فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۴۸، شمارهٔ ۳، پاییز ۱۳۹۷: ۶۹۷-۷۱۳

جنگ سایبری و توسعهٔ حقوق بین‌الملل منع توسل به زور

مسعود رضائی[۱]*، محمود جلالی[۲]

چکیده

استفاده از فضای سایبری برای دستیابی سریع و مؤثر به اهداف راهبردی، امروزه به ابزار جدید جنگی و مهم برای همهٔ بازیگران دولتی و غیردولتی تبدیل شده است. به همین سبب، ماهیت توزیعی و تعاملیِ فضای سایبری، به‌همراه هزینهٔ پایین ابزارهای پاسخگویی، عملکرد مؤثر و حملهٔ در فضای مجازی را افزایش داده است. به‌علاوه، گمنامی در این فضا، هماهنگی عملیاتیِ سریعی را در محدودهٔ جغرافیاییِ وسیعی تسهیل کرده و به وقوع حمله، تخریب و جرائمی در این فضا منجر شده که امنیت ملی و تمامیت ارضی کشورها را نقض کرده و در غیاب قواعد و قوانین حقوقیِ کارامد، مسئولیت بین‌المللیِ این جرائم و پیگیری حقوقیِ این حملات را در هاله‌ای از ابهام قرار داده است. ازاین‌رو مقالهٔ حاضر با بررسی و تفاسیر تعاریف حملات سایبری و همچنین شبیه‌سازی این رویداد، بر این موضوع تأکید می‌کند که اگرچه در شرایط کنونی استفاده از حملات سایبری به‌مثابهٔ توسل به زور در حقوق بین‌الملل مورد بحث و گمانه‌زنی است، لکن شناساییِ قلمرو حقوقیِ آن نیز با موانعی در شرایط مختلف و از جمله حقوق جنگ، توسل به زور و حق دفاع مشروع روبه‌روست که ورود حقوق بین‌الملل به بحث را با چالش مواجه کرده است.

کلیدواژگان

توسل به‌زور، حملات سایبری، حقوق بین‌الملل، دفاع مشروع، منشور ملل متحد.

۱. دانش‌آموخته دکتری روابط بین‌الملل، دانشگاه آزاد اسلامی، واحد اصفهان (نویسندهٔ مسئول).
تلفن: ۰۹۱۹۸۰۴۷۷۹۵ Email: msd.rezaei@yahoo.com
۲. دانشیار، دانشکدهٔ علوم اداری و اقتصاد، گروه حقوق، دانشگاه اصفهان، اصفهان.
تاریخ دریافت: ۱۳۹۴/۰۷/۱۸، تاریخ پذیرش: ۱۳۹۵/۰۴/۲۱

مقدمه

با توجه به رشد روزافزون کاربران فضای مجازی و عدم شناسایی کاربران در این محیط، و همچنین حرکت جهان به سمت استفادهٔ فراگیر از فناوری سایبری در کنار دیگر ویژگی‌های این قلمرو، عملاً زمینهٔ رقابت‌های دوطرفه و حتی چندگانه از زمین، هوا، دریا و حتی فضا، به سمت عرصهٔ پنجم رقابت یعنی قلمرو فضای سایبر سوق پیدا کرده است. ازاین‌رو بررسی حقوقیِ جنگ سایبری در این صورت اهمیت مضاعف یافته است. به‌دلیلِ همین اهمیت اساسیِ فضای سایبری در جامعهٔ مدرن، و نظر به آنکه همهٔ کشورها به توسعهٔ توانمندی‌های خود برای استفاده یا مبارزه در این فضا ادامه می‌دهند، کشورها بیش از پیش در معرض تهدید قرار گرفته‌اند. بنابراین فضای سایبری به ابزاری برای درگیری و مناقشه تبدیل شده است که هم بازیگران دولتی و هم کنشگران غیردولتی را در برمی‌گیرد. به همین سبب، گمانه‌ها در این خصوص بیشتر شده است که با توسعهٔ روزافزون علوم و فناوری فضای سایبری، این قلمرو نیز نیازمند چارچوب‌ها و قواعد حقوقی منسجم است. می‌دانیم که در تحلیل حقوقیِ جنگ یا حملات در فضای سایبری، پرداختن به موضوعات متعددی از اصول و قواعد حقوق بین‌الملل همچون بحث «شناسایی و انتساب» در حملات سایبری، «مسئولیت بین‌المللی دولت‌ها، اشخاص خصوصی و ارگان‌ها»، «اصل تناسب و اقدام متقابل»، «جبران خسارت»، «حق دفاع مشروع» و مباحثی از این دست نیز موضوعیت دارد و باید بررسی شود؛ با این حال، در این مقاله با فرضِ «دولتی بودنِ» وقوع جنگ در قلمرو فضای سایبری، مشخصاً بحث حقوقی «توسل به زور»[1] بررسی و تحلیل خواهد شد.

امروزه حقوق حاکم در زمینهٔ توسل به زور براساس بند ۴ مادهٔ ۲ منشور ملل متحد شکل گرفته است. البته در منشور ملل متحد تعریف دقیقی از آنچه توسل به زور به‌شمار می‌آید، ارائه نشده است. از همین رو تلاش‌ها برای تعریف حملات سایبری براساس این بند منشور بیشتر سبب دست‌وپاگیر شدن برداشت‌های سنتی از توسل به زور شده است. واکاویِ این موضوع که آیا حملات سایبری در حقوق جنگ[2] ـ بخشی از حقوق بین‌الملل که بر توسل به‌زور به‌عنوان ابزار سیاست داخلی حاکم است ـ قابل پذیرش و بررسی است یا خیر، در منابعی مانند ممنوعیت مطروحه در منشور ملل متحد (بند ۴ مادهٔ ۲)، شمای کلی امنیتی بخش هفتم این منشور، حق ذاتی دفاع از خود که در مادهٔ ۵۱ به آن اشاره شده و همچنین حقوق بین‌الملل عرفی که توسط رفتار مستمر دولت‌ها ایجاد شده، قابل جست‌وجو و ارزیابی است. بدین‌منظور، مقالهٔ حاضر، نخست با شبیه‌سازیِ بحث، قواعد و معاهدات حقوقیِ بین‌المللی مرتبط با موضوع

1. Use of force
2. Jus ad Bellum

را جست‌وجو و در نهایت امکانِ انطباق این موارد را با عنایت به اصل توسل به زور و حق دفاع مشروع مورد واکاوی و تتبع قرار خواهد داد.

چارچوب مفهومی

حقوق بین‌الملل نیز همچون سایر علوم در معرض آثار مثبت و منفی پیشرفت فناوری قرار دارد و برای انطباق خود با شرایط نوین، ناگزیر است به تعدیل، خلق و گاه انطباق قواعد موجود با زمینه‌های جدید بپردازد. چه‌بسا این سه گونه واکنش به‌صورت همزمان و در یک ظرف زمانی - که به تثبیت قواعدی حداقلی در زمینه‌های جدید منجر می‌شود - عمل کند. بی‌شک چالش‌های جدیدی که روزبه‌روز در مقابل حقوق بین‌الملل قرار می‌گیرند، همواره ظرفیت‌های این علم را محک زده و به شکوفایی گستره‌ای جدید در چشم‌انداز منابع و ابزارهای تفسیر منجر شده‌اند. فضای سایبر نیز از جمله چالش‌های اخیر حقوق بین‌الملل قلمداد می‌شود که پرسش‌های بنیادینی را در مقابلِ حقوقدانان بین‌المللی قرار داده است. همان‌گونه‌که اشاره شد، فضای مجازی، در آغاز به‌عنوان فضایی کاملاً مجزا از جهان فیزیکی انگاشته می‌شد. برخی نظریه‌پردازان تا آنجا پیش رفتند که ادعا می‌کردند فضای سایبری مرزهای جغرافیایی و ملی را در هم می‌نوردد، و در نتیجه مفاهیم سنتی حاکمیت و امنیت را با چالش مواجه می‌کند. با این حال، فضای سایبری اساساً یک محیط فیزیکی است، که با اتصال سیستم‌ها و شبکه‌های فیزیکی ایجاد شده و با اصول تعیین‌شده در نرم‌افزارها و پروتکل‌های ارتباطی مدیریت می‌شود که همگیِ آنها در مرزهای قدرتمند دولت- ملت‌ها قرار گرفته‌اند. امروزه غالب حقوقدانان بین‌المللی بر این باورند که فضای سایبر «منطقه‌ای خارج از حیطهٔ حقوق»[1] نیست و کسی نمی‌تواند در آن به فعالیت‌های خصمانه مبادرت ورزد؛ بدون اینکه دچار محدودیتی بوده یا از حیطهٔ حقوق و قانون خارج باشد (Hongju Koh,2012)؛ چراکه حقوق بین‌الملل، پیش از این نیز با نوآوری‌های جدید در عرصهٔ علمی مواجه شده و آن حوزه‌ها را نیز تحت قواعد و چارچوب‌های مربوطه درآورده است.

