



تحول مفهوم دفاع مشروع و تروریسم نوین (با تأکید بر تروریسم سایبری)^۱

احسان صادقی پور^۲
محمود گنج بخش^۳
کورش جعفرپور^۴

تاریخ دریافت مقاله: ۱۴۰۳/۰۶/۰۶ تاریخ پذیرش نهایی: ۱۴۰۳/۰۸/۳۰

چکیده

پدیده تروریسم در بستر پیشرفت جوامع با سرعت چشمگیری خود را دگرگون کرده است. امروزه از نوین‌ترین گونه‌های تروریسم که توجه بسیاری از اندیشمندان حقوقی را به خود جلب کرده تروریسم سایبری است. بدین ترتیب با افزایش روزافزون گونه‌های جدید تروریسم و به دنبال آن حملات تروریستی در نقاط مختلف جهان و واکنش دولت‌ها در برابر این حملات، سبب گردیده موضوع توسل به زور در قبال اقدامات تروریستی به مسأله مطرح در محافل حقوقی تبدیل گردد. در واقع پس از حادثه ۱۱ سپتامبر و گسترش تهدید فرامرزی تروریسم، گروهی از حقوقدانان دکترین حمله پیشدستانه و پیشگیرانه را در قالب تفسیر موسع از ماده ۵۱ منشور ملل متحد برای مقابله با تروریسم ارائه کردند. با در نظر گرفتن این که در عصر حاضر تروریسم از حالت سنتی خارج شده و اشکال مدرن آن تحت عنوان موج تروریسم نوین به مانند تروریسم سایبری در حال گسترش است، ضرورت دارد این مسأله بررسی شود که با توجه به تفاوت بنیادین بین تروریسم سنتی با تروریسم نوین استناد به دفاع مشروع در برابر تروریسم نوین (سایبری) مشروعیت حقوقی دارد؟ و متعاقباً توسل به حمله پیشدستانه و پیشگیرانه در مقابله با آن از منظر حقوق بین الملل چه توجیهی دارد؟ در این راستا جهت پاسخگویی به این مسأله از روش تحقیق توصیفی - تحلیلی با استفاده از ابزار کتابخانه‌ای بهره گرفته شده است. به نظر می‌رسد حمله تروریستی چنانچه پتانسیل ایجاد تخریب در حد یک حمله

^۱ این مقاله مستخرج از رساله دکتری تخصصی رشته حقوق بین‌الملل عمومی دانشگاه آزاد اسلامی واحد تهران جنوب با عنوان "واکاوی توسل به دفاع مشروع در مقابله با تروریسم نوین از منظر حقوق بین‌الملل با تأکید بر تروریسم سایبری" می‌باشد.
^۲ دانشجوی دکتری حقوق بین‌الملل عمومی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.
st_e_sadeghipoor@azad.ac.ir
^۳ استادیار گروه اقتصاد و بانکداری اسلامی، دانشکده اقتصاد، دانشگاه خوارزمی، تهران، ایران (نویسنده مسؤل):
Ganjbakhsh@khu.ac.ir
^۴ استادیار گروه حقوق خصوصی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران. K.Jafarpour@ut.ac.ir

مسلحانه را داشته باشد، مسلحانه فرض شده و دولت قربانی از حق دفاع مشروع برخوردار خواهد بود اما حقوق بین الملل چیزی به نام حمله پیشدستانه و پیشگیرانه شناسایی نکرده است.

کلید واژه‌ها

دفاع مشروع، حمله پیشدستانه، حمله پیشگیرانه، تروریسم نوین، تروریسم سایبری.

مقدمه

یکی از دغدغه‌های مهم در عرصه حقوق بین الملل، تروریسم بوده است که خود را به اشکال مختلف نشان داده است (نعمت پور و دیگران، ۱۴۰۲: ۱۷۴). به عبارتی تحول و پیشرفت فناوری‌های اطلاعاتی و ارتباطی به گروه‌های تروریستی این امکان را داده است تا به سرعت و به راحتی از یک مکان به مکان دیگر انتقال یابند (جان پرور و دیگران، ۱۳۹۷: ۱۰۰). این تغییرات سبب شده است تا اقدامات تروریستی طی دهه‌های اخیر وسعت جغرافیایی بیشتری یابد و با افزایش چشمگیر، وحشت حاصل از این اقدامات در میان عامه مردم رسوخ کند. در سال‌های اخیر تروریسم از حالت سنتی خارج شده و اشکال مدرن آن تحت عنوان موج تروریسم نوین در حال گسترش است. تروریسم سایبری از جدیدترین مصادیق آن می‌باشد. از تلاقی اعمال تروریستی و فضای سایبر گونه‌ای نوپا از اعمال تروریستی با عنوان تروریسم سایبری پا به عرصه وجود نهاده است که با وجود نوظهور بودن به مراتب خطرناک تر از تروریسم سنتی است و تهدیدات آن برای امنیت ملی کشورها به خطری بالقوه تبدیل شده است (عباسی کلیمانی و دیگران، ۱۳۹۹: ۱۴۷). این امر سبب شده است تا دولت‌های قربانی چنین حملاتی اغلب در پاسخ و با استناد به حق دفاع از خود دست به اقدامات گسترده نظامی علیه گروه‌های تروریستی مستقر در خاک دیگر کشورها بزنند. بدین ترتیب از نظر سنتی حمله مسلحانه فقط به حملاتی که از جانب دولت‌ها صورت می‌گرفت اطلاق می‌شد اما به رسمیت شناختن این که اعمال کنشگران غیردولتی می‌تواند منجر به یک حمله مسلحانه شود، بدون شک تحولی انقلابی در حقوق بین‌الملل است. در حالی که در حملات تروریستی فاجعه بار نظیر حملات القاعده شکل جدیدی از مخاصمه مسلحانه شکل گرفته است یعنی فراتر از حمله مسلحانه مندرج در ماده ۵۱ و در چنین وضعیتی دولت قربانی می‌تواند در جایگاه دفاع مشروع به زور متوسل شود (سرتیبی و دیگران، ۱۳۹۱: ۱۷). در واقع شورای امنیت با تصویب قطعنامه‌های مطابق با حقوق بین‌الملل نظیر قطعنامه ۱۳۶۸ با متصف کردن این اقدامات به توسل به زور مسیر را برای ظهور مفاهیم جدیدی از دفاع مشروع (حمله پیشدستانه و پیشگیرانه) هموار نمود و کشورها فرصت آن یافتند که در چارچوب دفاع مشروع به مبارزه با این پدیده هولناک بپاخیزند (شریفی طرازکوهی و فتح پور، ۱۳۹۶: ۲۱۲). به عبارتی پس از حادثه ۱۱ سپتامبر این مفاهیم تکوین یافته و به دلیل عدم کفایت و بسندگی منشور ملل متحد در مواجهه با معضل تروریسم، زیربنائی تئوریک برای

