۳۷). در این خصوص حمله باید ویژگی سایبری داشته باشد و ضرورتی ندارد که مکان مورد حمله از چنین ویژگی برخوردار باشد. هم‌چنین ضرورتی ندارد که مکان مورد حمله صرفاً یک مکان نظامی باشد و حتی اگر حمله شبکه‌ی رایانه‌ای یک بیمارستان غیر نظامی را هدف قرار دهد و با تأسیسات نظامی مرتبط نباشد، تأثیر مخرب این اقدام، آن را به یک حمله‌ی مسلحانه بدل می‌نماید (قاسمی و چهاربخش، ۱۳۹۱: ۱۳۲).

3. The Instrument-Based Approach

4. The Target-Based Approach

5. The Effects-Based Approach

6. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion (1996)

بررسی قواعدی که در خصوص یک سلاح معین اعمال می‌شود تلقی ننمود (Azzopardi, 2013: 179). شورای امنیت سازمان ملل نیز با پذیرش حق دفاع مشروع در پاسخ به حملات یازدهم سپتامبر ۲۰۰۱ جایی که هواپیماهای ربوده شده به عنوان سلاح مورد استفاده قرار گرفتند، این نتیجه‌گیری را مورد تایید قرار داده است.[۱] معیار هدف‌محور هم در مرحله‌ی اثبات با مشکلات متعددی مواجه می‌شود. بر خلاف معایب دو معیار نخست، معیار سوم نتایجی منطقی به دنبال دارد. دیوان بین‌المللی دادگستری نیز معیار اخیر را با ادبیات متمایزی پذیرفته است. در قضیه‌ی نیکاراگوئه (۱۹۸۶)، دیوان ضمن تصریح به لزوم تمایز میان اشکال استفاده از زور، ضابطه‌ی «اثرگذاری و مقیاس»[۲] را ارائه نمود که یک حمله‌ی مسلحانه[۳] را از یک «واقعه‌ی صرفاً مرزی»[۴] متمایز می‌نماید.[۵] به این ترتیب دیوان نشان می‌دهد که میان «توسل به زور» و «حمله‌ی مسلحانه» رابطه‌ی عموم و خصوص مطلق برقرار است و هرچند هر حمله‌ی مسلحانه‌ای توسل به زور است، ولی «هر استفاده از زوری، حمله‌ی مسلحانه تلقی نمی‌شود».[۶] دیوان در قضیه‌ی سکوهای نفتی (۲۰۰۳) اعلام کرد «از آن جا که اقدامات ایرانیان به سطح حمله‌ی مسلحانه نرسیده است، ایالات متحده حقی نسبت به واکنش بر مبنای دفاع مشروع ندارد».[۷] دستورالعمل تالین همین ملاک را در خصوص تلقی یک عملیات سایبری به عنوان استفاده از زور یا یک حمله‌ی مسلحانه ارائه می‌نماید.[۸] این مقررات «عملیات

I.C.J. Reports, para. 39

1. S/RES/1368 (2001) of 12 September 2001 and S/RES/1373 (2001) OF 28 September 2001

2. 'Scale and Effects' Test

3. Armed Attack

4. Mere Frontier Incident

5. Nicaragua v. United States of America, I.C.J. Reports 1986. para. 195

6. Nicaragua v. United States of America, I.C.J. Reports 1986. para. 195

7. Oil Platforms Case, I.C.J. Reports 2003, paras. 51,64

8. Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rule. 11

سایبری»[1] را به مانند ماده‌ی ۲(۴) منشور سازمان ملل شامل «تهدید یا توسل به زور علیه تمامیت سرزمینی یا استقلال سیاسی هر دولت یا هر رفتار برخلاف اهداف منشور ملل متحد»[2] تعریف نموده است؛ اما از آن جا که علمیات سایبری فی‌نفسه دارای اثر جنبشی نیست و باعث رویدادهای واجد اثر مخرب یا مرگ‌آور می‌شود، لذا این پرسش مطرح است که چه حدی از آثار را می‌توان آثار اقدام تلقی کرد. به عنوان مثال، اگر اقدام سایبری به بی‌ثباتی در بخش سیاسی منتهی شود؛ به گونه‌ای که مردم به خشم آیند و به مامورین پلیس حمله کرده و باعث قتل چند نفر شوند، این قتل‌ها را نمی‌توان دلیلی برای کشنده بودن حمله‌ی سایبری تلقی کرد و نتیجه گرفت که اقدام سایبری معادل حمله‌ی مسلحانه است؛ اما هم‌چنان که گروه متخصصان تالین نتیجه گرفته‌اند، اگر اقدامات تخریبی یا مرگبار را بتوان به طور منطقی از آثار قابل پیش‌بینیِ اقدام سایبری تلقی کرد، آن گاه حمله در حد حمله‌ی مسلحانه محسوب می‌شود. به عنوان مثال، اگر به یک کارخانه‌ی تصفیه‌ی آب حمله‌ی سایبری شود و در نتیجه‌ی آلوده شدن آب، افرادی بیمار یا فوت شوند، این حمله بدون تردید مسلحانه تلقی خواهد شد.[3] افزون بر این، بر اساس این معیار، عملیات سایبری که مسلحانه یا توسل به زور قلمداد نمی‌شود، به عنوان مداخلات نقض کننده‌ی «اصل عدم مداخله»[4] قابل بررسی است.[5]