بی‌شک کلید دستیابی به امنیت بیشتر، تعیین مجازات برای اعمال خصمانه در فضای سایبری است. اما می‌دانیم که بزرگ‌ترین ضعف موجود در مقابل جنگ‌های سایبری، عدم ظرفیت حقوقیِ تعریف‌شده و واکنش مناسب به این‌گونه اقدامات خصمانه بوده است. بدان‌معنا که تاکنون حقوق بین‌الملل یا بی‌تفاوت بوده است یا ناتوان. مسئله عبارت است از شناسایی و رسمیت یافتن آن دسته از قواعد و اقدامات حقوقی که بتوانند انگیزهٔ حملات سایبری یا جاسوسی سایبری را کاهش دهند تا بدین‌ترتیب امنیت سایبری در عرصهٔ جهانی محقق شود. اقدامات خصمانهٔ سایبری باید

1. law-free zone

متضمن مجازات‌های سیاسی و حقوقی بوده و حتی حق دفاع مشروع نظامی را نیز در پی داشته باشد. هنجارهای ضمنی رفتارهای دولت‌ها (برگرفته از رویه‌های بین‌المللی) می‌توانند این اقدامات خصمانه را کاهش دهند، اما این هنجارهای ضمنی برای تضمین امنیت بین‌المللی ناکافی به‌نظر می‌رسند؛ موضوعی که یکی از دلایل عدم تمایل قدرت‌های بزرگ در شناساییِ حقوقیِ اقدامات خرابکارانه یا حملات در فضای سایبری نیز به‌شمار می‌رود. از همین رو و با عنایت به چنین کاستی‌هایی در سطح بین‌الملل شاهد بروز تحولاتی در قالب وقوع جنگ و توسل به زور با روش‌های متفاوتیم و این موضوع با پیشرفت فناوری و شیوه‌های نوین جنگ و درگیری (همچون حملات هواپیماهای بدون سرنشین، جنگ‌های سایبری یا در آینده جنگ‌های رباتیک)، خلأ حقوقی خود را بیش از پیش نشان می‌دهند.

با وجود پیشرفت‌های بسیار در پرداختن به مقولهٔ امنیت فضای مجازی، حکومت‌ها و ارتش‌ها اغلب نمی‌توانند در مورد نحوهٔ تفکرشان دربارهٔ فضای مجازی به توافق برسند، چه برسد به اینکه بتوانند در مورد قواعد حقوقی حاکم یا عمل به آن موافقت، و راهکاری مشترک ارائه کنند. همکاری بین‌المللی نیز به همین ترتیب با موانعی روبه‌روست. طرز تفکر جامعهٔ بین‌المللی در مورد فضای مجازی از بسیاری لحاظ شبیه طرز فکر اواخر دههٔ ۱۹۴۰ در مورد سلاح‌های هسته‌ای است. این موضوع که بُعد جدید و قابل توجهی از جنگ ظهور و بروز یافته، مورد پذیرش همگانی است، اما مفاهیم بنیادینی همچون مسئولیت بین‌المللیِ این جنگ و موضوعیت ابعاد حقوقیِ این مهم نیز باید تعریف، ترویج و مورد شناساییِ اکثریت جامعهٔ جهانی واقع شود. اما در این شرایط، تنها می‌توان به قواعد حقوقیِ موجود اکتفا کرد و از این چارچوب‌های قانونیِ بهره گرفت. به‌طور مثال، در بند ۴ مادهٔ ۲ منشور، اهمیت و جایگاه ویژه‌ای برای اصل ممنوعیت کاربرد زور در روابط بین‌الملل لحاظ شده است و امروزه این اصل به‌صورت یک قاعدهٔ آمرهٔ بین‌المللی شناخته می‌شود. هرچند در منشور به‌جای واژهٔ جنگ، «کاربرد زور» آمده، اما مادهٔ ۲ و بند ۴ آن، توسل به‌زور را مغایر اهداف منشور ملل متحد شناخته است که در موضوع مورد بحث قابلیت سرایت دارد و در پی آن مادهٔ ۵۱ و حق دفاع مشروع نیز مطرح و پیچیدگی‌های آن مطمح‌نظر خواهد بود.

شبیه‌سازیِ حملهٔ سایبری در حقوق بین‌الملل

شبیه‌سازی تحولات اساساً یکی از روش‌های جدید در عرصهٔ روابط بین‌الملل، حقوق بین‌الملل و عرصهٔ دیپلماسی است که به‌منظور تربیت حرفه‌ای کارشناسان و متخصصان استفاده می‌شود تا هنگام مواجهه با مسائل و قضایای عملی، در پرتو پژوهش‌های پیشین و تجربه‌های به‌دست‌آمده از طریق اجرای برنامه‌های شبیه‌سازی، بتوانند به‌صورت موفق از عهدهٔ فهم مسائل برآیند و معادلات حقوقی و دیپلماتیک را به‌نحوی مؤثر به نفع منافع ملی خود هدایت کنند. امروزه

تأکید بر استفاده از این روش بیشتر از آن جهت واجد اهمیت است که نظریه‌پردازان و متخصصان روابط بین‌الملل و حقوق بین‌الملل، استفاده از بازی‌های سیاسی برای تصدیق فرضیات مربوط به جهان واقعی را ضروری می‌دانند. بنابراین، روش شبیه‌سازی در حل بحران‌هایِ حقوقیِ بین‌المللی، مؤثرترین شیوه برای یافتن مهارت در حوزهٔ حقوق بین‌الملل قلمداد می‌شود. حال نظر به آنکه در یک قرن گذشته، بیشتر جنگ‌افروزی‌ها در عرصهٔ جهانی با تلاش برای ایجاد حقانیت و اجماع جهانی و براساس ملاحظات حقوق بین‌الملل توجیه و استفاده شده‌اند، شبیه‌سازی مسائل مربوط به جنگ و حقوق بین‌الملل نیز در این چارچوب قابل تأمل و موضوعیت می‌یابد (رضائی، ۱۳۹۵: ۵). بر این اساس، اشاره شد که فضای سایبری محیط منحصربه‌فردی نیست. رفتار دولت‌ها در این فضا می‌تواند همچون رفتارشان در هر جای دیگر باشد. در فضای سایبری نمی‌توان دست به خلع سلاح زد و اجماع جهانی در خصوص تعریف و دامنهٔ حقوقیِ حملهٔ سایبری وجود ندارد. ازاین‌رو ما وارد دوره‌ای از رقابت پایدار و سطح پایین برای نفوذ شده‌ایم که در آن محاسبات و تفاسیر اشتباهِ رقبا می‌تواند برای همه مخاطره‌آمیز باشد (Lewis,2013). از همین رو شبیه‌سازیِ حملهٔ سایبری در حقوق بین‌الملل به درک بهتر ما در این خصوص کمک می‌کند:

۱. قیاس با جنگ هسته‌ای

مجمع عمومی ملل متحد در سال ۱۹۹۴ از دیوان بین‌المللی دادگستری تقاضای نظریهٔ مشورتی کرده و سؤال کرد که آیا تهدید یا استفاده از سلاح‌های هسته‌ای مشروعیت دارد یا خیر؟ دیوان نیز گفت که تهدید یا استفاده از سلاح‌های هسته‌ای «عموماً مغایر با قواعد حقوق بین‌الملل قابل اعمال در مخاصمات مسلحانه و بالأخص اصول و قواعد حقوق بشردوستانه است». اما «از منظر حقوق بین‌الملل موجود و مشخصه‌های واقعی تحت لوای آن، دادگاه نمی‌تواند قاطعانه نتیجه‌گیری کند که تهدید یا استفاده از سلاح‌های هسته‌ای در شرایط دفاع مشروع که در آن بقای یک کشور در معرض نابودی باشد، قانونی است یا خیر». در ادامه نیز دیوان اظهار داشت که اصول و قواعد حقوقی قابل اعمال در مخاصمات مسلحانه - که در قلب آن توجه اصلی به بشریت است - عملیات مسلحانه را مقید به شماری از الزامات مضیق می‌کند. بنابراین روش‌ها و وسایل جنگی که تمایز میان نظامیان و غیرنظامیان را غیرممکن می‌سازد یا منجر به درد و رنج بیهوده‌ای به نظامیان می‌شود، ممنوع است (Nuclear Weapons Advisory Opinion 95, at 32, 35 I.L.M. at 829). با توجه به ماهیت منحصربه‌فرد سلاح‌های هسته‌ای که دادگاه در بالا به آن اشاره کرد، در حقیقت استفاده از چنین سلاح‌هایی به‌سختی قابل انطباق با چنین ضرورت‌هایی است. چنانکه مشاهده شد، بعضی آثار سلاح‌های هسته‌ای می‌تواند با آثار بدترین نوع حملات سایبری مشابه باشد. حملات سایبری در مقیاس استونی، همچون

جنگ هسته‌ای، میان مبارزان و غیرنظامیان تفکیک قائل نشد و اصل تناسب را نیز رعایت نکرد. به‌نظر می‌رسد متجاوزان سایبری ممکن است پایگاه‌های غیرنظامی را به‌طور خاص هدف‌گیری کنند، درحالی‌که سلاح‌های هسته‌ای چنین هدف‌گیری مشخصی ندارند. با این حال دیوان از غیرقانونی اعلام کردن سلاح‌های هسته‌ای خودداری ورزید. گویی هنوز حقوق بین‌الملل عرفی مرتبط با به‌کارگیری حملات سایبری فراتر از آنچه در قضیهٔ نیکاراگوئه بیان شده است، وجود ندارد. در این قضیه دیوان می‌گوید: «هر کشور حاکمی [حق دارد] که امور داخلی خود را بدون دخالت خارجی سامان دهد... [این] بخشی از حقوق بین‌الملل عرفی است» (1968 I.C.J. 4, para, 202). بنابراین به‌نظر می‌رسد رویهٔ دولتی پس از حملات سایبری حاکی از محکومیت وسیع آن است، اما اجماعی بر چگونگی واکنش به آن، و اینکه یک حملهٔ سایبری در چه سطحی به مخاصمهٔ مسلحانه تبدیل می‌شود، حاصل نشده است (Guzman,1996).

۲. قیاس با حقوق فضا

معاهدهٔ فضای ماورای جو در سال ۱۹۶۷ جامع‌ترین توافق بین‌المللیِ پابرجا در زمینهٔ استفاده از فضا محسوب می‌شود. این معاهده فضا را به‌عنوان منطقه‌ای ماورای ادعای حق حاکمیت دولت‌ها تعریف می‌کند، اما توجه چندانی به موضوعات نظامی ندارد (به‌جز ممنوعیت استفاده از تسلیحات کشتارجمعی در مدار یا بر هر گونه جسم سماوی و ممنوعیت استفاده از اجسام سماوی جهت پایگاه‌های نظامی یا آزمایش تسلیحات) (Denmark & Mulvenon,2010: 16). فضای ماورای جو ذاتاً شبیه فضای سایبری است. هر دو به‌طور شگفت‌آوری پهناور و سرچشمهٔ منابع غنیِ مشترکات عمومی‌اند. هیچ‌یک از فضای ماورای جو و فضای سایبری براساس حقوق بین‌الملل قابل ملی‌سازی نیستند. در عین حال در خصوص اِعمال قواعد حقوق فضا بر فضای سایبری ضعف‌هایی وجود دارد. به‌طور مثال می‌توان به سکوت حقوق فضا در مورد اعمال آن در زمان مخاصمهٔ مسلحانه اشاره کرد. همچنین ممنوعیت کاملی در خصوص توسل و استفاده از سلاح‌های فضایی وجود ندارد. معاهدهٔ ماورای جو ملل متحد مصوب ۱۹۶۱ که تنها استقرار سلاح‌های کشتارجمعی [و نه دیگر سلاح‌ها] را ممنوع اعلام می‌کند، بیان می‌دارد: «کشورهای طرف این معاهده می‌پذیرند هیچ شیئی با قابلیت حمل سلاح‌های هسته‌ای یا هر سلاح دیگری را از نوع کشتارجمعی در مدار زمین قرار ندهند؛ چنین سلاح‌هایی را در اجرام سماوی مستقر نسازند و در ماورای جو به هر شکل دیگری جای ندهند». با این حال این ممنوعیت تنها به ماه و دیگر اجرام سماوی مربوط می‌شود و نه فضای خالی میان آنها (Shackelford,2009: 169). در حال حاضر هیچ ممنوعیتی در خصوص استقرار تسلیحات در فضای تهی میان اجرام سماوی وجود ندارد. ازاین‌رو تلاش برای کاهش اشاعهٔ سلاح‌های فضایی همان‌قدر شانس دارد که تلاش برای کاهش آن در فضای سایبری.

۳. بهره‌گیری از حقوق معاهدات و عرف‌های بین‌المللی

در حال حاضر تعداد اندکی معاهدهٔ بین‌المللی وجود دارند که می‌توانند تشکیل‌دهندهٔ یک عرف بین‌المللی باشند که نهایتاً در تنظیم جنگ سایبری تا حدودی به‌کار رود. برای مثال، معاهدهٔ «کنوانسیون بین‌المللی مخابرات»[1] و مادهٔ ۳۵ آن، هر گونه مداخلهٔ زیانبار با استفاده از ارتباطات از راه دور را ممنوع می‌کند.[2] مادهٔ ۳۷ همان نیز به‌گونه‌ای ممکن است بر جنگ‌های سایبری اثرگذار باشد. همچنین مادهٔ ۱۹ بند ۲ و مادهٔ ۲۰ این کنوانسیون نیز مستعد بهره‌گیری در این خصوص است (Schaap,2009: 21). بند ۷ مادهٔ ۲۳ «کنوانسیون لاهه»[3] نیز در بحث تناسب جنگ طرفین درگیر را در از بین بردن یا ضبط اموال دشمن، منع می‌کند[4]. اگرچه تأثیر معاهده می‌تواند به‌سبب استثنائاتی که دولت‌ها بر آن وارد می‌کنند محدود شود، اما تشبیهِ فضای مجازی به فضای جو، به طریقِ اولی موجب برآمدنِ نیاز روزافزون به وجود قوانین بین‌المللی در مورد فضای اینترنت می‌شود. البته تخطی از کنوانسیون بین‌المللی مخابرات، توسل به زور را آن‌گونه که مطمح‌نظر بند ۴ مادهٔ ۲ منشور ملل متحد است، تشکیل نمی‌دهد، و متعاقباً سبب ایجاد موضع‌گیری مشابهی در میان جامعهٔ بین‌المللی هم نمی‌شود.