قدرت‌های بزرگ برای مبارزه با تروریسم فراهم آورد. در حال حاضر قواعد منشور فقط از طریق تفسیر مورد تقویم قرار گرفته‌اند. لیکن در موارد زیادی این تفسیر باعث هماهنگی بیشتر آن با واقعیات جامعه‌ی امروز شده و در برخی موارد تفاسیر متفاوت موجب عدم تجانس گردیده‌اند. با در نظر گرفتن این که تروریسم نوین برخلاف تروریسم سنتی دارای ابعاد و مشخصه‌های پیچیده و گسترده‌ای است هدف این نوشتار پاسخ به این سؤال است که آیا امکان توسل به زور در مقام دفاع مشروع علیه تروریسم نوین (سایبری) وجود دارد؟ و این که استناد به دکترین توسعه دفاع مشروع در مقابله با آن چه توجیه حقوقی دارد؟ گسترش یافتن تروریسم نوین در میان کشورهای گوناگون و ماهیت سیال آن سبب شده است تا حقوق بین‌الملل نتواند اقدامات درخوری را در این خصوص انجام دهد. به نظر می‌رسد علاوه بر فقدان تعریف جامع از پدیده تروریسم که به اجماع جامعه بین‌المللی رسیده باشد، نقص اساسی منشور ملل متحد مزید بر علت است که هدفش صرفاً برخورد با موجودیتی به نام دولت بوده است. تهدیداتی مانند تروریسم از سوی حقوق بین‌الملل سنتی قابل پیش‌بینی نبوده و جای خالی آن به خوبی در منشور احساس می‌شود این دو عامل باعث شده است که دولت‌ها در راستای منافع ملی تفاسیری از ماده ۵۱ ارائه دهند که در هیچ جای منشور به چشم نمی‌خورد که قطعاً ادامه آن در دراز مدت موجب بی‌ثباتی و ناامنی در حقوق بین‌الملل را فراهم می‌کند. ناگفته نماند در زمینه موضوع مزبور پژوهش‌های حقوقی جامعه‌ی که منجر به نتایج وحدت بخش شود، انجام نشده و نکته جدیدی که بتواند راهگشای مشکلات ایجاد شده در این خصوص باشد، را ارائه نمی‌دهند. با توجه به این که مقوله دفاع مشروع نیز در روند تکامل و تحول در حقوق بین‌الملل در پی ورود موضوعاتی همچون تروریسم نوین نیازمند روشنگری و تبیین بیشتری می‌باشد. بر این اساس پژوهش حاضر ابتدا پدیده تروریسم نوین را تبیین می‌نماید، سپس به بررسی تحول دفاع مشروع و امکان سنجی توسل به آن در برابر حملات تروریسم نوین (سایبری) می‌پردازد و نهایتاً استناد به حمله پیشدستانه و پیشگیرانه در مقابله با آن و خلاء حقوق بین‌الملل در این زمینه را مورد ارزیابی قرار می‌دهد.

۱- تروریسم نوین^۱

اصطلاح «تروریسم نوین»، غالباً پس از رویداد ۱۱ سپتامبر ۲۰۰۱ متداول شده و محور مطالعات تروریسم را تشکیل داده است، اما قدمت این اصطلاح به سال‌های پایانی جنگ سرد باز می‌گردد تا این که در حادثه ۱۱ سپتامبر به اوج خود می‌رسد. به عبارتی بسیاری از تحلیل‌گران بر این باورند که از میانه دهه ۱۹۹۰ تروریسم به سمت شکل جدیدی تغییر جهت داده که خصوصیات جدیدی پیدا کرده است. وقوع حوادثی نظیر حملات ۱۱ سپتامبر ۲۰۰۱م، بمب‌گذاری در مرکز تجارت جهانی در ۱۹۹۳م و حمله به

¹ New terrorism

متروی توکیو در ۱۹۹۵م با گاز سارین نشانه‌هایی از تغییر اساسی در تروریسم بوده و بیان‌گر مسأله‌ای است که از آن به تروریسم نوین نام می‌برند. پژوهشگران مطالعات تروریسم در غرب و حتی در خاورمیانه، برای شناخت و بررسی تحول جدید در تروریسم، به مطالعه و تحلیل این رویداد می‌پردازند. به نظر ایزابیل دایوستین، استاد تاریخ روابط بین‌الملل در هلند، تروریسم نوین اولاً به لحاظ مرتکبان و سازمان‌دهی، سرشتی فرامرزی دارد؛ ثانیاً مبتنی بر نوعی افراط‌گرایی مذهبی است؛ ثالثاً هدفش حمله به بیشترین مردم ممکن است و به سلاح‌های کشتار جمعی دسترسی دارد و و رابعاً قربانیان خود را به دقت انتخاب و دستچین نمی‌کند، بلکه آن‌ها را به صورت غیر تبعیض‌آمیز انتخاب می‌کند. از این رو تروریسم نوین از قابلیت‌ها و امکانات دنیای مدرن بهره می‌برد. به گونه‌ای که عمل تروریستی در کیلومترها دورتر به منصفه ظهور می‌رسد اما گروه مزبور در یک منطقه از جهان برنامه ریزی عملیات را بر عهده می‌گیرد. به عبارتی فناوری‌های نوین، هدف‌گیری تروریستی را آسان‌تر و مقابله با آن را مشکل‌تر ساخته است. عصر کنونی، عصر تشدید درگیری‌های شدید کوتاه مدت است. به عنوان مثال در سال ۲۰۱۶ خط تلفن اضطراری ضد ترور اسکاتلند یارد ۲۲ هزار تماس تلفنی در رابطه با اطلاعات مربوط به پیشگیری و تحقیق درباره جنایات جهادی، دو برابر بیشتر از ۲۰۱۴ دریافت کرد (گوئرتز، ۱۴۰۱: ۱۲). به عبارتی تروریسم نوین در این عصر جهانی می‌اندیشد و جهانی عمل می‌کند (ناجی راد، ۱۳۹۸: ۲۸۵). در دسترس بودن سلاح‌های کشتار جمعی، به ویژه نوع هسته‌ای و بیولوژیکی آن، سبب شده است تا تروریست‌های معاصر خطرناک‌تر از قبل شوند. علاوه بر این تکنولوژی ارتباطات، ارتباط تروریست‌ها با یکدیگر را سهل کرده است. در واقع، گروه‌های تروریستی با بهره‌گیری از انواع نوآوری‌های عصر جدید، توانسته‌اند ابتکارات خود را توسعه دهند و به طور سریع راهبردهای خود را به کار گیرند، در حالی که در گذشته این امر امکان‌پذیر نبود. در جهانی که به طور فزاینده‌ای بر فناوری مبتنی است و تأمین امنیت دشوارتر شده است، با رمزگذاری سامانه‌های انتقال پیام، امکان شناسایی افراد و شبکه‌های تروریستی پیچیده‌تر شده است. شاید تنها ابزاری که جهانیان همگی به صورت مشترک از آن استفاده می‌کنند فناوری اطلاعات و ارتباطات الکترونیکی باشد. به همین دلیل، از آن جا که تروریست‌ها به دنبال انعکاس جهانی اقداماتشان هستند، این فضا می‌تواند بهترین انتخاب باشد چرا که هر گونه اختلال در آن به خوبی بازتاب جهانی دارد و به راحتی اعتبار یک کشور خدشه دار می‌شود.