۳. شناسایی مهاجم و انتساب حمله به یک دولت در حمله‌ی سایبری

هنگامی که یک حمله‌ی سایبری به عنوان مثال یک بدافزار از طریق بستر اینترنت به پایگاه‌های هسته‌ای یک کشور وارد می‌شود، به دلیل ماهیت غیر جنبشی عمل، تعیین مرتکب عمل چندان کار ساده‌ای نخواهد بود

1. Cyber Operation
2. Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rule. 10
3. Ibid., Commentary 10
4. The Principle of Non-Intervention
5. Nicaragua v. United States of America, I.C.J. Reports 1986. paras. 108,202

(Kilovaty, 2014:117). نقل و انتقال اطلاعات در اینترنت فضا و مکان نمی‌شناسد. حتی مسیر ارسال داده‌ها بین دو نقطه از جهان بر اساس سرعت رسیدن اطلاعات به طور اتوماتیک تعیین می‌شود و به این ترتیب اطلاعات که دراین جا کدهای مخرب است، به صورت بسته‌هایی در آمده و بر اساس سرعت رسیدن به مقصد، از مسیرهای مختلفی ارسال می‌شود. بنابراین اطلاعات به طور مستقیم از کشور الف به کشور ب ارسال نمی‌شود؛ هم‌چنین مهاجمان سایبری می‌توانند با استفاده از چند تکنیک سایبری از جمله کاربرد یک «نشانی آی پی»[1] جعلی، استفاده از «بات نت»[2] یا دیگر روش‌ها، کامپیوترهای دیگری را در نقطه‌ای از جهان به عنوان سکوی پرش خود انتخاب کرده و از طریق آن‌ها حمله‌ی خود را عملی کنند و به این ترتیب ماهیت خود را پنهان نمایند.

مشکل اساسی دیگر در حملات سایبری، انتساب اقدام به دولت است؛ زیرا اگر پس از تحقیقات فنی، نقطه‌ی واقعی آغاز حمله مشخص شد و معلوم گردید که حمله از کدام کشور انجام شده، هنوز نمی‌توان صرف شروع عملیات سایبری از خاک یا ساختارهای مربوط به یک کشور را دلیلی کافی برای انتساب عمل به دولت آن کشور برشمرد و این تنها می‌تواند به عنوان اماره‌ای در خصوص همراهی آن دولت با عملیات مذکور تلقی شود.[3] در عین حال، هنگامی که حمله‌ی نظامی از سوی نیروهای نظامی یک کشور انجام می‌شود،[4] موضوع انتساب حمله به دولتی که

---

1. IP. Address (Internet Protocol Address)

۲. بات‌نت‌ها (Botnet) به معنی شبکه‌ی روباتیک است و منظور شبکه‌ای از رایانه‌های شخصی هستند که با بدافزارها تروجان آلوده شده‌اند و حمله کننده می‌تواند از آن‌ها به مثابه یک شبکه‌ی مجازی برای حمله استفاده کند و بدین ترتیب بدون آن که خودش شناسایی شود، حملات خود را علیه قربانی هدایت نماید. برای اطلاعات تکمیلی بنگرید به:

What is a Botnet | Preventing Botnet Attacks | Kaspersky Lab US (at URL:https://usa.kaspersky.com/internet-security-center/threats/botnet-attacks (last accessed 12 -Mar-2017)

3. Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rules. 7,8

۴. در حال حاضر، کشورهای متعددی از جمله چین، ایالات متحده آمریکا، آلمان و ایتالیا، روسیه و ایران دارای چنین نیروهایی هستند.

این نیروهای نظامی ارگان آن محسوب می‌شوند، کار آسانی خواهد بود.[۱] هم‌چنین زمانـــی که یک دولت از افراد غیر نظامی متبـــوع خود در این جهت بهره می‌گیرد، یعنی زمانی که اشـــخاص یا نهادهای ظاهراً غیر دولتی برخی از وظایف یا اختیارات دولتی را اعمال می‌نمایند[۲] نیز انتســـاب سخت نیست. به عنوان مثال، بریتانیا یک «مرکز عملیات امنیتی سایبری»[۳] تاسیس نموده است که تهدیدهای سایبری علیه این دولت را شناسایی می‌کند و به طور مناسبی به آن‌ها پاسخ می‌دهد؛ یا «شبکه‌ی تجاری روســـیه»[۴] که به عنوان یک شرکت جرایم ســـایبری، فعالیت‌هایی از جمله سرقت، ساخت کد تقلبی، ایجاد وضعیت عدم دسترسی به خدمات از طریق سرریز کردن ســـرور با تقاضاهای بیش از حد و ســـرقت اطلاعات هویتی را انجام می‌دهد. بنابراین چنان‌چه این نوع نهادها مسؤول حمل[۵] باشند، انتساب آن به دولت صحیح به نظر می‌رســـد؛ کما این‌که شبکه‌ی تجاری روسیه متهم است که در سال ۲۰۰۸ حملات سایبری علیه گرجســـتان را انجام داده است (Roscini, 2010: 98-99). افزون بر موارد مذکور، هنگامی کـــه دولت مذکور، اعمال ارتکابی«هکر»[۶] یا هکرها را به عنوان رفتار خود تلقی و اعلام نماید،[۷] از مواردی اســـت که انتســـاب عمل به دولت در آن آســـان است؛ اما در برخی دیگر از وضعیت‌ها، انتساب اقدام خصمانه‌ی سایبری به دولت مشکل‌تر است؛ مثلا اگر یک دولت با «تحریک»[۸] هکرها از طریق «وب‌ســـایت»، «تالارهای گفت‌وگو»[۹] یا «ایمیل» موجب انجام حملات سایبری از ســـوی آنان شود، آیا رفتار ارتکابی به دولت مزبور قابل انتساب خواهد بود؟ دامنه‌ی

1. ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001, art. 4
2. ibid., art. 5
3. Cyber Security Operation Center
4. Russian Business Network (RBN)
5. Denial of Service (DoS) Attack
6. Hacker
7. ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001, art. 11
8. Incitement
9. Chat Rooms

رفتارهای تحریک‌آمیز می‌تواند بسیار متفاوت باشد و در بسیاری موارد برای انتساب عمل حمله‌ی نظامی به دولت کافی نیســت. این تحریکات ممکن است برای دولت مســؤولیت به همراه داشته باشد، ولی تنها هنگامی می‌توان دولت را مسؤول حمله تلقی کرد[1] که اقدامات دولت به میزانی باشد که فعالیت‌های افراد «تحت دستور یا کنترل»[2] آن دولت تلقی گردد؛ به عنوان مثال، پس از تصادم هواپیمای جاسوســی نیــروی دریایی ایالات متحده با یک جت جنگنده‌ی چینی در شــمال دریای چین (۲۰۰۱)، برخی ســایت‌ها دســتورالعمل‌هایی در خصوص چگونگی از کار انداختن رایانه‌های دولت آمریکا منتشر نمودند؛ اما شاید نتوان اقدامات انجام شده بر اساس ایــن اطلاعات را در حد کنترل دولــت چین بر اقدامات انجام شــده قلمداد کرد. وبلاگ‌ها، انجمن‌ها و سایت‌های روسی نیز اقدامی مشابه علیه وب‌سایت‌های دولت گرجستان در پیش گرفتند (Roscini, 2010: 101).

آن چه هنوز موجب اختلاف نظر اســت، انتخاب معیار مناسب در خصوص کنترل دولت بر افراد اســت. از آخر دهه‌ی نود میلادی حقــوق بین‌الملل با تقابل میان دو معیار «کنترل موثر»[3] و «کنترل کلی»[4] مواجه شــده است؛ معیارهایی که به ترتیب از ســوی دیوان بین‌المللی دادگســتری در قضیه‌ی نیکاراگوئه (۱۹۸۶) و شــعبه‌ی تجدید نظر دیوان بین‌المللی کیفری برای یوگســلاوی سابق در قضیه‌ی تادیچ[5] (۱۹۹۹) ارائه شــده است و تا جایی که به نظام مسؤولیت بین‌المللی مربوط می‌شــود می‌توان گفت معیار نخست بیش‌تر مورد پذیرش قرار گرفته است؛[6] با این

---

1. ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001, art. 8

2. Under the Direction or Control

3. Effective Control

4. Overall Control

5. The Tadić case (IT-94-1-A, Judgment, 15 July 1999)

۶. ماده‌ی ۷ طرح پیش‌نویس مســؤولیت بین‌المللی ســازمان‌های بین‌المللی (۲۰۱۱)، معیــار کنترل موثر را به صراحت می‌پذیرد. دیوان اروپایی حقوق بشــر در قضیه‌ی بهرامی و سراماتی (۲۰۰۷) با استفاده از معیار «کنترل و اقتــدار نهایــی» (Ultimate Authority and Control)، معیار کنترل موثــر را با ادبیات جدیدی تکرار و تایید نمود.

(Agim Behrami and Bekir Behrami v. France, Saramati v. France, Germany and

حال دستورالعمل تالین[1] با این استدلال که اثبات انتساب در عملیات سایبری بسیار پیچیده است، کنترل کلی را به عنوان معیار انتساب عمل پذیرفته است (Hayes and Kesan, 2014: 8)؛ انتخابی که نمی‌تواند در باب مسؤولیت چندان موجه باشد؛ زیرا همان طور که دیوان بین‌المللی دادگستری در قضیه‌ی نسل‌زدایی (۲۰۰۷) خاطرنشان کرده است، چیزی که شعبه‌ی تجدید نظر دادگاهِ رسیدگی به جنایات ارتکابی در یوگسلاوی سابق به دنبال آن بوده است، تشخیص این مطلب است که آیا مخاصمه در بوسنی ماهیت بین‌المللی داشته است؛ این مطلب ربطی به مساله‌ی مسؤولیت دولت ندارد که در صلاحیت آن دادگاه هم نیست. بنابراین منطقی نیست که در خصوص حل و فصل دو موضوع با ماهیت‌های کاملاً متفاوت از یک معیار انتساب استفاده نمود.[2] برای آن که دولتی را مسؤول حمله‌ی نظامی به دولت دیگر تلقی کنیم، باید در خصوص معیارهای انتساب سختگیری بیش‌تری اعمال شود.

