فصلنامهٔ مطالعات حقوق عمومی، دورهٔ ۴۸، شمارهٔ ۲، تابستان ۱۳۹۷: ۲۶۱-۲۸۰

قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی[1] دفاع مشروع مقرر در مادهٔ ۵۱ منشور سازمان ملل متحد

سید باقر میرعباسی[2]، مجید کورکی‌نژاد قرایی[3]*

چکیده

تروریسم با پیدایش جوامع انسانی آغاز شده و در بستر پیشرفت جوامع با سرعت فزاینده‌ای خود را دگرگون کرده است. از نوین‌ترین گونه‌های تروریسم که امروزه توجه بسیاری از اندیشمندان را به خود جلب کرده، باید به تروریسم سایبری اشاره کرد. این پدیده که از ابهامات تروریسم سنتی و فقدان تعریف و توافق بر سر آن رنج می‌برد، به‌دلیل بستر بی‌همتای ارتکاب آن یعنی فضای سایبر، دچار ابهامات بیشتری می‌شود که، سنگ بنای بررسی سایر جنبه‌های آن، بررسی قابلیت تحقق این پدیده در عالم واقع است. در این مقاله تلاش کرده‌ایم تا با استفاده از اطلاعات موجود، وجود چنین پدیده‌ای را اثبات و در نهایت ارتباط آن با مادهٔ ۵۱ منشور سازمان ملل متحد را بررسی کنیم، زیرا صدق عنوان حملهٔ مسلحانه بر اقدامات سایبری خود چالش بزرگ دیگری در خصوص این اقدامات است که تبعات بسیاری را ممکن است به‌همراه داشته باشد.

کلیدواژگان

تروریسم، تروریسم سایبری، حملهٔ مسلحانه، دفاع مشروع، فضای سایبر، مادهٔ ۵۱ منشور.

1. Inherent Right.

۲. استاد دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران. Email: mirabbasi@ut.ac.ir
۳. کارشناسی‌ارشد حقوق بین‌الملل دانشگاه تهران (نویسندهٔ مسئول). Email: Majid.gharaee1369@gmail.com

تاریخ دریافت: ۱۳۹۴/۱۱/۱۶، تاریخ پذیرش: ۱۳۹۵/۰۲/۰۱

مقدمه

دوران معاصر، عصر اطلاعات، دانش یا ارتباطات نام گرفته است (Rowe & Davis, 1996: 6). در این دوران تمام جوامع در این کرهٔ خاکی برای بسیاری از امور خود از جمله فراغت و تفریح، کنترل مراکز و حتی بهره‌برداری از دریا، خشکی و فضا از وسایل الکترونیکی و شبکهٔ اینترنت بهره می‌گیرند. با اینکه عصر اطلاعات شرایط زندگی ما را به‌نحو سودمندی تغییر داده است، نمی‌توان از مضرات آن نیز غافل شد. شاید بتوان عصر اطلاعات را تیغی دولبه دانست که در عین خدماتی که به ما ارائه می‌دهد، خطرهایی مثل سایبر تروریسم نیز دارد.

امروزه در عرصهٔ بین‌المللی در پذیرش تروریسم سایبری به‌عنوان نوع جدیدی از تروریسم کمتر تردیدی وجود دارد. شورای اروپا در گزارش وضعیت خود در سال ۲۰۰۴ با عنوان «جرایم سازمان‌یافته در اروپا: تهدید جرایم سایبری» با تصریح به اینکه تروریسم سایبری تهدید و نوع جدید و ویژه‌ای از تروریسم مدرن است، بر این نظر صحه گذاشته و به تعریف و بررسی جنبه‌های مختلف تروریسم سایبری پرداخته است (Council of Europe, 2205: 172).

این پدیدهٔ نوین از لحاظ حقوقی به‌حد کافی بررسی نشده و بیشتر تحلیل‌ها از لحاظ سیاسی و امنیتی بوده است. هدف ما در این مقاله اغلب بر این مبنا استوار شده که اثبات کنیم تروریسم سایبری قابلیت تحقق دارد، زیرا در تمامی مباحث معمولاً این امر را مسلم می‌پندارند، ولی به نظر نگارنده، اثبات وقوع پدیده‌ای شالودهٔ لازم برای تحقیقات متأخر در مورد آن پدیده است که در خصوص موضوع مورد بحث این اثبات صورت نپذیرفته و متعاقب آن نیز ابعاد و حدود سایبر تروریسم مدنظر قرار گرفته است و سپس آثار آن در دنیای واقعی بررسی می‌شود.

مفهوم فضای سایبری

تعاریف ارائه‌شده از فضای سایبر معمولاً چند دسته‌اند که هر کدام بر مبنای متفاوتی این فضا را تعریف می‌کنند. برخی تعاریف بر غیرواقعی بودن این فضا و هم‌عرضی آن با جهان واقعی تأکید دارند. دستهٔ دوم فضای سایبر را منبعی برای تبادل اطلاعات به‌شمار آورده و آن را بر این مبنا تعریف می‌کنند و دستهٔ آخر هم فضای سایبر را با دید سخت‌افزارانه می‌نگرند و آن را تشکیل‌یافته از اتصال بی‌شماری از رایانه‌ها و سامانه‌ها می‌دانند (پاکزاد، ۱۳۹۰: ۴۲). تعاریف زیر بیانگر همین مسئله است.

فرهنگ لغت «ماریام وبستر» فضای سایبر را «جهان آنلاین از شبکه‌های رایانه‌ای و به‌خصوص اینترنت» معرفی می‌کند (www.merriam-webster.com).

وزارت دفاع ایالات متحده نیز این فضا را یک قلمرو جهانی در محیط اطلاعات می‌داند که دربرگیرندهٔ شبکه‌ای به‌هم‌مرتبط از زیرساخت‌های فناوری اطلاعاتی و شامل اینترنت، شبکه‌های

ارتباطات از راه دور، سیستم‌های رایانه‌ای، کنترل‌گرها و پردازنده‌ها است (Defense Department Cyber Efforts, 2011: 13).

توماس وینگفیلد[1]، در کتاب *قانون نبرد اطلاعاتی: قانون امنیت ملی در فضای سایبر*، تعریف ساده‌تری ارائه می‌دهد: فضای سایبر یک مکان فیزیکی نیست. فضای سایبر به محیطی اشاره دارد که از ترکیب و یکی شدن شبکه‌های رایانه‌ای، سیستم‌های اطلاعاتی و زیرساخت‌های ارتباط از راه دور ایجاد شده که از آن به‌عنوان «شبکهٔ گستردهٔ جهانی[2]» یاد می‌شود (Wiengfield, 2000: 14).

مرکز پژوهش‌های کنگرهٔ آمریکا نیز در سال ۲۰۰۱ فضای سایبر را به‌عنوان کلیهٔ ارتباطات موجودات بشری از طریق رایانه‌ها و تکنولوژی‌های ارتباط از راه دور بدون توجه به جغرافیای فیزیکی تعریف کرد (Schaap, 2009: 125).

باید خاطرنشان ساخت که تعریف واحدی از فضای سایبر که همگان بر آن اتفاق نظر داشته باشند وجود ندارد، اما به نظر نگارنده می‌توان فضای سایبر را، محیطی تشکیل‌یافته از سامانه‌ها و شبکه‌های ارتباطی دانست که قابلیت رفتارهای گوناگون برحسب نیازهای متفاوت کاربران را دارد و نسبت به محیط فیزیکی دارای جنبه‌ها و ابعاد متفاوتی است.