یک سند حقوقی بین‌المللیِ دیگر که قابلیت ارتباط گرفتن با موضوع را دارد، «موافقت‌نامهٔ اجتناب از فعالیت‌های خطرناک نظامی»[5] است که در سال ۱۹۸۹بین ایالات متحدهٔ آمریکا و شوروی به امضا رسیده بود. این موافقت‌نامه هر گونه مداخلهٔ زیانبار در «سیستم‌های فرماندهی و کنترلی»[6] دشمن را ممنوع کرده بود که می‌توانست به‌عنوان امکان ایجاد رویه و عرفی شناخته شود که حملات واقع‌شده در فضای مجازی را نوعی توسل به زور به‌شمار می‌آورد. در اواخر قرن بیستم نیز با افزایش توجه رسانه‌ها و محافل دانشگاهی به مفهوم نوظهور جنگ سایبری، در جامعهٔ بین‌المللی تلاش‌هایی برای مذاکراتی برای انعقاد معاهده‌ای در این زمینه صورت گرفت. به‌طور نمونه، روسیه در اکتبر ۱۹۹۸ متولی تصویب قطعنامه‌ای در کمیتهٔ اول شورای امنیت سازمان ملل شد که به‌عنوان تلاشی آشکار برای جلب نظر ملل متحد به این موضوع شناخته می‌شود. این قطعنامه شامل فراخوانی برای دولت‌ها بود که از نظرهای آنها در مورد ایجاد نظام‌های حقوقی بین‌المللی به‌منظور تحدید، گسترش، ساخت و استفاده از سلاح‌های اطلاعاتی خاص حمایت کند. این تلاش با استقبال اندکی در جامعهٔ بین‌المللی مواجه شد و هرگز برای رأی‌گیری عمومی وارد مجمع عمومی ملل متحد نشد (Hoisington,2009: 445).

---

1. International Telecommunications Convention (ITC)
2. Article 35 of the ITC prohibits harmful interference with the radio spectrum: International Telecommunications Convention, Nairobi, Nov. 6, 1982, 32 U.S.T. 3821 [hereinafter ITU Convention].
3. The Hague Convention
4. Article 23 of The Hague Convention, (g) "to destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war."
5. Agreement on the Prevention of Dangerous Military Activities
6. Command and Control Systems

اینک شاید با گذشت دو دهه از طرح اولیهٔ آن و گسترش تهدیدات و حملاتی که برخی از آنها اشاره شد، جلب نظر جامعهٔ بین‌المللی به دشواری گذشته نباشد، اما احتمالاً پس از آنکه حملهٔ سایبری به حد مخاصمهٔ مسلحانه رسید، یک نظام امنیتی بین‌المللی که شامل حقوق بشردوستانهٔ بین‌المللی و حقوق بشر می‌شود، به جریان می‌افتد. طرح سال ۲۰۰۰ برای کنوانسیون بین‌المللی جرم و تروریسم سایبری که در دانشگاه استنفورد تهیه شده است، لزوم دستیابی به معاهدهٔ جامع را این‌گونه بیان می‌داشت که «مجرمان سایبری ضعف‌های حقوق و رویه‌های دولتی لازم‌الاجرا را بیرون کشیده و به تمام دولت‌ها خطرهایی وارد می‌سازند که خارج از توانایی یکجانبه یا دوجانبهٔ آنها برای واکنش است. سرعت و پیچیدگی تکنولوژیک اقدامات سایبری، لزوم اتخاذ روندهای تنظیم‌شده و توافق‌شده برای همکاری در تحقیقات و واکنش به این تهدیدات و حملات را نشان می‌دهد. همچنین مادهٔ ۱۲ طرح پیش‌نویس استنفورد، تأسیس یک نهاد بین‌المللی برای حفاظت از ساختار اطلاعاتی را پیشنهاد می‌دهد. مرکز دفاعی اینترنتی سایبری ناتو باید الگوی سازمانی برای ایجاد چنین نهادی باشد، که می‌تواند مرکز جهانی واکنش اضطراری سایبری نام بگیرد. البته طرح استنفورد عمل دولتی را استثنا کرده است و تنها به عمل افراد یا گروه‌ها اشاره دارد» (Sofaer,2000: Article 3 of Stanford Treaty Proposal, note 29). از سویی، فضای سایبری همچون بستر عمیق دریاها، منطقهٔ میراث مشترک بشریت سنتی نیست، اما با توجه به ماهیت گوناگون موجود در این فضا، قیاس گرفتن از منطقهٔ میراث مشترک بشریت مفید خواهد بود. افزون‌بر اینکه حمله‌های سایبری را در حقوق بین‌الملل نمی‌توان ممنوع دانست؛ چراکه همان ملاحظات مربوط به نظر دیوان بین‌المللی دادگستری در قضیهٔ سلاح‌های هسته‌ای را به‌همراه می‌آورد. ممنوع اعلام کردن برنامه‌های رایانه‌ای که قابلیت استفاده برای حملات سایبری را نیز دارند، به معنای تغییر ماهیت پویای اینترنت خواهد بود. برخلاف نظام معاهده‌ای قطب جنوب و ماورای جو، نیاز است که یک نهاد بین‌المللی مانند «مرکز جهانی واکنش اضطراری سایبری» تحت نظر ملل متحد تأسیس شود که اختیار تحقیق و مشارکت با دولت قربانی برای واکنش به حملات سایبری را به‌محض وقوع داشته باشد. امری که اساساً با رضایت و تمکین قدرت‌های بزرگ تحقق خواهد یافت که همچنان در مورد آن شک و تردید فراوان وجود دارد.

جایگاه منع توسل به‌زور و حق دفاع مشروع

همان‌گونه‌که اشاره شد، فضای سایبری گونه‌ای جدید از حملات و عملیات را به نمایش گذاشته است که بالقوه می‌تواند جایگزین سایر روش‌های ورود به جنگ توسط دولت‌ها و سایر بازیگران غیردولتی قلمداد شود. ماهیت منحصربه‌فرد تهدید به جنگ سایبری و موضوع توانایی یا ناتوانیِ

به‌کارگیرندگان این شکل از جنگ در ایراد جراحت، قتل یا ایجاد ویرانی‌های فیزیکی از طریق فضای مجازی، موجب گسترده‌تر شدن تعریف سنتی توسل به زور شده است. به‌منظور ترسیم صریح و واضح حقوق طرف‌های درگیر در جنگ سایبری مانند حق دفاع از خود، جامعهٔ جهانی می‌بایست در خصوص تعریف جنگ سایبری بر طبق الگوهای ارائه‌شده در «حقوق جنگ»[1] موجود به توافق و اجماع برسد. هر تعداد از مقاصدی که ممکن است یک کشور را به استفاده از جنگ سایبری تحریک کند و فارغ از در نظر گرفتن هدف، ارزیابی جامعهٔ بین‌المللی در این زمینه بر این مسئله متمرکز خواهد بود که آیا جنگ سایبری (چه در مقام حملهٔ و چه در قالب اقدام تلافی‌جویانه) می‌تواند نوعی توسل به زور غیرقانونی یا تهدید به آن که مخالف با حقوق بین‌الملل باشد تلقی شود یا خیر؟ از همین رو به‌منظور ارائهٔ تعریف مؤثری برای جنگ سایبری، جامعهٔ بین‌المللی باید در چارچوب منشور ملل متحد و به‌خصوص مادهٔ ۴ بند ۲ منشور ـ که توسل به‌زور را تنظیم می‌کند ـ و مادهٔ ۵۱ ـ که به حق دفاع از خود اشاره دارد، متمرکز شود.