نتیجه آن‌که، در مواردی که حمله‌ی سایبری از رایانه‌های واقع در سرزمین دولتی انجام می‌شود و این دولت صرفاً به سبب عدم اعمال «تدابیر منطقی و ضروری»[3] برای جلوگیری یا متوقف کردن آن اعمال مورد سرزنش است، انتساب عمل به دولت مزبور محل مناقشه است. بی‌تردید ترک فعل دولت،

Norway, App. Nos. 71412/01 & 78166/01, ECHR, 2007, paras. 129,133,134).
هم‌چنین دیوان بین‌المللی دادگستری پس از قضیه‌ی نیکاراگوئه (۱۹۸۶)، معیار کنترل موثر را در قضیه‌ی نسل‌زدایی ۲۰۰۷ (بوسنی و هرزگوین علیه صربستان)، قضیه لاکربی ۱۹۹۸ (لیبی علیه بریتانیا و ایالات متحده آمریکا)، قضیه‌ی کنگو علیه اوگاندا (۲۰۰۰) و قضیه‌ی نیکاراگوئه علیه هندوراس (۲۰۰۷) مورد استفاده قرار داد.
(ICJ Reports, 1993, p. 19, para. 33; ICJ Reports, 1998, p. 23, para. 38; ICJ Reports, 2000, p. 126, para. 36; Case Concerning Territorial and Maritime Dispute between Nicaragua and Honduras in the Caribbean Sea (Nicaragua v. Honduras), I.C.J, 2007)

1. Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rule. 22, Commentary 2

2. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), I.C.J. Reports 2007, paras. 403-405

3. Necessary and Reasonable Measures

نقض این تعهد دولت تلقی خواهد شد که هیچ دولتی نباید آگاهانه اجازه دهد تا از سرزمینش برای ارتکاب اعمالی برخلاف حقوق سایر دولت‌ها استفاده شود (Talbot Jensen, 2015: 79) قاعده‌ی مذکور که از آن تحت عنوان «اصل مراقبت مقتضی»[1] نیز یاد می‌شود، از سوی دیوان بین‌المللی دادگستری در قضیه‌ی کانال کورفو (۱۹۴۹) شناسایی شد[2] و در قضیه‌ی کاستاریکا علیه نیکاراگوئه (۲۰۱۵) به عنوان قاعده‌ی حقوق بین‌الملل عرفی تایید شد.[3] این قاعده که تعهد ناشی از آن، یک «تعهد به وسیله» و نه «تعهد به نتیجه» است،[4] در دستورالعمل تالین نیز پذیرفته شده است. از دید نویسندگان این دستورالعمل، دولت‌ها متعهد هستند اقدامات مقتضی را برای نظارت بر زیرساخت‌های سایبری خصوصی و دولتی خود انجام دهند والّا مسؤول رفتار سهل‌انگارانه‌ی خود خواهند بود.[5] در قضیه‌ی کورفو (۱۹۴۹)، دیوان بین‌المللی دادگستری در خصوص دولت‌های ناتوان از انجام تعهداتشان بر ضرورت اطلاع‌رسانی این شرایط به دولت قربانی تأکید نمود.[6] دیوان بین‌المللی دادگستری در قضیه‌ی کارخانه‌ی خمیر کاغذ (۲۰۱۰)، دامنه‌ی این اصل را توسعه داده و تمامی فعالیت‌های تحت صلاحیت و نظارت دولت، حتی در خارج از قلمرو سرزمینی را مشمول این حکم دانست.[7] عنصر «آگاهی» در خصوص این تعهد تعیین‌کننده است؛ بدین معنی که هرگاه

---

1. Due Diligence Principle

2. Corfu Channel Case, ICJ Reports 1949: 4, para. 22

3. Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), I.C.J Reports 2015, para. 104

4. See: Pulp Mills on the River Uruguay (Argentina v. Uruguay), ICJ Reports 2010, paras. 186-187; ILC Draft Articles on the Law of the Non-Navigational Uses of International Watercourse sand Commentaries thereto and Resolution on Transboundary Confined Groundwater', Commentary of Art. 7, Report of the International Law Commission on the Work of its Forty-sixth Session, 1994

5. Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rule. 5

6. Corfu Channel Case, ICJ Reports 1949: 4, para. 22

7. Pulp Mills on the River Uruguay (Argentina v. Uruguay), ICJ Reports 2010, para. 197

دولتی نسبت به سوءاستفاده از زیرساخت‌های مخـابراتی‌اش آگـاه باشد، در قبال آن مســـؤولیت دارد (Bannelier-Christakis, 2015: 29). با این وجود در خصوص مفروض دانســـتن علم دولت نسبت به چنین سوء اســـتفاده‌هایی تردید است؛ زیرا ســـرعت انجام اقدامات و حملات ســـایبری، انتساب نقض تعهد به تلاش مقتضی را بسیار دشوار می‌ســـازد؛ به گونه‌ای که در دستورالعمل تالین نیز تصریح شده است که مذاکره‌کنندگان نتوانســـتند در خصوص مســـؤول تلقی نمودن دولت، مبتنی بر این فرض که دولت باید می‌دانسته در سرزمینش چه اتفاقی افتاده، به توافقی دست یابند (Kilovaty, 2014: 121).