امکان‌پذیری وقوع تروریسم سایبری از نظر کارشناسان و تفاوت‌های آن با تروریسم سنتی

تروریسم پدیدهٔ قابل درک و پذیرفته‌شده‌ای است که بیشتر از جانب دولت‌های قوی علیه دولت‌های ضعیف‌تر اعمال می‌شود و دولت‌های ضعیف آن را به‌مثابهٔ دخالت در امور داخلی کشور خود می‌دانند. قدر متیقن امروزه تروریسم در معنای عام پدیده‌ای واقعی و مسجل است؛ اما نمونه‌های جدید مطرح‌شده از تروریسم مانند تروریسم هسته‌ای و سایبری هنوز هم در هاله‌ای از ابهام قرار دارند. اذهان عمومی هنوز هم از تروریسم همان قرائت سنتی را دارد و تروریسم را به معنای دولت مردکشی و کشتن افراد تعیین‌شده می‌داند. اما حقیقت این است که تروریسم امروزه آنقدر گسترده شده است که همگام با تحولات جوامع یا شتابان‌تر از آن، متحول شده و هر روز چهرهٔ جدیدی از خود نشان می‌دهد که همهٔ آنها را نمی‌توان با دید سنتی و ویژگی‌های آن تحلیل کرد. دستیابی تروریست‌ها به سلاح‌های کشندهٔ تشعشعی، میکروبی، شیمیایی و هسته‌ای دورنمایی غیرحصری از گونه‌های نوین تروریسم را در معرض چشم جهانیان قرار داده که بیانگر نیاز جامعهٔ جهانی برای انطباق خود با آنهاست. علاوه‌بر این موارد باید اقدامات تروریستی سایبری را نیز افزود که به عقیدهٔ برخی با توجه به ویژگی‌های

1. Thomas Wingfield.
2. World Wide Web.

منحصربه‌فرد فضای سایبر و دسترسی آسان تروریست‌ها به سلاح‌های سایبری (یک رایانه و اینترنت در هر جایی) به‌مراتب محتمل‌تر و پیچیده‌تر و خطرناک‌تر از اقسام جدید تروریسم می‌نماید (Berner & Goodman, 2002: 12-15).

تروریسم سایبری در جهانی متفاوت به نام جهان سایبر تولد یافته و رشد می‌یابد. حضور تروریست‌ها در جهان سایبر گویای این است که پدیدهٔ تروریسم گامی نو برداشته و به‌روز شده است. بهره‌گیری از فناوری‌های نوین در عملیات سایبری این سؤال را به ذهن متبادر می‌کند که این عملیات مشمول عنوان جرم سایبری است یا تروریسم سایبری؛ به‌عبارت دیگر، آیا تروریسم در فضای مجازی قابلیت تحقق دارد یا خیر؟ در ذیل با انطباق عملیات سایبری با ویژگی‌های تروریسم سنتی و فیزیکی و بهره‌مندی از نظر صاحب‌نظران فضای سایبر، به بررسی مسئله می‌پردازیم و جرایم سایبری را از تروریسم سایبری تفکیک می‌کنیم.

در ابتدا باید به این نکته اشاره داشت که اصطلاح تروریسم سایبری نیز مانند خود تروریسم لفظی چالش‌برانگیز و اختلافی است که در مورد تعریف و مصادیق آن اجماعی بین صاحب‌نظران وجود ندارد. برخی متخصصان آن را بسیار مضیق تعریف کرده‌اند و آن را صرفاً مرتبط با تجهیز نیرو در گروه‌های تروریستی شناخته‌شده برای حمله‌های ویرانگر بر ضد سیستم‌های اطلاعاتی با مقاصدی همچون هشداردهی یا ایجاد وحشت دانسته‌اند. با این تعریف محدود، مشکل بتوان یک نمونه اقدام تروریستی سایبری مثال زد. نقطهٔ مقابل این تعریف، تعریف کلی و عام تروریسم سایبری است که عبارت است از به‌کارگیری عامدانهٔ اعمال مخرب یا تهدید به آن علیه رایانه‌ها یا شبکه‌های داده با قصد ایراد صدمهٔ اجتماعی، عقیدتی، مذهبی، سیاسی یا موضوعاتی مشابه که این مقاله نیز تعریف دوم را پذیرفته و مبنای نظر خود قرار داده است.

اصطلاح سایبر تروریسم را اولین بار باری کالین[1]، محقق ارشد مؤسسهٔ امنیت و اطلاعات در کالیفرنیا، در دههٔ ۱۹۸۰ به‌کار برد. به اعتقاد او سایبر تروریسم عبارت بود از: «سوءاستفادهٔ عمدی از یک سیستم، شبکه یا مؤلفهٔ اطلاعاتی رایانه‌ای برای تحقق هدفی که مؤید یا تسهیل‌کنندهٔ اقدام تروریستی باشد» (Collin, 1997: 15-18). از آن زمان تاکنون نیز هیچ تعریفی ارائه نشده که مقبولیت جهانی یابد، زیرا تعیین قصد، شخصیت یا انگیزهٔ سیاسی حمله‌کننده یا حمله‌کنندگان بسیار دشوار و گاهی غیرممکن است و در برخی موارد نیز تعیین عامل آن کاری بسیار دشوار است.

مرکز حفاظت از زیرساخت‌های آمریکا[2] تروریسم سایبری را به‌عنوان یک عمل غیرقانونی ارتکاب‌یافته از طریق رایانه‌ها که به خشونت، مرگ یا تخریب منجر می‌شود و به‌منظور وادارسازی یک دولت به تغییر سیاستگذاری‌اش به‌کار می‌رود، تعریف می‌کند (Clay, 2003: 4).

1. Barry Collin.
2. National Infrastructure Protection Center.

دوروتی دنینگ[1] تعریف دیگری ارائه می‌دهد. او می‌گوید: «تروریسم سایبری عبارت است از تلاقی تروریسم با فضای مجازی. تروریسم سایبری اغلب به معنای حملات غیرقانونی ضد رایانه‌ها و اطلاعات ذخیره‌شده در آنهاست که هدف از آن ارعاب یا اجبار یک دولت یا اتباع آن به‌منظور پیشبرد اهداف سیاسی یا اجتماعی است. این حملات باید به اعمال خشونت علیه اشخاص یا دارایی‌ها منجر شود یا دست‌کم به‌اندازه‌ای آسیب وارد کند که ایجاد ترس و وحشت عمومی کند» (Denning, 2001: 241).

از نظر دنینگ، برای در نظر گرفتن این حملات به‌عنوان تروریسم سایبری، حمله باید به خشونت علیه اشخاص یا اموال یا حداقل ایجاد ترس و ارعاب عمومی منجر شود، مثلاً حمله باید به مرگ یا جرح، انفجار، سقوط هواپیما، آلودگی منبع آب یا خسارات شدید اقتصادی بینجامد (Denning, 2001: 241).

مخالفان وقوع تروریسم سایبری برای رد وقوع این پدیده، آن را با تروریسم فیزیکی مقایسه کرده و معتقدند برخی از ارکان اصلی تروریسم از جمله خشونت، ایجاد وحشت عمومی و خسارت جانی و مالی در این‌گونه از تروریسم وجود ندارد و به همین دلیل آنها معتقدند که این عملیات را باید جرم سایبری دانست نه تروریسم سایبری. به نظر آنها جرایم سایبری و تروریسم سایبری مانند هم نیستند و استفاده از رایانه‌ها به‌عنوان تسهیل‌کنندهٔ اقدامات تروریستی، اعم از اینکه برای تبلیغات، عضوگیری، استخراج اطلاعات، برقراری ارتباط یا مقاصد دیگر باشد، تروریسم سایبری نیست (Weimann, 2004: 2). آنها همچنین معتقدند که اگرچه این عملیات تروریسم سایبری نیستند، اما باید تأثیرات بالقوهٔ این عملیات را بررسی کرد، زیرا توانایی بسیاری در آسیب زدن به منافع دولت‌ها دارند (Weimann, 2005: 129) که به‌نظر می‌رسد تا حدودی با حرف قبلی آنها در تضاد باشد.

به‌نظر می‌رسد که تعریف مضیق ایراداتی دارد؛ اولاً قائلان به آن در اقلیت‌اند و بسیاری از حقوقدانان و کارشناسان سایبر آن را نپذیرفته و ناقص می‌دانند؛ ثانیاً این نظریه با واقعیات دنیای کنونی و نیازهای عملی آن مطابقت ندارد؛ ثالثاً بررسی و تطبیق تروریسم سایبری با تروریسم سنتی اشتباه است، زیرا آنها تفاوت‌های تعیین‌کننده‌ای دارند و مانند قیاس نادرست حقوق بین‌الملل با حقوق داخلی است؛ رابعاً ادعای این نظریه بر فقدان ویژگی‌های اصلی تروریسم در اعمال سایبری نادرست است و اتفاقاً این ویژگی‌ها با درجهٔ شدت بیشتری در اقدامات سایبری یافت می‌شود.

با توجه به موارد ذکرشده، تعریف ما از تروریسم سایبری شامل نه‌تنها شکلی از تهاجم می‌شود که در بالا ذکر شد، بلکه طرق گوناگون استفاده از اینترنت به‌منظور بقا و پیشبرد اهداف تروریستی را نیز شامل می‌شود. این مفهوم موسع همهٔ اقدامات مربوط به تروریسم را در برمی‌گیرد.