در اینجا لاجرم مبحث قواعد آمره مطمح‌نظر خواهد بود. بسیاری از کارشناسان معتقدند این قواعد، مباحث حقوق بین‌الملل را به‌طور عمده دچار سردرگمی کرده است، زیرا اعضای جامعهٔ حقوق بین‌الملل قادر به دستیابی به اجماع در مورد تعریف مناسبی از این واژه نیستند. این بدین معنی نیست که قواعد آمره قابل مثال زدن نیستند. متون حقوق بین‌الملل به‌وسیلهٔ پیشنهادهای فراوانی در مورد نامزد شدن برای قواعد آمره، این نکته را ثابت می‌کند. همان‌طورکه به‌نظر می‌رسد، کم‌مناقشه‌ترین مثال اصل عدم توسل به زور است.[2] به بیان دقیق‌تر، این یک قاعدهٔ قابل اجرای جهانی است. به هر حال با توجه به آنچه معمولاً مفروض است، اصل منع توسل به زور بیان‌شده در مادهٔ (۴) ۲ منشور ملل متحد (حداقل در اساس و بنیان) مربوط به محتویات موجود آن در حقوق بین‌الملل عرفی است. اگر یک دولت در راستای روابط بین‌المللی خود متوسل به زور علیه تمامیت ارضی و استقلال سیاسی دولت دیگر یا مغایر با اهداف ملل متحد شود، این عمل نقض قاعدهٔ آمرهٔ بین‌المللی است (Chetail,2003: 250-252). بی‌شک این تعریف کافی نیست. منع استفاده از زور (همان‌طورکه در منشور بیان شده) مطلق نیست. این اصل با توجه به شرایط خاصی اعمال می‌شود، یکی از آنها این است که قوهٔ قهریه می‌تواند با استناد به حق دفاع مشروع مندرج در مادهٔ۵۱ منشور توجیه شود. این مقرره نیز بازتابی از قواعد عرفی بین‌المللی تلقی می‌شود. اگر دولتی در راستای روابط بین‌المللی خود

---

1. *Jus ad Bellum*

۲. این عبارتی است که دیوان بین‌المللی دادگستری در قضیهٔ نیکاراگوئه به‌کار برده است. ن.ک:

- Military and Paramilitary Activities (Nicaragua. v. U.S.), 1986 I.C.J. 14, 530 (June 27) (Jennings, J., dissenting) (“There is no doubt that there was, prior to the United Nations Charter, a customary law which restricted the lawful use of force, and which correspondingly provided also for a right to use force in self defence.”).

متوسل به زور علیه تمامیت ارضی و استقلال سیاسی یک دولت دیگر یا مغایر با اهداف سازمان ملل متحد شود، و این عمل در مقابل یک حملهٔ نظامی انجام نگرفته باشد، آنگاه این عمل باید نقض قاعدهٔ آمرهٔ بین‌المللی تلقی شود.

این اظهار عقیده که حق دفاع مشروع بخشی از قاعدهٔ آمره است ممکن است برای همه به‌عنوان یک امر بدیهی حاصل نشود. در واقع با اینکه بسیاری از مفسران پذیرفته‌اند که مطابق مادهٔ ۵۱ منشور، قوهٔ قهریه نمی‌تواند برای اهداف مقدماتی توسط دولت‌ها به‌کار رود، آنها هنوز هم مدعی وجود حق مقدماتی (اولیه) یا پیشگیرانهٔ دفاع از خود در حقوق بین‌الملل عرفی‌اند (Brunée & Toope,2004: 373). در نتیجه، اگر ما خود را با این جستار هماهنگ کنیم که آیا مطابق حقوق بین‌الملل، توسل به زور می‌تواند توسط یک دولت برای اهداف اولیه (مقدماتی) (برای جلوگیری از یک حملهٔ قریب‌الوقوع) به‌کار رود یا خیر، پاسخ بسته به معیار خاصِ مفروض در این جستار متفاوت خواهد بود. به‌عبارت دیگر، حق مندرج در مادهٔ ۵۱ در تعارض با مفاد حقوق بین‌الملل عرفی است.

مطابق قاعدهٔ بیان‌شده در مادهٔ ۶۴ کنوانسیون ۱۹۶۹ وین، در خصوص مادهٔ ۴۴، هنگامی‌که یک قاعدهٔ آمره تضادی با یک مادهٔ معاهده نشان می‌دهد، این ماده (با در نظر گرفتن اینکه جدا از بقیهٔ معاهده است) باید بی‌اعتبار تلقی شود. بدیهی است اگر شخصی اصل منع توسل به زور را یک قاعده با خصیصهٔ آمره در نظر بگیرد و همزمان از این ایده که حقوق بین‌الملل عرفی (نه منشور ملل متحد) اجازهٔ به‌کارگیری حق دفاع مقدماتی (اولیه) یا پیشگیرانه توسط یک دولت را می‌دهد، دفاع کند، وی باید آثار منطقی آن را نیز بپذیرد که سال‌هاست مادهٔ ۵۱ منشور ملل متحد منسوخ شده است (Ulf, 2008: 861). اما زمانی‌که ایالات متحدهٔ آمریکا مخالفان حکومت مرکزیِ نیکاراگوئه را تسلیح نظامی و مالی می‌کرد، با دعوای نیکاراگوئه نزد دیوان بین‌المللی دادگستری، دیوان در رأی خود در سال ۱۹۸۶ به‌صراحت اعلام کرد که توجیه حقوقی ایالات متحده در مقام دفاع مشروع (مادهٔ ۵۱ منشور) فاقد مشروعیت بوده و این ماده تنها در درگیری واقعی قابلیت اعمال خواهد داشت[1] (Aspremont,2010: 1118). اگرچه در مادهٔ ۵۹ اساسنامهٔ د.ب.د آمده است که «احکام دیوان فقط دربارهٔ طرفین اختلاف و در موردی که موضوع حکم بوده الزام‌آور است»[2] و قابلیت تعمیم یا سرایت به دیگر موارد را ندارد، اما در واقع در رویهٔ قضائیِ د.ب.د کمتر موردی را می‌توان یافت که دیوان به آرای خود ارجاع نداده باشد. در مورد حملهٔ بدافزار استاکس‌نت و فِلیم علیه تأسیسات هسته‌ای نطنز نیز که در قالب موضوع «سایبر تروریسم» قرار می‌گیرد، آمریکا و اسرائیل همین توجیه را مطرح می‌کنند؛ بدین مفهوم که

1. Military and Paramilitary Activities (Nicaragua. v. U.S., 1986 I.C.J. 14, para.195 (June 27).
2. The decision of the Court has no binding force except between the parties and in respect of that particular case.

ایران در این سایت مشغول ساخت بمب هسته‌ای بوده و در صورت موفقیت، امکان حمله به خاک اسرائیل و منافع ایالات متحده در منطقه متصور بوده است. هرچند تاکنون واشنگتن و تل‌آویو مسئولیت این حمله را بر عهده نگرفته‌اند؛ لکن تلویحاً از اظهار نظرهای آنها در قضیهٔ هسته‌ای چنین استنباطی مستفاد می‌شود و این توجیه حقوقی در آن مستتر است.