موضوع هنگامی پیچیده‌تر می‌شود که از زیرساخت‌های چندین کشور چنین سوء استفاده‌هایی صورت گرفته باشد؛ به عنوان مثال، حمله‌ی سایبری علیه استونی (۲۰۰۷) از طریق کشـــورهایی چون ایالات متحده آمریکا، مصر، پرو و روسیه انجام گرفـــت (Shackelford, 2009: 204,231). در چنین مواردی، مشـــروط بر آن‌که معلوم باشد دولت‌های مذکور از جریان این اقدامات آگاه بوده و یا سهل‌انگاری غیر معقولی انجام داده‌اند، مسؤول دانستن هر یک از آن‌ها به استناد عدم رعایت «اصل مراقبت مقتضی» امکان‌پذیر است.[1] با توجه به رویه‌ی دیوان بین‌المللی دادگستری در قضیه‌ی «کانال کورفو» و قضیه‌ی «زمین‌های فسفات در نائورو»، به نظر می‌رسد بتوان برای دریافت خســـارت کامل به هر یک از این دولت‌ها مراجعه نمود؛ مشروط بر آن‌که زیان‌دیده بیش از خسارت وارده دریافت ننماید.[2] در قضیه‌ی کانال کورفو، ورود خســـارت به کشـــتی‌های بریتانیایی در نتیجه‌ی مین‌گذاری دولت یوگسلاوی و عدم اطلاع‌رســـانی دولت آلبانی به کشـــتی‌های مذکـــور در این خصوص بود؛ در حالی که دیوان بین‌المللی دادگستری به پرداخت کل خسارت وارده به کشتی‌های

1. ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001, Commentaries of Art. 47

۲. دیوان بین‌المللی دادگستری در قضیه‌ی سانحه‌ی هوایی (ایالات متحده آمریکا علیه بلغارستان (۱۹۵۵)) تصریح نمود برای دولت زیان‌دیده هیچ محدودیتی در مراجعه به دولت‌های مسؤول وجود ندارد و این دولت می‌تواند صرفاً تا میزان خسارت کامل خود به هر یک از دولت‌های مسؤول یا تمامی آن‌ها مراجعه نماید.

(Aerial Incident of 27 July 1955 (USA v Bulgaria) (Merits - Memorial submitted by the United States Government) [2 December 1958] Part I, 229)

بریتانیایی از سوی دولت آلبانی حکم داد.[1] در قضیه‌ی نائورو، دولت خوانده (استرالیا) در پاســـخ به ادعای خواهان (نائورو) در خصوص اعمال متخلفانه‌ی بین‌المللی مقام اداره کننده‌ی نائورو اســـتدلال کرد که بر اساس «موافقت‌نامه‌ی قیمومت نائورو»[2]، استرالیا یکی از سه دولت ایجادکننده‌ی این نهاد (بریتانیا، نیوزلند و استرالیا) است و مســـؤولیت ناشی از اعمال این نهاد، چنان ماهیتی دارد که صرفاً می‌تواند به طور مشـــترک علیه این سه دولت مطرح شود. دیوان بین‌المللی دادگستری در پاسخ به این ادعا اعلام نمود: «در حالی که تعهدات ناشـــی از موافقت‌نامه‌ی قیمومت ماهیت مشـــترک دارند، در آن واحد آن‌ها تعهدات شخصی هستند که می‌توانند مسؤولیت هر یک از سه دولت را به نحو جداگانه مطرح نمایند».[3]

با این وجود باید میان مسؤولیت دولت‌ها در قبال خسارات وارده‌ی ناشی از یک عملیات سایبری خصمانه و انتساب نقض بند ۴ ماده‌ی ۲ منشور ملل متحد به یک کشـــور تفاوت قائل شد؛ زیرا در تمام مواردی که دولتی ممکن است بر مبنایی مانند عدم رعایت «اصل مراقبت مقتضی» مسؤول جبران خسارات ناشی از اقدامات خصمانه‌ی سایبری قلمداد شود، لزوماً حمله‌ی مسلحانه و نقض قاعده‌ی منع توسل به زور به آن دولت قابل انتساب نیست. اثر این تفاوت را باید در عکس‌العمل نسبت به حمله‌ی سایبری ملاحظه کرد.

۴. عکس‌العمل دولت قربانی به توسل به زور سایبری

در خصـــوص روش‌های اصلی عکس‌العمل به توســـل به زور ســـایبری، به اختصار به دو اقدام «دفاع مشروع» و «اقدام متقابل» پرداخته می‌شود.