---

1. Dorothy Denning.

گفتیم که مخالفان وقوع تروریسم سایبری در قسمتی از استدلالات خود بـه فقـدان ارکـان اصلی تروریسم در اقدامات سایبری اشـاره داشـتند. اسـتدلال اول بـرای تحلیـل نظـر مخالفـان تروریسم سایبری به ویژگی خشونت مربوط می‌شود. استفاده از خشونت یا تهدیـد بـه آن اغلـب به‌عنوان یکی از ارکان اقدامات تروریستی مطـرح مـی‌شـود. اینکـه آیـا شـیوهٔ ارتکـاب اقـدامات تروریستی لزوماً باید خشونت‌آمیز باشد و از خود آثاری به‌جای بگذارد و اصولاً اینکه چه وسـایل یا روش‌هایی باید وجود داشته باشد که اقدامی تروریستی قلمداد شود، تا حدودی مبهم است.

مفهوم خشونت و رفتار خشن امری نسبی است که متناسب با زمـان و مکـان ممکـن اسـت شدت آن کم یا زیاد شود. از عبارت خشونت یا تهدید به آن در تعریف تروریسم، مشخص اسـت که ضرورتی ندارد که خشونت فیزیکی باشد، بلکه خشونت در هر شکل آن مـی‌توانـد موجبـات تحقق اقدامات تروریستی را فراهم آورد. باید گفت که حتی وقوع خشونت هم نیاز نیسـت، زیـرا صرف تهدید به خشونت هم اقدام را تروریستی می‌کند. تروریست با اسـتفاده از خشـونت سـعی دارد تا ترس و دلهرهٔ بی‌پایانی را در جامعه ایجاد کند و دامنهٔ آن را علاوه‌بـر قربانیـان مسـتقیم خود، به گروه زیادی از شاهدان و بینندگان نیز تعمیم دهد (Oots, 1990: 145-6). بایـد توجـه داشت که روش و شیوهٔ ارتکاب عمل تروریستی یا خشونت به‌کاررفتـه در آن در هـیچ سـند یـا حتی رویهٔ منطقه‌ای و بین‌المللی احصا نشده و در همه جا به نتیجهٔ این خشونت (ایجاد ترس و وحشت) توجه شده است (پاکزاد، ۱۳۹۰: ۷۱). اگر این استدلال را بپذیریم، مشـاهده مـی‌کنـیم که تروریسم سایبری توانایی ایجاد تـرس و وحشـت بسـیار فزاینـده‌ای را نسـبت بـه تروریسـم فیزیکی داراست، زیرا تروریسم در گذشته به حاکم‌کشی و دولتمردکشی مشغول بود و بـه‌دلیـل نبود سلاح‌هایی مانند شیمیایی، میکروبی، هسته‌ای و سایبری، رعب و وحشت نیز در مقایسه بـا تروریسم مدرن کمتر بود.

برعکس نظر مخالفان، کارشناسان حوزهٔ سایبر بر ایـن باورنـد کـه سـایبر تروریسـم توانـایی تخریـب بسـیار بیشـتری نسـبت تروریسـم فیزیکـی و سـنتی دارد(Knake, 2010: 1). ایـن نتیجه‌گیری در واقـع از ایـن حقیقـت سرچشـمه مـی‌گیـرد کـه تروریسـم سـایبری مـی‌توانـد زیرساخت‌های مربوط به اماکن حساس دولتی، کنترل مراکز امنیـت هواپیمـا، کنتـرل سـدها و مراکز دادهٔ پزشکی را علاوه‌بر زیرسـاخت‌هـای مـالی و تجـاری هـدف قـرار دهـد کـه خشـونت به‌کاررفته در آنها و نتیجهٔ آن می‌تواند فاجعه‌ای بشری را سبب گردد (Hensen, 2006: 4).

از آنجا که تاکنون مصادیق اقدامات تروریستی توأم با خشونت بوده‌اند، بـر ایـن ویژگـی تأکیـد شده است. به‌علاوه، صرف تهدید به خشونت هم اقدام تروریستی محسوب می‌شود، بنابراین تحقـق عینی خشونت در ارتکاب یک اقدام تروریستی ضرورت ندارد. اشکال جدیـد تروریسـم بـه‌ویـژه در تروریسم سایبری، خشونت به آن‌گونه که در سایر گونه‌های تروریسم وجود دارد، دیده نمی‌شـود و در واقع شاهد خشونت نرم در این حوادث هستیم، اما کسی منکر خشونت در این اقدامات نیست.

در قانونگذاری‌های اخیر هم از آنجا که تأکید افراطی بر روی لفظ خشونت موجب محدود شدن مصادیق تروریسم می‌شد، از واژه‌هایی استفاده شده است که تمام مواردی را که امنیت را به خطر می‌اندازد، در برگیرد. به‌طور مثال در قانون تروریسم مصوب ۲۰۰۰ انگلستان در بند B قسمت ۲ مادهٔ ۱، در مورد حمله، واژهٔ «خشونت» را که در قانون ۱۹۸۹ به‌کار رفته بود، به واژهٔ «آسیب» تغییر داد (Walker, 2006: 632) .

در نهایت می‌توان گفت که تفسیر واژه خشونت بسیار گسترده‌تر از معنای گذشته باید در نظر گرفته شود و بنا به نیاز و مقتضیات روز باید آن را تفسیر کرد و گاهی توسعه داد. به همین دلیل در تعاریف جدیدتر به‌جای خشونت از آسیب استفاده شده است.

نکتهٔ بعد در خصوص تحقق تروریسم سایبری به این نکته برمی‌گردد که آیا تروریسم سایبری قابلیت ایجاد خسارات جانی و مالی شدید به افراد را داراست یا خیر. مخالفان تحقق تروریسم سایبری بر این باورند که تروریسم سایبری حاصل بزرگ‌نمایی برخی دولت‌هاست و آنها در پی این هستند تا به این بهانهٔ دخالت خود در فضای سایبر را توجیه کنند و گسترش دهند(Brito & Watkings, 2011: 61).

آنچه در پاسخ به این ایراد مطرح می‌شود، در دو قسمت بیان می‌شود. در قسمت اول به بررسی این مسئله می‌پردازیم که برای تروریستی دانستن اقدامی، آیا آن اقدام باید حتماً به خسارات جانی یا مالی منتهی شود یا خیر؟ و قسمت دوم اینکه آیا تروریسم سایبری به خسارات جانی یا مالی منتهی می‌شود یا خیر؟

سوابق تجربی ثبت‌شدهٔ مربوط به رخدادهای واقعی تروریستی، شباهت اندکی با تصویرهای رسانه‌ای و باورهای عمومی رایج دارد. برای روشن‌تر شدن بحث اطلاعاتی را از پروژهٔ ایترات-۴(ITERATE-4)[1] استخراج کرده‌ایم که اثبات می‌کند تلفات جانی و مالی لزوماً شرط تروریستی دانستن اقدامی نیست، بلکه تلفات جانی و مالی حتی در حوادث تروریستی نیز استثناست تا قاعده.

واقعیت این است که تنها تعداد محدودی از حوادث تروریستی به مرگ اشخاص منجر شده است. مجموع تعداد تلفات ثبت‌شدهٔ ناشی از حوادث تروریستی بین‌المللی در بازهٔ زمانی سال‌های ۱۹۹۴-۱۹۶۸، برابر ۹۶۵۴ نفر ثبت شده است. نکتهٔ حائز اهمیت این است که براساس آمار این سایت، در این بازهٔ زمانی ۱۰۸۳۷ اتفاق و حادثهٔ تروریستی به‌وقوع پیوسته است. طبق اطلاعات پروژه، بیشتر این حوادث تروریستی (۹۲۱ مورد یا ۸۵/۵ درصد) اساساً بدون تلفات انسانی بوده است. در ۸۷۶ مورد (۸/۱ درصد) از این حوادث، تنها یک نفر جان باخته است. حوادث تروریستی بدون تلفات انسانی و آن دسته از حوادث که به مرگ یک نفر

۱. یک پایگاه اطلاعاتی دربارهٔ حوادث تروریستی که سال به سال اطلاعات حوادث تروریستی در سرتاسر جهان را نشان می‌دهد.

منجر شده است، در مجموع، ۹۳/۶ درصد از کل حوادث تروریستی بین‌المللی را تشکیل داده‌اند. طی دورهٔ زمانی ۲۷ سالهٔ مورد بحث در این پژوهش به‌طور میانگین ۱/۵۵ نفر در هر حادثهٔ تروریستی آسیب جسمی دیده و در ۸۹۰۷ مورد از حوادث تروریستی کسی حتی آسیب هم ندیده است(Flemming, 2000: 6-10). بنابراین اگرچه تصویری که از تروریسم در ذهن داریم به‌صورت حوادث بزرگ با کشته‌ها و مجروحان فراوان است، ولی واقعیت این است که اغلب حوادث تروریستی بین‌المللی بدون هیچ‌گونه تلفات یا با تلفاتی بسیار اندک و بدون آسیب دیدن کسی به پایان رسیده است.

حال با داده‌های کمی می‌توان به این نتیجه رسید که اقدامات تروریستی نیازی به ایجاد خسارات جانی یا مالی ندارد و ممکن است بدون تحقق آنها نیز آن اقدام را تروریستی قلمداد کرد. اگرچه وقوع حوادث پرتلفات را نیز نمی‌توان انکار کرد، اعداد نشان می‌دهند که این حوادث استثنا هستند و نباید هستهٔ اصلی اقدام تروریستی را وقوع خسارات شدید جانی یا مالی دانست، بلکه هستهٔ تروریسم و اقدامات تروریستی، ترس و ارعاب و اغلب انگیزهٔ سیاسی انجام آن است که این موارد در تروریسم سایبری نیز حتی با شدت بیشتری از تروریسم سنتی قابل مشاهده است. امروزه قطع برق، قطع سیستم کنترل هوایی یا باز کردن سدها به‌مراتب ایجاد رعب و وحشت بیشتری می‌کند و افراد بیشتری را درگیر می‌کند و در نظام اقتصاد کشور تأثیر شایان توجه‌تری نسبت به گذشته می‌گذارد.

بخش دوم بحث به این بازمی گرد که آیا تروریسم سایبری قابلیت تحقق نتیجهٔ فیزیکی و ورود خسارت را دارد یا خیر؟ نتیجه زمانی تحقق می‌یابد که حملهٔ سایبری به نتایجی ویران‌کننده منتهی شود که در مقایسه با تروریسم سنتی برای ایجاد ترس کافی باشد. در این رویکرد برخی مانند دنینگ که از نخستین نظریه‌پردازان جنگ اطلاعات و تروریسم سایبری است، بر تحقق نتیجهٔ فیزیکی تأکید دارند و معتقدند حمله به سامانه‌های رایانه‌ای باید به ورود خسارت مادی و فیزیکی و حتی مرگ اشخاص منتهی شود (Denning, 2001: 288).

این رویکرد که در واقع نخستین رویکرد به تروریسم سایبری بوده، با توجه به ذهنیت موجود از تروریسم سنتی مطرح شده است. در این ذهنیت، تروریسم سایبری صرفاً فن یا شیوهٔ جدید انجام اقدامات تروریستی سنتی محسوب می‌شود، یعنی اقدامات تروریستی سنتی در دنیای واقعی از طریق حمله به سامانه‌های رایانه‌ای کنترل‌کنندهٔ خدمات یا فعالیت‌ها در دنیای سایبر صورت گیرد.

ایرادات وارد به این رویکرد عبارت است از اینکه، همان‌گون‌که همگان در مورد آن اجماع دارند، حملات تروریستی سایبری می‌تواند به ایجاد خرابکاری در بسیاری از تأسیسات زیربنایی از جمله کنترل هواپیما، سدها، سیستم حمل‌ونقل عمومی، بیمارستان‌ها و مراکز حساس نظامی منجر شود. آیا به هم ریختن سیستم حمل‌ونقل عمومی یا بیمارستان‌ها یا به دست گرفتن

کنترل یک سد یا یک دستگاه هسته‌ای به ایجاد آسیب یا خسارت مالی منجر نمی‌شود؟ آیا سرازیر کردن آب یک سد بر روی شهر نزدیک آن که به‌وسیلهٔ حملات سایبری به مرکز کنترل آن سد امکان‌پذیر شده، کمتر از نتیجهٔ شلیک به یک گروه است؟ به‌نظر می‌رسد که هیچ چیزی وجود ندارد که ما را از این نتیجه که تروریسم سایبری به نتیجهٔ فیزیکی منجر می‌شود، بازدارد یا به‌عبارت دیگر می‌توان گفت که تأثیرات مخرب حادث‌شده از سایبر تروریسم علاوه‌بر فضای مجازی در دنیای واقعی نیز قابل رؤیت است. حتی به‌دلیل حساس بودن اماکنی که تروریست‌های سایبری آنها را هدف قرار می‌دهند، ممکن است حادثهٔ تروریستی بعدی پرل هاربر دیجیتال باشد.[۱]

ایراد دیگر وارد بر این رویکرد این است که جرایم تروریستی اصولاً و کلاً مقید به نتیجه نیستند، حال چگونه است که در تروریسم سایبری تحقق نتیجهٔ فیزیکی لازم و ضروری دانسته شده است. به‌علاوه، در تهدید به خشونت اصولاً خشونت و حمله‌ای واقع نمی‌شود، اما صرف تهدید به آن جزو حملات تروریستی محسوب می‌شود و نیازی به تحقق نتیجه در عالم واقع لازم دانسته نمی‌شود (Sieber, 2012: 12).

رویکرد اخیر به نظر با ماهیت تروریسم سایبری سازگارتر است، زیرا مقید کردن حمله‌های سایبری به تحقق نتیجهٔ فیزیکی ایراداتی اساسی دارد: اولاً دلیلی بر این محدودیت و مقید کردن وجود ندارد؛ ثانیاً چه‌بسا اهمیت آسیب‌ها و صدمات غیرفیزیکی ناشی از حمله‌های تروریستی سایبری بیش از صدمات فیزیکی باشد؛ ثالثاً چنانچه ما خود را در قلمرو آنچه تروریسم سنتی نامیده می‌شود محصور کنیم، فقط می‌توانیم حملاتی را تروریسم بدانیم که شاید بدترین فجایع ممکن در زمان حیات بشریت باشند. اما واقعیت‌ها نشان می‌دهد که همان‌گونه‌که تروریسم سنتی را بسیار گسترده در نظر گرفتیم، تروریسم سایبری را نیز به‌حدی موسع در نظر بگیریم که دربردارندهٔ دامنهٔ کاملی از تهدیدات، آسیب‌پذیری‌ها، خطرها و موضوعات فنی باشد.

با توجه به استدلالات مطروحه و تا حدودی قیاس شروط تروریسم سایبری با تروریسم فیزیکی سنتی از یک سوی، و اجماع کارشناسان در خصوص وجود حملات سایبری می‌توان به این نتیجه رسید که تروریسم سایبری قابلیت تحقق در فضای سایبر را دارد. اگر حملات

---

۱. نیروی هوایی و دریایی ژاپن در هفتم دسامبر ۱۹۴۱ به پایگاه دریایی آمریکا در پرل هاربر، واقع در جزایر هاوایی در اقیانوس آرام، حمله کردند و صدمات بسیار سنگینی به آمریکایی‌ها وارد ساختند. نتیجهٔ این حمله برای نیروی دریایی آمریکا یک فاجعهٔ کامل بود. ۳۶۰ هواپیمای ژاپنی توانستند ۵ نبردناو بزرگ آمریکایی را به‌همراه ۳ کشتی کوچک‌تر غرق کنند. ۳ نبردناو دیگر به‌گونه‌ای آسیب دیدند که توان عملیاتی خود را از دست دادند. علاوه‌بر آن، ۱۸۸ هواپیمای آمریکایی بر روی زمین نابود شدند و ۱۵۵ هواپیمای دیگر آسیب دیدند. در پایان آن روز بیش از ۲۴۰۰ کشته و ۱۲۴۰ مجروح نیز بر دست نیروی دریایی آمریکا مانده بود.

سایبری شدید باشد و به‌حدی برسد که موجب ترس عمومی مردم شود و با انگیزهٔ سیاسی (اصولاً) صورت پذیرد، می‌توان گفت که آن حملهٔ تروریسم سایبری بوده است و احکام تروریسم را بر آن بار کرد. قسمت دوم بحث در خصوص این مسئله خواهد بود که آیا در صورت وقوع حملات سایبر تروریسم آیا دفاع مشروع و مادهٔ ۵۱ مندرج در منشور سازمان ملل متحد قابل اعمال است؟ و این دفاع مشروع شامل چه اقداماتی است؟ آیا الزاماً باید در فضای مجازی باشد یا امکان توسل به قوای نظامی نیز وجود دارد؟

تروریسم سایبری و نقض مقررهٔ منع توسل به زور مندرج در منشور ملل متحد

منشور سازمان ملل متحد و حقوق بین‌الملل بر ممنوعیت استفاده از زور توسط دولت‌ها تأکید دارند. منشور در بند ۴ مادهٔ ۲ مقرر داشته است که: کلیهٔ اعضا در روابط بین‌المللی خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری یا هر روش دیگری که با مقاصد ملل متحد مباینت داشته باشد خودداری خواهند کرد. این ماده با ممنوعیت توسل به زور به‌جای جنگ، از بحث در مورد اینکه آیا هر مخاصمه‌ای جنگ است یا خیر، خودداری کرده است. اگرچه برخی نویسندگان تفسیری مضیق از بند ۴ مادهٔ ۲ منشور داشته و بر این عقیده‌اند که در مواردی اعضا می‌توانند به زور متوسل شوند، بدون آنکه آن زور علیه تمامیت ارضی یا استقلال سیاسی کشوری دیگر یا به شیوه‌ای مغایر با اهداف سازمان ملل در نظر گرفته شود؛ اما رویکرد عمومی آن است که هر گونه توسل به زور از طرف یک کشور علیه نیروهای کشور دیگر یا در قلمرو دولت دیگر، با مادهٔ ۲(۴) مغایرت خواهد داشت (دیتر فلیک و دیگران، ۱۳۸۷: ۲۰-۱۹)؛ به‌استثنای مورد «حق ذاتی دفاع مشروع» که در مادهٔ ۵۱ منشور آمده است (Ziccardi Capaldo, 2007: 105). منشور عبارت توسل به زور را به‌کار برده است تا هر نوع برخورد مسلحانه و تجاوز را در برگیرد و اقدامات خصمانه کمتر از جنگ از دایرهٔ ممنوعیت خارج نشود.

در پروندهٔ «نیکاراگوئه علیه ایالات متحده»، «دیوان بین‌المللی دادگستری[1]» تأیید کرد که ممنوعیت استفاده از زور همچنین اصلی از «حقوق بین‌الملل عرفی» است (Case concerning to military and paramilitary activities in and against Nicaragua, Merits,1986: para. 186). با این حال، از آنجا که منشور سازمان ملل هیچ‌یک از این عبارات را تعریف نکرده، تعیین دقیق اینکه چه نوع عملی مصداق استفاده از زور یا حمله مسلحانه است، جای بحث و تفسیر دارد. یکی از موارد خوب برای فهم استفاده از زور یا حملهٔ مسلحانه قطعنامه مجمع عمومی سازمان ملل در خصوص تعریف تجاوز است (Schaap, 2009: 129).

1. International Court of Justice.

مادۀ ۱ از این قطعنامه ادبیاتی شبیه بند ۴ مادۀ ۲ منشور را به‌کار می‌برد و می‌گوید: «تجاوز عبارت است از استفاده از نیروی مسلح توسط یک کشور علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی کشوری دیگر یا به صورتی برخلاف منشور سازمان ملل متحد» (General Assembly 3314 Resolution on the Definition of Aggression, 1974: 2). مادۀ ۳ از این قطعنامه هفت اقدام را به‌عنوان مصداق تجاوز ذکر کرده و مادۀ ۴ نیز عنوان می‌دارد که این فهرست کامل نیست (Ibid: 3).

برای تحلیل این موضوع که عملیات سایبر ناقض تمامیت ارضی کشوری دیگر است یا نه، حادثۀ «یو-۲»[1] در سال ۱۹۶۰ می‌تواند مورد خوبی باشد. این حادثه به سرنگونی هواپیمای شناسایی غیرمسلح آمریکا با موشک زمین به هوا در ۱۲۰۰ مایلی درون مرزهای اتحاد جماهیر شوروی مربوط می‌شد. اتحاد جماهیر شوروی اظهار داشت که پروازهای یو-۲ بر فراز قلمرو شوروی اقدامی تجاوزکارانه است؛ با این حال، شورای امنیت سازمان ملل مخالفت کرده و نتیجه‌گیری کرد که هرچند پرواز یو-۲ نقض حریم هوایی شوروی بوده، ولی مصداق استفادۀ غیرقانونی از زور با توجه به بند ۴ مادۀ ۲ منشور سازمان ملل نمی‌شود (S/Agenda/857, 1960: 2). با توجه به این قضیه و با عطف به این مسئله که امروزه کارشناسان فضای مجازی را در کنار قلمرو دریایی، زمینی و هوایی، چهارمین عرصۀ نبرد در میان کشورها می‌دانند، شاید بتوان گفت که اگر نقض فضای هوایی حاکم بر کشور دیگر مصداق استفادۀ غیرقانونی از زور نیست، شاید نقض شبکه‌های مجازی کشوری دیگر نیز به‌طور خودکار مصداق استفادۀ غیرقانونی از زور نشوند. با این حال، وقتی اقداماتی بیش از گردآوری صرف اطلاعات صورت پذیرد، آنگاه مسئله کمی دچار ابهام می‌شود و به تحلیل بیشتری نیاز دارد.

رابطۀ اقدامات سایبری با نقض قاعدۀ منع توسل به زور و حق ذاتی دفاع مشروع

ممنوعیت توسل به زور مندرج در مادۀ ۲ منشور، به میزان زیادی به‌عنوان سنگ بنای منشور ملل متحد و حقوق بین‌الملل عرفی پذیرفته شده است. اما مادۀ ۲ معنای دقیق واژۀ «زور» را مقرر نداشته و همین مسئله باب تفاسیر متعددی را در این خصوص باز کرده است.

در خصوص مسئلۀ اقدامات سایبری نیز این سؤال طرح می‌شود که آیا این اقدامات را می‌توان ناقض اصل منع توسل به زور دانست که متعاقباً برای پاسخ به آن به حق ذاتی دفاع مشروع مقرر در مادۀ ۵۱ منشور توسل پیدا کرد یا خیر؟

1. U-2 Incident.

به‌طور کلی می‌توان دو دیدگاه را در خصوص اینکه آیا حملهٔ سایبری می‌تواند مشمول عنوان «توسل به زور» باشد یا خیر، بیان داشت. یک دیدگاه بر این است که ممنوعیت توسل به زور تنها محدود به حملهٔ مسلحانه و با سلاح‌های سنتی و توسط یک دولت است و بنابراین حملهٔ سایبری خارج از شمول مادهٔ ۲(۴) منشور است. این رویکرد، رویکردی مضیق به قواعد ایجادشده توسط جامعهٔ بین‌المللی است و مقرر می‌دارد که هر چیزی که خارج از این ممنوعیت قرار گیرد، قانونی است. دیدگاه دوم رویکردی است موسع و مقرر می‌دارد از آنجا که یکی از اهداف منشور حفظ صلح و امنیت بین‌المللی است و منشور هر گونه توسل به زور که صلح و امنیت بین‌المللی را به مخاطره افکند، ممنوع کرده است. این رویکرد دلالت دارد که تمام انواع فشار در یک مرتبه و جایگاه قرار دارد و میان فشار نظامی با فشار سیاسی، اقتصادی و سایبری تفاوتی وجود ندارد. بنابر این رویکرد می‌توان گفت که حملات سایبری که زیرساخت‌های حیاتی یک دولت را هدف قرار می‌دهند و موجب خسارت می‌شوند، می‌تواند در محدودهٔ مادهٔ ۲(۴) منشور قرار گیرد. بر این اساس هدف نویسندگان منشور تنها ممنوع ساختن تعارضات مسلحانه نبوده، بلکه هر اقدامی که می‌توانسته صلح و امنیت بین‌المللی را به مخاطره اندازد، مورد نظر بوده است. مادهٔ ۲ منشور توسل به زور را از هر طریقی که مغایر با اهداف منشور باشد، ممنوع کرده است. از سوی دیگر، این ماده دولت‌ها را از توسل به زور علیه تمامیت ارضی دولت دیگر منع کرده است. عبارت «تمامیت ارضی» را می‌توان به طرق گوناگونی تفسیر کرد، از جمله اینکه تمامیت ارضی یک دولت، فضای سایبری او را هم در برمی‌گیرد، بنابراین هر گونه خرابکاری در این فضا، تجاوز به تمامیت ارضی آن دولت است.

هرچند محتوای هر دو دیدگاه مورد مجادلات و مباحثات فراوانی قرار گرفته، اهمیت اساسی آنها در این حقیقت نهفته است که هر دو دیدگاه به این نکته اذعان دارند که حملهٔ سایبری در بعضی حالات می‌تواند حملهٔ مسلحانه و نقض اصل منع توسل به زور حساب شود.

باید توجه داشت که این دیدگاه در خصوص حملات سایبری است که مستقلاً صورت پذیرند و نه به‌عنوان مقدمه یا ضمیمهٔ صف‌آرایی نیروهای نظامی، هوایی و دریایی در مقابل هم، زیرا در مواردی که حملات سایبری به موازات حملهٔ مسلحانهٔ زمینی، دریایی و هوایی به قلمرو یک کشور صورت گیرد، شبیه آنچه در حملات سایبری علیه گرجستان واقع شد، تردیدی در حملهٔ مسلحانه بودن آن وجود ندارد (Sharp, 1999: 60). از سوی دیگر به‌دلیل ناکافی بودن اسناد و تفاسیر مربوط به منشور سازمان ملل، برای جواب بهتر این سؤال باید به نظریات حقوقدانان بین‌المللی مراجعه کرد. به نظر آقای «برانلی» اقدامات سایبری را می‌توان ناقض اصل مندرج در مادهٔ ۲ منشور دانست. استدلال او هم این است که باید نتیجه را در نظر بگیریم. او اذعان می‌دارد که استفاده از سلاح‌های شیمیایی، میکروبی، هسته‌ای و سایبری باید به‌منزلهٔ توسل به زور در نظر گرفته شوند، زیرا این ابزارها برای نابودی اموال و نفوس به‌کار می‌روند (Brownlie, 1963: 362).

در حملات سنتی هدف از حمله نقش اساسی در آن ندارد و در هر صورت بـه دولـت مـورد هدف امکان دفاع مشروع می‌دهد، زیرا صرف مخدوش شدن تمامیت ارضی کشور در اثـر حملـه کافی به‌نظر می‌رسد. بنابراین اگر یک حمله بـا توسـل بـه سـلاح‌هـای سـنتی علیـه تأسیسـات غیرنظامی در قلمرو دولت هدف، حمله‌ای مسلحانه محسـوب مـی‌شـود؛ حتـی اگـر هـیچ عضـو نیروهای مسلح دولت هم صدمه نبیند یا اموال نظامی نیز تخریب نشود، دلیلی وجود ندارد که در خصوص حملات سایبری علیه سیستم‌های رایانه‌ای همانند سیستم‌های سدها و بیمارستان‌ها ولو خصوصی، به نتیجه‌ای مخالف برسیم و آن را حملهٔ مسلحانه ندانیم (Dinstein, 2005: 115).

در اینجا نقش مفهوم زیرساخت‌های حیاتی بسیار پررنگ است، زیـرا حملـهٔ سـایبری علیـه شبکهٔ رایانه‌ای هر ساختاری را نمی‌توان حملهٔ مسلحانه سایبری دانست، بلکه این ساختارها باید زیرساخت‌های حیاتی باشند. در این خصوص شایان ذکر است که در سطح بین‌المللی هیچ‌گونـه اجماعی در خصوص اینکه چه زیرساخت‌هایی حیاتی‌اند، وجود ندارد. سـازمان ملـل متحـد نیـز مقـرر داشـته کـه هـر کشـوری خـود زیرسـاخت‌هـای حیـاتی اطلاعـاتی‌اش را مشـخص می‌سازد(A/Res/58/199, 2004: 1) و بر این ابهام دامن زده است.

«یورام دینستین[1]» نیز نتیجهٔ خشونت‌آمیز را کلید حل مشکلات مربوط به اقدامات سایبری می‌داند. به نظر او از دیدگاه حقوقی دلیلی ندارد بین ابزارهای فیزیکی و الکترونیکی برای حمله، تمایز قائل شویم. اگر اقدامات سایبری بتواند نتایج مـورد نظـر را ایجـاد کنـد، مـی‌توانـد حملـهٔ مسلحانه قلمداد شود. به نظر او دشواری مسئله در وسیلهٔ ارتکاب نیست _چه توپخانـهٔ دشـمن باشد چه یک سرور رایانه‌ای_، بلکه در میزان و وقوع نتایج است (Dinstein, 2005: 103). البتـه همان‌طورکه توضیح داده شد، براساس نتایج تحقیقات وقـوع نتیجـه نیـز شـرط ضـروری بـرای تروریستی دانستن اقدامات نیست.

به‌طور کلی تا زمانی‌که اجماعی در جامعهٔ جهانی در این خصـوص بـه‌وجـود نیایـد، تفاسـیر متفاوتی در این زمینه وجود خواهد داشت که انطباق حملهٔ سایبری با مفهـوم توسـل بـه زور را دشوار خواهد ساخت.

علاوه‌بر اسناد و منشور سازمان ملل متحد و پس از بررسی نظر حقوقدانان می‌توان برای جواب این سؤال به رویهٔ قضایی رجوع کرد. به‌نظر می‌رسد که رویـهٔ قضـایی نیـز تـا حـدودی بـه سـمت تعریف موسع از زور که در این مقاله نیز مبنا قـرار گرفتـه اسـت، تمایـل دارد. دیـوان بـین‌المللـی دادگستری در قضیهٔ تنگهٔ کورفو ادعای دولت بریتانیا مبنی بر اینکه عملیات مین‌روبی در آب‌هـای سرزمینی دولت آلبانی نقض مادهٔ ۲(۴) نبوده، زیرا با هدف نقـض تمامیـت ارضـی آلبـانی صـورت نگرفته است، تعریف مضیق از توسل به زور را نپذیرفت و اعـلام کـرد کـه اقـدام بریتانیـا در اعـزام کشتی‌های جنگی برای پاکسازی مین‌ها از کانال کورفو، برخلاف خواسـتهٔ صـریح آلبـانی، موجـب

1. Yoram Dinstein.

اعمال نوعی سیاست زور و تجاوز شده است که در حقوق بین‌الملل محملی ندارد (Case concerning to Corfu channel 1948: para. 13). دیوان همچنین در نظریهٔ مشورتی سلاح‌های هسته‌ای بیان داشت که به‌منظور اعمال حقوق منشور در مورد توسل به زور و حقوق قابل اعمال در مخاصمات مسلحانه، باید ویژگی منحصربه‌فرد سلاح‌های هسته‌ای مورد نظر قرار گیرد (Legality of the threat or use of nuclear weapons (Advisory opinion 1996: para 36). همین رویکرد را باید در خصوص اقدامات تروریستی سایبری نیز مورد توجه قرار داد.

در آوریل ۲۰۰۷، وب‌سایت‌های مهمی در کشور استونی، از سوی یک سری «حملات قطع سرویس» (DOS[1]) مورد هجوم قرار گرفتند. این حملات تا مدت‌ها به‌صورت منقطع نیز ادامه پیدا کردند و تبعات سوء اجتماعی، اقتصادی زیادی برای استونی به‌همراه داشت و در نهایت به این نتیجه منجر شد که رئیس‌جمهور استونی از کشورش به‌عنوان اولین کشور قربانی تروریسم سایبری نام ببرد و این حمله نیز به «پرل هاربر دیجیتال»[2] معروف شد که تا آن روز بزرگ‌ترین و طولانی‌ترین حملهٔ سایبری به‌شمار می‌رفت (Myres, 2007: 1). سخنگوی وزارت دفاع استونی در این زمینه اعلام داشت که اگر شما با موشکی به کشوری حمله کنید یا اگر عملیاتی را طراحی کنید که غیرقانونی و خشونت‌آمیز باشد که با ایجاد ترس و ارعاب در میان مردم شما را به خواسته‌های سیاسی یا غیرسیاسی شما برساند، این عملیات جنگ یا تروریسم نام دارد. سپس این سؤال را مطرح می‌کند که اگر همین نتیجه از طریق رایانه‌ها و اینترنت و موارد مشابه به‌دست آید، شما نام آن را غیر از تروریسم سایبری چه می‌گذارید (Aaviksoo, 2010: 14)؟ این سؤال دقیقاً با نظریات برانلی و دینستین و نظریهٔ تفسیر موسع هماهنگ است.

جاک آویکسو[3]، وزیر دفاع استونی این حملات را وضعیت امنیت ملی نامید و آن را با تعطیلی بنادر دریایی مقایسه کرد. چنین مقایسه‌ای جالب توجه است، زیرا بند «ج» مادهٔ ۳ از قطعنامهٔ مجمع عمومی سازمان ملل در تعریف تجاوز «محاصرهٔ بنادر یا سواحل یک کشور از سوی نیروهای مسلح کشوری دیگر» را به‌عنوان اقدامی تجاوزکارانه طبق مفاد ماده ۵۱ منشور قلمداد می‌کند. با این حال باید بیان داشت که مادهٔ ۴۱ از منشور سازمان ملل «وقفهٔ کامل یا جزیی از روابط اقتصادی و نیز خطوط راه‌آهن، دریایی، هوایی، پستی، تلگراف، رادیو و دیگر امکانات ارتباطاتی» را به‌عنوان «اقدامی که شامل نیروی مسلح نمی‌شود» مورد توجه قرار می‌دهد. آویکسو پس از مذاکره با مقامات ناتو گفت: «در حال حاضر، ناتو عملیات سایبر را به‌عنوان یک اقدام صریحاً نظامی تعریف نمی‌کند. این بدان معناست که مقررات مادهٔ ۵ از پیمان آتلانتیک شمالی یا به کلام دیگر دفاع از خود دسته‌جمعی، به‌طور خودکار به کشور

1. Denial of Service.
2. Digital Pearl Harbor.
3. Jaak Aaviksoo.

قربانی این عملیات اطلاق پیدا نمی‌کند» (Russia Accused of Unleashing Cyber Warfare to Disable Estonia, 2007: 1).

بحث در مورد اینکه آیا این نوع عملیات سایبر را می‌توان مصداق استفاده از زور دانست، در اوت ۲۰۰۸ و در پی اتهامات گرجستان به روسیه برای حمله به سایت‌های دولتی این کشور پس از آغاز حملهٔ نظامی به آن، دوباره بر سر زبان‌ها افتاد. در ۷ اوت ۲۰۰۸ و در پی تحرکات جدایی‌طلبانه در گرجستان، نیروهای گرجستان حمله‌ای غافلگیرانه علیه نیروهای جدایی‌طلب را اجرا کرد. در ۸ اوت، مسکو این اقدام تفلیس را با عملیات نظامی در خاک گرجستان تلافی کرد که از نگاه مقامات این کشور تجاوز نظامی علیه آن بود. غروب ۷ اوت و قبل از تهاجم روسیه به گرجستان، حملات سایبری علیه وب‌سایت‌های دولتی تفلیس شروع شد که خود از اولین نمونه‌هایی بود که در آن یک تهاجم سایبری هماهنگ با نبرد سیاسی و نظامی همراه می‌شد.

اسکات برگ[1]، رئیس «واحد پیامدهای سایبر ایالات متحده»[2]، از نهادهای فکری مشاور دولت و کمپانی‌های آمریکایی، در آن زمان عنوان داشت که «در جهانی به‌سر می‌بریم که دولت‌ها هنوز در مورد ابزارهای حملات سایبر تصمیم‌گیری نکرده‌اند» و «برداشت بین‌المللی حقیقتاً روشنی در مورد این موضوعات نداریم»(Gorman, 2008: 1). سخنگوی پنتاگون هم در همین زمینه اضافه کرد که «در نهایت این به نظر کشور تحت حمله بستگی دارد که این اقدامات را حملهٔ نظامی بداند یا خیر، زیرا اجماع یا قاعده‌ای در خصوص این مسئله وجود ندارد و این مسئله از چالش‌های نوین عرصهٔ بین‌الملل محسوب می‌گردد» (Gorman, 2008: 1).

اکنون این سؤال مطرح است که چه سطحی از پیامد این‌گونه حملات موجب می‌شود موضوع به استفاده از زور ارتباط یابد و چه سطحی از انتساب به دولت در این حملات استفاده دفاعی از زور علیه یک کشور را توجیه می‌کند؟ بی‌شک اقدامی فراتر از ورود به یک وب‌سایت دولتی یا ایجاد اختلال حداقلی در خدمات یک دولت برای مصداق یافتن استفاده از زور نیاز است. با این حال، در مورد ورود یا اختلال در سیستم‌های کسب داده‌ها و کنترل عناصر شبکه‌های برق، شبکه‌های کنترل ترافیک و نیروگاه‌های هسته‌ای چه می‌توان گفت؟ احتمالاً این یکی از سناریوهای بعدی در مورد استفاده از زور و حملهٔ مسلحانه در حوزهٔ عملیات سایبر خواهد بود. در یکی از تحقیقات انجام‌گرفته توسط پژوهشگران دولت آمریکا موسوم به «آزمایش ژنراتور آرورا»[3] میزان آسیب‌پذیری در رایانه‌های یکی از شرکت‌های برق این کشور بررسی شد. آزمایش مذکور نشان از آسیب‌پذیری آن شرکت در مقابل حملات سایبر داشت.

در زمان پاسخ به چنین حمله‌ای، باید به‌خاطر داشت که هیچ چیزی در مادهٔ ۵۱ پاسخ یک

1. Scott Borg.
2. The U.S Cyber Consequences Unit.
3. Aurura Generator Test.

کشور به نوع حملهٔ مورد استفاده از سوی مهاجم را محدود نمی‌سازد. ایالات متحده نیز به‌صورت رسمی بیان کرده است که واکنش به حملات سایبری با هر وسیلهٔ مقتضی، از جمله حملهٔ نظامی را سیاست خود قرار می‌دهد (Verton, 2002: 1).

با توجه به مصادیق حملات سایبری که طی سال‌های ۲۰۰۷ و ۲۰۰۸ به استونی و گرجستان صورت گرفت یا پس از آن حملهٔ سایبری که به قطع برق در چند شهر از ایالات متحدهٔ آمریکا منجر شد (Bogdanski, 2013: 62)، پس از در نظر گرفتن بحث‌های مطرح‌شده توسط متخصصان در این زمینه می‌توان این‌گونه برداشت کرد که این حملات فی‌نفسه و اگر به خسارت و ارعاب منجر نشود و با قصد سیاسی نباشد، جرم سایبر است و در قالب مادهٔ ۵۱ منشور سازمان ملل و بحث حملهٔ مسلحانه نمی‌گنجد و نمی‌توان در مقابل آن به دفاع مشروع فردی یا جمعی دست زد. در نهایت باید گفت که اگر بتوان آن را به دولتی منتسب کرد، آن دولت مطابق با مقررات بین‌المللی مسئولیت خواهد یافت. ناتو نیز در زمان بررسی حملهٔ صورت‌گرفته به استونی به این مهم اشاره کرد (CCDCOE, International cyber incidents: legal considerations, 2010: 26). اما این حملات اگر با خسارت و ارعاب همراه باشد و به قصد وادار ساختن دولتی به انجام کار خاصی یا تغییر ساختار همراه باشد، می‌توان آن را تروریسم سایبری در نظر گرفت و حرف کارشناسان را که بر این باورند تروریسم در فضای سایبری قابلیت تحقق ندارد رد کرد، زیرا تحقیق ژنراتور آرورا ثابت کرد که رایانه‌ها در تمام مناطق جهان در قبال حملات صفر و یک دارای ضعف و آسیب‌پذیری بوده و از دیگر سوی ثابت شده است که این‌گونه حملات اگر به‌سوی زیرساخت‌های حساسی مانند رآکتورهای اتمی، شبکه‌های برق، امکانات بهداشتی و پزشکی یا منبع‌های آب صورت گیرند، قابلیت تحقق خسارت و ارعاب را به‌صورت بالفعل دارند که حوادث تروریستی‌ای مانند چرنوبیل یا متروی لندن یا توکیو یا حتی حادثهٔ ۱۱ سپتامبر به گرد آن هم نمی‌رسند. انگیزهٔ سیاسی که معمولاً در بیان ویژگی‌های عملیات تروریستی مطرح می‌کنند هم، ویژگی‌ای شخصی است که فقط منحصر به عملیات سنتی نیست و در حملات سایبری هم امکان وقوع دارد.

نتیجه‌گیری

تروریسم سایبری امروزه به نگرانی‌های حقوقی و سیاسی بین‌المللی در زمینهٔ تروریسم اهمیت دوچندانی بخشیده است. مشکل فقدان تعریف موجود در تروریسم سنتی بر سر این نوع جدید از تروریسم سایه افکنده و آن را با پیچیدگی‌های فزاینده‌ای همراه کرده است. از دیگر سوی چالش‌های ذاتی فضای سایبر نیز مزید بر علت شده و این اصطلاح را به چالش‌برانگیزترین مباحث روز مبدل ساخته است. در تمام متن‌های کارشده در این زمینه همگی متخصصان تروریسم سایبری را امری بدیهی پنداشته و در پی روشن ساختن ابعاد و زوایای پنهان آن بودند

که البته در این عرصه موفق هم بودند، اما کمتر کسی در پی اثبات حقوقی این مسئله بود و به‌راحتی از کنار آن می‌گذشتند. در این مقاله سعی کردیم تا با مطالب موجود دست به استدلال، قیاس و کاهی تفسیر موسع بزنیم و وجود و قابلیت اثبات این امر را حداقل به‌صورت ناقص و ضعیف محرز کنیم تا هم تفکر جامعهٔ حقوقی را به این سمت متوجه سازیم و هم آغازگری باشیم برای مطرح شدن استدلالات متقن و مستدل در این عرصه. در نهایت نیز با بررسی ابعاد و ویژگی‌های تروریسم سنتی و نوین به این نتیجه رسیدیم که هزارهٔ جدید با آمدن خود بسیاری از مفاهیم و اصول مسلم را دچار تغییر کرد و از جملهٔ آنها ویژگی‌ها و برداشت‌های سنتی و خشک از تروریسم بود. نیازها و اقتضائات عصر جدید دیگر در چارچوب برداشت‌های سنتی نمی‌گنجد و از جملهٔ این اقتضائات تروریسم سایبری بود. در این تحقیق تروریسم سایبری را با برداشت‌های نوینی از ویژگی‌های تروریسم سنتی مطرح ساختیم و به این نتیجه رسیدیم که حتی با در نظر گرفتن ویژگی‌های تروریسم سنتی نیز، تروریسم سایبری قابلیت تحقق دارد. در قسمت دوم نیز دیدیم که این اقدامات قابلیت این را دارند که در شرایط خاصی مشمول مادهٔ ۵۱ منشور ملل متحد و تابع حق ذاتی دفاع مشروع قرار گیرند.

منابع

۱. فارسی

الف) کتاب‌ها

۱. پاپ، دانیل و دیوید آلبرتس (۱۳۸۵). *امنیت در عصر اطلاعات، الزامات امنیت ملی در عصر اطلاعات*، ترجمهٔ علی‌آبادی و رضا نخجوانی، چ اول، تهران: انتشارات پژوهشگاه مطالعات راهبردی.

۲. پاکزاد، بتول (۱۳۹۰). *تروریسم سایبری تهدیدی نوین علیه امنیت ملی*، تهران: انتشارات معاونت آموزشی دانشگاه آزاد.

۳. دیترفلک و دیگران (۱۳۸۷). *حقوق بشردوستانه در مخاصمات مسلحانه*، ترجمهٔ قاسم زمانی، نادر ساعد و دیگران، چ اول، تهران: مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهر دانش.

۴. نیاورانی، صابر (۱۳۸۹). *تحول مفهوم دفاع مشروع در حقوق بین‌الملل*، رسالهٔ دکتری، دانشگاه شهید بهشتی

۵. هیبلز گری، کریس (۱۳۸۱) *جنگ پست‌مدرن، سیاست نوین درگیری*، ترجمهٔ احمدرضا تقاء، تهران: انتشارات دورهٔ عالی جنگ.

ب) مقالات

۶. ملکی‌زاده، امیرحسین (۱۳۹۱). «تحلیل مفهوم قابلیت انتساب مسئولیت بین‌المللی در رویهٔ دیوان بین‌المللی دادگستری»، *فصلنامهٔ راهبرد*، سال بیست‌ویکم، ش ۶۴، ص ۲۷۳.

۲. لاتین

A) Book

7. CCDCOE, *International cyber incidents: legal considerations*, 2010.
8. Brownlie, Ian, (1963). *International law and the use of force by states*, Oxford University press.
9. Denning, Dorothy, (2001). *Activism, Hacktivism and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy*, In: Aquila and Ronfeldt, Networks and Net wars: the Future of Terror, Crime, and Militancy, Santa Monica, RAND Corporation.
10. Dinstein, Yoram, (2005). *War, Aggression and self-defense*, Cambridge University press, 4th ed.
11. Flemming, Peter, (2000). *Myths and Realities of Cyberterrorism*, Office of International Programs and the Center for Education and Research in Information Assurance and Security, Purdue University.
12. Oots, Kent, (1990). *Bargaining with Terrorist: Organizational Consideration, Terrorism*, vol.13.
13. Rowe, A.J and S.A Davis. (1996). *the Intelligent Information Systems: Meeting the Challenge in the Knowledge Era*, Greenwood Publishing Group
14. Sharp, Walter gray, (1999). *cyber warfare and the use of force*, Aegin research corporation.
15. Wingfield, Thomas (2000). the Law of Information Conflict: National Security Law in Cyberspace
16. Verton, Dan, (2002). *The prospect of Iraq conflict raises new cyber-attack fears*, computerworld.

B) Article

17. Aaviksoo, Jaac, (2010). Cyber-attacks against Estonia Raised Awareness of Cyber threats*", Defenses against Terrorism Review,* Vol.3, No2
18. Bogdanosky, Mitko, (2013). Cyber Terrorism˚ Global Security Threat, International Scientific Defence*", Security And Peace Journal,* NO. 24(13)
19. Brenner, Susan &Marc Goodman, (2002). In Defense of Cyberterrorism: An Argument for Anticipating Cyber Attacks*", Journal of Law, Technology and Policy.*
20. Brito, Jerry and Tate Watkins, (2011). *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, Harvard National Security Journal, Vol.3
21. Capaldo, Giuliani ziccardi, (2007). providing a Self-Defense against large scale

attacks by irregular forces: The Israeli- Hezbollah conflict*"*, *Harvard international law journal*, vol. 48
22. Clay, Wilson, (2003). Information Warfare and Cyberwar: Capabilities and Related Policy Issues*", CRS Report RL31787*.
23. Collin, Barry, (1997). *The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge*, 11th Annual International Symposium on Criminal Justice Issues.
24. Cornish, Paul and et seq, (2010). *on cyber Warfare, A Chatham House Report".*
25. Gorman, Siobhan, (2008). Cyber Attacks on Georgian Websites are Re-igniting Washington Debate*", The Wall Street Journal*.
26. Hansen, James and et seq, (2006). *Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection*, Decision Support System, Vol.43(4).
27. Hessbrugge, Jan Arna, (2004). The historical development of attribution and due diligence in international law*", New York University journal of international law*, Vol.36
28. Roscini, Marco, (2010). world wide warfare- jus ad bellum and use of cyber force*", Max plunk yearbook of united nation law*, Vol. 14.
29. Schaap, A.J, (2009). Cyber Warfare Operations: Development and Use under International law*", Air Force law review*, vol 64.
30. Schmitt, Micheal N., (2012). Attack as a Term of Art in International law: the Cyber Operations Context*"*, 4th international conference on cyber conflict, Tallinn: NATO CCD COE Publications.
31. Walker, Clave, (2006). Cyberterrorism: Legal Principle and Law in the United Kingdom*", Penn State Law Review*, vol.110:3
32. Weimann, Gabriel, (2005). Cyberterrorism: The Sum of All Fear*?"* 28 Studies in Conflict and Terroris

C) Document

33. Council of Europe, (2005). Organized Crime in Europe: The Threat of Cybercrime, Situation Report 2004, Council of Europe Publishing
34. Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities, (2011)
35. Inter-American commission on human rights (Valesquez Rodrigues V Honduras), (1998). Series C, Decisions and Judgments, No. 04
36. Sieber, Ulrich, Cyber terrorism: Use the Internet for Terrorism Purposes, UNODC Report, 2012.
37. Trail Smelter Case (US V Canada), (1931). UN Reports of international arbitration awards
38. Weimann, Gabriel, (2004). Cyberterrorism: How Real is the Threat? United States Institute for Peace, Special Report 119, 2004.

Websites:

39. http://daccess-ods.un.org/TMP/4252361.05918884.html
40. http://itlaw.wikia.com/wiki/Estonia_cyberattack
41. http://www.cfr.org/terrorism-and-technology/cyberterrorism-hype-v-fact/p21434
42. http://www.cnet.com/news/cia-cyberattack-caused-multiple-city-blackout/
43. http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html?_r=0
44. http://www.theguardian.com/world/2007/may/17/topstories3.russia
45. http://www.merriam-webster.com/dictionary/cyberspace
46. https://en.wikipedia.org/wiki/Cyberterrorism