از دیگر سو، با اینکه تعریف دقیقی در مورد توسل به زور صورت نگرفته است، برخی پارامترهای سازندهٔ این جرم به‌خوبی تعریف شده‌اند. برای مثال، حمله با استفاده از سلاح‌های متعارف در تعریف موجود در بند ۴ مادهٔ ۲ گنجانده شده است. از این گذشته، آن دسته از حملات سایبری که به قصد ایجاد مستقیم خسارت فیزیکی به دارایی‌های قابل لمس یا ایراد جراحت به افراد یا کشتن انسان به‌راه انداخته می‌شوند، ضرورتاً به‌عنوان استفاده از نیروی نظامی شناخته خواهند شد، و متعاقباً مشمول ممنوعیت مدنظر منشور می‌شوند. برعکس، با وجود تلاش‌های کشورهای در حال توسعه برای وارد کردن اجبارها و تهدیدات اقتصادی به عناوین مجرمانهٔ مطرح در بند ۴ مادهٔ ۲ منشور، این اقدامات صریحاً از این محدوده خارج شده‌اند. بنابراین، تحلیلی که بخواهد بر پایهٔ متن بند ۴ مادهٔ ۲ یا پیش‌زمینهٔ تاریخی، تدوین آن بنا شود، نیاز به تفسیری دارد که اجبار یا تهدید اقتصادی و سیاسی را از حیطهٔ دیدگاه این ماده خارج کند. از سویی امکان اعمال احتمالی بند ۴ مادهٔ ۲ منشور در مورد جنگ سایبری مشکلات تفسیری زیادی ایجاد خواهد کرد که دلیل آن هم تمایز موجود میان «زور» و «اجبار یا تهدید» است. وارد کردن تمام فعالیت‌های مرتبط با جنگ سایبری ذیل تعریف توسل به زور نیازمند گسترش عمدهٔ دامنهٔ شمول بند۴ مادهٔ ۲ است. برخی معتقدند چنین تعریف موسعی از توسل به زور، مانع خارج کردن اجبار یا تهدید از دامنهٔ شمول بند ۴ مادهٔ ۲ می‌شود، زیرا حقوق بین‌الملل می‌بایست میان آن دسته از حملات سایبری که خسارات فیزیکی به‌جا نمی‌گذارند ـ مانند دزدی الکترونیکی یا محاصرهٔ الکترونیکی ـ با فعالیت‌هایی مانند اجبار یا تهدید اقتصادی و سیاسی ـ مانند تحریم اقتصادی که به شکل سنتی از شمول این ماده خارج شده‌اند، - اما ممکن است تأثیر مشابهی داشته باشند ـ تمایز قائل شود (Barkham,2001: 84-85).

در ۲۵ مارس ۲۰۱۳ مرکز جنگ سایبری ناتو اعلام کرد که حملات سایبری آمریکا و اسرائیل علیه جمهوری اسلامی ایران، استفاده از زور محسوب شده و مطابق با قوانین بین‌المللی غیرقانونی ارزیابی می‌شود. متن تهیه‌شده به سفارش ناتو، «راهنمای تالین در خصوص حقوق بین‌الملل قابل اعمال بر جنگ‌افزارهای سایبری»[1] نام دارد و توسط یک گروه بیست‌نفره از حقوقدانان به سرپرستی «مایکل اشمیت»[2]، استاد حقوق بین‌الملل در کالج نبرد دریایی آمریکا (نیوپورت، رودآیلند) تهیه شده است. بنابر این گزارش ۳۰۰ صفحه‌ای که متخصصان مرکز دفاع

1. Tallinn Manual on the International Law Applicable to Cyber Warfare
2. Michael Schmitt

سایبری تالین مستقر در استونی تهیه کرده‌اند، «اقدامات سایبری که به کشتن یا زخمی کردن اشخاص یا آسیب رساندن و نابودی اشیا و تأسیسات بینجامد، به‌روشنی مصداق استفاده از زور است» (Schmitt,2013). مایکل اشمیت در تلاش برای حل مشکل طبقه‌بندی، مرز اجبار و تهدید اقتصادی و سیاسی را با استفاده از شش معیار مشخص می‌کند: شدت، مستقیم و بی‌واسطه بودن، صراحت، حالت تهاجمی داشتن، ۵) قابلیت اندازه‌گیری داشتن، و مشروعیت مفروض. براساس این مشخصات، عواقب عمل جنگ سایبری با این معیارها سنجیده می‌شوند تا مشخص شود که این عواقب بیشتر شبیه به نتایج نبردهای مسلحانه‌اند یا بهتر است که خارج از محدودهٔ ممنوعیت توسل به زور قرار گیرند. به نظر اشمیت، این تکنیک اجازه می‌دهد که محدودهٔ تعریف «زور» گسترش یابد تا خلأهایی را پر کند که در نتیجهٔ ظهور توان اجبار یک دولت توسط دولت دیگر ـ که ریشه در پیشرفت‌های تکنولوژیکی دارد ـ ایجاد شود، بدون اینکه وزن موجود در چارچوب فعلی را بر هم بزند (Hoisington,2009: 448). البته در این زمینه، چند نکتهٔ انتقادی بسیار مهم وجود دارد که در ارزیابی این اقدامات و نوع جهت‌گیری‌های مبنایی گروه ناتو در ارتباط با این مطالعه، نیازمند توجه راهبردی هستند. گفتنی است که بسیاری از مجامع حقوقی بین‌المللی به این گزارش انتقادهای زیادی را ابراز داشته‌اند. در این زمینه، باید تهدیدهای حقوقی بین‌المللی نهفته در این گزارش را مورد توجه داشت. تفسیر موسع از توسل به زور، درست برخلاف جهتی است که به تدوین منشور ملل متحد انجامیده است. براساس اصول اساسی تدوین‌شده در منشور ملل متحد، توسل به زور ناظر بر اقدامات نظامی در روابط بین‌الدولی است و جنگ اساساً در همین قالب مشمول ممنوعیت قرار گرفته است. بر این اساس، از آنجا که اصل بر منع این نوع توسل به زور است، مسائل مرتبط با دفاع مشروع و اقدامات قهری شورای امنیت نیز تنها استثناهایی هستند که توسل به زور را مشروعیت می‌بخشند. از آنجا که روسیه، چین و ایران هدف راهبردی نبردهای سایبری غرب به‌ویژه آمریکا بوده و هستند، توسعهٔ مفهوم توسل به زور به معنای موجه ساختن جنگ سایبری علیه این کشورها در قالب دفاع مشروع است.[1] با وجود این، با استفاده از تکنیک اشمیت در تعیین اینکه آیا یک حملهٔ سایبری در تعریف اثرمحور و انعطاف‌پذیرتر «زور» قابل گنجاندن است یا خیر، ماهیت آن دسته از عواقب عمل که عقلاً پیش‌بینی‌پذیرند، ارزیابی می‌شوند تا مشخص شود که آیا به عواقب حملات مسلحانه شباهت دارند یا شباهتی میان این دو وجود ندارد. اگر این عواقب شبیه به نتایج حملات مسلحانه باشد، توسعهٔ گسترهٔ ممنوعیت توسل به زور توجیه‌پذیر است. اما اگر امکان این تشبیه وجود نداشته باشد، عدم مشروعیت اقدام به حملهٔ سایبری در حقوق بین‌الملل باید با توسل به مقرراتی غیر از آنها که حاوی ممنوعیت توسل به زورند، تعیین شود.

---

۱. در این زمینه، ر.ک: نادر ساعد، «نقدی حقوقی بر اهداف پنهان راهنمای جنگ سایبری تالین ۲۰۱۳»، خبرگزاری فارس، ۱۳۹۲/۸/۱.