۲- تروریسم سایبری^۱ مصداقی از تروریسم نوین

در حال حاضر ما شاهد موج پنجم تروریسم یا همان تروریسم سایبری هستیم. چرا که فناوری سایبری با از بین بردن مرزها، تهدیدات خطرناک و نوینی را برای تمدن بشری به ارمغان آورد (فرشاسعید و

^۱ Cyber terrorism

دیگران، ۱۴۰۱: ۱۷۲). از آن جا که بحث تروریسم سایبری به دلیل نوظهور بودن فضای سایبر جدید است و همانند تروریسم سال‌ها موضوع تحقیق و مطالعه نبوده است، نمی‌توان انتظار داشت به آن اندازه تعاریف و تحلیل‌های گوناگون موجود باشد. به عبارتی در مورد تعریف پدیده تروریسم سایبری به مانند تروریسم اجماع تعریف بین کارشناسان این حوزه وجود ندارد و همچنان واژه‌ای بحث برانگیز است. اصطلاح تروریسم سایبری را اولین بار محقق ارشد موسسه امنیت و اطلاعات کالیفرنیا باری کالین،^۱ به کار برد. از نظر وی سایبر تروریسم: سوءاستفاده عمدی از یک سیستم، شبکه یا مؤلفه اطلاعاتی رایانه‌ای برای تحقق هدفی که مؤید یا تسهیل کننده اقدام تروریستی باشد (رزمخواه، ۱۴۰۲: ۵) یا دوروتی دیننگ^۲ استاد علوم رایانه‌ای در سال ۲۰۰۱ تروریسم سایبری را چنین تعریف می‌نماید: حملات غیرقانونی غیرقانونی و تهدید علیه رایانه‌ها، شبکه و اطلاعات به منظور ارباب مردم و حاکمیت برای پیشبرد اهداف سیاسی و اجتماعی می‌باشد (امیرلی و تقفی، ۱۳۹۸: ۳۹۵). نبرد در محیط سایبر به دلیل ارزان بودن حملات، مجهول ماندن هویت حمله‌کنندگان، مشکلات موجود در بحث انتساب و مبهم بودن قواعد قابل اعمال در فضای سایبر در مقایسه با جنگ‌های سنتی از استقبال بیشتری برخوردار است. فضای سایبری شرایطی را فراهم کرده است که با هزینه پایین می‌توان اقدامات خطرناکی را در مدت زمان کم و با سرعت بالایی انجام داد. هر فرد برای انجام حمله سایبری تنها به ارتباط اینترنتی، یک رایانه و دانش فنی محدود در زمینه فضای سایبری نیاز دارد. البته، انجام حملات سایبری شدیدتر مستلزم صرف هزینه‌های بالاتری است. بنابراین فضای سایبری و فناوری‌های مرتبط با آن یکی از مهمترین منابع قدرت در هزاره سوم می‌باشند (Li & Liu, 2021: 8184). حمله ویروس استاکس نت به تأسیسات هسته ایران نمونه بارزی از حمله سایبری است. استاکس نت به عنوان کرم صنعتی با هدف حمله سایبری به زیر ساخت‌های حیاتی صنعت ایران و آسیب رسانی به تأسیسات هسته‌ای نظیر طراحی و منتشر شده بود. مورد دیگر، براساس گزارش‌ها القاعده اطلاعات خود درباره هدف هایش را از راه اینترنت بدست می‌آورد و از همان راه نیز رمزگذاری می‌کرد. در سپتامبر ۲۰۰۲، گزارش‌ها نشان می‌دهند که سلول‌های القاعده در آمریکا برای ارتباط با سلول‌های این گروه در مناطق دیگر، از تلفن اینترنتی بهره می‌برده‌اند. یا حملات سایبری از سوی گروه هکری وابسته به تروریسم سازمان مجاهدین خلق به وب سایت‌های وزارت خانه‌ها و سازمان‌های حساس ایران مثل وزارت کشور و وزارت خارجه. این رویدادها نشان می‌دهند که اینترنت به یک ابزار جنگ مجازی برای تروریست‌ها تبدیل شده است. بدین گونه تروریست سایبری می‌تواند با از کار انداختن امکانات فنی، رایانه‌ها را که زندگی اجتماعی، و اقتصادی مردم وابسته با آن است، در مقیاس وسیع تری بر آن‌ها زیان رسانیده و در سطح گسترده تری

¹ Barry Collin

² Dorothy E. Denning

کشتار راه بیندازد و نیز از طریق تهدید به حمله بیشتر، از طرف‌های مقابل خود امتیاز بگیرد به هر حال، امروزه دنیای رایانه، دنیایی است که هر لحظه مورد تهدید تروریست‌ها است و احتمال حملات آتی هر چه بیشتر مردم را دچار وحشت می‌کند. در واقع این برآیند از این واقعیت نشأت می‌گیرد که حملات تروریسم سایبری علاوه بر زیرساخت‌های مالی، می‌تواند پایه‌های مربوط به اماکن حساس دولتی و یا حیاتی را شامل شود در نتیجه این امر منجر به فجایع گسترده انسانی و یا زیست محیطی شود (Hansen et.al., 2007: 4). در تعریف تروریسم، مشخص است که ضرورتی ندارد که خشونت فیزیکی باشد. خشونت در هر شکل آن می‌تواند موجبات تحقق اقدامات تروریستی را فراهم آورد. باید گفت که حتی وقوع خشونت هم نیاز نیست، زیرا صرف تهدید به خشونت هم اقدام را تروریستی می‌کند. تروریست با استفاده از خشونت سعی دارد تا دلهره بی‌پایانی را در جامعه ایجاد کند و دامنه آن را علاوه بر قربانیان مستقیم خود به خیل عظیمی از بینندگان نیز تعمیم دهد. بنابراین مفهوم خشونت امری نسبی است که ممکن است شدت آن متناسب با زمان و مکان کم یا زیاد شود.

۳- تحول مفهوم دفاع مشروع و تروریسم نوین

در حال حاضر حق دفاع مشروع دولت‌ها علیه حملات تروریستی مورد پذیرش حقوق بین الملل قرار گرفته است. لذا دولت‌های قربانی چنین حملاتی، می‌توانند به منظور دفاع از سرزمین خود، حملات نظامی علیه گروه‌های تروریستی ترتیب دهند.

۳-۱ حملات تروریسم نوین و نقض اصل منع توسل به زور

بدون احتساب مواد ۵۳ و ۱۰۷ منشور ملل متحد که مجوز توسل به زور علیه آلمان و متحدانش در جنگ جهانی دوم را در صورت لزوم صادر می‌کنند و بدین خاطر موضوعیت خود را از دست داده و متروک شده اند فقط دو ساز و کار را منشور ملل متحد جهت توسل به زور به رسمیت شناخته است، اول امنیت جمعی بر مبنای ماده ۳۹ و مواد بعد از آن؛ دوم دفاع مشروع فردی و جمعی بر مبنای ماده ۵۱. علی‌رغم این که منشور از تمام دولت‌ها می‌خواهد که برای حل و فصل مسالمت آمیز اختلافات تلاش کنند، هیچ یک از این مواد خللی به حق دفاع مشروع وارد نمی‌سازد. بنابراین گرچه توسل به زور در حقوق بین‌الملل ممنوع شده اما در بعضی از موارد استفاده از زور می‌تواند مشروع باشد. رژیم حقوقی بین‌الملل می‌کوشد در وهله اول از وقوع جنگ جلوگیری کند اما در صورت نقض پیمان استثنائاتی را آن هم در مقام دفاع می‌پذیرد. به طور سنتی، توسل به زور در مقام دفاع مشروع در برابر دولت‌ها مجاز تلقی می‌شد و در مقابل بازیگران غیردولتی مشروع تلقی نمی‌شد. با این همه پس از وقوع حملات ۱۱ سپتامبر شورای امنیت دو قطعنامه بر اساس فصل هفتم منشور صادر کرد که موجب تحول عینی در مواجهه با حملات تروریستی شد. به عبارتی قطعنامه‌های ۱۳۶۸ و ۱۳۷۳ اهمیت بسزایی در بحث دفاع مشروع در پاسخ به حملات تروریستی

و یا توسل به زور در قبال تروریسم داشتند. در پی صدور این قطعنامه‌ها دولت آمریکا با استناد به دفاع مشروع، اقداماتی را علیه طالبان و سازمان القاعده در افغانستان انجام داد. براساس تعریف ماده ۵۱ از دفاع مشروع در صورتی که یک عضو ملل متحد مورد تجاوز مسلحانه واقع شود، هیچ یک از مقررات این منشور به حق طبیعی دفاع مشروع انفرادی یا اجتماعی تا موقعی که شورای امنیت اقدام لازم برای حفظ صلح و امنیت بین‌المللی به عمل آورد لطمه وارد نخواهد آورد (ملکی زاده، ۱۳۹۷: ۲۸). بنابراین توسل به دفاع مشروع صرفاً در صورتی امکان پذیر است که حمله مسلحانه‌ای علیه هر یک از دولت‌های عضو ملل متحد به وقوع پیوسته باشد (موسی زاده و کوهی، ۱۳۸۹: ۱۲۹). سؤالی که در این خصوص مطرح است این است که آیا بر اساس ماده ۵۱ منشور ملل متحد می‌توان جهت مقابله با تروریسم نوین به حق دفاع مشروع استناد نمود؟ در پاسخ مثبت به سؤال فوق می‌توان استدلالات عدیده‌ای رو مطرح کرد: عبارت حمله مسلحانه در ماده ۵۱ منشور ملل متحد به طور مشخص تعریف نشده و ناچاراً قطعنامه ۳۳۱۴ مورخ ۱۴ دسامبر ۱۹۷۴ تحت عنوان «تعریف تجاوز» تعریف مشخصی را از آن ارائه نموده است (ICJ Reports, 2004: 139). ماده ۵۱ فقط وجود «یک حمله مسلحانه» و نه «حمله مسلحانه توسط یک دولت» را ضروری دانسته است. این عبارت نشان می‌دهد که مدونین منشور قصد داشته اند تا تمامی اشکال حمله مسلحانه را پوشش دهند. در حقیقت منشأ حمله از منظر منشور موضوعیت ندارد (Martinez Sponda, 2023: 72). این جمله بندی به اندازه کافی عام تدوین شده است تا اجازه استناد به دفاع مشروع، در برابر حمله مسلحانه، از جانب موجودیت‌های غیردولتی را نیز می‌دهد. از طرف دیگر به منظور بررسی سایر شرایط حاکم بر اعمال دفاع مشروع از جمله ضرورت، تناسب، فوریت و همچنین مفهوم حمله مسلحانه باید به حقوق عرفی موجود در این خصوص رجوع نمود. به عبارت دیگر ماده ۵۱ انعکاس بخشی از حقوق بین‌الملل عرفی می‌باشد که تنها قسمتی از ضوابط توسل به دفاع مشروع را مورد توجه قرار داده است (بهستانی، ۱۳۸۷: ۱۳۴). طبق ماده ۳۸ اساسنامه دیوان بین‌المللی دادگستری، یکی از منابع حقوق بین‌الملل، عرف بین‌المللی است که دارای دو عنصر مادی و معنوی می‌باشد. عنصر مادی همان رویه دولت‌ها و سایر تابعان حقوق بین‌الملل می‌باشد و عنصر معنوی به معنی اعتقاد حقوقی یا ضرورت وجود آن است. بدین ترتیب رویه یک شکلی از سوی دولت‌ها به تدریج و در دوره زمانی طولانی تکرار شده و تداوم یافته و به عنوان قاعده حقوق بین‌الملل عرفی پذیرفته شده است مثل حمله ایالات متحده آمریکا به لیبی به دلیل حمایت دولت لیبی از گروه‌های تروریستی، اقدام ایالات متحده علیه افغانستان به سال ۱۹۹۸ به دلیل پایگاه‌های آموزشی تروریستی بن لادن در افغانستان، اقدام ایران علیه پایگاه‌های سازمان منافقین در عراق در سال ۲۰۰۱ و... رویه همراه با اعتقاد حقوقی دولت‌ها از این نظر پشتیبانی می‌کند که کنشگران غیردولتی نیز مرتکب حمله مسلحانه می‌شوند و بدین گونه در مقابل آن حق دفاع مشروع به وجود می‌آید، که چنین روندی می‌تواند منجر به شکل‌گیری قاعده عرفی بین‌المللی باشد. نکته این است که هر چند عکس‌العمل بین‌المللی به اقدام دفاع مشروع در پاسخ به حملات

تروریستی در مواردی منفی بود اما در دهه ۹۰ و به ویژه بعد از ۱۱ سپتامبر عکس العمل بین المللی نیز تغییر کرد و در جهت تأیید این رویه پیش رفت. از طرف دیگر قطعنامه‌های سازمان ملل متحد (شورای امنیت و مجمع عمومی) نیز در برخی موارد ممکن است به عنوان دلیل حقوق بین الملل عرفی محسوب شوند یا در تشکیل حقوق عرفی جدید مؤثر باشند. شورای امنیت در قطعنامه ۱۳۶۸ با استناد به ماده ۵۱ منشور بر حق ذاتی دفاع مشروع فردی و جمعی دولت‌ها در مقابل تروریست تأکید نمود. به عبارتی شورای امنیت مسیر را برای این گفتار که ماده ۵۱ منشور، ضمن این که حاکم بر روابط میان دولت است، بر روابط بین دولت‌ها و کنشگران غیردولتی نیز حاکم است، هموار کرد. چنانچه در قطعنامه ۲۲۴۹ (مورخ ۲۰ نوامبر ۲۰۱۵) که یک هفته پس از حادثه تروریستی در پاریس، تصویب شد (SC/Res/2249, 2015: para5)، تحولی مهم محسوب می‌شود که با ایجاد عرف خلق الساعه مبنی بر تجویز دفاع مشروع در قبال گروه‌های تروریستی موجد هنجار نوین حقوق بین الملل عرفی شده است (کفایی فر و تیموری، ۱۴۰۲: ۸۴۲). حتی حقوقدانان شرکت کننده در تدوین سند اصول حقوق بین الملل در زمینه توسل به زور در دفاع مشروع بیان داشتند که حق دفاع مشروع یک حق ذاتی است و دولت قربانی حمله ی کنشگران غیردولتی در هر حال می‌تواند در برابر حمله مسلحانه به دفاع مشروع متوسل شود حتی اگر آن حمله منتسب به دولت میزبان نباشد (عزیزی و نظری، ۱۳۹۳: ۲۳۵). به هر حال در این چارچوب به موضوع توسل به دفاع مشروع در مقابله با تروریسم به عنوان بازیگری غیردولتی مورد توجه واقع شده است. پر واضح است وقایع بعد از ۱۱ سپتامبر خصوصاً جنایات دهشتناک دولت اسلامی عراق و شام و سایر گروه‌های تروریستی به مرور حقوق بین الملل را متقاعد می‌کند که دفاع مشروع در برابر حملات تروریستی بازیگران غیردولتی نوین را مجاز بدانند. در مجموع خلاء تعریف جامع از دفاع مشروع در منشور جهت توسل دولت‌ها به حق دفاع مشروع یعنی عدم اشاره به ماهیت آغازگران حمله مسلحانه (دولت‌ها یا بازیگران غیردولتی) و گسترش تهدید فرامرزی تروریسم سبب گردیده در زمینه توسل به ماده ۵۱ جهت مقابله با تروریسم، تفاسیر متفاوت حمله پیشدستانه و حمله پیشگیرانه ارائه گردد. بدین گونه به نظر می‌رسد که رویه کنونی توجه متزاید به تفسیر موسع و در جهت فاصله گرفتن از مفهوم سنتی دفاع مشروع دارد. در ادامه بحث قبل از ورود به ارزیابی وجاهت حقوقی استناد به حمله پیشدستانه و پیشگیرانه در برابر بازیگران غیردولتی نوین، حملات تروریسم سایبری و امکان توسل به دفاع مشروع را بررسی می‌کنیم.

۳-۲ حمله تروریسم سایبری به مثابه حمله مسلحانه

منشور ملل متحد در بند ۴ ماده ۲ تصریح می‌دارد: در روابط بین المللی تمامی اعضای ملل متحد از توسل به زور یا تهدید به زور علیه استقلال سیاسی یا تمامیت سرزمینی هر دولت دیگر و نیز از هر اقدامی که مابین با اهداف ملل متحد باشد، اجتناب خواهند کرد. مسأله‌ای که مطرح می‌شود این است که آیا حمله

سایبری می‌تواند نقض بند ۴ ماده ۲ منشور تلقی شود؟ بند ۴ ماده ۲ منشور ملل متحد بدون آن که تعریفی از زور ارائه دهد، ممنوعیت تهدید و توسل به زور را اعلام می‌کند، ممنوعیتی که در عین ابهام، بی‌پروا است و طبیعت پیچیده‌ی آن مهبیای تحلیل‌های مختلف است. رویکرد عمومی آن است که هر گونه توسل به زور با بند ۴ ماده ۲ منشور ملل متحد مغایرت خواهد داشت مگر تحت استثنائاتی. منشور عبارت توسل به زور را به کار برده است تا هر نوع برخورد مسلحانه را دربرگیرد و اقدامات خصمانه کمتر از جنگ از دایره ممنوعیت آن خارج نشود (میرعباسی و کورکی نژادفرایی، ۱۳۹۷: ۲۷۰). سلاح نیز ابزار مورد استفاده یا طراحی شده برای استفاده جهت صدمه زدن به دیگری یا قتل وی است. تقریباً تمامی اشیاء می‌توانند به عنوان سلاح به کار روند؛ در صورتی که قصد دارنده‌ی آن خصمانه باشد. دیوان بین‌المللی دادگستری در نظر مشورتی خود در خصوص مشروعیت تهدید یا استفاده از سلاح‌های هسته‌ای، تصریح می‌کند که بند ۴ ماده ۲ و همچنین مواد ۵۱ و ۴۲ منشور ملل متحد به سلاح خاصی اشاره نکرده‌اند. آن‌ها بر هر گونه توسل به زور، صرف نظر از سلاح مورد استفاده اعمال می‌شوند (ICJ Reports, 39: 1996). به عبارتی نظرمشورتی مذکور تأییدی است غیرمستقیم بر این مسأله که عملیات سایبری می‌تواند از مصادیق توسل به زور تلقی شود (Melzer, 2011: 21-24). دلیلی وجود ندارد در خصوص حملات سایبری به استنتاجی نقیض برسیم و حملات سایبری علیه نهادهای عمومی و یا خصوصی را حمله مسلحانه تلقی نکنیم. به طور کلی به نظر می‌رسد که با توجه به تکامل جنگ افزارها و منطق مستتر در بند ۴ ماده ۲ منشور، محدودیتی برای گسترش ممنوعیت موجود در آن به منظور در برگرفتن موارد نوین استفاده از زور نمی‌گردد چون این مقرر به صراحت به نیروی مسلح یا نظامی اشاره نمی‌کند. نکته قابل توجه در خصوص نبرد سایبری این است که برخی حملات در فضای سایبر را باید در درجه‌ای پایین‌تر از جنگ قلمداد کرد چرا که از شدت کمتری برخوردارند. در آوریل ۲۰۰۷ تعدادی از تارنماهای مهم نهادهای دولتی کشور استونی مانند تارنمای ریاست جمهوری، پارلمان، وزارتخانه‌ها، احزاب سیاسی، رسانه‌های خبری و دو بانک مهم این کشور مورد حمله سایبری قرار گرفتند و در این میان، اتهام متوجه روسیه شد. اما ناتو اعلام کرد در این بازه زمانی، حملات سایبری را یک کار نظامی مسلم نمی‌شناسد تا ماده (۵) پیمان ناتو درباره دفاع دسته جمعی مورد استناد قرار گیرد. یا در درگیری میان روسیه و گرجستان در سال ۲۰۰۸، تأثیرات حمله سایبری بسیار محدود بوده و حتی از لحاظ زمانی نیز این حملات به اندازه‌ای طول نکشیدند که بخواهند تشکیل یک حمله مسلحانه بدهند. هر حمله سایبری علیه شبکه رایانه‌ای هر ساختاری را نمی‌توان حمله مسلحانه سایبری دانست، به عبارتی مقوله زیرساخت‌های حیاتی نقش بسیار اساسی دارد، چرا که این ساختارها باید زیرساخت‌های بنیادین باشند. به هر حال ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلالی می‌تواند تأثیرات و پیامدهای به مراتب بیشتری از جنگ در فضای واقعی در پی داشته باشد. وقوع حمله‌های سایبری و در نتیجه آن، بروز اختلال در شبکه‌ها می‌تواند موجب ایجاد خسارت به اموال، اطلاعات

حساس و حتی از دست دادن جان انسان‌ها شود، زیرا در این گونه مواقع، زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند.

۳-۳ استناد به حمله پیشدستانه^۱ و پیشگیرانه^۲ در پیکار علیه تروریسم نوین (تروریسم سایبری)

در اصل قضیه ظاهراً دولت‌ها اتفاق نظر دارند اما در تفسیر منشور ملل متحد مابین حقوقدانان و نیز رویه دولت‌ها در این زمینه اختلاف نظر شدید وجود دارد. در واقع جهان سیاست بیش از آن که زیر چتر حقوق و تعهد قرار داشته باشد از سیاست رنگ می‌گیرد (بهستانی، ۱۳۸۷: ۱۳۴). پاره‌ای از حقوق دانان معتقدند می‌بایست ماده ۵۱ منشور ملل متحد را به طور گسترده تأویل کرد، چرا که دولت دفاع کننده مجبور باشد حمله بدوی دشمن را که احياناً ویرانگر باشد، تحمل کند این برای اهداف منشور ملل متحد مذموم است. بدین ترتیب قرائت تحت اللفظی از دفاع مشروع به جانبداری از حق حمله آغازین متهاجم منتهی می‌شود. از این جهت به منظور امتناع از این برآیند باید این گونه بیان کرد که ماده ۵۱ حق دفاع مشروعی را مورد شناسایی قرار داده که قبل از تصویب منشور ملل متحد بسط یافته است. تفسیر گسترده استثنائات وارد بر اصل ممنوعیت توسل به زور را بیش از دفاع مشروع و اقدام جمعی کشورهای عضو ملل متحد می‌داند به عبارت دیگر این تأویل مرزهای مدّ نظر دیوان بین‌المللی دادگستری در خصوص دفاع مشروع را درهم پیچیده و گستره توسل دولت‌ها به این ماده جهت مقابله با تهدیدات فراروی را توسعه می‌دهد (صحرائی، ۱۳۸۸: ۱۱۲۹). در قضیه نیکاراگوئه و ایالات متحده دیوان چنین بیان می‌دارد: دیوان نمی‌تواند تصور کند تأمین تسلیحات برای مخالفان در کشور دیگر، حمله مسلحانه علیه آن کشور است حتی با فرض این که تأمین تسلیحات برای مخالفان السالوادور قابل انتساب به نیکاراگوئه باشد، برای توجیه توسل به دفاع مشروع فردی و جمعی طبق حقوق بین الملل عرفی علیه نیکاراگوئه (لازم است تأمین تسلیحات) با حملات علیه نیکاراگوئه یکسان شمرده شود (ICJ Reports, 1986: 228). برابر نظر دیوان بر وقوع حمله مسلحانه می‌توان چنین نتیجه گرفت که، دفاع در وضعیتی که هنوز حمله‌ای آغاز نشده مردود است. در تفسیر موسع از ماده ۵۱ مفاهیم حمله پیشگیرانه و حمله پیشدستانه مورد توجه و پذیرش قرار می‌گیرند. در همین راستا باید اشاره کرد که حمله پیش دستانه متفاوت از حمله پیشگیرانه است. بر این اساس حمله پیشدستانه، پاسخ مسلحانه به حملات قریب الوقوع یا حمله‌ای که وقوع یافته و دولت قربانی دریافتی است که حملات بیشتری در حال وقوع است (رجبی تاج امیر و رضازاده سلطان آباد، ۱۴۰۰: ۱۰۲). در مقابل، اصطلاح حمله پیشگیرانه؛ زمانی که هیچ دلیل و اعتقادی مبنی بر طراحی حمله وجود

¹ Preemptive attack

² Preventive attack

ندارد و مواردی که هیچ حمله اولیهای صورت نگرفته است اشاره دارد. به عبارتی بسط تهدیدات فرامیزی تروریسم باعث شده تفاسیر حمله پیشدستانه و حمله پیشگیرانه در زمینه توسل به دفاع مشروع جهت مقابله با تروریسم مطرح گردد (2: Young, 2022). مدافعان این دکترین معتقدند در صورتی که تروریست‌ها در عصر تسلیحات اتمی به انواع تسلیحات کشتار جمعی پیشرفته دسترسی پیدا نکنند بسیار مضحک است که خود را در یک حالت انتظار انفعالی قرار دهیم در حالی که خطر یک حمله قریب الوقوع را در کنار خود داریم. چه بسا هنگام برآمدن داعش و تسلط بر مناطق زیادی از عراق و سوریه و تهدید حمله به کشورهای همسایه مثل ایران و اقداماتی همچون نسل کشی، برده داری، تجاوز، طی کمترین زمان ممکن که هیچ یک از دولت‌های مورد هدف حتی به ذهنشان چنین وضعیتی خطور نمی‌کرد. بدون شک هر حمله تروریستی سایبری که به ایراد خسارات فیزیکی به اموال یا سلب حیات منجر شود، تحت شمول ممنوعیت مندرج در بند ۴ ماده ۲ منشور ملل متحد قرار خواهد گرفت و متعاقباً هیچ چیزی در ماده ۵۱ پاسخ یک کشور به نوع حمله مورد استفاده از سوی مهاجم را محدود نمی‌سازد. چنانچه برخی از کشورها از جمله ایالات متحده واکنش نظامی را در برابر حملات سایبری سیاست خود قرار داده‌اند. این گونه حملات اگر به سوی زیر ساخت‌های حساسی مانند راکتورهای اتمی، صورت گیرند، قابلیت تحقق خسارت را به صورت بالفعل دارند. بنابراین، می‌توانند صلح و امنیت بین المللی را تهدید کنند. اما واضح است که توسل به حمله پیشدستانه و پیشگیرانه از زور فاقد وجاهت است. موضوعی تحت عنوان حمله پیشدستانه و پیشگیرانه در هیچ کجای منشور ثبت نشده است. همان طور که همگان تصدیق می‌کنند تفسیر ماده ۵۱ منشور نمی‌تواند چنان گسترش یابد که به انکار اصل کلی ممنوعیت توسل به زور منجر شود چرا که استثنایی بر بند ۴ ماده ۲ منشور ملل متحد است و لذا می‌بایست طبق قاعده کلی، به‌طور متناسب با آن اصل مورد تفسیر قرار گیرد. به واقع نمایندگان دول در سانفرانسیسکو عقیده داشتند که حق دفاع مشروع فقط یک استثناء محسوب می‌شود، زیرا مقصود اصلی منشور این بوده که استعمال یک جانبه زور در جایگاه دفاع مشروع تحت کنترل سازمان ملل درآید. چنانچه به موجب ماده ۵۱ هم حق دفاع مشروع تا موقعی می‌تواند اعمال شود که شورای امنیت اقدامات مقتضی را برای حفظ و اعاده صلح بین المللی اتخاذ نماید و اقداماتی که اتخاذ می‌شود، فوراً بایستی به شورای امنیت اطلاع داده شود. از همه مهمتر هدف اصلی سازمان ملل متحد حفظ صلح و امنیت بین المللی است و تأمین این هدف ارزشمند جز از طریق محدود ساختن هر چه بیشتر استعمال زور در روابط بین المللی میسر نخواهد بود.

۴- خلاء حقوقی بین المللی در خصوص تهدید و حملات تروریسم نوین

در حال حاضر عرصه جدال بازیگران دولتی و غیردولتی در سطح بین المللی فضای سایبری است؛ به گونه‌ای که هر روزه حملات سایبری متعددی در این فضا انجام می‌گیرد. واضح است که در این میان نقص جدی هنجارهای بین المللی وجود دارد و نیاز به اقدامات دسته جمعی بین المللی برای کنترل این

میدان جنگ مجازی احساس می‌شود. با نگاهی به اسناد بین‌المللی درباره تروریسم سایبری می‌توان به این نتیجه رسید که اقدامات درخور و شایسته‌ای به منظور مقابله با تروریسم سایبری صورت نپذیرفته است. مهمترین معاهدات بین‌المللی در حوزه سایبری کنوانسیون ۲۰۰۱ جرایم سایبری و پروتکل الحاقی ۲۰۰۶ آن و توافقنامه امنیت اطلاعاتی بین‌المللی سازمان همکاری شانگهای ۲۰۰۹ هستند (فرشاسعید و دیگران، ۱۴۰۰: ۲۶). علی‌رغم وجود اسنادی در نظام‌های حقوقی ملی و بین‌المللی، متأسفانه هیچ یک از آن‌ها وضعیتی مقبول را در مواجهه با تهدیدات نوین فراهم نکرده است. به واقع، هنگام تدوین منشور در سال ۱۹۴۵ بنیان آن در پی ممانعت از منازعاتی بودند که در جنگ جهانی دوم رخ داده بود پس نه سلاح‌های کشتار جمعی و نه کنشگران غیردولتی در این حیطة مدنظر نبوده‌اند. تعیین این امر که کدام دولت و چه زمانی قصد دارد از سلاح هسته‌ای استفاده کند اقدامی سخت بوده، پس دشوار است بتوان در مقابل آن دفاع اثرگذاری به عمل آورد. به همین ترتیب تروریست‌ها نیز از راهکارهایی استفاده می‌کنند که بسیار مشکل است که زمان وقوع حملات آنان را دریافت. اما به نظر می‌رسد نه فقط قواعد و مقررات منشور، بلکه عملکرد ابر قدرت‌ها در زمینه حمایت از تروریسم یا لاقابل‌زمینه‌سازی برای ظهور آن در اقصی نقاط جهان، عدم کفایت ماده ۵۱ منشور را شدت می‌بخشد. در عصر سلاح‌های اتمی و دسترسی به این نوع سلاح‌ها به همراه پتانسیل تخریب گسترده و افسار گسیخته آن‌ها، اگر از این تئوری دفاع شود که دولتی در حالی که کاملاً از جنبه ویران‌کننده وسایل تخریبی به کار گرفته شده آگاه است، باید صبر کند تا حمله صورت گیرد. در زمان معاصر منطق حکم می‌کند نمی‌توان نیازمند تفسیری از یک اصل تاریک در یک متن ماند و بیان کرد یک دولت قبل از آن که بتواند از خود دفاع نماید، باید منفعلانه در انتظار تقدیر خویش بماند. فرضاً سلاح‌های بیولوژیک که در عملیات نظامی مورد استفاده قرار می‌گیرند، در این سلاح‌ها به جای مواد منفجره از عوامل بیولوژیک استفاده می‌شود که با انفجار، این عوامل در هوا به صورت ذرات معلق و در آب به صورت قطره‌های ریز پخش می‌شوند که اثرات مخرب آن‌ها می‌تواند تا مدت‌ها در محیط باقی بماند (جلالی و اقالر، ۱۴۰۲: ۹). اگر بنا بود که ممنوعیت استفاده از زور از سوی دولت‌ها علیه تمامیت ارضی یا به هر روش دیگری که مابین با اهداف ملل متحد، ممنوع باشد، به نظر نمی‌رسد در عمل تحقق یافته باشد. چرا که در طی مدت مدیدی که از انعقاد منشور ملل متحد سپری می‌شود رویه دولت‌ها به شدت متمایز از زمان منشور است. یازدهم سپتامبر ۲۰۰۱ سرآغاز جدیدی در ماهیت تروریسم و دیدگاه جامعه بین‌الملل به پدیده تروریسم را ایجاد نمود (نعمت پور و همکاران، ۱۴۰۰: ۱۷۱). شورای امنیت با صدور قطعنامه ۱۳۷۳ و طرح دفاع مشروع به عنوان حق ذاتی کشورها تلویحاً مجوز حمله به افغانستان را صادر نمود. شورا برایش مهم نبود که تکنیک مندرج در ماده ۵۱ دچار چه سرنوشتی می‌شود. به عبارتی شورا در این مرحله ترجیح داد به عنوان یک قانونگذار نامحدود اقتدار گرای خود را به منصف ظهور برساند. به هر روی در زمان حاضر شیوه‌های جدیدی از سوی بازیگران غیردولتی برای آسیب رسانی به دولت‌ها ایجاد گردیده است که حقوق بین‌الملل برای مقابله با

این معضل جهانی و تعیین حقوق و تکالیف اعضای جامعه بین‌المللی در برخورد با این پدیده با چالش‌های متعددی روبروست نه کنوانسیون جامعی در این زمینه وجود دارد و نه عرف بین‌المللی واحدی که دولت‌های قربانی بدانند در برابر آن‌ها به چه اقداماتی متوسل شوند. به نظر می‌رسد تصمیم‌گیری در خصوص حمله پیشدستانه و پیشگیرانه به خصوص در برابر کنشگران غیرمترافع یکی از چالش‌های اساسی نظام حقوق بین‌الملل فعلی است.

نتیجه‌گیری

ظهور بازیگران غیردولتی که دست به عملیات تروریستی دهشتناک می‌زنند، بخشی از ساختار سنتی حقوق بین‌الملل، به ویژه اصل ممنوعیت توسل به زور، را به مرور متحول نموده و شکل‌های تازه‌ای از حمله مسلحانه و متقابلاً دفاع مشروع را مورد توجه قرار داده است. آن چه در ۱۱ سپتامبر رخ داد شکلی وحشتناک از صورت جدید تروریسم بود که شورای امنیت را وادار کرد تا با طلبیدن دولت‌ها به نبرد همه جانبه با تروریسم با بهره جویی از تمام امکانات مطابق حقوق بین‌الملل، مسیر را برای پیکار در چارچوب دفاع مشروع علیه تروریسم هموار سازد. چنین عملکردی سبب شد تا در دو دهه اخیر دولت‌ها هم توسل به زور علیه تروریسم را تصدیق کنند. اما متعاقب قطعنامه‌های شورای امنیت تغییراتی در رویکرد مبارزه با تروریسم و برداشتی موسع از مفهوم دفاع مشروع به صورت اقدام مسلحانه پیشدستانه و پیشگیرانه مشاهده می‌کنیم. به هر حال با توجه به مجموعه مباحث و ادله مطرح شده در مقاله به این نتیجه می‌رسیم که تفسیر موسع از ماده ۵۱ منشور به گونه‌ای که موجب دفاع پیش از حمله شود، امکان پذیر نیست و دکتترین حمله پیشدستانه و پیشگیرانه از نظر مبانی حقوق بین‌الملل مورد قبول نیست. البته در مورد تأثیر دفاع مشروع بر جلوگیری از تروریسم نوین نباید خیلی آرمان‌گرایانه اندیشید. هر چند پیدایش این قاعده تحول بزرگی در مقابله با تروریسم نوین می‌باشد اما به نظر نمی‌رسد که بتواند به طور کلی آن را ریشه کن کند. از آن جا که اقدام دفاع مشروع در پاسخ به حملات تروریسم نوین علیه دولت‌های حامی گروه تروریستی صورت می‌گیرد، تأثیر عمده این قاعده بر دولت‌های حامی تروریسم خواهد بود چرا که موجب می‌شود که این دولت‌ها حمایت‌های خود از این گروه‌ها را کاهش دهند. در این راستا پژوهش حاضر در خصوص اقدام مسلحانه علیه تروریسم نوین بر اساس حقوق بین‌الملل پیشنهاد می‌نماید: در جهت اتخاذ اقداماتی واحد علیه تروریسم بهتر است که دولت‌ها معاهده بین‌المللی جامع منعقد نمایند و در آن به مسأله تعریف تروریسم، شناسایی انواع گونه‌های آن و تدوین قواعد مبارزه با آن بپردازند. همچنین با توجه به تحولات جدید سیاسی، اقتصادی و ارتباطاتی جهان اصلاحاتی در منشور صورت گیرد از جمله تعریف تجاوز، ارتقاء نقش مجمع عمومی از طریق گسترش اختیارات آن، شناسایی و رفع عوامل مؤثر در ضعف شورای امنیت، کارآمد شدن سیستم امنیت جمعی، تبیین قاعده دفاع مشروع با تصریح شرایط آن مثل ضرورت، تناسب و فوریت تا از این رهگذر از تفاسیر مختلف توسط دول در

راستای حفظ منافعشان که باعث بر هم زدن صلح و امنیت بین المللی می شود جلوگیری نمود و صلح را برای بشریت به ارمغان آورد.

منابع و مأخذ

فارسی

کتاب

- ۱- گوئرتز، استفان (۱۴۰۱) تروریسم نوین: بازیگران، راهبردها و تاکتیک‌ها، ترجمه عسگر قهرمان پور، چاپ اول، تهران، انتشارات جوینده.
- ۲- ملکی زاده، امیرحسین (۱۳۹۷) دفاع مشروع در رویه دیوان بین‌المللی دادگستری با تأکید بر قضیه سکوه‌ای نفتی، چاپ اول، تهران، انتشارات مجد.
- ۳- موسی زاده، رضا، کوهی، ابراهیم (۱۳۸۹) حقوق سازمان‌های بین‌المللی: حقوق شورای امنیت، چاپ اول، تهران، نشر میزان.
- ۴- ناجی راد، محمد علی (۱۳۹۸) جهانی شدن تروریسم، چاپ اول، تهران، انتشارات وزارت امور خارجه.

مقالات

- ۱- امیرلی، حسین، ثقفی، کامیار (۱۳۹۸) ارائه مدل مفهومی ارزیابی تهدیدات تروریسم سایبری، فصلنامه امنیت ملی، دوره ۹، شماره ۳۳.
- ۲- بهستانی، مجید (۱۳۸۷) دفاع پیشگیرانه در حقوق بین‌الملل جدید، فصلنامه حقوقی گواه، شماره ۱۲.
- ۳- جان پرور، محسن، صالح ابادی، ریحانه، احمدی، سیروس (۱۳۹۷) کنترل تروریسم سایبری با مدیریت مرزهای فضای سایبر راهبردی، فصلنامه مطالعات قدرت نرم، دوره ۸، شماره ۲.
- ۴- جلالی، محمود، اقالر، علی اصغر (۱۴۰۲) توسل به بیوتروریسم از منظر حقوق بین‌الملل، فصلنامه مطالعات حقوق عمومی، دوره ۵۳، شماره ۴.
- ۵- رجیبی تاج امیر، ابراهیم، رضازاده سلطان آباد، محمد (۱۴۰۰) دفاع مشروع پیشدستانه در برابر گروه‌های غیر دولتی از منظر حقوق بین‌الملل، فصلنامه تحقیقات حقوق بین‌المللی، دوره ۱۴، شماره ۵۳.
- ۶- رزمخواه، نجمه (۱۴۰۲) نقدی بر پیش نویس قانون اتحادیه اروپا در همسان سازی قوانین حاکم بر هوش مصنوعی، از منظر مقابله با تروریسم سایبری، فصلنامه مطالعات حقوق عمومی.
- ۷- سرتیبی، حسین، بردبار، احمدرضا، موسی زاده، محمد (۱۳۹۱) بررسی و نقد ترور هدفمند، مبارزه با تروریسم و حقوق مخاصمات مسلحانه بین‌المللی، فصلنامه پژوهش حقوق عمومی، دوره ۱۴، شماره ۳۸.
- ۸- شریفی طرازکوهی، حسین، فتح پور، فاطمه (۱۳۹۶) الزامات مقابله با تروریسم در پرتو روند انسانی شدن حقوق بین‌الملل، فصلنامه مطالعات حقوقی، دوره ۹، شماره ۲.

- ۹- صحرائی، محمدرضا (۱۳۸۸) مشروعیت توسل به زور در مبارزه با تروریسم، فصلنامه سیاست خارجی، دوره ۲۳، شماره ۴.
- ۱۰- عباسی کلیمانی، عاطفه، محبوبی، ملیکا، نوری، فاطمه (۱۳۹۹) راهبردهای نوین پیشگیری از وقوع تروریسم سایبری، فصلنامه رهیافت پیشگیری از جرم، دوره ۳، شماره ۱.
- ۱۱- عزیزی، ستار، نظری، خاطره (۱۳۹۳) حدود دفاع مشروع دولت قربانی علیه کنش گران غیردولتی، فصلنامه سیاست جهانی، شماره ۱۰.
- ۱۲- فرشاسعید، پرویز، جلالی، محمود، گودرزی، مهناز (۱۴۰۰) ضرورت تدوین کنوانسیون بین المللی حملات سایبری، فصلنامه مطالعات حقوقی، دوره ۱۳، شماره ۱.
- ۱۳- فرشاسعید، پرویز، جلالی، محمود، گودرزی، مهناز (۱۴۰۱) ضرورت همکاری دولت‌ها در تقویت امنیت سایبری، فصلنامه مطالعات بین المللی، دوره ۱۹، شماره ۲.
- ۱۴- کفایی فر، محمدعلی، تیموری، محمد (۱۴۰۲) تحولات حقوق بشر و بشردوستانه ناشی از تأثیر چندپارگی حقوق بین الملل بر مفهوم تروریسم، فصلنامه مطالعات حقوق عمومی، دوره ۵۳، شماره ۲.
- ۱۵- میرعباسی، سیدباقر، کورکی نژاد قرایی، مجید (۱۳۹۷) قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی دفاع مشروع مقرر در ماده ۵۱ منشور سازمان ملل متحد، فصلنامه مطالعات حقوق عمومی، دوره ۴۸، شماره ۲.
- ۱۶- نعمت پور، اردشیر، تقی زاده انصاری، مصطفی، ببری گنبدی، سکینه (۱۴۰۲) مسؤلیت دولت‌ها در مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور، فصلنامه مطالعات بین المللی، دوره ۱۹، شماره ۴.
- ۱۷- نعمت پور، اردشیر، تقی زاده انصاری، مصطفی، ببری گنبدی، سکینه (۱۴۰۰) مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور در قواعد حقوق بین الملل، فصلنامه مطالعات بین المللی، دوره ۱۸، شماره ۳.

English

- Hansen, James V., Lowry, Paul Benjamin, Rayman D., Meservy, McDonald, Daniel M. (2007). Genetic programming For prevention of cyberterrorism through dynamic and evolving intrusion detection, Decision Support System, Vol. 43(4).
- ICJ Reports. (1996). Advisory Opinion on the Legality of the Threat or use of Nuclear weapons.
- ICJ Reports. (2004). legal consequences of the construction of a wall in occupied Palestinian territory, Advisory opinion.
- ICJ Reports. (1986). Military and paramilitary activities in and against Nicaragua. Nicaragua v. United States .
- Li, Yuchong, Liu, Qinghui. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. Energy Reports, 7, 8176-8186.
- Martínez Esponda, Pedro. (2023). Norm-instability as a Strategy in International Lawmaking: The Case of Self-defence against Non-state Actors', in Nico Krisch, and Ezgi Yildiz (eds), The Many Paths of Change in International Law

- (Oxford, 2023; online edn, Oxford Academic, 14 Dec at: <https://academic.oup.com/book/55327/chapter/428795311>.
7. Melzer, Nils. (2011). Cyberwarfare and international Law, UNIDIR RESOURCES.
 8. SC/Res/2249. (2015). threats to international peace and security caused by terrorist acts https://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2249.pdf.
 9. YOUNG, Stephen. (2022). Contesting Subjects: International Legal Discourses on Terrorism and Indigenous Peoples' Human Rights Asian Journal of International Law, First View.



The evolution of the concept of self-defence and new terrorism (with an emphasis on cyber terrorism)

Ehsan sadeghipoor^{*}
Mahmoud Ganj Bakhsh^{**}
Kourosh Jafarpour^{***}

Abstract

The phenomenon of terrorism has transformed itself at a remarkable speed in the context of the development of societies. Today, one of the newest types of terrorism that has attracted the attention of many legal scholars is cyber terrorism. In this way, with the increasing number of new types of terrorism, followed by terrorist attacks in different parts of the world and the reaction of governments to these attacks, It has caused the issue of use of force against terrorist acts to become an raised issue in legal circles. In fact, after the September 11 incident and the spread of the cross-border threat of terrorism, a group of lawyers presented the doctrine of preemptive and preventive attack in the form of an expanded interpretation of Article 51 of the United Nations Charter to combat terrorism. Taking into consideration that in the current era, terrorism has gone out of the traditional mode and its modern forms are spreading under the name of new wave of terrorism such as cyber terrorism It is necessary to examine the issue that, considering the fundamental difference between traditional terrorism and modern terrorism, is it legal to refer to a preemptive and preventive attack against such an entity? Is citing self-defence against modern (cyber) terrorism legal? And subsequently, what is the justification for resorting to a preemptive and preventive attack in dealing with it from the point of view of international law? In this regard, in order to answer this problem, a descriptive-analytical research method has been used using library tools. It seems that if a terrorist attack has the potential to cause destruction to the extent of an armed attack, it is assumed to be armed and the victim government will have the right to self-defence, but international law has not recognized anything called a preemptive and preventive attack.

Key Words

self-defence, preemptive attack, preventive attack, new terrorism, cyber terrorism.

^{*} PhD student of Public International Law, South Tehran Branch, Islamic Azad University, Tehran, Iran. st_e_sadeghipoor@azad.ac.ir

^{**} Assistant Professor, Department of Economics and Islamic Banking, Faculty of Economics, Kharazmi University, Tehran, Iran (corresponding author): Ganjbakhsh@khu.ac.ir

^{***} Assistant Professor, Department of Private Law, South Tehran Branch, Islamic Azad University, Tehran, Iran. K.Jafarpour@ut.ac.ir