فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۴۸، شمارهٔ ۲، تابستان ۱۳۹۷: ۴۱۹-۴۴۱

عملیات سایبری به‌مثابهٔ توسل به زور

فریده شایگان[1]*، سید حامد صفوی کوهساره[2]

چکیده

فناوری سایبر قواعد بازی را در حوزه‌های مختلف متحول ساخته و توسل به زور نیز از این قاعده مستثنا نیست. افزایش حملات سایبری علیه دولت‌ها و پیچیدگی روزافزون آنها در سال‌های اخیر حکایت از آینده‌ای مبهم دارد. این مقاله پس از بررسی مفهوم سنتی توسل به زور، به این مسئله خواهد پرداخت که آیا قواعد موجود در خصوص فناوری‌های آنالوگ می‌توانند در مورد فناوری‌های نوین دیجیتال استفاده شوند. این مطالعه نشان خواهد داد که نیرو یا زور سایبری تا چه حد می‌تواند با حقوق توسل به زور معاصر انطباق یابد. پرسش کلیدی در این مسیر آن است که آیا کاربرد زور سایبری یک توسل به زور در معنای بند ۴ مادهٔ ۲ منشور ملل متحد محسوب می‌شود. در پاسخ به این پرسش به قواعد تفسیر مندرج در کنوانسیون وین در مورد حقوق معاهدات و رویکردهای مختلف در حوزهٔ دکترین پرداخته خواهد شد. مقاله با ارائهٔ چشم‌اندازی عملی در خصوص قاعده‌مندسازی این شکل نوین از زور پایان می‌یابد. نگارندگان با ادغام روشمند رویکردهای موجود، نظر خود را در مورد توسل به زور سایبری ارائه خواهند داد.

کلیدواژگان

بهره‌برداری سایبری، توسل به زور، حملهٔ سایبری، عملیات سایبری، مداخلهٔ سایبری.

۱. عضو هیأت علمی پردیس بین‌المللی کیش دانشگاه تهران (نویسندهٔ مسئول).
Email: farideh.shaygan@ut.ac.ir
۲. دانشجوی دورهٔ دکتری پردیس بین‌المللی کیش دانشگاه تهران. Email: hf.safavi@ut.ac.ir
تاریخ دریافت: ۱۳۹۶/۰۴/۲۱، تاریخ پذیرش: ۱۳۹۶/۰۷/۱۰

مقدمه

منشور ملل متحد برای اولین بار ممنوعیت تهدید و استفاده از زور در روابط بین‌المللی دولت‌ها علیه تمامیت ارضی یا استقلال سیاسی یکدیگر یا به هر نحو دیگری که با اهداف ملل متحد مغایرت داشته باشد را اعلام می دارد. با توجه به اینکه از واژهٔ زور در بند ۴ مادهٔ ۲ منشور ملل متحد هیچ تعریفی به‌عمل نیامده است، سه رویکرد عمده در دورهٔ پسامنشور شکل گرفت. رویکرد غالب در میان کشورهایی چون ایالات متحدهٔ آمریکا و متحدانش این بوده است که بند ۴ مادهٔ ۲ منشور ملل متحد مکمل مادهٔ ۵۱ منشور بوده و در محدودهٔ حملات نظامی یا خشونت‌های مسلحانه معنا می‌یابد و دیگر جنبه‌های ساختاری منشور ملل متحد نیز از این دیدگاه حمایت می کند (Farer, 1985: 405-408) .

رویکرد دوم، از بند ۴ مادهٔ ۲ منشور قرائتی موسع ارائه می‌دهد، به این صورت که به ابزار و وسیلهٔ مورد استفاده توجه ندارد، بلکه هدف از حمله و اثر کلی آن را در نظر می‌گیرد که همان ممنوعیت زور است. به موجب این رویکرد نیروی نظامی را می‌توان ابزاری برای اجبار و اغلب ساده‌ترین راه قابل مشاهدهٔ کاربرد آن در نظر گرفت. این تفسیر متن‌محور، بر نص صریح بند ۴ مادهٔ ۲ تمرکز دارد. به احتمال زیاد اعمال فشار بر یک کشور یا تهدید به هزینه‌های فلج‌کننده در بخش مالی براساس این رویکرد نامشروع تلقی می‌شود. در دوره‌های مختلف تاریخی برخی از کشورهای در حال توسعه و در دوران جنگ سرد کشورهای جهان سوم تصور می‌کردند که زور شامل انواع دیگری از فشار مانند اجبار سیاسی و اقتصادی نیز می‌شود (Randelzhofer, 2002: 118)، مشکل رویکرد مذکور ترسیم خطی میان اجبار غیرقانونی و فشار قانونی بود، چراکه اجبار در مفهوم کلی همیشه در روابط بین‌الملل جریان دارد و بخشی از روابط روزانه میان دولت‌هاست.

رویکرد سوم، در تفسیر بند ۴ مادهٔ ۲ و مادهٔ ۵۱ منشور، بر نقض حاکمیت سرزمینی و حق دفاع یک دولت تمرکز دارد. چنین رویکردی ممکن است مفهومی از زور یا اجبار را در برگیرد که انواع مداخله در امور داخلی دولت‌ها را به‌جای مجموعهٔ محدودی از ابزارها و وسایل شامل شود. این دیدگاه نیز به‌سان دیدگاه پیشین، به‌ویژه در سه دههٔ نخست پس از تصویب منشور توسط کشورهای در حال توسعه حمایت می شد و منتج به تصویب قطعنامه‌ای در این زمینه در مجمع عمومی شد (GA Res. 2131 (XX), 1965: paras. 1, 2). با این حال تلاش‌ها به‌منظور توسعهٔ گسترهٔ مفهوم زور، به موجب بند ۴ مادهٔ ۲ منشور هرگز به تسری آن به اقدامات غیرنظامی که نقض حاکمیت تلقی می‌شوند (مانند تبلیغات خصمانه برای براندازی سیاسی) منجر نشد، چراکه ملاحظات عملی مانع از پذیرش تفسیر موسع بود. به هر تقدیر برداشت مضیق از بند ۴ مادهٔ ۲ منشور با پایان جنگ سرد به نفع تمرکز محدود بر نیروی نظامی تثبیت

شد. ولی در حال حاضر ورود فناوری‌های مدرن به صحنهٔ نبرد، آزمون و چالشی بر مرزهای منشور است. این فناوری‌های نوین که با وجود برخی شباهت‌ها با نیروی نظامی و اجبار اقتصادی، ویژگی‌های منحصربه‌فردی دارند، به‌سرعت در حال تحول هستند و موجب تغییر رویکرد برخی کشورها مانند ایالات متحده شده‌اند.[۱]

هرچند به‌نظر می‌رسد که چارچوب حقوقی حاکم بر استفاده از زور چنانکه در منشور ملل متحد تدوین شده تا حدودی در خصوص حملات سایبری منسوخ شده است، با وجود این باید توجه داشت که این مقررات مبین حقوق موضوعهٔ موجود است. ازاین‌رو برای کاهش تعارضات و پاسخگویی به این چالش‌ها می‌توان تئوری‌ها و روش‌های مفیدی را پیشنهاد کرد. از سوی دیگر، هرچند حقوق توسل به زور رهنمودهای مفیدی را برای پرداختن به برخی از خطرناک‌ترین انواع حملات سایبری ارائه می‌دهد، چارچوب حقوق توسل به زور در نهایت تنها در مورد جزء کوچکی از حملات سایبری بالقوه می‌تواند کاربرد داشته باشد (Hathaway, 2012: 817). گذشته از صحت و سقم ادعای مذکور، احتمالاً مقررات مذکور برای ارزیابی اعمالی که در حیطهٔ حقوق توسل به زور قرار می‌گیرند، اعم از اینکه سایبری باشند یا نباشند، ارزشمند است. در خصوص قابلیت اعمال قواعد حقوق توسل به زور بر حملات سایبری سه رویکرد عمده وجود دارد: رویکرد ابزارمحور، رویکرد هدف‌محور و رویکرد نتیجه‌محور که به فراخور هر بخش از مقاله کنکاش و بررسی خواهند شد.

تعیین آستانه برای استفاده از زور در فضای سایبر به‌مثابهٔ حملهٔ مسلحانه

همان‌طورکه اشاره شد، بند ۴ مادهٔ ۲ منشور ملل متحد ممنوعیت تهدید و توسل به زور را اعلام می‌کند، بدون آنکه تعریفی از زور ارائه دهد، ممنوعیتی که در عین ابهام بی‌پرده است و سرشت پیچیدهٔ آن مستعد تجزیه‌وتحلیل‌های متفاوت و حتی متضاد است. ازاین‌رو ناگزیریم برای درک معنای زور به معیارهای کلی تفسیر معاهدات، مندرج در بند ۱ مادهٔ ۳۱ کنوانسیون ۱۹۶۹ وین در خصوص حقوق معاهدات رجوع کنیم، چراکه گزینش یکی از معیارهای تفسیر تحت‌اللفظی[۲] یا مبتنی بر متن[۳] به‌منظور مشخص کردن معنای "زور" منتج به نتایجی مجمل خواهد شد. درج واژهٔ "زور" در مقدمهٔ منشور و مواد ۴۱ و ۴۶ با صفت مسلح، و مادهٔ ۴۴ که آشکارا به نیروی مسلح اشاره دارد، اغلب مفسران را متقاعد کرده که گام در مسیر تفسیری

---

۱. استراتژی بین‌المللی سال ۲۰۱۱ ایالات متحده برای فضای سایبر متذکر می‌شود که «طبق منشور ملل متحد، دولت‌هایی که احتمالاً هدف اقدامات خاص تهاجمی در فضای سایبر بوده‌اند، حقی ذاتی برای دفاع از خود خواهند داشت» (International Strategy for Cyberspace, 2011: 10)