مایکل اشمیت، بر این باور است تمامی محققانی که این گزارش را تهیه کرده‌اند، بر این موضوع اتفاق‌نظر دارند که استفاده از ویروس سایبری استاکس‌نت علیه ساختارهای سایبری ایران در سال ۲۰۰۹م، مصداق بارز توسل به زور است. گفته می‌شود که واشنگتن و تل‌آویو به‌طور مشترک، این نرم‌افزار مخرب را توسعه داده‌اند، اگرچه تاکنون هیچ‌کدام مسئولیت این حمله را بر عهده نگرفته‌اند. نوعاً در این خصوص به فرض قبول مسئولیت این حملهٔ توسط اسرائیل و آمریکا، آیا دفاع از خود در برابر تهدیدات احتمالیِ ایران، خود می‌تواند امری دفاعی تلقی شود یا اگر به‌عنوان حملهٔ نخست و توسل به زور شناسایی شود، آیا ایران مطابق مادهٔ ۵۱ منشور قادر خواهد بود به عمل متقابل یا حتی حملهٔ نظامی متوسل شود؟ اهمیت انتشار راهنمای ناتو در این است که این حق را برای ایران ایجاد می‌کند که چه از طریق نظامی و چه مقابله با مثل، از خود "دفاع مشروع" کند. اما چون تقریباً اثبات منشأ حملات سایبری هنوز ناممکن است، چنین مقابله به مثلی ممکن است حملهٔ اولیه تلقی شود. ضمن اینکه هم‌اکنون با عدم قبول مسئولیت این حمله توسط این کشورها ایران قادر نیست اقامهٔ دعوا کند و به لحاظ تکنیکی معلوم نیست زمینهٔ اثبات منشأ حملات به چه ترتیب خواهد بود؛ اما لازم است ایران در این خصوص شواهد و مستندات را جمع‌آوری کند و حتی با تبلیغات رسانه‌ای، توجهات را بیشتر به ابعاد این موضوع جلب و در راستای مشروعیت بخشی به اقدامات متقابل و دفاع مشروع در آیندهٔ محتمل، زمینهٔ پذیرش افکار عمومی جهانی را فراهم آورد (رضائی، ۱۳۹۲). از دیگر سو و در قضیهٔ استونی، صرف‌نظر از میزان دخالت روسیه در آن، گفته می‌شود که این حملهٔ سایبری به حد مخاصمهٔ مسلحانه نرسید تا حقوق بشردوستانهٔ بین‌المللی قابل اعمال باشد. با این حال نباید پنداشت که حملات سایبری مسئولیتی در پی ندارد. در صورت اثبات انتساب حملهٔ سایبری به روسیه نقض مقررات اتحادیهٔ بین‌الملل مخابرات محقق شده است و استونی می‌تواند مطالبهٔ غرامت کند. همچنین استونی می‌تواند مسئولیت نیابتی شرکت‌های اینترنتی را مطرح سازد، درصورتی‌که مشخص شود این شرکت‌ها از اقدام خلاف قانون مطلع بوده‌اند. همین‌طور از آنجا که استونی کشوری ساحلی است می‌تواند با استناد به ممنوعیت حملات مداخله‌آمیز در امنیت یا نظم عمومی یک کشور ساحلی، مقرر در معاهدهٔ حقوق دریاها، به این معاهده توسل جوید. ازاین‌رو متجاوزان سایبری که از طریق کابل‌های دریایی به کشور ساحلی کدهای خرابکارانه ارسال کرده‌اند، ناقض تعهدات حقوقی و عرفی بین‌المللی خود هستند.

در پایان مهم‌ترین پاسخ به پرسش اصلیِ مقاله، اینکه فعالیت‌های سایبری می‌تواند موجد نوعی توسل به زور نیز تلقی شود، می‌توان گفت که فعالیت‌های مزبور می‌تواند در برخی شرایط موجد مفهوم توسل به زور مندرج در منشور ملل متحد و عرف بین‌المللی باشد. این‌گونه فعالیت‌ها اگر به مرگ، صدمه یا خسارت جدی منجر شوند، می‌توانند به‌عنوان توسل به زور قلمداد شوند. البته در این خصوص باید چند عامل مورد توجه و مطمح‌نظر قرار گیرند: نخست،

زمینهٔ حادثه‌ای که به خسارات مورد اشاره منجر می‌شود، عاملی که مرتکب این اقدام مـی‌شـود (برای مسئلهٔ چالش‌برانگیز انتساب عمل)، هدف و محل، قصد و اثرات و موارد احتمالی دیگـر. از طرفی مثال‌های مشترکی که برای فعالیت سایبری منجر به توسل به زور می‌شود عبـارت‌انـد از: عملیاتی که تأسیسات هسته‌ای را در یک بحران قرار می‌دهند؛ عملیاتی که منجر به بـاز شـدن یک سد روی جمعیت انسانی و متعاقباً آسیب جانی به همراه داشته باشد. عملیاتی که به اخلال در ترافیک هوایی منجر شود و در نتیجه، تصادمات هوایی را در پی داشته باشـد. در واقـع، اگـر آثار فیزیکی ناشی از یک حملهٔ سایبری همانند رها کردن یک بمب یا شلیک یک موشک باشد، حملهٔ سایبری مزبور نیز باید به‌عنوان توسل به زور ارزیابی شود.

نتیجه‌گیری

محیط جنگ سایبری، نامتمرکز، آشفته، به لحاظ حیطه گسـترده و بـه لحـاظ سـرعت شـتابان است. انقلاب اطلاعاتی موجب شده حمـلات سـایبری (و آنچـه آن را جنـگ سـایبری در پرتـو رایانه‌ها و اینترنت می‌خوانیم) وسعت بسیاری پیدا کند. حمـلات سـایبری و آمـادگی‌هـایی کـه اکنون برخی کشورها کسب کرده‌اند، نشان می‌دهد که رقابـت بـرای فـائق آمـدن در حمـلات و دفاع سایبری آغاز شده است. این موضوع بیـانگر عمـق ورود فضـای سـایبری بـه عملکردهـای راهبردی دولت‌هاست. این مسئله همچنین نشان می‌دهد که چنـین حملاتـی بسـیار راهبـردی هستند و در مرکز امنیت ملی هر کشور قرار دارند. ازاین‌رو یکی از مسـائل مـورد توجـه حقـوق بین‌الملل مدرن، پدیدهٔ رو به افزایش حملات سایبری است. آنچه بیش از همه در این زمینه در کانون توجه حقوقدانان قرار گرفته، این است که آیـا عملیـات خرابکارانـهٔ سـایبری یـا حمـلات سایبری به‌عنوان جنگ تلقی می‌شود یا خیر؛ و جوانب حقوقی آن چگونه اسـت. فـارغ از اینکـه چنین حملاتی تروریستی باشد یا نه، اولین سؤال اساسی در این زمینه، ایـن اسـت کـه بـا چـه شرایطی می‌توان چنین حملاتـی را تجـاوز و متعاقبـاً وضـعیت را وضـعیت مخاصـمهٔ مسـلحانهٔ بین‌المللی دانست. بند ۴ مادهٔ ۲ منشور تهدید یا توسل به زور علیه تمامیت ارضی یـا اسـتقلال سیاسی یک کشور را تجاوز دانسته است. مادهٔ ۱ قطعنامهٔ تعریف تجاوز نیز عنصر حاکمیت را به اهداف مورد حمله اضافه کرده است. اینکه چگونه تفسیری باید از مفهوم تجاوز و موضـوعات آن در حقوق موضوعه و رویه بین‌المللی داشت، از چالش‌های پیش روی دوران کنونی است. دومین سؤال، به نظام حقوقی ناظر بر فضای انتزاعی حاکم در رایانه‌های موجود در سراسر دنیـا مربـوط می‌شود. اینکه حاکمیت از آنِ کدام کشور است و اعمال مغایر با حقوق بین‌الملل چگونه باید بـه دولتی منتسب شود، از دیگر موضوعاتی است که مباحث حقوقی بر آن مترتب است. اگرچـه در نبود نظام حقوقی کارامد در خصوص فضای سایبری تردیدی نیسـت، لـیکن آنچـه مهـم جلـوه

می‌کند، تلاش برای وام گرفتن اصول و قواعدی حقوقی از دیگر نظام‌های موجود حقوق بین‌الملل و سنجش میزان مشابهت آنها با فضای سایبری است.