هنگامی که توســـل به زور ســـایبری بخشـــی از یک حمله‌ی مســـلحانه‌ی گســـترده‌تر مشتمل بر عملیات نظامی جنبشی است، دفاع مشروع در قبال عملیات سایبری ویژگی خاصی ندارد؛ زیرا دفاع در قبال تمامی اقدامات نظامی تجاوزکارانه

---

1. Corfu Channel Case, ICJ Reports 1949: 244, 250

2. The Trusteeship Agreement for the Territory of Nauru (New York, 1 November 1947), Article 2, Entry into Force: 01 November 1947

3. Certain Phosphate Lands in Nauru (Nauru v Australia) (Preliminary Objections) [1992] ICJ Rep 240; ICGJ 91, para. 48

صورت می‌گیرد و قواعد عمومی دفاع مشروع در خصوص آن مخاصمه جاری است؛ اما هنگامی که توسل به زور سایبری به طور مستقل صورت می‌گیرد و حمله‌ی مسلحانه‌ی سایبری صرفاً اقدام تجاوزکارانه است، موضوع پیچیدگی‌های خاص خود را دارد[1] و پرسش‌های متعددی به این شرح در خصوص آن مطرح است:

آیا اصل تناسب ایجاب می‌کند که حملات سایبری فقط با حملات سایبری پاسخ داده شود؟

آیا دفاع سایبری باید همواره دفاعی انفعالی و محدود به اقداماتی شود که مانع نفوذ یا اثرگذاری حمله شود؛ مانند فعال کردن دیواره‌ی آتش و خاموش کردن اینترنت؛ و یا آن‌که می‌تواند فعال و مشتمل بر اقداماتی نظیر از کار انداختن منبع حمله با امکانات سایبری یا از هر طریق دیگر باشد؟

آیا دفاع‌کننده‌ی سایبری می‌تواند بدون توجه به این که سامانه‌های کامپیوتری حمله‌کننده مبدأ اصلی حمله هستند یا نقطه‌ی پرشی برای حمله‌کننده‌ی ثالث محسوب می‌شوند، اقدامات دفاعی خود را علیه تمامی مبادی حمله به خود سامان دهد؟

آیا در این جا هم موضوع «دفاع مشروع پیش‌دستانه»[2] مطرح است یا اگر کشوری که به طور تبعی قربانی یک حمله‌ی سایبری باشد و موضوع اصلی حمله نباشد، می‌تواند به دفاع مشروع مبادرت ورزد؟

این‌ها پرسش‌هایی هستند که در نوشتار حاضر مجال پرداختن به آن‌ها نیست؛ اما به این موضوع بسنده می‌شود که در حوزه‌ی دفاع مشروع نیز اختلاف دیدگاه‌ها بسیار است؛ برای مثال دستورالعمل تالین حاوی پاسخ‌هایی به پرسش‌های مذکور است که محل تردید است؛ از جمله آن‌که دیوان بین‌المللی دادگستری در قضیه‌ی سکوهای نفتی (۲۰۰۳) اعلام نمود که یک حمله‌ی مسلحانه باید با «قصد خاص ورود صدمه»[3] واقع گردد؛[4] این در حالی است که دستورالعمل

---

۱. برخی دولت‌ها از جمله ایالات متحده آمریکا و روسیه حق دفاع مشروع در برابر حملات سایبری را در دکترین دفاعی خود محفوظ دانسته‌اند؛ حتی مقامات دولت روسیه به صراحت اعلام کرده‌اند که در واکنش به حملات سایبری می‌توانند متوسل به سلاح اتمی شوند (خلف رضایی، ۱۳۹۲: ۱۳۰).

2. Preemptive Self-Defence or Anticipatory Self-Defence

3. The Specific Intention of Harming

4. Oil Platforms (Islamic Republic of Iran v. USA), ICJ Reports 2003, para. 64

تالین امکان توسل به دفاع مشروع از سوی دولت صدمه دیده‌ی غیر هدف را پذیرفته است؛ مشروط بر آن‌که آثار و صدمات وارده به کشور ثالث، به مقیاس لازم برای تلقی حمله‌ی سایبری به عنوان حمله‌ی مسلحانه رسیده باشد.[۱] هم‌چنین این دستورالعمل امکان دفاع مشروع پیش‌دستانه در مقابل حمله‌ی سایبری «قریب‌الوقوع»[۲] را پذیرفته است.[۳] حال آن‌که ماده‌ی ۵۱ منشور حق دفاع مشروع را در مقابل حملات مسلحانه‌ای به رسمیت شناخته که رخ داده باشند، نه آن که احتمال وقوع آن‌ها باشد.

باید توجه داشت که چنان‌چه حمله‌ی سایبری خاتمه یافته باشد، دفاع مشروع موضوعیت خود را از دست می‌دهد؛ زیرا دفاع عملی فوری است و در صورتی که پس از خاتمه‌ی حمله، قربانی بخواهد به اقدام نظامی سایبری یا فیزیکی مبادرت ورزد، این اقدام مقابله به مثل تلقی شده و ممنوع است. در نظام حقوقی بین‌المللی پس از منشور، اقدامات متقابل نباید شامل تهدید یا توسل به زور باشد یا تعهدات حقوق بشر، حقوق بشردوستانه یا «قواعد آمره»[۴] را نقض نماید.[۵] بنابراین عمل متقابل در قبال اقدامات سایبری هنگامی موضوعیت می‌یابد که شدت آن اقدامات کمتر از توسل به زور باشد (Blank, 2014: 23). دستورالعمل تالین نیز تصریح می‌کند هنگامی که حمله‌ی سایبری خاتمه یابد، ادامه دادن اقدام متقابل قابل توجیه نیست.[۶]

---

1. Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rule. 13, Commentary 12
2. Imminence
3. Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rule. 15
4. jus cogens
5. ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001, art. 50
6. Tallinn Manual on the International Law Applicable to Cyber Warfare, (Michael Schmitt ed., Cambridge University Press 2013), Rule. 3, Commentary. 8

برآمد

۱- تعداد حملات سایبری در دو دهه‌ی اخیر افزایش قابل ملاحظه‌ای یافته است؛ این امر عمدتاً به سبب جایگاهی است که فن‌آوری در زندگی امروز پیدا کرده و مزایایی است که این قسم حملات در مقایسه با حملات نظامی متداول دارد. با توجه به این که خلاء قواعد معاهده‌ای و عرفی در حوزه‌ی جنگ سایبری کاملاً احساس می‌شود، اغلب دولت‌ها و سازمان‌های بین‌المللی معتقدند که قواعد موجود در خصوص حق توسل به مخاصمات مسلحانه در حوزه‌ی جنگ سایبری نیز امکان اعمال دارد. در عین حال، به سبب شرایط خاص حملات سایبری، برخی از این قواعد قابلیت اجرا ندارند؛ به عنوان مثال، شرط فوریت در توسل به دفاع مشروع در مقابل حملات سایبری به سبب دشواری انتساب این حملات، با چالش مواجه می‌گردد.

۲- معیار تعیین و تلقی حملات سایبری به عنوان حمله‌ی مسلحانه از اهمیت بسیاری برخوردار است؛ چنان‌چه یک حمله‌ی سایبری، حمله‌ی مسلحانه تلقی شود، به واسطه‌ی نقض اصل عدم توسل به زور، امکان دفاع مشروع در مقابل آن متصور است؛ و در صورتی که چنین امری احراز نگردد، صرفاً ممکن است به سبب نقض اصل عدم مداخله، برای دولت قربانی به اتخاذ اقدامات متقابل قائل شویم. در عین حال، اقدامات متقابل نیز ممکن است در مواردی چون اختلال سایبری جزئی در مراکز غیر مهم یا جاسوسی سایبری اجازه داده نشود.

۳- به دلیل ماهیت غیر فیزیکی اقدامات سایبری و استفاده از تکنیک‌های رایانه‌ای در جهت مخفی ماندن ماهیت مهاجم، موضوع انتساب این اعمال می‌تواند در عمل دشواری‌هایی را ایجاد نماید؛ زیرا بدون امکان انتساب حتمی حملات سایبری به یک دولت، امکان دفاع مشروع و اقدام متقابل در عمل ممکن نیست. به نظر می‌رسد هم‌چنان که در حقوق کلاسیک پذیرفته شده است که هنگامی حمله به یک دولت منتسب می‌شود که مهاجمان یا هکرها، ارگان دولت باشند، بخشی از اختیارات دولتی را اعمال کنند، تحت کنترل یا دستور دولت اقدام کنند و یا این که یک دولت، حملات سایبری واقع شده را به عنوان رفتار خود تلقی نماید؛ در عین حال دولت‌ها متعهد هستند تا تلاش خود را در خصوص عدم استفاده از سرزمینشان در جهت مغایرت با حقوق سایر دولت‌ها انجام دهند و عدم توجه به این تعهد، مسؤولیت آن‌ها را در پی خواهد داشت.

فهرست منابع

آهنی امینه، محمد و فتح‌اللهی، فاطمه زهرا، ***«حقوق بین‌الملل مدرن در مواجهه با جنگی پست‌مدرن (نبرد سایبری)»***، فصل‌نامه‌ی راهبرد، شماره‌ی ۷۲، پاییز ۱۳۹۳.

خلف رضایی، حسین، ***«حملات سایبری از منظر حقوق بین‌الملل (مطالعه‌ی موردی: استاکس نت)»***، مجله‌ی مجلس و راهبرد، شماره‌ی ۷۳، بهار ۱۳۹۲.

صلاحی، سهراب و کشفی، سید مهدی، ***«جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تالین»***، مطالعات قدرت نرم، شماره‌ی ۱۴، بهار و تابستان ۱۳۹۵.

قاسمی، علی و چهاربخش، ویکتور بارین، ***«حملات سایبری و حقوق بین‌الملل»***، مجله‌ی حقوقی دادگستری، شماره‌ی ۷۸، تابسستان ۱۳۹۱.

Azzopardi, Myrna, ***"The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Brief Introduction on Its Treatment of Jus Ad Bellum Norms,"*** ELSA Malta Law Review, Vol. 3, 2013.

Bannelier-Christakis, Karine, ***"Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?,"*** Baltic Yearbook of International Law Online, Vol. 14, Issue 1, 2015.

Blank, Laurie R, ***"Cyberwar/Cyber Attack The Role of Rhetoric in the Application of Law to Activities in Cyberspace,"*** Cyber-war: Law & Ethics for Virtual Conflicts, Oxford University Press, Emory Legal Studies Research Paper No. 14-286, 2014.

Boer, Lianne J.M.; Lodder, Arno R, ***"Cyberwar: What Law to Apply? And to Whom?,"*** Cyber Safety: An Introduction-edited by Leukfeldt/Stol, Eleven Publishing, 2012.

Brenner, SusanW.; Clarke, Leo L, ***"Civilians in Cyberwarfare: Conscripts,"*** Vanderbilt Journal of Transnational Law, Vol. 43, 2010.

Bronk, Christopher; Tikk-Ringas, Eneken, ***"Hack or Attack? Shamoon and the Evolution of Cyber Conflict,"*** James A. Baker III Institute for Public Policy,Working Paper, 2013.

Delibasis, Dimitrios, ***The Right to National Self-Defence in Information Warfare Operations***, Arena Books, 2007.

Eichensehr, Kristen E, ***"Cyberwar & International Law Step Zero,"*** Texas International Law Journal, Vol. 50, Symposium Issue. 2, 2015.

Graham, David E, ***"Cyber Threats and the Law of War,"*** Journal of National Security Law & Policy, Vol. 4, 2010.

Gross, Oren, ***"Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents,"*** Cornell International Law Journal, Vol. 36, Issue. 48, 2015.

Grosswald, Levi, ***"Cyberattack Attribution Matters Under Article 51 of the U.N. Charter,"*** Brooklyn Journal of International Law, Vol. 36, Issue. 3, 2011.

Hathaway, Oona A.; Crootof, Rebecca; Levitz, Philip; Nix, Haley; Nowlan, Aileen; Perdue, William; Spiegel, Julia, ***"The Law of Cyber-Attack,"*** California Law Review, Vol. 100, 2012.

Hayes, CarolM; Kesan, Jay P, ***"Law of Cyber Warfare,"*** International Encyclopedia of Digital Communication and Society, Illinois Program in Law, Behavior and Social Science Paper No. LBSS14-25, Illinois Public Law Research Paper No. 14-26, 2014.

Hinkle, Katharine C, ***"Countermeasures in the Cyber Context: One More Thing to Worry About,"*** The Yale Journal of International Law Online, Vol. 37, 2011.

Joiner, Christopher C; Lotrionte, Catherine, ***"Information Warfare as International Coercion: Elements of a Legal Framework,"***

EuropeanJournal of International Law, Vol. 12, No. 5, 2001.

Kerschischnig, Georg, ***Cyberthreats and International Law***, Eleven International Publishing, 2012.

Kilovaty, Ido, ***"Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare,"*** National Security Law Brief, Vol. 5,Issue. 1, 2014.

Liivoja, Rain; McCormack, Tim, ***"Law in Virtual Battlespace: The Tallinn Manual and the jus in bello,"*** Yearbook of International Humanitarian Law, Vol. 15, 2013.

O'Connell, Mary Ellen, ***"Cyber Mania,"*** International Law: Meeting Summary: Cyber Security and International Law-edited byO'Connell, Mary Ellen and Arimatsu, Louise and Wilmshurst, Elizabeth, Chatham House, 2012.

Roscini, Marco, ***"World Wide Warfare - Jus Ad Bellum and the Use of Cyber Force,"*** Max Planck UNYB 14, 2010.

Roscini, Marco, ***Cyber Operations and the Use of Force in International Law***, Oxford University Press, 2014.

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

Schmitt, Michael N, ***"The Law Of Cyber Warfare: Quo Vadis,"*** Stanford Law & Policy Review, Vol. 25, 2014.

Shackelford, Scott J, ***"From Nuclear War to Net War: Analogizing Cyber Attacks in International Law,"*** Berkeley Journal of International Law, Vol. 27, 2009.

Shakarian, Paulo, ***"Stuxnet: Cyberwar Revolution in Military Affairs,"*** Small Wars Journal, 2011.

Shrivastava, Rishabh, ***"International Law and Cyber Warfare,"*** SSRN Electronic Journal, 2013.

Sklerov, Lieutenant Matthew J, ***"Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defences against States Who Neglect their Duty to Prevent,"*** 201 MIL. L. Rev 1, 2009.

Talbot Jensen, Eric, ***"State Obligations in Cyber Operations,"*** Baltic Yearbook of International Law Online, Volume 14, Issue 1, 2015.

Theohary, Catherine A.; Rollins, John W, ***"Cyberwarfare and Cyberterrorism: In Brief,"*** Congressional Research Service, 2015.

Tsagourias, Nicholas, ***"The Law Applicable to Countermeasures Against Low-Intensity Cyber Operations Baltic,"*** Yearbook of International Law Online, Volume 14, Issue 1, 2015.

Watts, Sean, ***"Low-intensity Cyber Operations and the Principle of Non-intervention,"*** Baltic Yearbook of International Law Online, Vol. 14, Issue 1, 2014.

Yoo, Christopher S, ***"Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures,"*** Faculty Scholarship, Paper 1540, 2015.