2. Literal
3. Contextual

مبتنی بر متن گذاشته و مدعی شوند که چون در سایر مواد منشور "زور" در معنای نیروی مسلح به‌کار رفته، حتی به‌رغم عدم تصریح در بند ۴ مادهٔ ۲، در مورد این مقرره نیز صادق است (Randelzhofer & O. Dörr, 2012: 209) در مقابل، مخالفان این رویکرد معتقدند در مواردی که تدوین‌کنندگان اراده کرده‌اند، به نیروی مسلح اشاره کنند، به‌صراحت آن را ذکر کرده‌اند، با وجود این در بند ۴ مادهٔ ۲ چنین نکرده‌اند و فقط واژهٔ "زور" در آن به‌کار رفته است. بنابراین آنها احتمالاً اشاره به مفهوم موسع‌تری از زور داشته‌اند. با این حال به‌نظر می‌رسد، تفسیر غایی از بند ۴ مادهٔ ۲ مؤید یک خوانش مضیق از مقررهٔ مذکور است که دامنهٔ آن را منحصراً به نیروی مسلح محدود می‌کند. کارهای مقدماتی[1] منشور نیز نشان می‌دهد که تدوین‌کنندگان منشور قصد منع اجبار اقتصادی و فشار سیاسی را نداشته‌اند. اگرچه راندل ژوفر اظهار می‌دارد که از رد اصلاحیهٔ برزیل نمی‌توان به‌عنوان دلیلی برای اثبات این ادعا استفاده کرد که بند ۴ مادهٔ ۲ درصدد ممنوعیت استفاده از زور اقتصادی نبوده است (Harris, 2004: 890)، با این حال به‌نظر می‌رسد که رد اصلاحیهٔ برزیل مبنی بر ممنوعیت تهدید یا توسل به اقدامات اقتصادی در کنفرانس سانفرانسیسکو مؤید این ادعاست که اصطلاح زور در این مادهٔ بدون اشاره صریح به اقدامات اقتصادی، برای شمول آن بر این نوع کاربرد زور کفایت نمی‌کند (Randelzhofer, 2002: 118). هرچند در این مورد هیچ نتیجهٔ قطعی حاصل نشد، آنچه مسلم است، منع اشکال خفیف‌تر زور در قطعنامه‌های بعدی مجمع عمومی سازمان ملل متحد، از جمله اعلامیهٔ ۱۹۷۰ دربارهٔ روابط دوستانه (A/RES/25/2625,1970)، قطعنامهٔ ۳۳۱۴ مصوب۱۹۷۴ مربوط به تعریف تجاوز (A/RES/29/3314,1974)، و اعلامیهٔ ۱۹۸۷ در خصوص عدم توسل به زور (A/RES/42/22,1987)، به‌طور کلی دلالت بر این دارند که ممنوعیت اشکال کم‌شدت زور ناشی از بند ۴ مادهٔ ۲ نیست.

ادوارد گوردُن در بررسی پیشینهٔ تاریخی بند ۴ مادهٔ ۲ اذعان می‌دارد که مشکلات تفسیری به این دلیل حادث شده که این قاعدهٔ حقوقی در متن یک معاهدهٔ چندجانبه متجلی شده و نیازمند سازگاری با شرایط در حال تحول است؛ چالش در اینجا وفادار ماندن به معنای اصلی است بدون فدا کردن آن انعطاف‌پذیری که به‌طور معمول لازمهٔ تفسیر قواعد اساسی است (Gordon, 1985: 271-272)، هرچند رویهٔ قضایی بین‌المللی حاکی از آن است که مفهوم زور به نیروی نظامی محدود می‌شود (Nicaragua Case, 1986: para. 228)، اما تعریف زورِ نظامی موسع است. به هر حال اینکه آیا عملیات سایبری تحت شمول بند ۴ مادهٔ ۲ قرار می‌گیرد یا خیر، در نهایت به این بستگی دارد که کدام‌یک از سه رویکرد تحلیلی برای فهم ماهیت توسل به زور مورد پذیرش قرار گیرد. در ادامه رویکردهای مذکور جداگانه بررسی خواهند شد.

---

1. travaux préparatoires

به موجب مادهٔ ۳۲ کنوانسیون وین راجع به حقوق معاهدات، کارهای مقدماتی هر معاهده وسیلهٔ مکمل تفسیر معاهده‌اند.

۱. رویکردهای تحلیلی برای درک ماهیت توسل به زور در فضای سایبر

برای درک این موضوع که آیا عملیات سایبری تحت شمول بند ۴ مادهٔ ۲ قرار می‌گیرد، سه رویکرد عمده مطرح شده است، رویکرد ابزارمحور[1]، بر ابزار مورد استفاده برای انجام عمل، یعنی سلاح تمرکز دارد، و به‌طور سنتی برای تمیز نیرو یا زور مسلح از فشار اقتصادی و سیاسی به‌کار رفته است. به موجب این رویکرد، حملهٔ سایبری زمانی به‌عنوان حملهٔ مسلحانه تلقی می‌شود که سلاح‌های نظامی متعارف را به‌کار بندد. ازاین‌رو، درصورتی‌که بمباران کابل‌های اینترنتی یا سرورهای رایانه‌ای دارای شدت کافی باشد، عمل مذکور می‌تواند در معنای ابزار مورد توجه قرار گیرد (Hathaway, 2012: 817). به‌نظر می‌رسد اعمال رویکرد ابزاری، ممنوعیت توسل به زور را در خصوص حملهٔ سایبری به سیستم‌های ارتباطی منتفی می‌سازد (Hollis, 2007: 1042).

طرفداران رویکرد هدف‌محور[2] استدلال می‌کنند که عملیات سایبری زمانی به آستانهٔ توسل به زور می‌رسد که علیه زیرساخت‌های حیاتی ملی صورت گیرد، خواه به چنین زیرساخت‌هایی لطمه بزند یا دارای چنین ماهیتی باشد. به موجب دکترین مذکور، حتی اگر عملیات سایبری علیه زیرساخت‌های ملی و حیاتی منتج به تلفات یا خسارات مادی نشود، به‌مثابهٔ توسل به زور تلقی می‌شود (DeLuca, 2013: 34). در واقع، مبنای رویکرد هدف‌محور تمرکز صرف بر عواقب شدید وابستگی جوامع معاصر به زیرساخت‌های اطلاعاتی و ارتباطاتی است (Waxman, 2013: 120). بنابراین به موجب دیدگاه مذکور حتی حملات سایبری که بعید است موجب سلب حیات، صدمه یا تخریب، و آسیب شوند، اگر با هدف از کار انداختن زیرساخت‌های حیاتی حاکمیتی صورت گیرند، می‌توانند به آستانهٔ حملهٔ مسلحانه برسند (Melzer, 2011: 21). ایراد عمدهٔ رویکرد هدف‌محور این است که گرایش زیادی به توسعه و گسترش دارد (Hollis, 2007: 1042). طرفداران این رویکرد با تأکید بر لزوم توجه ویژه به حملاتی که زیرساخت‌های حیاتی ملی را به مخاطره می‌اندازند، این خطر را نادیده می‌گیرند که اعمال چنین رویکردی می‌تواند موجب تشدید وضعیت بحرانی شود (Sklerov, 2009: 70) بسیاری از محققان بر این باورند که در صورت توسل به این رویکرد، صلح به‌صورت چشمگیری در معرض خطر قرار خواهد گرفت (Hathaway, 2012: 817).

رویکرد سوم (رویکرد نتیجه‌محور یا اثرمحور)[3]، مورد حمایت ایالات متحده است. به موجب این رویکرد هرچند اصطلاح "حملهٔ مسلحانه" به‌خودی‌خود متضمن استفاده از سلاح است، با این حال اصول راهنمای حقوق توسل به زور، متکی بر ابزار خاصی برای توسل به زور نیستند، بلکه بیانگر مدلی‌اند که مستلزم "مقیاس و آثار[4]" خاص است. به موجب این دیدگاه «اگر

1. Instrument-based approach
2. Target-based approach
3. Consequence-based approach.
4. scale and effect.

پیامدهای فیزیکی حملات سایبری عملکردی مشابه انواع خسارات فیزیکی بمب یا شلیک موشک داشته باشند، باید به‌طور مشابه، توسل به زور تلقی شوند» (Koh, 2012: 595). مدافعان دیدگاه مذکور برای تأیید ادعای خود به رأی دیوان بین المللی دادگستری که به‌صراحت اظهار می‌دارد، بند ۴ مادهٔ ۲، مادهٔ ۴۲ و مادهٔ ۵۱ منشور ملل متحد «بر هر گونه توسل به زور صرف‌نظر از سلاح مورد استفاده در آن» اعمال می‌شوند (ICJ, 1996: paras.37-50, particularly para.39) استناد می‌کنند و اعتقاد دارند که رأی مذکور تأییدی است غیرمستقیم بر این مسئله که عملیات سایبری می‌تواند از مصادیق توسل به زور تلقی شود (Melzer, 2011: 21-24). البته این دیدگاه اعمال بند ۴ مادهٔ ۲ منشور را به آن دسته از عملیات سایبری که به آثاری مشابه آثار ناشی از به‌کارگیری سلاح‌های فیزیکی- حرکتی[1] منجر می‌شوند، محدود می‌کند. با این حال نباید از نظر دور داشت که وابستگی جوامع مدرن به رایانه، سیستم‌های رایانه‌ای و شبکه‌ها، دستیابی به نتایج مخاطره‌آمیزِ مشابه از طرق دیگر و با ابزارهای غیرمخرب را امکان‌پذیر می‌سازد. با آگاهی از این معضلات، مایکل اشمیت مجموعه‌ای از هشت عامل غیرحصری را به‌تفصیل شرح داده تا در مواردی که دامنه و آثار عملیات سایبری و پیامدهای مخاطره‌آمیز آنها به اندازهٔ کافی با آثار انواع فیزیکی- حرکتی توسل به زور مشابهت دارد، ارزیابی شوند؛ این عوامل عبارت‌اند از: شدت[2]، فوریت[3]، مستقیم بودن[4]، تهاجمی بودن[5]، قابلیت اندازه‌گیری آثار[6]، خصیصهٔ نظامی[7]، مداخلهٔ دولت[8] و مشروعیت احتمالی[9]. (Schmitt,1999: 914–15). به نظر وی نیرو یا زور مسلح را می‌توان از دیگر اشکال اجبار تفکیک کرد، چراکه موجب صدمهٔ عمدهٔ فیزیکی یا تخریب اموال، با فوریت بیشتر و به روشی مستقیم‌تر می‌شود. به باور وی زور مسلح همچنین مشتمل بر مداخلهٔ گسترده‌تری در حقوق دولت قربانی است که ارزیابی پیامدهای منفی آن راحت‌تر از سایر اشکال اجبار است. با وجود این معیارهای اشمیت، بدون اشکال به‌نظر نمی‌رسند. برای مثال، وی مستقیم بودن را لزوماً ویژگی ذاتی استفاده از نیروی مسلح تلقی کرده است، ولی به موجب قطعنامهٔ تعریف تجاوز، اقدام تجاوزکارانه یعنی "جدی‌ترین و خطرناک‌ترین شکل استفاده نامشروع از زور" (A/RES/29/3314, 1974, preamble) نه‌تنها منحصر به بمباران و استفاده از سلاح‌های دیگر نیست، بلکه همچنین اقداماتی را که الزاماً در بردارندهٔ آثار مخرب مستقیم نیستند، از جمله نقض موافقت‌نامه‌ای که به موجب آن دولت میزبان به دولت دیگر اجازهٔ استقرار نیرو در سرزمینش را داده است نیز، در

1. Kinetic.
2. Severity.
3. Immediacy.
4. Directness.
5. Invasiveness.
6. measurability of effects.
7. military character.
8. state involvement.
9. presumptive legality.

برمی‌گیرد (Report of the Special committee on defining Agression, UN Doc. A/8019: 60) دیوان بین‌المللی دادگستری نیز در رأی نیکاراگوئه، تسلیح و آموزش گروه‌های مسلح - اقداماتی را که مستقیماً مخرب نیستند- به‌مثابهٔ توسل به زور تلقی کرد (Nicaragua Case, 1986: para. 228).

مشکل دیگرِ معیارِ مستقیم بودن این است که به اندازهٔ کافی بیانگر این واقعیت نیست که یکی از ویژگی‌های اصلی عملیات سایبری تولید آثار خطرناک غیرمستقیم است، این مخاطرات خود پیامد تغییر، حذف یا تخریب داده یا نرم‌افزار یا از دست رفتن قابلیت زیرساخت‌اند (Dinniss, 2012: 65–6). عامل فوریت نیز در چارچوب سایبر در عمل با ایراداتی مواجه است. بمب‌های هوشمند یا زمان[1]، اسب‌هایی ترواییِ[2] هستند که برای تولید آثار مشخص در زمان یا شرایط خاصی طراحی شده‌اند، و می‌توانند بعد از دسترسی غیرمجاز به داده‌های رایانه‌ای، به آسیب منجر شوند. در نهایت دکترین مشروعیت احتمالی براساس آنچه قاضی سیما آن را به‌مثابهٔ "رویکردی منسوخ به حقوق بین‌الملل" تلقی کرده، بنا شده که به موجب آن «هر عملی که منع نشده مجاز است» (Tallinn Manual, 2017: 336).

به نظر نویسندگان این سطور، استفاده از نیرو یا زور مسلح باید با رجوع به ابزار مورد استفاده یعنی سلاح، توصیف شود. توسل به روش ابزارمحور، معیاری را در اختیار صاحب‌نظران قرار می دهد که پیش‌بینی ماهیت اعمال ارتکابی را بدون خدشه به انسجام درونی آنها تسهیل می‌کند. واقعیت‌های موجود نیز ما را به این نتیجه رهنمون می‌سازد که جامعهٔ بین‌المللی اغلب به‌منظور پیشگیری از سردرگمی ناخواسته و جلوگیری از بروز اختلافات به اتخاذ این رویکرد تمایل بیشتری دارد (Schmitt, 1999: 935). این دیدگاه با معنای متداول عبارات مندرج در منشور انطباق بیشتری دارد. «تردیدی وجود ندارد، آنچه از این رویه فهمیده می‌شود این است که هر نوع استفادهٔ گسترده از نیروی نظامی مورد نظر بوده است» (Brownlie, 1963: 87).

این امر بررسی مفهوم سلاح را لازم می‌گرداند. مطالعهٔ کمیتهٔ بین‌المللی صلیب سرخ در خصوص حقوق بین‌الملل بشردوستانهٔ عرفی، سلاح را این‌گونه تعریف می‌کند: «ابزاری برای ارتکاب اقدامات خشونت‌بار علیه عوامل انسانی یا مادی نیروهای دشمن، خواه خشونتی به‌همراه داشته یا نداشته باشد» (Henckaerts & Doswald-Beck, 2005: Vol I, Rule 6, 23). کتابچهٔ راهنمای اچ پی سی آر[3] در خصوص حقوق قابل اعمال بر جنگ هوایی و موشکی نیز یکی از

1. Logic Bomb.
بمب هوشمند یا زمان، قطعه کد رایانه‌ای است که محمولهٔ نرم‌افزاری معینی را در زمانِ از پیش تعریف‌شده یا با وقوع شرایط معینی اجرا می‌کند. استفاده از "بمب هوشمند" به‌جای بمب منطق" که ترجمهٔ لفظی صحیح‌تری از logic bomb است، به‌منظور تسهیل درک آن برای خوانندهٔ فارسی‌زبان صورت گرفته است.
2. Trojan Horse.
3. HPCR: Manual on International Law Applicable to Air and Missile Warfare.

ویژگی‌های اصلی هر سلاح را «توانایی وارد کردن جراحت/مرگ افراد یا صدمه/ تخریب اموال» می‌داند ((HPCR Manual, 2013: 49, rule 1(ff)). حداقل مخرج مشترک میان تعاریف موجود، پیامدهای خشونت‌بار ایجادشده توسط ابزار مورد استفاده است. بنابراین سلاح‌ها به‌واسطهٔ اثراتشان بازشناسی می‌شوند، نه به‌واسطهٔ مکانیسمی که از طریق آنها به تخریب یا ایجاد خسارت منجر می‌شوند (Ziolkowski, 2010: 69). در صورت صحت این ادعا، زور مسلح در معنای بند ۴ مادهٔ ۲ می‌تواند به‌مثابهٔ شکلی از مداخله توسط دولت تعریف شود که تحمیل‌کنندهٔ آن اجباری به دولت دیگر است که مستلزم استفاده از وسیله‌ای(سلاح) است که قادر به تولید عواقب خشونت‌بار است. به این ترتیب در بررسی دقیق‌تر، مباحثات و اختلاف‌نظر میان حامیان رویکرد ابزارمحور و رویکرد اثرمحور اهمیت خود را تا حدود زیادی از دست می‌دهد، چراکه این دو رویکرد باید در ترکیب با هم مورد توجه قرار گیرند. این ابزار مورد استفاده است که نیرو یا زور مسلح را معرفی می‌کند، با این حال خود این ابزار به‌واسطهٔ پیامدهای (خشونت‌بار) آن بازشناسی می‌شود. تمرکز بر ابزار روشن می‌سازد که چرا دیوان بین‌المللی دادگستری مسلح کردن و آموزش گروه‌های مسلح را اگرچه به‌طور مستقیم مخرب نیستند، به‌مثابهٔ توسل به زور تلقی کرده است، زیرا این فعالیت‌ها به‌شدت با سلاح ارتباط دارند و به‌منظور قادر ساختن افراد برای استفاده از آنها صورت می‌گیرند.

پس اگر استفاده از زور مسلح یا نظامی به موجب بند ۴ مادهٔ ۲ نیازمند سلاح است، پرسش بعدی که باید به آن پاسخ داده شود این است که آیا بدافزارها می‌توانند واجد چنین شرایطی باشند. دیوان بین‌المللی دادگستری در رأی مشورتی خود در خصوص مشروعیت تهدید یا استفاده از سلاح‌های هسته‌ای، تصریح کرد که «بند ۴ مادهٔ ۲، و همچنین مواد ۵۱ و ۴۲ منشور ملل متحد به سلاح خاصی اشاره نکرده‌اند. آنها بر هر گونه توسل به زور، صرف‌نظر از سلاح مورد استفاده اعمال می‌شوند» (Nuclear Weapons, Advisory Opinion, 1996: para.39). بنابراین به موجب آن مواد، دلیلی ندارد که سلاح‌ها لزوماً اثرات انفجاری داشته باشند یا برای اهداف تهاجمی ساخته شده باشند. ضمن اینکه «مرگ، جراحت، صدمه یا ایراد خسارت لزوماً نتیجهٔ اصابت فیزیکی نیست. به‌طور خاص، سخت‌افزار، نرم‌افزار و کدهای حمله از طریق شبکهٔ رایانه، سلاح‌هایی هستند که می‌توانند از طریق انتقال جریان داده‌ها به چنین اثراتی منجر شوند» (HPCR Manual, 2013: 49).

۲. گونه‌شناسی عملیات سایبری

عملیات سایبری ممکن است در اشکال مختلفی مانند بهره‌برداری سایبری برای جمع‌آوری اطلاعات و شناسایی و مبادرت به حملهٔ سایبری صورت گیرد و در مورد اخیر حتی موجب حذف، تحریف یا جابه‌جایی داده‌ها یا نرم‌افزارها با داده‌ها یا نرم‌افزارهایی شود که موجب ایراد

صدمات فیزیکی به اموال یا اشخاص یا نقص در عملکرد زیرساخت‌ها یا اخلال در ارائهٔ خدمات شوند. این تنوع در پیامدهای عملیات سایبری مانع از ارزیابی آنها به‌مثابهٔ یک کل و دلیل گونه‌شناسی‌های[1] مختلفی است که در ادامه جداگانه بررسی خواهند شد.

۲. ۱. حملات سایبریِ موجد آسیب فیزیکی به اموال، سلب حیات یا ایراد صدمه به افراد

عملیات سایبری می‌تواند موجد آثار متعددی باشد که عمده‌ترین و اصلی‌ترین آنها متأثر کردن رایانه، سیستم رایانه‌ای یا شبکه مورد حمله با حذف، تحریف، تغییر داده یا نرم‌افزار، قطع سیستم از طریق محروم‌سازیِ توزیع‌شده از خدمات[2] یا سایر حملات سایبری است. آثار ثانویهٔ این نوع عملیات عبارت‌اند از: تخریب یا از کار افتادن کلی یا جزیی زیرساخت‌ها به‌واسطهٔ سیستم یا شبکهٔ مورد حمله. سومین نوع تأثیرات، آن دسته از اثراتی هستند که به‌واسطهٔ تخریب یا از کار انداختن سیستم یا زیرساخت مورد حمله، افراد را تحت تأثیر قرار می‌دهند. پس آسیب فیزیکی به اموال، سلب حیات، و صدمه به افراد هرگز از آثار اولیه و مستقیم عملیات سایبری نیست. خسارت به اموال صرفاً می‌تواند اثر ثانویهٔ عملیات سایبری باشد، درحالی‌که مرگ یا صدمه به افراد می‌تواند از آثار نوع سوم عملیات مذکور به‌حساب آید. با این حال «وابستگی شدید جوامع مدرن به سیستم‌های اطلاعاتیِ به‌هم‌پیوسته بدان معناست که آثار غیرمستقیم و ثانویهٔ حملات سایبری می‌توانند دارای اهمیتی بیش از آثار مستقیم و فوری باشند» (Waxman, 2011: 445). ازاین‌رو به‌نظر می‌رسد مشکلی برای اعمال قواعد حقوق توسل به زور بر این وضعیت‌ها وجود ندارد.

ایان براون لی در سال ۱۹۶۳ در پاسخ به این پرسش که آیا استفاده از سلاح‌هایی که فاقد اثر انفجاری ناشی از امواج و گرما هستند در زمرهٔ توسل به زوری که در بند ۴ مادهٔ ۲ به آنها اشاره شده، قرار می‌گیرند، اظهار داشت که استفاده از این نوع سلاح‌ها باید به‌منزلهٔ توسل به زور تلقی شود، زیرا این سلاح‌ها برای نابودی اموال و نفوس به‌کار می‌روند (Brownlie, 1963: 362). ازاین‌رو بی هیچ شک و شبهه‌ای هر حملهٔ سایبری که به ایراد خسارت فیزیکی به اموال یا سلب حیات یا صدمه به افراد منجر می‌شود یا به‌طور منطقی به احتمال زیاد دارای چنین آثاری خواهد بود، تحت شمول ممنوعیت مندرج در بند ۴ مادهٔ ۲ منشور ملل متحد قرار خواهد گرفت.

---

1. Typologies.
2. Distributed Denial of Service (DDoS).
محروم‌سازی توزیع‌شده از خدمات، به‌طور کلی شامل تلاش برای قطع موقت یا دائمی یا تعلیق ارائهٔ خدمات میزبانِ متصل به اینترنت است. منظور از میزبان، فراهم‌کنندهٔ فضایی است که کاربر می‌تواند فایل‌های وبگاه خود را در آن قرار دهد. یکی از روش‌های معمول حمله شامل اشباع رایانه‌های هدف با درخواست‌های ارتباط خارجی است، به‌طوری‌که نتواند به ترافیک موجود پاسخ دهد یا پاسخ‌ها با سرعت کم داده شود یا حتی به دلیل ترافیک بالا از دسترس خارج شود (SearchSecurity, 2017).

در اینجا این سؤال مطرح می‌شود که آیا یک آستانهٔ حداقلی برای شدت آثار مخرب به‌منظور تحقق عملیات سایبریِ ناقض بند ۴ مادهٔ ۲ منشور و نه صرفاً ناقض اصل عدم مداخله، ضروری است؟ مشاور سابق وزارت امور خارجهٔ ایالات متحده، برای این منظور تفکیکی میان صدمه/مرگ افراد از یک سو و خسارت به اموال از سوی دیگر قائل می‌شود، وی معتقد است که "اقدامات سایبری با نتایجی مانند مرگ، صدمه یا تخریبِ قابل توجه را می‌توان به‌مثابهٔ توسل به زور تلقی کرد (koh,2012: 4). فراسوی چارچوب سایبری، تشخیص کمیسیون مستقل بین‌المللی حقیقت‌یاب در جنگ گرجستان در گزارش سال ۲۰۰۹ این بود که «ممنوعیت توسل به زور، تمامی زور فیزیکی را که دارای حداقل آستانهٔ شدت باشند، پوشش می‌دهد» و «حوادث بسیار جزیی مانند کشتار هدفمندِ افراد خاص، آدم‌ربایی افراد مشخص یا رهگیریِ یک هواپیمای منفرد، زیر این آستانه قرار می‌گیرند» (Report of the Independent Fact-Finding Mission on the Conflict in Georgia, 2009: 242). به‌نظر می‌رسد که حمایت محتاطانه‌ای نیز از این دیدگاه در رأی ۱۹۹۸ دیوان بین‌المللی دادگستری در قضیهٔ صلاحیت ماهیگیری صورت گرفته است. در این قضیه اسپانیا بر آن بود که اقدامات اجرایی علیه کشتی استای[1] به حد نقض بند ۴ مادهٔ ۲ رسیده است، اما دیوان اظهار داشت که «استفاده از زورِ مجاز به موجب قوانین و مقررات کانادا در حیطهٔ آنچه عموماً به‌عنوان اجرای تدابیر حفاظتی و مدیریتی فهمیده می‌شود، قرار می‌گیرد» و «براساس تفسیر "طبیعی و معقول" این مفهوم، ورود، بازرسی، دستگیری و استفادهٔ حداقلی از زور برای آن اهداف، همگی داخل در مفهوم اجرای تدابیر حفاظتی و مدیریتی قرار دارند» (Fisheries Jurisdiction, 1998: para. 84).

هرچند هیچ واژه‌ای در بند ۴ مادهٔ ۲ منشور ملل متحد نمایانگر این نیست که میان موارد استفاده از زور برحسب شدتشان می‌بایست تفکیک قائل شد. با این حال تفسیر عبارات بند ۴ مادهٔ ۲ نباید به «نتیجه‌ای آشکارا بی‌معنی یا غیرمنطقی منتهی شود» (Vienna Convention on the Law of Treaties, 1969: Article 32). بدین‌سان، یک عملیات سایبری که موجد آسیب حداقلی مانند تخریب یک رایانه یا سرور واحد می‌شود، در دامنهٔ مقررهٔ مذکور قرار نمی‌گیرد.

سؤال بعدی این است که آیا از حیث قابلیت اعمال مادهٔ ۲(۴) منشور، می‌توان داده‌ها را همسان دارایی‌های فیزیکی تلقی کرد، به‌طوری‌که حتی بدون ورود آسیب فیزیکی یا از کار افتادن زیرساخت‌ها، حذف، تغییر یا تحریف آنها به‌مثابهٔ توسل به زور محسوب شوند؟ به عقیدهٔ اشمیت «آستانهٔ توسل به زور جایی است در امتداد زنجیرهٔ بین اجبار اقتصادی و سیاسی از یک سو، و اعمالی که موجب آسیب فیزیکی می‌شوند، از سوی دیگر» (Schmitt, 2011: 575). البته وی نیز در مسیر احتیاط گام بر می‌دارد و مدعی می‌شود که به استثنای تخریب داده‌هایی مانند داده‌های بانکی که طراحی شده‌اند تا بلادرنگ به اشیای ملموس مبدل شوند، تخریب یا صدمه

1. Estai.

به داده‌ها، خودبه‌خود برای رسیدن به آستانهٔ حملهٔ مسلحانه کافی نیست. این نتیجه‌گیریِ اشمیت را می‌توان به توسل به زور در بند ۴ مادهٔ ۲ تسری داد. در هر صورت به‌نظر می‌رسد احتمالاً رویهٔ آتی این مسئله را آشکار خواهد کرد.

۲. ۲. حملات سایبری مختل‌کنندهٔ زیرساخت‌های حیاتی

اگر آن دسته از حملات سایبری را که به ایراد خسارات مادی به اموال یا صدمه به افراد منتج می‌شوند یا به‌طور منطقی احتمال زیادی دارد که چنین آثاری را به‌بار آورند، با حملات حرکتی-فیزیکی همسان تلقی کرد و در مورد شمول مادهٔ ۲(۴) منشور بر آنها تردید نداشت، اما در خصوص عملیات مختل‌کننده[1] یا به‌عبارت دیگر، عملیاتی که زیرساخت‌ها را بدون وارد کردن خسارت فیزیکی به آنها، از کار می‌اندازند یا آنها را بلااستفاده می‌کنند، چنین توافقی وجود ندارد. ادعای نگارندگان نوشتار حاضر این است که عملیات سایبریِ مختل‌کننده نیز اگر اختلالِ ناشی از آن به اندازهٔ کافی مهم باشد و امنیت دولت را تحت تأثیر قرار دهد، تحت شمول بند ۴ مادهٔ ۲ منشور قرار می‌گیرد، برای مثال اگر این عملیات زیرساخت‌های حیاتی ملی را هدف قرار دهد، طبیعتاً در حیطهٔ بند ۴ مادهٔ ۲ قرار خواهد گرفت. با وجود این، هیچ‌گونه توافق کلی در این خصوص که کدام زیرساخت حیاتی تلقی می‌شود، وجود ندارد. قانون وطن‌پرستی ایالات متحده زیرساخت‌های حیاتی را این‌گونه تعریف می‌کند: «سیستم‌ها و دارایی‌ها، اعم از فیزیکی و مجازی که به قدری برای ایالات متحده حیاتی‌اند که از کار افتادن یا انهدام چنین سیستم‌ها و دارایی‌هایی تأثیر تضعیف‌کننده‌ای بر امنیت، امنیت اقتصادی ملی، سلامت یا ایمنی عمومی ملی، یا ترکیبی از آنها دارند» (USA Patriot Act, 2001: Section 1015, p.401, para.3(e)). استرالیا زیرساخت‌های حیاتی را این‌گونه تعریف می‌کند: «آن دسته از امکانات فیزیکی، چرخهٔ تولید، فناوری اطلاعات و شبکه‌های ارتباطی که در صورت از بین رفتن، تخریب یا از دسترس خارج شدن آنها برای مدت طولانی، تأثیر منفی بر بهروزی اجتماعی و اقتصادی ملی دارد یا توانایی‌های استرالیا را برای مراقبت از امنیت ملی، به‌ویژه در بخش‌های: «بانکداری و مالی، ارتباطات، خدمات اورژانسی، انرژی، چرخهٔ مواد غذایی، سلامت (شخصی)، خدمات آب، اجتماعات مردمی، و حمل‌ونقل (حمل‌ونقل هوایی، دریایی و زمینی) متأثر می‌کند» (Australian Cyber Security Strategy, 2009: 20). در نهایت، کمیسیون اتحادیهٔ اروپا زیرساخت‌های حیاتی را شامل «آن دسته از منابع فیزیکی، خدمات، و تأسیسات فناوری اطلاعات، شبکه‌ها و دارایی‌های زیرساختی که اختلال و تخریب آنها اثر جدی بر سلامت، ایمنی، امنیت یا بهروزی اقتصادی شهروندان یا عملکرد مؤثر حکومت دارد» می‌داند (European Commission, 2005: para. 3.1).

1. Disruptive.

به نظر مجمع عمومی سازمان ملل متحد « ... تولید، انتقال و توزیع انرژی، حمل‌ونقل هوایی و دریایی، بانکداری و خدمات مالی، تجارت الکترونیک، تأمین آب، توزیع مواد غذایی و بهداشت عمومی و زیرساخت‌های اطلاعاتیِ حیاتی که به‌طور فزاینده‌ای آنها را به هم پیوند داده‌اند و بر عملیات آنها تأثیر می‌گذارند» زیرساخت حیاتی تلقی می‌شوند. با این حال مجمع عمومی با اشاره به تعاریف متنوع صریحاً تصدیق کرده است که «هر کشور زیرساخت‌های اطلاعاتی حیاتی خود را تعیین خواهد کرد» (A/RES/58/199, 2004: preambular paras. 3 and 4).

در هر حال، حداقل مخرج مشترک تعاریف مذکور این است که چنین زیرساخت‌هایی برای امنیت ملی در تمام ابعاد آن، اساسی‌اند. هرچند خصیصهٔ اساسی زیرساختِ هدف تنها عامل تعیین‌کننده برای حامیان رویکرد مبتنی بر هدف نیست، خصیصهٔ مذکور عنصری اساسی برای اظهارنظر در این مورد است که آیا آن عملیات سایبریِ مختل‌کننده، به‌حد توسل به زور ممنوعه به موجب بند ۴ مادهٔ ۲ رسیده است. اگر زیرساختِ هدف حیاتی نباشد، بسیار بعید است که آثار اختلال ایجادشده بر کارکردهای ضروری دولت و نظم عمومی داخلی آن مؤثر باشد. ازاین‌رو اینکه آیا عملیات سایبری مختل‌کننده به سطح توسل به زور می‌رسد یا خیر، نه‌تنها لزوماً به خصیصهٔ حیاتی زیرساختِ هدف بستگی دارد، بلکه همچنین به عوامل دیگری مانند جدی بودن این اختلال، مدت زمان آن، پیچیدگی ابزارهای مورد استفاده و میزان اتکای دولت قربانی به سیستم‌های اطلاعاتی بستگی دارد[۱] (Tsagourias, 2012: 232).

به‌طور کلی به‌نظر می‌رسد که «چون مادهٔ ۲(۴) منشور به‌صراحت به نیروی مسلح یا نظامی اشاره نمی‌کند، تفسیری انعطاف‌پذیر، با توجه به تکامل جنگ‌افزار و منطق نهفته در این مقرره، مانع از گسترش ممنوعیت موجود در آن به‌منظور در برگرفتن موارد نوین استفاده از زور نمی‌گردد» (Segura-Serrano, 2006: 224-5). باید توجه داشت که در حوزهٔ سایبر، تمرکز صرف بر عواقب فیزیکی مخرب برای افراد و اموال کمرنگ شده است، چراکه «جوامع مدرن وابسته به وجود و عملکرد صحیح یک زیرساخت گسترده‌اند که به‌طور فزاینده‌ای توسط فناوری اطلاعات کنترل می‌شود. بنابراین، اقداماتی که به‌طور چشمگیری با عملکرد آن زیرساخت‌ها تداخل دارند، می‌توانند به‌طور منطقی به‌مثابهٔ توسل به زور تلقی شوند، خواه بلادرنگ به خسارت فیزیکی منجر بشوند یا خیر» (Owens & Dam, 2009: 254).

برخی دولت‌ها نیز آشکارا از کار انداختن برخی زیرساخت‌ها به‌وسیلهٔ حملهٔ سایبری را به‌منزلهٔ استفاده از زور دانسته‌اند. برای مثال، «دولت مالی» مدعی شده که «استفاده از سلاح اطلاعاتی را می‌توان به‌منزلهٔ عمل تجاوز تفسیر کرد، درصورتی‌که دولت قربانی دلایلی برای این

---

۱. مشاور حقوقی وزارت امور خارجهٔ ایالات متحده در این مورد به عواملی از جمله زمینه‌های رویداد مورد نظر، بازیگرانی که مرتکب عمل مورد نظر می‌شوند، هدف و محل، اثرات و قصد و ... به‌منظور ارزیابی عملیات سایبری به‌عنوان استفاده از زور اشاره کرد. (Koh, 2012: 595)

باور داشته باشد که آن حمله به‌وسیلهٔ نیروهای مسلح دولت دیگر و با هدف ایجاد اختلال در عملکردِ تسهیلات نظامی، انهدام قابلیت‌های دفاعی و اقتصادی یا نقض حاکمیت دولت بر یک سرزمین خاص انجام گرفته است» (UN Doc A/64/129/Add.1, 2009: 8, para.22). ایالات متحده در مورد امنیت اطلاعات به‌نحوی که در گزارش دبیر کل سازمان ملل متحد درج شده، اظهار داشته است که « فعالیت مختل‌کننده در فضای سایبر می‌تواند در برخی اوضاع و احوال حملهٔ مسلحانه [و در نتیجه، توسل به زور] تلقی شود» (UN Doc A/66/152, 2011:18).

هرچند هیچ مانع منطقی برای تلقی عملیات سایبری مختل‌کنندهٔ زیرساخت‌های حیاتی به‌مثابهٔ توسل به زور وجود ندارد، بعید است که کشورها به‌زودی از طریق ابزارهای حقوقی جدید مرزهای مجاز اقدام در این حوزه را ترسیم کنند، به احتمال زیاد طرح و تحول آهسته و پیوستهٔ تفاسیر با آشکار شدن بحران‌ها به‌عنوان بازتاب توزیع قدرت، خطوط رژیم منشور را در خصوص حملات مختل‌کنندهٔ سایبری ترسیم و گسترش خواهد داد.

وضعیت عملیات سایبری با آستانهٔ پایین

همان‌طورکه اشاره شد، یک آستانهٔ پایین‌تر از توسل به زور در روابط بین‌الملل شناسایی شده است که هرچند مغایر برخی قواعد حقوق بین‌الملل است، نقض بند ۴ مادهٔ ۲ منشور محسوب نمی‌شود، برای مثال، در حوزهٔ مورد بحث نوشتار حاضر، عملیات سایبری که موجد آسیب حداقلی مانند تخریب یک رایانه یا سرور واحد می‌شود، در محدودهٔ مقررهٔ مذکور قرار نمی‌گیرد. هولیس در این خصوص به‌درستی به این نتیجه می‌رسد که نباید چنین اعمال منفردی را به‌عنوان عملی واجد خصوصیات توسل به زور یا فرصت مناسبی برای دفاع از خود تلقی کرد. به اعتقاد او حتی با تصور بالا بودن امکان چنین وقایعی برای مثال نمی‌توان سرنگونی هر هواپیمای غیرنظامی را به‌منزلهٔ توسل به زور ممنوعه تلقی کرد. دولت‌ها حادثهٔ لاکربی را این‌گونه تلقی نکرده‌اند و به‌جای آن یک رویکرد حقوق کیفری را در قبال دو عامل اطلاعاتی لیبی که متهم به دست داشتن در سقوط هواپیمای پان آمریکن ۱۰۳ بودند، اعمال کردند (Hollis, 2007: 1042). عملیات سایبریِ مختل‌کننده نیز اگر اختلالِ ناشی از آن به اندازهٔ کافی مهم نباشد و امنیت دولت را تحت تأثیر قرار ندهد، در حیطهٔ بند ۴ مادهٔ ۲ قرار نخواهد گرفت. ازاین‌رو احتساب تمامی انواع عملیات سایبری به‌مثابهٔ توسل به زور، خروج از منطق حقوقی بند ۴ مادهٔ ۲ منشور خواهد بود.

۱. حملات سایبری با آستانه‌ای پایین‌تر از سطح توسل به زور

این واقعیت که حملات سایبریِ فاقد شدت لازم ولی مختل کننده یا حملات شدید سایبری که

زیرساخت‌های غیرحساس را مختل می‌کنند، نقض بند ۴ مادهٔ ۲ تلقی نمی‌شوند، به معنای مشروعیت آنها نیست. حملات مذکور را زمانی‌که قابلیت انتساب به یک دولت را داشته باشند، می‌توان به‌مثابهٔ نقض اصل عدم مداخله در امور داخلی دولت دیگر تلقی کرد (Tallinn Manual, 2013: Rule 10, 45). این قاعده صرفاً در روابط میان دولت‌ها قابل اجراست، برای مثال اگر یک شرکت خصوصی واقع در سرزمین یک دولت عملیات سایبری خصمانه‌ای را علیه زیرساخت‌های سایبری[1] دولت دیگر ترتیب دهد، چنین اقدامی را نمی‌توان به‌مثابهٔ نقض اصل عدم مداخله تلقی کرد، مگر اینکه اعمال شرکت مذکور را بتوان به موجب حقوق مسئولیت دولت، به دولت میزبان منتسب دانست.

هرچند اصل عدم مداخله در اصل تساوی حاکمیت دولت‌ها (بند ۱ مادهٔ ۲ منشور) مستتر است و از آن به‌طور ضمنی استنتاج می‌شود، اما منشور به‌صراحت ممنوعیت مداخلهٔ دولت‌ها در امور داخلی یکدیگر را مقرر نداشته است. با وجود این، در طول حیات این سازمان تعدادی از معاهدات و قطعنامه‌های مصوب این سازمان که مهم‌ترین آنها اعلامیهٔ روابط دوستانه است، بر این اصل تأکید کرده‌اند (Tallinn manual, 2013: p.46, rule 10, para.6). به‌نظر دیوان بین‌المللی دادگستری نیز اصل مذکور «بخشی از حقوق بین‌الملل عرفی است» (ICJ, Nicaragua Case, 1986, para.202). کمیسیون حقوق بین‌الملل سازمان ملل متحد نیز اصل مذکور را یک اصل مربوط به حقوق بین‌الملل عرفی دولت‌ها محسوب کرده است (ILC Declaration on Rights and Duties of states, 1949, art.3).

اگرچه هر مداخلهٔ سایبری به‌طور خودکار نقض حقوق بین‌الملل تلقی نمی‌شود و همان‌طورکه دیوان بین‌المللی دادگستری اشاره کرده است، «مداخله‌ای نامشروع است که با استفاده از روش‌های قهرآمیز صورت گیرد» (ICJ, Nicaragua Case, 1986, para.205)، با وجود این، صِرف قهری بودن روش مورد استفاده برای مداخله، برای اینکه آن را ناقض اصل عدم مداخله گرداند، کافی نیست. اجبار باید در ارتباط با موضوعی باشد که دولت قربانی آزادانهٔ حق تعیین و اعمال آن را دارد. به‌عبارت دیگر، عنصر صدمه به حقوق حاکمیتی دولتِ قربانی شاخص مشترک تمامی اشکال اقداماتی است که مداخله محسوب می‌شوند. همان‌طورکه دیوان بین‌المللی دادگستری در قضیهٔ نیکاراگوئه اظهار داشت، «مداخلهٔ ممنوع باید مربوط به اموری باشد که هر دولت به موجب اصل حاکمیت دولت مجاز است آزادانه در مورد آن تصمیم بگیرد»، مانند «انتخاب نظام سیاسی، اقتصادی، اجتماعی و فرهنگی، و تنظیم سیاست خارجی» (ICJ, Nicaragua Case, 1986: para.205). ازاین‌رو گروه کارشناسان تدوین‌کنندهٔ کتابچهٔ راهنمای تالین اتفاق نظر داشتند که هرچند به‌دلیل خصیصهٔ در حال تکامل و درهم‌تنیدهٔ روابط

۱. زیرساخت‌های سایبری شامل ارتباطات، ذخیره‌سازی، و منابع محاسباتی است که سیستم‌های اطلاعاتی براساس آنها عمل می‌کنند (Tallinn Manual, 2013: 258).

بین‌المللی، خطوط دقیقی برای ترسیم ممنوعیت مداخله وجود ندارد، با وجود این، مداخلهٔ منع‌شده دارای دو عنصر است: نخست، عمل مورد نظر باید با امور داخلی یا خارجی دولت قربانی مرتبط باشد؛ دوم، عمل مذکور ذاتاً قهری باشد (Tallinn manual, 2017: rule 66, para 6).

هرچند به‌طور سنتی، ارزیابی حقوقی مداخله در امور داخلی دولت‌ها از چشم‌انداز توسل به زور امکان‌پذیر است (Damrosch, 1989: 1-3) ، همان‌طورکه دیوان بین‌المللی دادگستری در قضیهٔ نیکاراگوئه متذکر شد، توسل به زور نمونهٔ بارز مداخلهٔ نامشروع است (ICJ, Nicaragua Case, 1986: para.205)، اما عکس آن صادق نیست و هر مداخلهٔ ممنوعی لزوماً توسل به زور محسوب نمی‌شود. بنابراین، با آنکه حقوق بین‌الملل عرفیِ مربوط به مداخله در حال حاضر تا حد چشمگیری در کنار ممنوعیت فراگیرتر توسل به زور در نظر گرفته می‌شود، مداخله هنوز مفهومی مجزاست (Jennings & Watts, 1992: 429). اعمالی با هدف تغییر رژیم مانند مداخلهٔ قهرآمیز سیاسی، اغلب به‌مثابهٔ نقض آشکار این اصل تلقی شده اند. مواردی مانند دستکاری سایبریِ انتخابات یا مهندسیِ افکار عمومی در آستانهٔ انتخابات، برای مثال در مواقعی که خدمات اخبار آنلاین به نفع حزب خاصی تغییر می‌کند، یا اخبار دروغ پخش می‌شود، یا سرویس های آنلاین یک حزب از کار می افتد، ضابطهٔ اجبار در هاله‌ای از ابهام است. بنابراین نمی‌توان تمامی اشکال مداخلهٔ سیاسی یا اقتصادی را به‌مثابهٔ نقض اصل عدم مداخله تلقی کرد (Tallinn manual,2013: p.47, rule 10, para 7). مداخله همچنین شامل وضعیت‌هایی است که در آن مداخلهٔ غیرسایبری در فعالیت های سایبری مربوط به امور داخلی و خارجی دولت دیگر صورت می‌گیرد. برای مثال می‌توان به مداخله با استفاده از ابزار غیرسایبریِ قهری توسط یک دولت برای وادار کردن دولت دیگر به وضع قانون داخلی در مورد مسئولیت ارائه‌دهندهٔ خدمات اینترنتی یا واداشتن آن به خودداری از عضویت در معاهدهٔ چندجانبهٔ مربوط به خلع سلاح سایبری[1] یا حقوق بشر، از طریق اینترنت و به‌نحو برخط،[2] اشاره کرد (Tallinn manual, 2017: rule 66, para.2).

به‌رغم عدم درج اصل ممنوعیت مداخلهٔ دولت‌ها در امور داخلی یکدیگر در منشور ملل متحد، اصل یادشده در موافقت‌نامه‌های بین‌المللیِ منطقه‌ای متعددی گنجانده شده است (OAS Charter, Art. 19; ASEAN, Art 2(2)(e); SCO, Art. 2). بند ۱ اعلامیهٔ ۱۹۶۵ مجمع عمومی سازمان ملل متحد در خصوص غیرقابل قبول بودن مداخله در امور داخلی دولت‌ها و حمایت از استقلال و حاکمیت آنها «مداخلهٔ مسلحانه و تمامی اشکال دیگر مداخله یا اقدام به تهدید علیه شخصیت دولت یا علیه عناصر سیاسی، اقتصادی و فرهنگی آن» را محکوم می‌کند. بند ۲ این سند نیز اعلام می‌دارد که «هیچ دولتی نمی‌تواند دولتی دیگر را به استفاده یا تشویق به استفاده

1. cyber disarmament.
2. Online.

از اقدامات اقتصادی، سیاسی یا هر گونه اقدام دیگری به‌منظور تحصیل تبعیت آن در اِعمال حقوق حاکمیتی‌اش یا تضمین کسب امتیازاتی از آن، از هر نوع، وادار کند» (GA Res. 2131 (XX), 1965: paras. 1, 2). زبان گسترده به‌کاررفته در این اعلامیه شامل حملات سایبری با آستانه‌ای کمتر از سطح توسل به زور نیز می‌شود. اعلامیهٔ نهایی کنفرانس هلسینکی نیز با به‌کارگیری زبان مشابهی در اصل ششم خود همهٔ اشکال مداخله را محکوم می‌کند (CSCE, 1975: 1294–5). بند ۴ قطعنامهٔ ۱۹۷۶ مجمع عمومی سازمان ملل متحد که «تمامی اشکال آشکار، ظریف، و تکنیک‌های بسیار پیچیدهٔ اجبار، براندازی و هتک حرمت با هدف اخلال در نظم سیاسی، اجتماعی یا اقتصادی سایر دولت‌ها یا بی‌ثبات‌سازی حکومت‌هایی که درصدد رها کردن اقتصاد خود از کنترل یا دست‌اندازی خارجی‌اند» را محکوم می‌کند نیز، قابل تعمیم به حملات سایبری است (GA Res. 31/91, 1976: para.4). مجمع عمومی سازمان کشورهای آمریکایی طی دو قطعنامهٔ مجزا اصل عدم مداخله را تأیید کرده است (AG/RES. 128; AG/RES.78). برخی وضعیت‌های احصاشده در اعلامیهٔ ۱۹۸۱ مجمع عمومی موسوم به اعلامیهٔ نایروبی در خصوص غیرقابل قبول بودن مداخله و دخالت در امور داخلی دولت‌ها نیز قابل انطباق با عملیات خاص سایبری‌اند. اعلامیه مذکور به‌طور خاص «حق دولت‌ها و ملت‌ها را بر دسترسی آزاد به اطلاعات و توسعهٔ کاملِ سیستم اطلاعات و رسانه‌های جمعی‌شان بدون مداخله، و استفاده از رسانه‌های اطلاعاتی‌شان به‌منظور پیشبرد منافع و آرمان‌های سیاسی، اجتماعی، اقتصادی و فرهنگی خود، از جمله براساس موادی از اعلامیهٔ جهانی حقوق بشر و اصول نظم نوین بین‌المللی اطلاعات» را یادآور می‌شود (GA Res.36/103, 1981: para. 2(I)(c)).

هرچند با بررسی اسناد موجود و رویهٔ دولت‌ها درمی‌یابیم که «شکافی جدی میان دیدگاه موسع در خصوص قاعدهٔ عدم مداخله و آنچه دولت‌ها در واقع انجام می‌دهند، وجود دارد» (Damrosch, 1989: 3) ، امکان تغییر دامنهٔ اصل مذکور صراحتاً توسط دیوان بین‌المللی دادگستری در قضیهٔ نیکاراگوئه تأیید کرده است (Nicaragua Case, 1986: paras.206-207).

با توجه به نظر دیوان حداقل به لحاظ نظری هیچ مشکلی برای تلقی حملات سایبریِ مختل‌کننده به‌مثابهٔ مداخلهٔ غیرقانونی در مواردی که برای واداشتن دولتی دیگر به تبعیت از آن در اِعمال حق حاکمیتش استفاده می‌شود، وجود ندارد، چه این مداخله در سطح توسل به زور یا کمتر از آن باشد (A/RES/25/2625, 1970: third principle) . در واقع، در قرن حاضر مفهوم مداخله به‌عنوان پیامد «افزایش همکاری‌های بین‌المللی میان دولت‌ها راه‌های بسیار ظریف‌تر و زیرکانه‌تری از مداخله، بدون استفاده از زور [فیزیکی] را، ممکن می‌سازد» که حملهٔ سایبری نیز یکی از آنهاست (Kunig, 2012: 290). ازاین‌رو تفسیر موسع از مداخلهٔ حملات سایبری را نیز در برمی‌گیرد که در حال حاضر با توجه به ارتباط درهم‌تنیده و اتکای جوامع مدرن به سیستم‌های

اطلاعاتی این‌گونه تفسیر ضروری می‌نماید. برای نمونه می‌توان بدافزار باج‌گیر "وناکرای[1]" را بررسی کرد، بدافزاری که اخیراً با بهره‌گیری از یک ضعف امنیتی در سیستم‌های عامل ویندوز وارد سیستم رایانهٔ قربانی شده و تاکنون اطلاعات صدها هزار سیستم متعلق به بیمارستان‌ها، بانک‌ها و سایر سازمان‌ها را در سرتاسر جهان رمزگذاری کرده است. عملکرد این بدافزار فراتر از بهره‌برداری سایبری[2] است، چراکه علاوه‌بر ورود غیرمجاز به سیستم رایانهٔ قربانی، با کدگذاری بر روی فایل‌های سیستم هدف، دامی تهاجمی پهن کرده و از مالک سیستم اخاذی می‌کند. اگر معلوم شود که بدافزار مذکور توسط یک دولت برای اجبار دولتی دیگر به تبعیت در اِعمال حق حاکمیتش استفاده شده، بی‌شک می‌توان بهره‌برداری از آن را به‌مثابهٔ مداخله در امور داخلی دولت دیگر تلقی کرد (UN NEWS Centre, 2017) . نمونهٔ دیگری که می‌توان در این زمینه ذکر کرد، وضعیتی است که در آن دولت "الف" که دارای دو زبان رسمی برای گروه‌های قومی اقلیت و اکثریت است تصمیم بگیرد یک همه‌پرسی برگزار کند که در آن تنها زبان اکثریت به‌عنوان زبان رسمی تلقی شود. اما دولت "ب" که زبان رسمی‌اش زبان اقلیت دولت "الف" است، در تلاش برای مجبور کردن دولت "الف" به معکوس کردن تصمیمش و حفظ وب‌سایت‌ها به دو زبان، مبادرت به حملهٔ محروم‌سازی از خدمات به وب‌سایت‌های کلیدیِ حکومتی دولت "الف" (البته فقط حمله به وب‌سایت‌هایی که به زبان اکثریت هستند، یا به صفحاتی با زبان اکثریت در سایت‌های دوزبانه) کند. از آنجا که سیاست زبانی هر دولت موضوعی مربوط به امور داخلی است، این حمله ماهیتاً اقدامی قهری در جهت مداخلهٔ ممنوعه محسوب می‌شود. به‌طور منطقی باید توجه داشت که اجبار باید دارای قابلیتی برای قانع کردن دولت قربانی به انجام عملی باشد که در صورت نبود آن قابلیت، اجبار واقع نمی‌شد.

نه‌تنها ممکن است حملات سایبریِ موجد سطح پایینی از اختلال، مداخلهٔ نامشروع تلقی شوند، بلکه می‌توان آن حملاتی که وب‌سایت‌ها را به‌منظور دامن زدن به نزاع داخلی در یک دولت از کار می‌اندازند یا به‌منظور تأثیرگذاری بر نتیجهٔ انتخابات در دولت دیگر هزاران ایمیل به رأی‌دهندگان ارسال می‌کنند را نیز، نمونه‌ای از مداخلهٔ ممنوعه تلقی کرد. برای مثال، در سپتامبر ۲۰۱۲ جمهوری آذربایجان حملات سایبری گروه موسوم به "ارتش سایبر ارمنستان" را که تحت "هدایت و کنترل" دولت ارمنستان اقدامات تروریستی را مورد تمجید قرار داده و به قربانیان اقدامات تروریستی اهانت کرده و همچنین درصدد تحریک نفرت قومی و مذهبی، تبعیض و خشونت بود را، تقبیح کرد (UN Doc. A/66/897–S/2012/687, 2012: para. 1). شایان ذکر است که تبلیغات خصمانه در اعلامیه‌های مجمع عمومی، ۱۹۷۶ (A/RES/31/91, 14 December 1976, para. 4) و ۱۹۸۱ (A/RES/36/103,

1. WannaCry.
2. Cyber exploitation.

1981: para. 2(II)(j)) به‌ترتیب در مورد عدم مداخله و غیرقابل قبول بودن مداخله در امور داخلی دولت‌ها، محکوم شده است.

۲. بهره‌برداری سایبری

بهره‌برداری سایبری مشتمل بر اقدامات یا عملیاتی است که ممکن است در یک دورهٔ زمانی طولانی برای به‌دست آوردن اطلاعات محرمانهٔ موجود در سیستم‌های رایانه‌ای یا در حال عبور از سیستم‌های مذکور یا شبکه‌های دشمن استمرار داشته باشد. بهره‌برداری سایبری معمولاً مخفیانه و با کوچک‌ترین مداخلهٔ ممکن برای استخراج اطلاعات مورد نظر صورت می‌گیرد (Lin, 2010: 63). واژه‌نامهٔ ناتو بهره‌برداری سایبری را به‌صورت مبهم‌تر و به‌مثابهٔ «اقدام به استفاده از رایانه یا شبکهٔ رایانه‌ای، و همچنین اطلاعاتی که توسط آنها به‌منظور کسب مزیت، میزبانی می‌شوند»، تعریف کرده است (NATO Glossary of Terms and Definitions, 2013: 2–C–11) فصل مشترک تعاریف مذکور دسترسی‌های غیرمجاز به رایانه‌ها، سیستم‌های رایانه‌ای یا شبکه‌های دیگر به‌منظور برداشتن مخفیانهٔ اطلاعات، بدون تأثیر بر یا بدون تحریف، اصلاح یا حذف داده‌ها یا عملکرد سیستمی است که دسترسی به آن ایجاد شده است. ازاین‌رو عملیات مذکور را نمی‌توان توسل به زور به موجب بند ۴ مادهٔ ۲ منشور ملل متحد تلقی کرد. اگرچه مبانی فنی و ملاحظات عملیاتی این دو با هم شباهت‌هایی دارند و برای تحقق حملات سایبری و استثمار سایبری وجود آسیب‌پذیری، دسترسی به آسیب‌پذیری مذکور، و محموله‌ای برای اجرای آن ضروری است، با این حال تفاوت عمدهٔ فنی میان حملهٔ سایبری و بهره‌برداری سایبری در سرشت محموله‌ای است که اجرا می‌شود؛ محمولهٔ حملهٔ سایبری مختل‌کننده است، درحالی‌که محمولهٔ بهره‌برداری سایبری اطلاعات را بدون ایجاد اختلال در سیستم هدف جمع‌آوری می‌کند. به‌علاوه، به این دلیل که بهره‌برداری سایبری نباید آشکارا صورت گیرد، عملیات سایبری مذکور نیز باید به کمترین حد ممکن وضعیت طبیعی رایانهٔ مورد نظر را بر هم زند، به‌عبارت دیگر، جمع‌آوری اطلاعات نیازمند توانایی برای پنهان کردن حضور بر روی رایانه یا شبکهٔ دشمن است (Lin, 2010: 63). عملیات بهره‌برداری سایبری بر جمع‌آوری اطلاعات، نظارت و شناسایی متمرکز است نه ایجاد اختلال در سیستم و می‌تواند مقدمه‌ای برای یک حملهٔ فیزیکی- حرکتی یا سایبری باشد که مهاجم را به‌واسطهٔ نقشه‌برداری از معماری شبکه یا سیستم عامل یا به‌واسطهٔ شناسایی آسیب‌پذیری‌های ناشناخته، قادر به حمله می‌سازد.

برخی از عملیات بهره‌برداری سایبری از اشکال امروزی شناسایی یا جاسوسی نظامی‌اند. شایان یادآوری است که اگرچه جاسوسی در حقوق داخلی کشورها جرم‌انگاری شده، به موجب مقررات بین‌المللی منع نشده است (Dinstein, 2002:101). عملیات جاسوسی سایبری و بهره‌برداری سایبری فاقد عامل اجبار است و ناقض اصل عدم مداخله به‌شمار نمی‌آید. نفوذ صرف در

سیستم‌های دولت دیگر اصل عدم مداخله را نقض نمی‌کند. به نظر گروه بین‌المللی کارشناسان این رویکرد حتی در مواردی که چنین نفوذی نیاز به شکستن موانع محافظ مجازی دارد (برای مثال شکستن فایروال یا کرک[1] رمز عبور)، صادق است. (Tallinn manual, 2013: 47, rule 10, para 8).

بعید به‌نظر می‌رسد که دولت‌های قربانی، دستیابی و سرقت اطلاعات را به‌منزلهٔ توسل به زور تلقی کنند، با وجود این، عملیات بهره‌برداری سایبری در مواقعی که مستلزم نفوذ غیرمجاز به زیرساخت‌های سایبری (چه دولتی و چه خصوصی) واقع در دولت دیگری باشد، می‌تواند نقض حاکمیت دولتِ هدف تلقی شود (Heinegg, 2013: 129). هرچند این اقدام را نمی‌توان توسل به زور تلقی کرد و برخی آن را حتی مداخله با شدتی کمتر از توسل به زور نیز نمی‌دانند، چراکه آن را فاقد عامل اجبار می‌پندارند (Woltag, 2012: 989)، باید گفت از منظر حقوق بین‌الملل، هر عملی که بتوان آن را ناقض حاکمیت دولت هدف محسوب کرد، لزوماً عملی است که بدون رضایت آن دولت انجام گرفته است و در نتیجه، عملیاتی قهری محسوب خواهد شد. حتی به‌نظر گروه کارشناسان تدوین‌کنندهٔ کتابچهٔ راهنمای تالین (۲۰۱۷)، هرچند اقداماتی مانند غیرفعال کردن سازوکار امنیتی سایبری به‌منظور پایش ضربات وارده بر صفحه کلید با وجود تهاجمی بودن آن، از مصادیق توسل به زور تلقی نمی‌شود، اقدام به جاسوسی سایبری را نمی‌توان به‌طور کلی خارج از حوزهٔ توسل به زور تلقی کرد. برای مثال نمی‌توان در مورد استفاده از ابزار سایبری برای وارد کردن آسیب به زیرساخت های سایبری که در نتیجهٔ پنهان کردن یک نقص فنیِ ناشی از بهره‌برداری سایبری از زیرساخت های مذکور صورت گرفته، با قاطعیت اظهارنظر کرد ((Tallinn manual, 2017: rule 69, para 9(d)). با این حال در مواردی که بهره‌برداری سایبری در امتداد طیف گسترده‌ای از عملیات سایبری صورت می گیرد، وضعیت برای تعیین اینکه آیا اصل عدم مداخله نقض شده است، پیچیده‌تر می شود، به‌خصوص تعیین اینکه آیا عنصر اجبار محقق شده، به اوضاع و احوال خاص هر قضیه بستگی دارد (Tallinn manual, 2013: 47, rule 10, para 9).

همان‌طورکه اشاره شد، مشکل عمده در خصوص بهره‌برداری سایبری آن است که نرم‌افزارهایی که برای بهره‌برداری استفاده می‌شوند، اغلب کاربرد دوگانه دارند، به این معنا که آنها را می‌توان هم برای سرقت اطلاعات یا حملهٔ مختل‌کننده یا غیر آن، به‌کار برد. حتی کُد نرم‌افزاری که در ابتدا برای جمع‌آوری اطلاعات به‌کار می‌رفت، ممکن است طی برنامه‌ریزی بعدی، متعاقباً به عامل مختل‌کننده تبدل شود. با این حال، مشکل کاربرد دوگانه، خاص فضای سایبر نیست و در زمینهٔ خلع سلاح و در مواردی که به سازوکارهای تأیید و کنترل پرداخته می‌شود، به‌خوبی شناخته شده است.

---

۱. کرَک کردنِ (Crack) نرم‌افزار یعنی ایجاد تغییر در نرم‌افزار به‌منظور غیرفعال کردن روش‌ها و ابزارهای حفاظتی آن نرم‌افزار یا سیستم.

نتیجه‌گیری

برخی مدعی شده‌اند که حقوق بین‌الملل کنونی به‌خوبی از عهدهٔ قانونمندسازی اقدامات غیرحرکتی- غیرفیزیکی برنمی‌آید و احتمالاً "یک معماری هنجاری جدید" برای اعمال در چنین مواردی ضرورت دارد (Schmitt, 1999: 914-915). برخی صاحب‌نظران معتقدند که حقوق توسل به زور به‌حد کافی خود را با انواع شیوه‌ها و ابزارهای جدید جنگی انطباق داده است. یکی از وضعیت‌های چالش‌برانگیز، حملهٔ سایبری است که در محیطی خاص و غیرطبیعی واقع می‌شود که وجود فیزیکی ندارد و در عین حال می‌تواند هم موجب خسارات فیزیکی (سخت‌افزاری) و هم خسارات غیرمادی (نرم‌افزاری) شود. باید توجه داشت که اگرچه حقوق توسل به زور به‌صراحت حملات سایبری را نظم نبخشیده است، با وجود این، هنوز می‌تواند در آن حوزه به‌مثابهٔ «یک مدل برای ایجاد قواعدی جدید» به‌کار آید (Brown, 2006: 183). مخرج مشترک تمامی نظریه‌های موجود در این زمینه آن است که «اگر توسل به زور به‌گونه‌ای ایستا تعریف شود، ممنوعیت‌های موجود در آن به‌تدریج آثار مطلوب خود را به شیوه‌ای که تدوین‌کنندگان منشور در نظر داشته‌اند، از دست خواهد داد» (Bond, 1996: 29). ازاین‌رو برآنیم که در فقدان یک معاهدهٔ بین‌المللی خاص در مورد عملیات سایبری که انعقاد آن حداقل در کوتاه‌مدت بعید است، بی‌تردید هر حملهٔ سایبری که به ایراد خسارات فیزیکی به اموال یا سلب حیات یا صدمه به افراد منجر می‌شود یا به‌طور منطقی به احتمال زیاد دارای چنین آثاری خواهد بود، تحت شمول ممنوعیت مندرج در بند ۴ مادهٔ ۲ منشور ملل متحد قرار خواهد گرفت. از سوی دیگر، عملیات سایبری مختل‌کننده که دربرگیرندهٔ خسارات فیزیکی نیستند، درصورتی‌که اختلال ناشی از آنها به اندازهٔ کافی مهم باشد، می‌توان آنها را تحت شمول بند ۴ مادهٔ ۲ منشور قرار داد. با این اوصاف، هرچند حملات سایبریِ فاقد شدت ولی مختل‌کننده یا حملات سایبری شدید که زیرساخت‌های غیرحساس را مختل می‌کنند، نقض بند ۴ مادهٔ ۲ منشور تلقی نمی‌شوند، ولی این به معنای قانونی بودن آنها نیست. حملات مذکور درصورتی‌که به یک دولت قابل انتساب باشند، می‌توانند به‌عنوان نقض اصل عدم مداخله در امور داخلی دولت دیگر محسوب شوند.

منابع

A) Books

1. Brownlie, Ian (1963). *International law and the Use of force by state*, Oxford, Oxford University Press.
2. Harris, D.J.,(2004). *Cases and Materials on International Law*, 6th edn, London, sweet & Maxwell.
3. Harrison Dinniss, Heather (2012). *Cyber Warfare and the Laws of War*,

Cambridge, Cambridge University Press.
4. Henckaerts, Jean-Marie., Doswald-Beck, Louise (2005).*Customary International Humanitarian Law*, Vol.I, New York, Cambridge University Press.Owens, William A. Dam, Kenneth W. and Lin, Herbert S. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, The National Academies Press.

B) Articles

5. Brown, D. (2006). "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*"*, *Harvard International Law Journal*, Vol**.** 47, No. 1, pp. 179-221.
6. DeLuca, Christopher D. (2013). "The Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors", *Pace International Law Review*, Vol. 3, No. 9 <http://digitalcommons.pace.edu/pilronline/34/> (15 December 2016).
7. Dinstein, Yoram (2002). "Computer Network Attacks and Self-Defense", *International Law Studies*», Vol.76, pp 99–121.
8. Farer,Tom J. (1985). "Political and Economic Coercion in Contemporary International Law", *American Journal of International Law*, Vol. 79, No. 2, PP. 405-408.
9. Gordon, Edward (1985). "Article 2(4) in Historical Context", *Yale Journal of International Law*, Vol. 10, No.2, pp. 271-278.
10. Hathaway, Oona A., Crootof , Rebecca., Levitz ,Philip., Nix, Haley., Nowlan, Aileen., Perdue, William., Julia Spiegel, Julia. (2012). "The Law of Cyber-Attack", *California Law Review*, Vol.100, No.4, 817-885.
11. Hollis, Duncan B. (2007). "Why States Need an International Law for Information Operations", *Lewis Clark Law Review*, Vol. 11, No.4, pp.1023-1061.
12. Kunig, *Philip*, (2012). "Intervention, Prohibition of", *Max Planck Encyclopedia of Public International Law*, Vol VI, PP. 289-300.
13. Lin, Herbert S.(2010). " Offensive Cyber Operations and the Use of Force", *Journal of National Security Law and Policy*, Vol. 4, No.63, pp. 63-86.
14. Randelzhofer, A., Dörr, O. (2012). "Article 2 (4)", in: *The Charter of the United Nations: A Commentary*, Simma, Bruno, Khan, Daniel-Erasmus, Nolte, Georg and Paulus, Andreas (eds), Oxford, *Oxford University Press*, Vol. I, pp. 118-213.
15. Schmitt, M. (1999). "Computer network attack and use of force in international law", *Columbia Journal of Transnational Law*, Vol.37, 885-937.
16. Sklerov, Matthew J. (2009). "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent", *Military Law Review*, Vol. 201, pp 1–85.
17. Segura-Serrano, Antonio (2006). "Internet Regulation and the Role of

International Law", *Max Planck Yearbook of United Nations Law*, Vol. 10, pp. 191–272.
18. Tsagourias, Nicholas (2012). "Cyber Attacks, Self-Defence and the Problem of Attribution", *Journal of Conflict and Security Law*, Vol. 17, No. 2, pp. 229–44.
19. Waxman, Matthew C (2011). "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", *Yale Journal of International Law*, Vol. 36, No.2, pp. 420–58.
20. Waxman, Matthew C. (2011). "Cyber Attacks as "Force" under UN Charter Article 2(4)", *International Law Studies*, Vol. 87, No.2 , pp. 43-57.
21. Waxman, Matthew C. (2013). "Self-Defensive Force against Cyber Attacks: Legal", *Strategic and Political Dimensions*, International Law Studies, Vol. 89, pp 108–22.
22. Woltag, Johann-Christoph. (2011). "Computer Network Operations below the Level of Armed Force"**,** *European Society of International Law Conference Paper Series*, No.1, PP. 1-18.
23. Ziolkowski, Katharina (2010). "Computer Network Operations and the Law of Armed Conflict", *Military Law and the Law of War Review*, Vol. 49, pp 47–94.

C) Documents

24. Australian Government, Cyber Security Strategy, (2009).
25. Creation of a global culture of cybersecurity and the protection of critical information infrastructures, UN Doc. A/RES/58/199, 2004.
26. Definition of Aggression, UN Doc. A/RES/29/3314, 1974.
27. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, UN Doc. A/RES/2131 (XX), 1965.
28. European Commission (2005). Communication from the Commission to the Council and the European Parliament—Critical Infrastructure Protection in the fight against terrorism.
29. Helsinki Final Act of the Conference on Security and Co-operation in Europe (CSCE), (1975).
30. HPCR (2013). *Manual on International Law Applicable to Air and Missile Warfare*, produced by the Program on Humanitarian Policy and Conflict Research at Harvard University, Cambridge, Cambridge University Press.
31. International Law Commission, *Declaration on Rights and Duties of States*, annexed to GA Res. 375 (IV), 6 December 1949, Art. 3.
32. NATO Glossary of Terms and Definitions, (2013).
33. Montevideo Convention on the Rights and Duties of States, (1933).
34. Report of Special Committee on Defining Aggression, UN General Assembly, 25th Session, Official Records, 13 July- 14 August, 1970, Sup. 19, A/8019, p.60.
35. Report of the Independent Fact-Finding Mission on the Conflict in Georgia (2009). Vol II.
36. 2013 Report of the United Nations Group of Governmental Experts (UN GGE)

on Developments in the Field of Information and Telecommunications in the Context of International Security Recalls, UN.
37. Doc A/64/129/Add.1, 2013.
38. Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge, Cambridge University Press.
39.Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare (2017). prepared by 39.the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge, Cambridge University Press.
40. United States Patriot Act (2001).
41. Vienna Convention on the Law of Treaties (1969).

D) votes

42. Fisheries Jurisdiction (Spain v Canada), Judgment of 4 December 1998, ICJ Reports 1998.
Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, ICJ Reports 1996.
43. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US), Merits, Judgment of 27 June 1986, ICJ Reports 1986.

E) other reference

44. Melzer, Nils (2011). Cyberwarfare and International Law, UNIDIR.
45. Sklerov, M. (2009). Solving the Dilemma of State Responses to Cyberattacks: A justification for the use of active Defenses against States Who Neglect Their Duty to Prevent, Master's Thesis, The Judge Advocate General's School, USA.
46. Koh, Harold(2012). 'International Law in Cyberspace', Speech at the USCYBERCOM Inter-Agency Legal Conference, <http://www.state.gov/documents/organization/ 211955. Pdf>.