تحت قواعد حقوق بین‌الملل، برابری حاکمیت دولت‌ها سنگ بنای سیستم حقوقی بین‌المللی است. اصل برابری حاکمیت دولت‌ها، مشروعیت خود را از بند ۱ مادهٔ ۲ منشور ملل متحد گرفته است که اذعان می‌دارد "سازمان بر مبنای اصل برابری حاکمیتی تمامی دولت‌ها بنا نهاده شده است". برابری دولت‌ها به این معناست که شأن، شخصیت و استقلال یک دولت و همچنین حاکمیت ارضی آن مورد احترام‌اند. درحالی‌که حقوق بین‌الملل حق تعیین سرنوشت را تضمین می‌کند، در خصوص دخالت خارجی نیز محدودیت‌هایی را مقرر می‌دارد. این موضوع به‌رسمیت شناخته‌شده‌ای است که یکی از عناصر حاکمیت این است که باید در محدودهٔ سرزمینی اعمال شود. حملهٔ روسیه به استونی در سال ۲۰۰۷ یا حملهٔ به گرجستان در سال ۲۰۰۸ و همچنین استفاده از حملات سایبری توسط اسرائیل و آمریکا علیه ایران، نقض آشکار حاکمیت دیگر دولت‌ها و توسل به زور تلقی می‌شود. بنابراین، حملات سایبری می‌توانند صلح و امنیت جهانی را تهدید کنند و این امر نیاز به تعریف قواعد جدید و منطبق با اصول حقوق بین‌الملل و منشور ملل متحد را گوشزد می‌کند. چنین اسنادی می‌توانند همانند سایر کنوانسیون‌های بین‌المللی که حاکم بر روابط بین دولت‌هاست، کشورهای عضو را ملزم به عدم انجام حملات سایبری علیه یکدیگر کنند. از طرفی امروزه قوانین بین‌المللی دربارهٔ سربازی که برای مثال اقدام به پرتاب نارنجک به آن سوی مرز می‌کند، وجود دارد، اما در مقایسه، قوانین دربارهٔ سربازان سایبری که نهادهای نظامی، اقتصادی و مالی کشورهای دیگر را هدف قرار می‌دهند و آسیب‌های جدی به‌جای می‌گذارند، فاقد موضوعیت‌اند. واضح است که در این میان کمبود جدی هنجارهای بین‌المللی وجود دارد و نیاز به اقدامات دسته‌جمعی بین‌المللی برای کنترل این "میدان جنگ دیجیتالی" احساس می‌شود. از دیگر سو، اشاره شد که متأسفانه حملات سایبری را در حقوق بین‌الملل نمی‌توان ممنوع دانست، چراکه همان ملاحظات مربوط به نظر دیوان بین‌المللی دادگستری در قضیهٔ سلاح‌های هسته‌ای را به‌همراه می‌آورد. ممنوع اعلام کردن برنامه‌های رایانه‌ای که قابلیت استفاده برای حملات سایبری را نیز دارند، به معنای تغییر ماهیت پویای اینترنت خواهد بود. در مجموع، تلاش‌ها برای ایجاد قواعد جهانی در زمینهٔ ممنوعیت حملات سایبری به‌ویژه قوانینی که زیر نظر اتحادیهٔ بین‌المللی ارتباطات (آی.تی.یو) قرار دارند، به‌دلیل وجود اختلاف‌نظرهای موجود هنوز به سند حقوقی بین‌المللی الزام‌آور منتج نشده است. به همین دلیل، تدوین یک سند حقوقی بین‌المللی برای مقابله با این حملات، یک نیاز و خواستهٔ جهانی و دغدغهٔ مشترک بشری است که نیازمند تعریف قواعد جدید و منطبق با اصول حقوق بین‌الملل و منشور ملل متحد را گوشزد می‌کند؛ صرف‌نظر از اینکه کجا زندگی می‌کنیم یا چگونه فکر می‌کنیم.

منابع

۱. فارسی

۱. رضائی، مسعود (۱۳۹۵). «شبیه‌سازیِ اقدام نظامی آمریکا علیه سوریه در چارچوب ملاحظات حقوق بین‌الملل»، *فصلنامهٔ مطالعات حقوقی*، دورهٔ هشتم، ش دوم، تابستان.

۲. ---------- (۱۳۹۲). *حملهٔ سایبری استاکس‌نت به‌مثابهٔ توسل به زور در حقوق بین‌الملل*، مؤسسهٔ فرهنگی مطالعات و تحقیقات ابرار معاصر ایران، ۱۷ فروردین.

۲. انگلیسی

A) Books

3. Abraham M. Denmark, James Mulvenon. (2010). *Contested Commons: The Future of American Power in a Multipolar World*, Center for New American Security (CNAS).
4. Hess, Charlotte. (1996). "*Untangling the Web: The Internet as a Commons." Workshop in Political Theory and Policy Analysis*", Indiana University
5. Schmitt, Michael N. (2013). *Tallinn Manual on the International Law: Applicable to Cyber Warfare*, Cambridge University Press.

B) Articles

6. Aspremont, Jean D' (2010). "*Mapping the Concepts behind the Contemporary Liberalization of the Use of Force in International Law*", http://ssrn.com/author=736816.
7. Barkham, Jason. (2001). "*Information Warfare and International Law on the Use of Force*", 34 N.Y.U. J. Int'l L. & Pol.
8. Brunnée, Jutta and Stephen J. Toope. (2004). "Slouching Towards New 'Just' Wars: International Law and the Use of Force After September 11th", *Netherlands International Law Review*, Vol 51 / Issue 03 / December
9. Chetail, Vincent. (2003). "*The Contribution of the International Court of Justice to International Humanitarian Law*", http://www.icrc.org/eng/assets/files/other/irrc_850_chetail.pdf
10. Davis, Joshua, (2007). "Hackers Take down the Most Wired Country in Europe", *Wired Magazine*, Aug. 21, http://www.wired.com/politics/security/magazine/15-09/ffestonia (detailing a rogue computer network's assault on Estonia).
11. Goldsmith, Jack. (2013). "How Cyber Changes the Laws", *The European Journal of International (EJIL)*, Vol. 24 No. 1.
12. Hoisington, Matthew (2009). Cyber-warfare and the Use of Force Giving Rise to the Right of Self-Defense, *Boston College International and Comparative Law Review*, Volume 32, http://lawdigitalcommons.bc.edu/iclr/vol32/iss2/16
13. Hongju Koh, Harold (2012). International Law in Cyberspace, Legal

Advisor U.S. Department of State, *USCYBERCOM Inter-Agency Legal Conference*, September 18, 2012, http://www.state.gov/s/l/releases/remarks/197924.htm

14. Lewis, James A., (2013). "Conflict and Negotiation in Cyberspace", *Center for Security and International Studies*, February csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf
15. Linderfalk, Ulf, (2008). "The Effect of Jus Cogens Norms: Whoever Opened Pandora's Box, Did You Ever Think about the Consequences?" *The European Journal of International Law*, Vol. 18 No.5, http://www.ejil.org/pdfs/18/5/248.pdf
16. Schaap, Arie J. (2009). "Cyber warfare operations: development and use under international law", *Air Force Law Review*, December http://www.thefreelibrary.com/Cyber+warfare+operations%3A+development+and+use+under+international+law.-a0212035712
17. Shackelford Scott J. (2009). "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law:, *Berkeley Journal of International Law*, Volume 27, see on: http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil
18. Sofaer, Abraham D. (2000). "*Stanford University. A proposal for an International Convention on Cyber Crime and Terrorism*", http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm