DOI: 10.22034/ISJ.2025.443148.2146

International Studies Journal (ISJ)
Vol. 21, No. 3 (83), Winter 2025
Reseived Date: 2024/3/13
Accept Date: 2024/12/18
Article Type: Original Research
PP: 257-276

فصلنامه مطالعات بین‌المللی
سال ۲۱، شماره ۳ (۸۳)، زمستان ۱۴۰۳
تاریخ دریافت: ۱۴۰۲/۱۲/۲۳
تاریخ پذیرش: ۱۴۰۳/۹/۲۸
نوع مقاله: علمی- پژوهشی
صفحات: ۲۷۶-۲۵۷

استناد به دکترین تفسیر موسع از حق دفاع مشروع در مقابله با تروریسم پسامدرن: با تأکید بر تروریسم سایبری سازمان مجاهدین خلق*

احسان صادقی پور** - دکتر محمود گنج بخش*** - دکتر کوروش جعفرپور****

چکیده

واقعه ۱۱ سپتامبر۲۰۰۱ شورای امنیت را بر آن داشت تا با تصویب قطعنامه‌هایی مطابق با حقوق بین‌الملل، به ظهور مفاهیم جدیدی از دفاع مشروع (حمله پیشدستانه و پیشگیرانه) کمک کند. زیرا اعمال کنشگران غیردولتی می‌تواند منجر به یک حمله مسلحانه شود، از آن جا که اقدامات تروریستی معاصر از حالت سنتی خارج شده و اشکال مدرن آن تحت عنوان موج تروریسم پسامدرن مانند تروریسم سایبری در حال گسترش است. براساس رویکرد موسع باری بوزان به امنیت ملی، این مقاله به‌دنبال پاسخ گویی به این سؤال است که، از منظر ماده ۵۱ منشور ملل متحد، توسل به حمله پیشدستانه و پیشگیرانه در برابر تروریسم پسامدرن (تروریسم سایبری سازمان مجاهدین خلق) چگونه توجیه می‌شود؟ روش مطالعه این پژوهش توصیفی- تحلیلی است. هدف پژوهش حاضر آن است که میان دو حوزه حقوقی و سیاسی در برابر تهدیدات پست مدرن تروریسم (مطالعه موردی تروریسم سایبری سازمان مجاهدین خلق) مفاهمه برقرار نماید. نتایج نشان می‌دهد که رویه حقوقی بین‌المللی حکایت از مشروعیت توسل به دفاع مشروع در برابر حملات تروریستی گروه‌های غیردولتی دارد و نظریه منتخب امنیت ملی این مطلب را تأیید می‌کند. هرچند حقوق بین‌الملل چیزی به نام حمله پیشدستانه و پیشگیرانه شناسایی نکرده است اما در نبود نظام حقوقی کارآمد در خصوص فضای سایبری تردیدی در حق دفاع مشروع در مقابله با تروریسم پسامدرن نمی‌باشد.

کلیدواژگان: حمله پیشدستانه، حمله پیشگیرانه، رویکرد باری بوزان به امنیت ملی، تروریسم سایبری، سازمان مجاهدین خلق.

---

* مقاله برگرفته از رساله دکتری حقوق بین‌الملل عمومی احسان صادقی‌پور با راهنمایی دکتر محمود گنج‌بخش است.

** دانشجوی دکتری حقوق بین الملل عمومی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.
*** استادیار گروه اقتصاد و بانکداری اسلامی، دانشکده اقتصاد، دانشگاه خوارزمی، تهران، ایران./ نویسنده مسئول/ ایمیل: Ganjbakhsh@khu.ac.ir
**** استادیار گروه حقوق خصوصی، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.

Article Link: https://www.isjq.ir/article_212904.html

مقدمه

در سال‌های اخیر تروریسم از حالت سنتی خارج شده و اشکال مدرن آن تحت عنوان موج تروریسم پسامدرن در حال گسترش است. تروریسم سایبری[1] از جدیدترین مصادیق تروریسم پسامدرن[2] می‌باشد که از تلاقی اعمال تروریستی و فضای سایبر[3] به‌عنوان گونه‌ای نوپا از تروریسم پا به عرصه وجود نهاده است. سایبر تروریسم، با وجود نوظهور بودن به مراتب خطرناک‌تر از سایر گونه‌های تروریسم پسامدرن است، که تهدیدات آن برای امنیت ملی کشورها به خطری بالقوه تبدیل شده است. در گذشته رقابت اصلی دولت‌ها در عرصه های نظامی و فناوری‌های مرتبط با این حوزه بود اما در زمان حاضر رقابت به محیط مجازی تسری یافته است و گاهی اوقات اخباری در رسانه ها منتشر می گردد که علیه کشوری چه از طرف بازیگران غیردولتی و چه از طرف دولت‌ها حمله سایبری[4] صورت گرفته است. به طوری که می‌توان ادعا کرد که امروزه با توجه به پیشرفت‌های تکنولوژی، فضای سایبر به منزله پنجمین میدان نبرد بعد از زمین، دریا، هوا و جو شناخته می‌شود. دولت‌های قربانی حملات تروریستی اغلب در پاسخ و با استناد به حق دفاع از خود، اقدامات گسترده نظامی علیه گروه‌های تروریستی مستقر در خاک دیگر کشورها نموده‌اند.

بدین ترتیب دیدگاه سنتی که حمله مسلحانه را فقط حملات دولت‌ها تلقی می‌نمود اقدامات مسلحانه کنشگران غیردولتی را نیز به‌عنوان حمله مسلحانه به‌رسمیت شناخت، این تلقی جدید تحولی در حقوق بین‌الملل محسوب می گردد. اما شورای امنیت با تصویب قطعنامه‌هایی نظیر قطعنامه ۱۳۶۸ با متصف کردن این اقدامات به قاعده توسل مشروع به زور، مسیر را برای ارائه مفاهیم جدیدی از دفاع مشروع (حمله پیشدستانه[5] و حمله پیشگیرانه[6]) فراهم نمود. در موارد زیادی تفاسیر قواعد منشور 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 پسامدرن برخلاف تروریسم سنتی دارای ابعاد و مشخصه‌های پیچیده و گسترده‌ای است، در دنیای معاصر که ساختار اقتصادی و خدمات رسانی کشورها مبتنی بر فناوری‌های اطلاعاتی و نظام ارتباطی است، تروریسم سایبری خطرناک‌تر از تروریسم سنتی به‌شمار می‌آید.

این پژوهش درصدد پاسخگویی به این سؤال است که، از منظر ماده ۵۱ منشور ملل متحد، توسل به حمله پیشدستانه و پیشگیرانه در برابر تروریسم پسامدرن (تروریسم سایبری سازمان مجاهدین خلق) چگونه توجیه می‌شود؟ براساس فرضیه منتخب، هرچند حقوق بین‌الملل حمله پیشدستانه و پیشگیرانه را شناسایی نکرده است، اما رویه بین‌المللی حکایت از مشروعیت توسل به دفاع مشروع

---

1. Cyber Terrorism
2. Postmodern Terrorism
3. Cyber Space
4. Cyber attack
5. Preemptive attack
6. Preventive attack

در برابر حملات تروریستی گروه‌های غیردولتی دارد. ماهیت سیال تروریسم پسامدرن و بسط یافتن آن در میان کشورهای مختلف عملاً باعث می‌شود تا حقوق بین‌الملل از انجام اقدامات متناسب عاجز بماند. به‌نظر می‌رسد علاوه بر فقدان تعریف جامع و مورداجماع جامعه بین‌المللی از پدیده تروریسم، منشور ملل متحد با تلقی دولت به‌عنوان تنها بازیگر بین‌المللی نقص اساسی دارد. پر واضح است حوادث ۱۱ سپتامبر سبب پیدایش رویکردهای جدید در سیاست، امنیت وحقوق بین‌الملل شد، به گونه‌ای که برخی از مفاهیم متروک و مهجور مانند جنگ عادلانه، در جهت حل معضلات جهانی و برقراری امنیت، جایگاهی نوین یافت.

این که با وجود اجماع نظر موجود درباره تهدیدهای ناشی از تروریسم، چرا تاکنون همکاری‌های بین‌المللی برای مبارزه با این پدیده ناکارامد بوده است. در ابتدا درک متفاوت دولت‌ها و اختلاف نظر در تعریف عملیات تروریستی، مانع بزرگ همکاری‌های بین‌المللی بود. اما پس از مدت کوتاهی فاصله موجود در اولویت‌بندی دولت‌ها بر اساس منافع ملی هر یک از آن ها، همکاری‌های بین‌المللی را به شدت تحت تاثیر قرار داد. همچنین تلاش قدرت‌های بزرگ در جهت پیشبرد منافع و اهداف خود، زمینه‌های اصلی ناکامی همکاری‌های بین‌المللی در مبارزه با تروریسم گردید. این که آیا یک قاعده عرفی در حقوق بین‌الملل وجود دارد که استفاده از حمله پیشدستانه و پیشگیرانه را مجاز می‌داند یا خیر، تا حدود زیادی به تعریف کشورهایی که به‌طور خاص تحت تأثیر تروریسم قرار گرفته‌اند، بستگی دارد. این دولت‌ها نقشی غالب در ایجاد این قاعده دارند. همچنین رویکرد دولت‌های مهاجم بحث‌برانگیزتر می‌شود، زیرا قدرت‌هایی که با این ادعا حملاتی را انجام داده‌اند، توجیه و تفسیر یکسانی دارند.

۱- پیشینه تحقیق

نعمت‌پور و همکاران (۱۴۰۰) در مقاله «مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور در قواعد حقوق بین‌الملل» بیان می‌کنند جامعه حقوقی در سطح بین‌الملل همگام با اشکال مدرن تروریسم حرکت نمی‌نماید و همواره یک یا چند مرحله عقب است. پژوهش مزبور در پاسخ به پرسش اصلی خود یعنی مقابله باحمله فیزیکی تروریستی به زیرساخت‌های حیاتی یک کشور تحت حاکمیت چه قاعده بین‌المللی قرار دارد، می‌باشد، در عین حال به مسأله مهم زیرساخت‌های حیاتی و اسناد مربوط به مقابله با تروریسم می‌پردازد (نعمت‌پور و همکاران، ۱۴۰۰: ۱۶۵)؛(Nematpour et. al., 2021: 165).

ایرنه کوزیگو (۲۰۲۲) در مقاله «جرم انگاری تروریسم آنلاین اسناد مقدمات مطابق حقوق بین‌الملل» در این مقاله نویسنده بر نحوه کنترل تروریسم سایبری و یا آنلاین در حقوق بین‌الملل تأکید می‌ورزد و بیان می‌کند سازمان‌های تروریستی به‌طور فزاینده ای برای ترویج تروریسم، جذب تروریست‌های جدید، برنامه ریزی و تأمین مالی عملیات خود به اینترنت متوسل می‌شوند. این مقاله ابتدا تعریفی از تروریسم، تروریسم سایبری و اقدامات مقدماتی تروریسم آنلاین ارائه می‌کند. سپس تجزیه و تحلیل می‌کند که آیا اسناد الزام آور بین‌المللی فعلی در مورد تروریسم، جنایت سازمان یافته یا جرایم سایبری می‌تواند مانع از اقدامات تروریسم سایبری بشود؟ نویسنده به این نتیجه می‌رسد

که هیچ خلاء قانونی در حقوق بین‌الملل برای نظارت بر حملات تروریسم سایبری وجود ندارد (Couzigou, 2022: 1-2).

ایان اسکوبی (۲۰۲۰) در مقاله «دفاع مشروع به‌عنوان یک استثناء در ممنوعیت استفاده از زور» به بررسی توسعه دکترین امنیت جمعی به‌عنوان ارزش وحدت‌بخش روابط بین‌الملل در پایان جنگ جهانی اول و پس از آن می‌پردازد و تحلیل می‌کند که برای یک قرن، از پایان جنگ جهانی اول، مقدمه اساسی نظام حقوقی و سیاسی بین‌المللی دکترین امنیت جمعی بوده است که در ابتدا در محدودیت‌های توسل به جنگ در میثاق جامعه ملل بیان شد و تا ممنوعیت از توسل به جنگ به عنوان ابزار سیاست ملی در پیمان پاریس، و در نهایت به ممنوعیت استفاده از زور مندرج در ماده ۲ (۴) منشور سازمان ملل به اوج خود رسید(Scobbie, 2020: 1-47).

شارف و همکاران (۲۰۲۰) در مقاله «توسل به زور در دفاع مشروع علیه بازیگران غیردولتی» توسل به زور علیه داعش را بررسی می‌کند و بیان می‌دارد که در سال ۲۰۱۴، یک گروه شبه نظامی که خود را دولت اسلامی (داعش) می‌نامد، به سرعت بیش از ۳۰ درصد از خاک سوریه و عراق را تصرف کرد. در نهایت، بررسی می‌کند که چگونه واکنش جامعه بین‌المللی به حملات هوایی ایالات متحده علیه داعش در سوریه ممکن است مفهوم جدیدی از دفاع مشروع در برابر بازیگران غیردولتی را متبلور کند (Scharf et.al., 2020: 29-30).

۲- چارچوب مفهومی و مبانی نظری

بعد از حادثه ۱۱ سپتامبر ۲۰۰۱، شورای امنیت با استناد به ماده ۵۱ منشور ملل متحد در قطعنامه ۱۳۶۸ آمادگی خود را به منظور هر نوع همکاری برای پاسخ به این حملات تروریستی و مبارزه با تمام اشکال تروریسم بیان کرد و بر حق ذاتی دفاع مشروع فردی و جمعی دولت‌ها در مقابل تروریست‌ها تأکید نمود. به‌نظر می‌رسد شورای امنیت حملات تروریستی را در حکم حمله مسلحانه تلقی نمود و راه را برای این تفسیر که ماده ۵۱ منشور، علاوه بر این که حاکم بر روابط میان دولت است، بر روابط میان دولت‌ها و بازیگران غیردولتی نیز حاکم است، باز کرد. براساس مطالب فوق و همچنین رویکرد موسع مکتب کپنهاگ به امنیت ملی، مناسب‌ترین اقدام در برابر تروریسم سایبری توسل به دکترین تفسیر موسع از حق دفاع مشروع، استفاده از نظریه‌های حمله پیشدستانه و حمله پیشگیرانه است که توسط حقوقدانان نامی چون استون، مک دوگال، اسکار اسکچر و آنتونی کلارک مطرح شده‌اند. لذا به‌عنوان چارچوب نظری بحث، ابتدا به مطالعه و بررسی این نظریه‌ها می‌پردازیم. حمله پیشدستانه دارای مفهومی جدا از مفهوم حمله پیشگیرانه می‌باشد. طبق دکترین حمله پیشدستانه، پاسخ مسلحانه به حملات قریب‌الوقوع یا آن جا که حمله‌ای وقوع یافته و دولت قربانی دریافته است که حملات بیشتری در حال طراحی است مجاز می‌باشد. پر واضح است امنیت ملی به معنی محفوظ بودن یک کشور از کلیه تهدیدات و خطراتی است که متوجه بنیان‌های ملی آن کشورند. بر اساس ...تعریف پنلوپه هارتلند-تانبرگ،[1] امنیت ملی یعنی توانایی یک ملت برای پیگیری موفقیت‌آمیز

[1]. Penelope Hartland –Thunberg

منافع ملی خود در هر جای جهان به همان نحوی که خودش آن ها را می‌بیند... (قنبرلو، ۱۳۹۷: ۴۳)؛ (Qanbarlu, 2018: 43).

تحولات پس از دهه ۱۹۷۰ موجب ظهور جریان فکری مهمی بنام مکتب کپنهاگ شد که جایگاه موسع‌تر و عمیق‌تری برای مفهوم امنیت ملی ترسیم می‌نمود. باری بوزان[1] از اولین تئوری پردازان برجسته این مکتب در چاپ دوم کتاب «مردم دولت‌ها و هراس» در سال ۱۹۹۱ با اشاره به کاهش تهدیدات نظامی در دهه ۱۹۸۰ تصور سایر تهدیدات را مطرح نمود. به‌نظر ایشان مفهوم امنیت بایستی در دو جهت گسترش یابد اول این که از حوزه نظامی فراتر رفته و دارای معنای عام تری باشد که نه فقط در عرصه نظامی بلکه در حوزه‌های اقتصادی اجتماعی سیاسی و زیست محیطی نیز کاربرد داشته باشد دوم این که آنچه باید امن بماند از حوزه دولت فراتر رفته و کنشگرانی چون افراد درون دولت و نهادهای بین‌المللی را نیز در برگیرد. در مکتب کپنهاگ امنیت ملی مرکز ثقل امنیت تلقی می‌شود. پنج بخش به هم پیوسته امنیت عبارت از: امنیت نظامی، امنیت سیاسی، امنیتی اقتصادی، امنیت اجتماعی، امنیت زیست محیطی.

...سه دلیل عمده بوزان برای بسط مفهوم امنیت عبارت اند از: ۱- تغییر واقعیت‌های جهان در چارچوب افزایش وابستگی متقابل، کاهش تهدیدات نظامی و اهمیت یافتن انواع دیگر تهدیدات. ۲- مفهوم بست یافته امنیت می‌تواند دارای ویژگی‌های سیاسی مطلوب‌تری باشد چرا که برای ممانعت از سوء استفاده حکومت از مفهوم امنیت ملی شرایط مناسب فراهم می‌گردد هرچند بعد نظامی امنیت میزان قابل توجهی از پنهانکاری را موجب می‌شود اما ابعاد غیرنظامی امنیت موضوعات خاصی هستند که دولت را به اولویت دادن به موضوعات خاص وادار می‌کند و از ایجاد تغییرات و تحولات نامطلوب جلوگیری می‌نماید. ۳- بست مفهوم امنیت رشته مطالعات روابط بین‌الملل را یکپارچه‌تر و منسجم‌تر نموده و یک ایده سازمان دهنده در مطالعات بین‌المللی ایجاد می‌نماید و پیامدهای سیاسی مخرب کمتری دارد. این مفهوم بازیگران غیردولتی را نیز در بر گرفته و حتی اجازه تسلط و تفوق به آنان می‌دهد... (قنبرلو، ۱۳۹۷: ۵۳-۵۶)؛(Qanbarlu, 2018: 56).

به‌نظر رابرت ماندل به‌دلیل یک‌دست شدن جامعه جهانی، همه مسایل مثل جامعه سیاسی داخلی به یکدیگر مرتبط و نزدیک شده‌اند که از جمله این مسائل امنیت خواهد بود. «یعنی مفهوم امنیت یک مفهوم متقابل، مساوی و یکسان برای همه دولت‌ها خواهد شد که همان دیدگاهی است که شاید جهان گرایان به آن اشاره می‌کند و طراح آن بوده‌اند» (رامهر، ۱۳۸۵: ۳۱-۳۰)؛ (Ramehr, 2006: 30-31).

۳- استناد به دکترین تفسیر موسع از حق دفاع مشروع در مقابله با تروریسم پسامدرن

بیشترطرفداران تفسیر موسع به واژه «ذاتی» مندرج در ماده ۵۱ منشور استدلال می‌نمایند. براین اساس که ماده ۵۱ به حق ذاتی دفاع از خود که قبل از منشور به صورت عرفی وجود داشت لطمه‌ای وارد ننموده است. «پرفسور لوئیس هنکین بیان می‌کند که این تئوری به هنگام «بحران سوئز» به منظور

[1]. Barry Buzan

توجیه توسل به زور علیه مصر، به دنبال ملی شدن کانال سوئز توسط جمال عبدالناصر شکل گرفت» (سپهر، ۱۳۸۴: ۳۳۳)؛(Sepehr, 2005: 333).

به عبارت دیگر مسأله توسعه دفاع مشروع در پاسخ به حملات تروریستی بین‌المللی مسأله چندان جدیدی نیست. قبل از ۱۱سپتامبر ۲۰۰۱ نیز برخی دولت‌ها با استناد به حمله پیشدستانه و پیشگیرانه به پایگاه‌های تروریست‌ها در دولت میزبان حمله می‌نمودند. درسال۱۹۸۶ در پی حادثه بمب‌گذاری در برلین و کشته و مجروح شدن عده‌ای از اتباع آمریکا، ایالات متحده بیان داشت که شواهد متقاعد کننده‌ای در مورد بمب‌گذاری با حمایت دولت لیبی و احتمال حملات بیشتری برای آینده وجود دارد. براین اساس و با استناد به دکترین تفسیر موسع از دفاع مشروع درراستای امنیت ملی، ایالات متحده حملات هوایی علیه لیبی انجام داد. رویه دولت‌ها بعد از صدور قطعنامه‌های ۱۳۶۸ و ۱۳۷۳ مصدق این دکترین است.

٤- تحول پدیده تروریسم در قالب کنشگران غیردولتی پسامدرن (سایبری)

پدیده تروریسم با گذر زمان و متناسب با شرایط نظام بین‌المللی، تحولاتی داشته است. ...بسیاری از تحلیل گران بر این باورند که از میانه دهه ۱۹۹۰ تروریسم به سمت شکل جدیدی تغییر جهت داده که خصوصیات جدیدی پیدا کرده است... (بهاری و بخشی شیخ احمد، ۱۳۸۸: ۶)؛ (Bahari & Bakshi Sheikh Ahmad, 2009: 6) وقوع حوادثی نظیر حملات ۱۱ سپتامبر ۲۰۰۱ نشانه‌هایی از تغییر اساسی در تروریسم بوده و بیان‌گر مسأله‌ای است که از آن به تروریسم پسامدرن نام می‌برند. در مفهوم تروریسم پسامدرن اگرچه هدف نهایی و اصلی ترور دستیابی به امیال و خواسته‌های سیاسی می‌باشد، ولی علاوه بر ابزارهای نظامی از ابزار و روش‌های متفاوت غیرنظامی هم استفاده می‌کنند. «در برخی مواقع بازیگران غیردولتی با استفاده از امکاناتی که اینترنت در اختیار آن‌ها قرار داده، بدون این که گلوله‌ای شلیک شود اعمالی را مرتکب می‌شوند که خسارات ناشی از آن بیشتر از خسارات برخی جنگ‌های مسلحانه است» (قاسمی و بارین چهاربخش، ۱۳۹۱: ۱۱۶)؛ (Qasemi & Barin Chaharbakhsh, 2012: 116)

٤-١ تعریف تروریسم سایبری

از نظر باری کالین تروریسم سایبری عبارت است از «سوءاستفاده عمدی از یک سیستم، شبکه یا مؤلفه اطلاعاتی رایانه‌ای برای تحقق هدفی که مؤید یا تسهیل کننده اقدام تروریستی می‌باشد» (Collin, 1997: 15-18). تروریسم سایبری، موج پنجم تروریسم می‌باشد. «فناوری سایبری با از بین بردن مرزها تهدیدات خطرناک و نوینی را برای تمدن بشری به ارمغان آورده است» (فرشاسعید و همکاران، ۱۴۰۱: ۱۷۲)؛(Farshasaid et. al., 2022: 172). امروزه گروه‌های هکری دولتی و یا غیردولتی مثل تروریسم سایبری سازمان مجاهدین خلق از مهمترین گروه‌های تروریستی نوینی هستند که درصدد خرابکاری یا حمله به زیرساخت‌های حیاتی کشورها هستند. از آن‌جا که بحث تروریسم سایبری به‌دلیل 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. «براساس بررسی محققین هیچ تعریف پذیرفته شده جهانی در مورد تروریسم وجود ندارد» (فضائلی، ۱۴۰۲: ۱۱۵)؛(Fazaeli, 2023: 115). «در مورد پدیده تروریسم سایبری نیزمانند تروریسم تعریف اجماعی وجود ندارد» (جلالی فراهانی، ۱۳۸۵: ۹۵)؛(Jalali Farahani, 2006: 95) و همچنان واژه‌ای بحث برانگیز است (رزمخواه، ۱۴۰۲: ۵)؛(Razmkhah, 2023: 5).

...به هرحال در جنگ سایبر به ساز و برگ های نظامی و ارتش های بزرگ نیاز نیست... (کیانی‌زاده و همکاران، ۱۳۹۷ : ۷۲)؛(Kyanizadeh et. al., 2018: 72). ...در این جنگ خساراتی ممکن است وارد شود که جبران آن‌ها می‌تواند از خسارت‌های ناشی از موشک و بمب به مراتب مشکل تر باشد چرا که افراد کمی با برخورداری از مهارت های بالا می‌توانند به زیرساخت‌های حیاتی یک کشور خسارات زیادی وارد کنند... (عباسی و مرادی، ۱۳۹۴: ۴۲)؛ (Abassi & Moradi, 2015: 42) ...به همین دلیل در مقایسه با هزینه هایی که دیگر گونه‌های تروریسم پسامدرن برای تهیه سلاح، مسافرت های بین‌المللی و امکانات آموزشی متحمل می‌شوند، تروریسم سایبری نسبتاً ارزان تر و کم زمان بر است... (Stark, 1999: 9).

امروزه داعش مصداق بارز تروریسم جهادی است که از بستر فضای مجازی در راستای تحقق اهداف خود استفاده می‌کند. «در ژانویه ۲۰۱۵ داعش حساب شبکه های اجتماعی مرکزی آمریکا را هک و اسنادی که شامل اسامی و آدرس مقامات نظامی ایالات متحده بود منتشر کرده بود» (The U.S. Army Training & Doctrine Command, 2016: 1). «در صورتی مشخص نیست که آیا داعش خود دارای مهارت حمله سایبری هست یا نه، این امکان وجود دارد که این سازمآن‌های تروریستی هکرهای سایبری به کار گرفته باشند تا اقدامات سایبری را برای آن ها انجام دهند» (زواره‌ئی و سلیمی، ۱۴۰۱: ۸۳)؛(Zavarei & Salimi, 2022: 83). یا حملات سایبری از سوی گروه هکری وابسته به تروریسم منافقین به وب سایت های وزارت خانه ها و سازمآن‌های حساس ایران مثل وزارت کشور و وزارت خارجه. در قرن حاضر روش‌های جدیدی از سوی کنشگران غیردولتی برای آسیب‌رسانی به دولت‌ها ایجاد گردیده است که حقوق بین‌الملل برای مواجهه با این معضل جهانی و تعیین حقوق و تکالیف اعضای جامعه بین‌المللی در برخورد با این پدیده با چالش های بسیاری روبه‌روست. در مجموع مختصات ذکر شده سبب می‌شوند تا تحلیل ابعاد حقوقی تروریسم پسامدرن (سایبری) با دشواری هایی همچون بحث دفاع مشروع روبه‌رو شود.

٤-٢- تحول مفهوم دفاع مشروع در ارتباط با تروریسم پسامدرن

در حال حاضر حق دفاع مشروع دولت‌ها علیه حملات تروریستی مورد پذیرش حقوق بین‌الملل قرار گرفته است. لذا دولت‌های قربانی چنین حملاتی، می‌توانند به منظور دفاع از سرزمین خود، حملات نظامی علیه گروه‌های تروریستی ترتیب دهند. بدین‌ترتیب جا دارد قبل از ورود به بحث اصلی، استدلالاتی در تأیید رویه فعلی حقوق بین‌الملل به صورت مختصر بیان شود.

٤-٢-١-دفاع مشروع

ماده ۵۱ منشورملل متحد، توسل هر یک از دول عضو ملل متحد به دفاع مشروع را تنها در صورتی امکان پذیر می‌داند که حمله‌ای مسلحانه علیه آن‌ها صورت پذیرد. ...عبارت حمله مسلحانه

در منشور ملل متحد به‌طور مشخص تعریف نشده است در حقیقت منشأ حمله ازمنظر منشور موضوعیت ندارد... (Martínez 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 موجودیت های غیردولتی را نیز می‌دهد. پر واضح است ماده ۵۱ تنها بخشی از چارچوب توسل به دفاع مشروع را مورد توجه قرار داده و به منظور بررسی دیگر ضوابط حاکم بر اعمال دفاع مشروع از جمله تناسب و مفهوم حمله مسلحانه باید به حقوق عرفی موجود مراجعه نمود. «به عبارت دیگر این ماده منعکس کننده بخشی از حقوق بین‌الملل عرفی می‌باشد» (بهستانی، ۱۳۸۷: ۱۳۴)؛(Behestani, 2008: 134). «رویه شورای امنیت؛ با صدور قطعنامه‌هایی نظیر ۱۳۶۸ با استناد به ماده ۵۱ منشور بر حق ذاتی دفاع مشروع فردی و جمعی دولت‌ها در مقابل تروریست تاکید نمود» (محبی و شفیعی،۱۳۹۶: ۱۰۵)؛(Mohebbi & Shafiei, 2017: 105) «یا در قطعنامه ۲۲۴۹ (مورخ ۲۰ نوامبر ۲۰۱۵) که یک هفته پس از حادثه تروریستی در پاریس، تصویب شد تحولی مهم محسوب می‌شود» (SC/Res 2249, 2015: 5) «که با ایجاد عرف خلق الساعه مبنی بر تجویز دفاع مشروع در قبال گروه‌های تروریستی موجد هنجار نوین حقوق بین‌الملل عرفی شده است» (کفایی فر و تیموری، ۱۴۰۲: ۸۴۲)؛(Kefaei Far & Timuri, 2023: 842). حتی رویه دولت‌ها؛ نیز در تحول است. رویه همراه با اعتقاد حقوقی دولت‌ها از این نظر پشتیبانی می‌کند که کنشگران غیردولتی نیز مرتکب حمله مسلحانه می‌شوند و بدین‌ترتیب در مقابل آن‌ها حق دفاع مشروع به وجود می‌آید، که چنین روندی می‌تواند منجر به شکل‌گیری قاعده عرفی بین‌المللی باشد.

٤-۲-۲- حملات تروریسم سایبری به مثابه نقض اصل منع توسل به زور و امکان توسل به دفاع مشروع

حسب بند ۴ ماده ۲ منشور ملل متحد: ...کلیه اعضا در روابط بین‌المللی خود از کاربرد یا تهدید به کاربرد زور علیه تمامیت سرزمینی یا استقلال سیاسی هر دولت دیگر و نیز از هر عملی که به نحوی از انحاء مغایر با اهداف ملل متحد باشد، خودداری خواهند کرد... (ممتاز و صابری انصاری، ۱۳۹۱: ۱۷۹-۱۸۰)؛(Momataz & Saberi Ansari, 2012: 179-180). مسأله‌ای که مطرح می‌شود این است که آیا حمله سایبری می‌تواند نقض بند ۴ ماده ۲ منشور تلقی شود؟ این بند بدون آن‌که تعریفی از زور ارائه دهد، ممنوعیت تهدید و توسل به زور را اعلام می‌کند، «ممنوعیتی که در عین ابهام، بی‌پروا است و طبیعت پیچیده آن مهیای تحلیل‌های مختلف است» (فلک و همکاران، ۱۳۸۷: ۲۰-۱۹)؛(Fleck et.al., 2008: 19-20).

در متن منشور عبارت توسل به زور آمده است. بنابراین می‌توان گفت «لفظ مسلحانه به معنی تجهیز به یک سلاح یا درگیری با استفاده از یک سلاح است» (Garner, 2009: 123). سلاح نیز ابزار مورد استفاده یا طراحی شده برای استفاده جهت صدمه زدن به دیگری یا قتل وی است. تقریباً تمامی اشیاء می‌توانند به‌عنوان سلاح به کار روند؛ در صورتی که قصد دارنده آن خصمانه باشد. دیوان بین‌المللی دادگستری در نظر مشورتی خود در خصوص مشروعیت تهدید به 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 (ICJ Reports, 1996: 39). ...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). ...بنابراین، لزومی ندارد تسلیحات مذکور برای اهداف تهاجمی ساخته شده باشند و یا دارای آثار انفجاری باشند... (ICJ Reports, 1986: 228). حمله استاکس‌نت مصداق بارز این استدلال تلقی می‌شود. ویروس استاکس‌نت موجب ورود خسارت و تخریب فیزیکی سانتریفیوژها در تأسیسات نطنز شد، در حالی که سلاح مورد استفاده به‌عنوان سلاح فیزیکی شناخته نمی‌شود. ...بنابراین می‌توان گفت که شرط لازم برای تحقق ممنوعیت توسل به زور براساس موازین حقوق بین‌الملل حاصل شده است... (اصلانی، ۱۳۹۴: ۲۳۹)؛(Aslani, 2015: 239). منشور ملل متحد جهت توسل به زور دو ساز و کار را به رسمیت شناخته است، اول امنیت جمعی بر مبنای ماده ۳۹ و مواد بعد از آن دوم دفاع مشروع فردی یا جمعی بر مبنای ماده ۵۱. بدین‌ترتیب علی‌رغم این که منشور از تمام دولت‌ها می‌خواهد که برای حل و فصل مسالمت‌آمیز اختلافات تلاش کنند، هیچ یک از این مواد خللی به حق دفاع مشروع وارد نمی‌سازد.

٤-۲-۳- توسل به حمله پیشدستانه و پیشگیرانه در مبارزه با تروریسم پسامدرن (تروریسم سایبری سازمان مجاهدین خلق)

در اصل قضیه دولت‌ها اتفاق نظر دارند اما در تفسیر منشور ملل متحد مابین حقوقدانان و نیز رویه دولت‌ها اختلاف نظر شدید وجود دارد. «پیچیدگی روابط بین‌المللی امروزین و فضای در حال تغییر بین‌المللی مورد توجه بسیاری از مفسرین واقع شده است و مباحثی را در رابطه با توسعه فرایندهای قاعده سازی ایجاد کرده است» (نعمت‌پور و همکاران، ۱۴۰۲: ۱۷۶)؛ (Nematpour et. al., 2023: 176) «به گونه‌ای که به ویژه پس از حادثه ۱۱ سپتامبر جدال‌های بسیاری در خصوص توسعه حق دفاع مشروع صورت گرفت» (پلاسعیدی و رنجبریان، ۱۴۰۱: ۱۷۲۸)؛ (Plasaeidi & Ranjbarian, 2022: 1728). «در واقع جهان سیاست بیش از آن‌که زیر چتر حقوق و تعهد قرار داشته باشد از سیاست رنگ می‌گیرد» (بهستانی، ۱۳۸۷: ۱۳۴)؛(Behestani, 2008: 134).

پاره‌ای از حقوق‌دانان معتقدند می‌بایست ماده ۵۱ منشور ملل متحد را تفسیر موسع نمود، درغیر این‌صورت دولت دفاع‌کننده مجبور است حمله بدوی دشمن را که احیاناً ویرانگر می‌باشد، تحمل کند. «بدین‌ترتیب قرائت تحت اللفظی از دفاع مشروع به جانبداری از حق حمله آغازین متهاجم منتهی می‌شود» (Ackerman, 2003: 2). از این جهت به منظور امتناع از این برآیند باید این‌گونه بیان کرد که ماده ۵۱ حق دفاع مشروعی را مورد شناسایی قرار داده که قبل از تصویب منشور ملل متحد بسط یافته است. تفسیر موسع، 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 فرارو را توسعه می‌دهد...(صحرایی، ۱۳۸۸: ۸۵)؛ (Sahrai, 2009: 1129). «دیوان در قضیه نیکاراگوئه و ایالات متحده نیز چنین بیان می‌دارد: 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 بین‌الملل عرفی علیه نیکاراگوئه (لازم است تأمین تسلیحات) با حملات علیه نیکاراگوئه یکسان شمرده شود و دیوان نمی‌تواند تصور کند تأمین تسلیحات برای مخالفان در کشور دیگر، حمله مسلحانه علیه آن کشور است» (ICJ Reports, 1986: 228). از تأکید دیوان بر وقوع حمله مسلحانه می‌توان این گونه نتیجه گرفت که برابر نظر دیوان، 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 پیشدستانه متفاوت از حمله پیشگیرانه است.

«این تفکیک را می‌توان در گزارش ۲۱ مارس ۲۰۰۵ که توسط دبیرکل سازمان ملل متحد تهیه شده ملاحظه کرد» (موسوی و حاتمی، ۱۳۸۵: ۳۰۴)؛(Mousavi & Hatami, 2006: 304). ...در حمله پیشدستانه نکته محوری، فوری و قطعی بودن اصل تهدید است و این یقین وجود دارد که اهتمام برای جلوگیری از وقوع چنین حمله ناموفق، بی‌نتیجه و حمله همه‌جانبه دشمن در حال انجام است... (ظریف و آهنی امینه، ۱۳۹۱: ۴۶)؛(Zarif & Ahani Amine, 2012: 46). ...در مقابل اصطلاح حمله پیشگیرانه به مواردی گفته می‌شود که یک دولت برای سرکوب هرگونه احتمال حمله آتی توسط دولتی دیگر به زور متوسل می‌شود حتی در مواردی که هیچ دلیل و اعتقادی مبنی بر طراحی حمله وجود ندارد و مواردی که هیچ حمله اولیه‌ای صورت نگرفته است... (شریفی، ۱۳۸۲ :۹۷)؛ (Sharifi, 2003: 97). در مجموع خلاء تعریف جامع از دفاع مشروع در منشور نظیر عدم اشاره به ماهیت شروع‌کنندگان حمله مسلحانه و «بسط تهدیدات فرامرزی تروریسم باعث شده تفاسیر حمله پیشدستانه و حمله پیشگیرانه در زمینه توسل به دفاع مشروع جهت مقابله با تروریسم مطرح گردد» (Young, 2022: 2).

مدافعان این دکترین معتقدند در صورتی که تروریست‌ها در عصر تسلیحات اتمی به انواع تسلیحات کشتارجمعی پیشرفته دسترسی پیدا بکنند بسیار مضحک است که خود را در یک حالت انتظار انفعالی قرار دهیم در حالی که خطر یک حمله قریب‌الوقوع را درکنار 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 نسل‌کشی، برده داری، تجاوز، طی کمترین زمان ممکن که هیچ یک ازدولت‌های مورد هدف، حتی به ذهنشان چنین وضعیتی خطور نمی‌کرد. دلیلی وجود ندارد که به برآیندی نقیض برسیم و حملات سایبری علیه سیستم‌های رایانه‌ای همانند سیستم های سدها و بیمارستان‌ها ولو خصوصی، را حمله مسلحانه قلمداد نکنیم. البته تفسیر ماده ۵۱ منشور نمی‌تواند چنان گسترش یابد که به انکار اصل کلی ممنوعیت توسل به زور منجر شود. در خصوص تروریسم سایبری سازمان مجاهدین خلق مستنداتی هست که نشان می‌دهد گروه نامبرده از خاک کشور آلبانی در دو سال اخیر اقدام به حملات سایبری علیه سازمان‌های دولتی و غیردولتی ایران کرده‌اند. منافقین پس از اخراج از عراق و انتقال به آلبانی دچار محدودیت شدید برای انجام عملیات تروریستی در داخل ایران شدند، بنابراین تمرکز خود را به روی اقدامات سایبری و فعالیت‌های جاسوسی قرار دادند. «در اولین اقدام سایبری هک صدا و سیمای جمهوری اسلامی در تاریخ ۷

بهمن ۱۴۰۰ را مرتکب شدند.

گروهی سایبری وابسته به مجاهدین خلق مسؤلیت این اقدام را بر عهده گرفتند که در پی آن چند شبکه تلویزیونی قطع شد» (صدای ایران، ۱۴۰۰: ۱)؛(Seday iran, 2021: 1). «در تصدیق این حمله یکی از مدیران صدا و سیما در این زمینه بیان کردند که احتمالاً سرورهای صدا و سیما مورد حمله هکری قرار گرفته است» (اقتصاد نیوز، ۱۴۰۰: ۱)؛(Eghtesad news, 2021: 1). «در دومین اقدام در روز دوشنبه ۲۳ اسفند ۱۴۰۰ این گروه اعلام کرد چندین سامانه و سایت وزارت فرهنگ و ارشاد اسلامی را از دسترس خارج کرده و اسناد آن را در اختیار خود گرفته است» (نواندیش، ۱۴۰۰: ۱)؛(Noandish, 2021: 1). «در ۱۲ خرداد ۱۴۰۱ سایت شهرداری و دروبین‌های کنترلی شهرداری تهران را هک کردند. خبرگزاری رسمی ایران نیز در پیامی در این‌باره نوشت که براساس پیگیری‌های صورت گرفته، بخشی از شبکه دوربین‌های نظارتی شهرداری و همچنین زیرساخت‌های خدماتی همچون سایت تهران من، سایت شهرداری تهران و نیز بخشی از سامانه‌های داخلی همچون اتوماسیون داخلی و دیگر سامانه‌های ارتباطی کارکنان شهرداری تهران مختل شده است» (انصاف، ۱۴۰۱: ۱)؛(Ensaf, 2022: 1).

طبق گفته پلیس آلبانیا سرورهایی از محل استقرار سازمان مجاهدین خلق کشف شده که نشان می دهد مرتکب حمله سایبری شده‌اند. «برخی حملات در فضای سایبر را باید در درجه ای پایین‌تر از جنگ قلمداد کرد چرا که از شدت کمتری برخوردارند» (Cornish et.al., 2010: 10). بنابراین در مورد تلقی حملات یاد شده به‌عنوان حمله مسلحانه به وب‌سایت‌های صداوسیما و یا چند وزارت خانه قدری ابهام وجود دارد. اما چنانچه شدت حملات به سطحی برسد که بتوان در چارچوب حمله مسلحانه ارزیابی شود و مخل امنیت ملی تلقی گردد، در این‌صورت حق پاسخگویی برای ایران محفوظ خواهد بود. چرا که مطابق دکترین نتیجه محور فلسفه اصلی دفاع مشروع جلوگیری از ورود خسارت‌های مالی و جانی به یک کشور است. امروزه اتفاق نظریه وجود دارد که حمله پیشگیرانه و پیشدستانه خود نوعی تجاوز محسوب می‌شود و در حقوق بین‌الملل هیچ جایگاهی ندارد. اما جمهوری اسلامی ایران گزینه‌های حقوقی و سیاسی مختلفی را پیش‌رو دارد که می‌تواند برای دفاع از خود در برابر چنین حملاتی در آینده به این تدابیر متوسل شود. البته مواضع سیاسی ایران قاعدتاً بر تدابیر و راهکارهای حقوقی نیز تاثیرگذار هستند. ایران می‌تواند در مجامع بین‌المللی و به ویژه در صحن سازمان ملل با صدور بیانیه‌ای اعلام کند که مورد حمله غیرقانونی قرار گرفته و این حمله را مصداق نقض ممنوعیت توسل به زور علیه خود بداند که در این صورت مسأله به صورت جدی مورد توجه افکار جهانی قرار خواهد گرفت.

٤-۳- نقض حق دفاع مشروع منشور ملل متحد در تقابل با بازیگران غیردولتی

هنگام تدوین منشور در سال ۱۹۴۵ بانیان آن در پی پیشگیری از منازعاتی بودند که در جنگ جهانی دوم رخ داده بود پس نه سلاح‌های کشتار جمعی و نه کنشگران غیردولتی در این حیطه مدنظر نبوده‌اند. «به همین ترتیب تروریست‌ها نیز از راهکارهایی استفاده می‌کنند که بسیار مشکل است که زمان وقوع حملات آنان را دریافت» (Arend, 2003: 97). اما به نظر می‌رسد نه فقط قواعد و مقررات

منشور، بلکه عملکرد ابر قدرت‌ها در زمینه حمایت از تروریسم یا لااقل زمینه‌سازی 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 آن‌ها، نمی‌توان از این تئوری دفاع نمود که دولت برای دفاع از خود، باید صبر کند تا حمله صورت گیرد... (جلالی و اقالر، ۱۴۰۲: ۹ ؛(Jalali & Aqalar, 2023: 9). ممنوعیت استفاده از زور از سوی دولت‌ها علیه مواردی که مخل امنیت ملی است مباین با اهداف ملل متحد نیست و ممنوع نمی‌باشد. «رویه دولت‌ها در طی مدت مدیدی که از انعقاد منشور ملل متحد سپری می‌شود موید این مطلب است»(نعمت‌پور و همکاران، ۱۴۰۰: ۱۷۱)؛(Nematpour et. al., 2021: 171).

نتیجه گیری

مفهوم دفاع مشروع پس از ۱۱ سپتامبر ۲۰۰۱ تغییر یافته است و حمله تروریستی به‌عنوان حمله مسلحانه تلقی می‌شود که می‌توان در پاسخ به آن به دفاع مشروع فردی یا جمعی استناد کرد. شورای امنیت با صدور قطعنامه ۱۳۷۳ و طرح دفاع مشروع به‌عنوان حق ذاتی کشورها تلویحاً مجوز حمله به افغانستان را صادر نمود. برای شورا مهم نبود که تکنیک مندرج در ماده ۵۱ دچار چه سرنوشتی می‌شود. شورا در این مرحله ترجیح داد به‌عنوان یک قانونگذار مقتدر اقتدارگرایی خود را به‌منصه ظهور برساند. در حال حاضر شیوه‌های جدیدی از سوی بازیگران غیردولتی برای آسیب‌رسانی به دولت‌ها و اخلال در امنیت ملی آن‌ها ایجاد گردیده است که حقوق بین‌الملل برای مقابله با آن و تعیین حقوق و تکالیف جامعه بین‌المللی در برخورد با این پدیده با چالش‌های متعددی روبه‌روست نه کنوانسیون جامعی در این زمینه وجود دارد و نه عرف بین‌المللی که دولت‌های قربانی بدانند در برابر آن‌ها به چه اقداماتی متوسل شوند. به‌نظر می‌رسد تصمیم‌گیری در مورد حمله پیشدستانه و پیشگیرانه در برابر کنشگران غیرمتعارف و مخل امنیت ملی یکی از چالش‌های اساسی نظام حقوق بین‌الملل فعلی است.

بنابراین مناسب است با توجه به تحولات جدید سیاسی، اجتماعی و اقتصادی جهان و نظریات مطرح علمی مانند براساس رویکرد موسع مکتب کپنهاگ به امنیت ملی اصلاحاتی در منشور صورت گیرد از جمله مقابله جدی با تجاوز و تروریسم و کارآمد شدن سیستم امنیت جمعی، شناسایی و رفع عوامل مؤثر در ضعف شورای امنیت، تبیین چارچوب قاعده دفاع مشروع با تصریح قیودی چون ضرورت، تناسب و فوریت تا از این رهگذر از تفاسیر مختلف منشور توسط دول در راستای حفظ منافعشان‌که باعث بر هم زدن صلح و امنیت بین‌المللی می‌شود جلوگیری نمود وصلح و آرامش را برای بشریت به ارمغان آورد.

منابع فارسی

۱. اصلانی، ج. (۱۳۹۴). ایران، استاکس نت و چالش‌های حقوقی پیش رو در مواجهه با حملات سایبری. *مجموعه مقالات ایران و چالش‌های حقوقی بین‌المللی معاصر*، تهران: انتشارات شهر

دانش.
۲. اقتصاد نیوز. (۱۴۰۰). اتفاق بی سابقه؛ حمله هکری منافقین به صدا و سیما. *پایگاه خبری اقتصاد نیوز*، در: https://www.eghtesadnews.com/%D8%A8%D8%AE%D8%B4%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1-%D8%B3%DB%8C%D8%A7%D8%B3%DB%8C-57/472081-%D8%A7%D8%AA%D9%81%D8%A7%D9%82-
۳. انصاف. (۱۴۰۱). سایت و شبکه دوربین شهرداری تهران هک شد. *پایگاه خبری و تحلیلی انصاف نیوز*، در: http://www.ensafnews.com/349452/%D8%B3%D8%A7%DB%8C%D8%AA-%D9%88-
۴. بهاری، ب.، بخشی شیخ احمد، م. (۱۳۸۸). چیستی تروریسم جدید و ویژگی‌های آن. *مجله پژوهش حقوق و سیاست*، ۱۱(۲۷)، ۲۰-۱.
۵. بهستانی، م. (۱۳۸۷). دفاع پیشگیرانه در حقوق بین‌الملل جدید. *فصلنامه حقوقی گواه*، (۱۲)، ۱۳۶-۱۳۳.
۶. پلاسعیدی، پ.، رنجبریان، ا. (۱۴۰۱). بازخوانی انتقادی مفهوم امنیت جمعی در نظام کنونی بین‌الملل. *فصلنامه مطالعات حقوق عمومی*، ۵۲(۴)، ۱۷۳۷-۱۷۱۷. doi: 10.22059/JPLSQ.2020.289395.2175
۷. جلالی فراهانی، ا. (۱۳۸۵). تروریسم سایبری. *فصلنامه حقوق اسلامی*، ۳(۱۰)، ۱۱۲-۸۵.
۸. جلالی، م.، اقالر، ع. (۱۴۰۲). توسل به بیوتروریسم از منظر حقوق بین‌الملل. *فصلنامه مطالعات حقوق عمومی*، ۵۳(۴)، ۲۰۵۷-۲۰۷۹. doi: 10.22059/jplsq.2021.296700.2311
۹. رامهر، ا. (۱۳۸۵). بررسی مفهوم امنیت ملی. *فصلنامه علوم و فنون نظامی*، ۳(۵)، ۲۵-۳۳.
۱۰. رزمخواه، ن. (۱۴۰۲). نقدی بر پیش نویس قانون اتحادیهٔ اروپا در همسان سازی قوانین حاکم بر هوش مصنوعی، از منظر مقابله با تروریسم سایبری. *فصلنامه مطالعات حقوق عمومی*، ۲۷-۱. doi: 10.22059/jplsq.2022.343006.3086
۱۱. زواره‌ئی، م.، سلیمی، ص. (۱۴۰۱). اعمال اصل صلاحیت جهانی بر جرایم علیه امنیت سایبری در هوانوردی بین‌المللی. *مجله پژوهش‌های حقوقی*، ۲۱(۵۲)، ۶۵-۸۹. doi: 10.48300/jlr.2021.299970.1741
۱۲. سپهر، ح. (۱۳۸۴). واکنش شورای امنیت به رویه دولت‌ها در مبارزه با تروریسم بین‌الملل. *فصلنامه راهبرد*، ۱۳(۲)، ۳۳۵-۳۳۸.
۱۳. شریفی، م. (۱۳۸۲). تحول مفهوم دفاع مشروع در حقوق بین‌الملل با تأکید بر تحولات بعد از ۱۱ سپتامبر ۲۰۰۱. *فصلنامه سیاست خارجی*، ۱۷(۱)، ۱۱۲-۹۱.
۱۴. صحرایی، م. (۱۳۸۸). مشروعیت توسل به زور در مبارزه با تروریسم. *فصلنامه سیاست خارجی*، ۲۳(۴)، ۱۱۳۶-۱۱۱۵.

۱۵. صدای ایران. (۱۴۰۰). ماجرای هک شدن صدا و سیما چیست؟. *پایگاه خبری صدای ایران*، در:
https://sedayiran.com/fa/news/271584/%D9%85%D8%A7%D8%AC%D8%B1%D8%A7%

۱۶. ظریف، م.، آهنی امینه، م. (۱۳۹۱). دفاع مشروع پیشدستانه مشروعیت کاربرد زور در روابط بین‌الملل. *فصلنامه تحقیقات سیاسی بین‌المللی*، (۱۲)، ۸۲-۴۱.

۱۷. عباسی، م.، مرادی، ح. (۱۳۹۴). جنگ سایبر از منظر حقوق بین‌الملل بشردوستانه. *فصلنامه مجلس و راهبرد*، دوره۲۲(۸۱)، ۶۸-۳۷.

۱۸. فرشاسعید، پ.، جلالی، م.، گودرزی، م. (۱۴۰۱). ضرورت همکاری دولت‌ها در تقویت امنیت سایبری. *فصلنامه مطالعات بین‌المللی*، ۷۴(۲)، ۱۷۸-۱۶۳. doi: 10.22034/isj.2022.305392.1603

۱۹. فضائلی، م. (۱۴۰۲). رابطه میان تروریسم و مخاصمات مسلحانه؛ با نگاهی به وضعیت افغانستان. *فصلنامه تحقیقات حقوقی*، ۲۶ (۱۰۲)، ۱۴۰-۱۱۳. doi: 10.48308/jlr.2022.224025.2008

۲۰. فلک، د.، باث، م.، فیشر، ه.، پیترگاسر، ه.، گرین وود، ک.، هینشل فان هینگ، و.، اپین، ن.، اوتر، ا.، ژوزف پارش، ک.، رابوس، و.، ولفروم، ر. (۱۳۸۷). *حقوق بشردوستانه در مخاصمات مسلحانه*. ترجمه سید قاسم زمانی، نادر ساعد، حسین شریفی طرازکوهی، هاجر سیاه رستمی، فاطمه کیهانلو، میرشهبیز شافع، محمد جعفر ساعد، کتایون حسین نژاد، تهران: موسسه مطالعات و پژوهش های حقوقی شهر دانش، چاپ اول.

۲۱. قاسمی، ع.، بارین چهاربخش، و. (۱۳۹۱). حملات سایبری و حقوق بین‌الملل. *مجله حقوقی دادگستری*، ۷۶(۷۸)، ۱۴۵-۱۱۵.

۲۲. قنبرلو، ع. (۱۳۹۷). امنیت ملی: مفهوم، تئوری، و عمل. فصلنامه *سیاست کاربردی*، ۱(۱)، ۶۷- ۴۱.

۲۳. کفایی فر، م.، تیموری، م. (۱۴۰۲). تحولات حقوق بشر و بشردوستانه ناشی از تأثیر چندپارگی حقوق بین‌الملل بر مفهوم تروریسم. *فصلنامه مطالعات حقوق عمومی*، ۵۳(۲)، ۸۵۱-۸۳۱. doi: 10.22059/jplsq.2021.307614.2513

۲۴. کیانی‌زاده، ع.، وثوق، م.، بیرجندی، ف.، قاسمی، ز. (۱۳۹۷). چالش‌های تروریسم نوین از منظر حقوق بین‌الملل بشردوستانه. *نشریه آفاق علوم انسانی*، (۲۳)، ۸۱-۶۵.

۲۵. محبی، م.، شفیعی، ا. (۱۳۹۶). تحول مفهوم دفاع مشروع: حقوق بین‌الملل و بازیگران یردولتی. *فصلنامه تحقیقات حقوقی*، ۲۱(۸۱)، ۱۱۳-۸۹. doi: 10.22034/jlr.2018.120863.1134

۲۶. ممتاز، ج.، صابری انصاری، ب. (۱۳۹۱). تاثیر رویه بعدی دولت‌ها بر اصل منع تهدید و توسل به زور. *فصلنامه راهبرد*، ۲۱(۲)، ۲۰۴-۱۷۵.

۲۷. موسوی، س.، حاتمی، م. (۱۳۸۵). دفاع مشروع پیشدستانه در حقوق بین‌الملل. *مجله دانشکده*

حقوق و علوم سیاسی، ۷۲(۰)، ۳۰۳-۳۲۴.

۲۸. نعمت‌پور، ا.، تقی زاده انصاری، م.، ببری گنبدی، س. (۱۴۰۲). مسؤلیت دولت‌ها در مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور. *فصلنامه مطالعات بین‌المللی*، ۱۹(۴)، ۱۷۱-۱۸۷. doi: 10.22034/isj.2023.365506.1912

۲۹. نعمت‌پور، ا.، تقی زاده انصاری، م.، ببری گنبدی، س. (۱۴۰۰). مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور در قواعد حقوق بین‌الملل. *فصلنامه مطالعات بین‌المللی*، ۱۸(۳)، ۱۸۵-۱۶۵. doi: 10.22034/isj.2022.301984.1573

۳۰. نواندیش. (۱۴۰۰). حمله سایبری به سایت وزارت ارشاد و نمایش تصاویر گروهک منافقین. *پایگاه خبری- تحلیلی نواندیش*، در: https://noandish.com/fa/news/138788/%D8%AD%D9%85%D9%84%D9%87

English References

1. Ackerman, D. (2003). International Law and the Preemptive Use of Force Against Iraq. *CRS Report of Congress Aprill 11*. 1-6.
2. Arend, A. (2003). International Law and the Preemptive Use of Military Force. *The Washington Quarterly*. Vol. 26. 89-103.
3. Collin, B. (1997). The future of Cyberterrorism: Where the Physical and Virtual Worlds Converge. *11th Annual International Symposium on Criminal Justice Issues*.
4. Cornish, P., Livingstone, D., Clemente, D., Yorke, C. (2010). On Cyber Warfare. *A chatham House Report*. 1-49.
5. Couzigou, I. (2022). The Criminalization of Online Terrorism Preparatory Acts under International Law. *Studies in Conflict and Terrorism*. Vol. 45. 535-554.
6. Garner, B. (2009). *black\s law dictionary*. USA: Thomson West, 9th ed.
7. ICJ Reports. (1986). Military and Paramilitary Activities in and Against Nicaragua (Nicaragua V United states). at: https://www.icj-cij.org/node/100900.
8. ICJ Reports. (1996). on the Legality of the Threat or use of Nuclear weapons. at: Reportshttps://www.refworld.org/cases,ICJ,4b2913d62.html.
9. Martínez Esponda, P. (2023). Norm-instability as a Strategy in International Lawmaking: The Case of Self-defence against Non-State Actors. *The Many Paths of Change in International Law*. 69-88. doi: org/10.1093/oso/9780198877844.003.0003
10. Melzer, N. (2011). Cyberwarfare and international Law. *UNIDIR*. 1-38.
11. Scharf, P., Sterio, M., Williams, P. (2020). *Use of Force in Self-Defense against Non-State Actors*, in: *The Syrian Conflict's Impact on International Law*. London: Cambridge University Press. doi: https://doi.org/10.1017/9781108863650.005.
12. Scobbie, I. (2020). self—defence as an exception to the prohibition on the use of force.

Oxford University Press. 149-178. doi: org/10.1093/oso/9780198789321.003.0009.

13. SC/Res/2249. (2015). threats to international peace and security caused by terrorist acts at: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2249.pdf.
14. Stark, R. (1999). *cyber Terrorism: Rethinking New Technology*. Department of Defence and Strategic Studies.
15. The U.S. Army Training and Doctrine Command. (2016). Threat tactics report: islamic state of Iraq and the levant. *U.S. Army Training and Doctrine Command*. 1-44.
16. Young, S. (2022). Contesting Subjects: International Legal Discourses on Terrorism and Indigenous Peoples' Human Rights. *Asian Journal of International Law*, 13(2). 273-293. doi: https://doi.org/10.1017/S2044251322000534.

Translated References to English

1. Abbasi, M., Moradi, H. (2015). Cyber war from the perspective of international humanitarian law. *Majlis and Strategy Quarterly*, Volume 22(81), 37-68. **(In Persian)**
2. Ackerman, D. (2003). International Law and the Preemptive Use of Force Against Iraq. *CRS Report of Congress Aprill*. 1-6.
3. Arend, A. (2003). International Law and the Preemptive Use of Military Force. *The Washington Quarterly*. Vol. 26. 89-103.
4. Aslani, J. (2015). Iran, Stuxnet and upcoming legal challenges in the face of cyber attacks. *A collection of articles on Iran and contemporary international legal challenges*, Tehran: Shahr Danesh Publications, first edition. **(In Persian)**
5. Bahari, B., Bakshi Sheikh Ahmad, M. (2009). What is new terrorism and its characteristics. *Research Journal of Law and Politics*, 11(27), 1-20. **(In Persian)**
6. Behestani, M. (2008). Preventive defence in new international law. *Evidence Legal Quarterly*, (12), 133-136. **(In Persian)**
7. Collin, B. (1997). The future of Cyberterrorism: Where the Physical and Virtual Worlds Converge. *11th Annual International Symposium on Criminal Justice Issues*.
8. Cornish, P., Livingstone, D., Clemente, D., Yorke, C. (2010). On Cyber Warfare. *A chatham House Report*. 1-49.
9. Couzigou, I. (2022). The Criminalization of Online Terrorism Preparatory Acts under International Law. *Studies in Conflict and Terrorism*. Vol. 45. 535-554.
10. Eghtesad News. (2021). an unprecedented event; Hacking attack of hypocrites on radio and television. *Eghtesad News news base*, at:

https://www.eghtesadnews.com/%D8%A8%D8%AE%D8%B4-%D8%A7%D8%AE%D8%A8%D8%A7%D8%B1-%D8%B3%DB%8C%D8%A7%D8%B3%DB%8C-57/472081-%D8%A7%D8%AA%D9%81%D8%A7%D9%82 **(In Persian)**

11. Ensaf. (2022). The site and camera network of Tehran Municipality was hacked. *Insaf News news and analysis database*, at: http://www.ensafnews.com/349452/%D8%B3%D8%A7%DB%8C%D8%AA-%D9%88 **(In Persian)**
12. Farshasaid, P., Jalali, M., Guderzi, M. (2022). The need for governments to cooperate in strengthening cyber security. *International Studies Quarterly*, 74(2), 163-178. doi: 10.22034/isj.2022.305392.1603. **(In Persian)**
13. Fazaeli, M. (2023). the relationship between terrorism and armed conflicts; Looking at the situation in Afghanistan. *Legal Research Quarterly*, 26(102), 113-140. doi: 10.48308/jlr.2022.224025.2008. **(In Persian)**
14. Fleck, D., Bath, M., Fischer, H., Pietergasser, H., Greenwood, K., Hinschel van Heing, W., Ippen, N., Otter, A., Joseph Parrish, K., Rabus. , W., Wolfrum, R. (2008). *Humanitarian rights in armed conflicts*, translated by Seyed Ghasem Zamani, Nader Saed, Hossein Sharifi Tarzkohi, Hajar Siah Rostami, Fatemeh Kihanlou, Mirshahbiz Shafe, Mohammad Jafar Saed, Katayoun Hosseinnejad, Tehran: Shahr Danesh Institute of Legal Studies and Research, first edition. **(In Persian)**
15. Garner, B. (2009). *black\s law dictionary*. USA: Thomson West, 9th ed.
16. ICJ Reports. (1986). Military and Paramilitary Activities in and Against Nicaragua (Nicaragua V United states). at: https://www.icj-cij.org/node/100900.
17. ICJ Reports. (1996). on the Legality of the Threat or use of Nuclear weapons. at: Reportshttps://www.refworld.org/cases,ICJ,4b2913d62.html.
18. Jalali Farahani, A. (2006). Cyber terrorism. *Islamic Law Quarterly*, 3(10), 85-112. **(In Persian)**
19. Jalali, M., Aqalar, A. (2023). recourse to bioterrorism from the perspective of international law. *Quarterly Journal of Public Law Studies*, 53(4), 2057-2079. doi: 10.22059/jplsq.2021.296700.2311. **(In Persian)**
20. Kefaeifar, M., Timuri, M. (2023). Developments of human and humanitarian rights caused by the impact of the fragmentation of international law on the concept of terrorism. *Quarterly Journal of Public Law Studies*, 53(2), 831-851. doi: 10.22059/jplsq.2021.307614.2513. **(In Persian)**
21. Kyanizadeh, A., Vathouq, M., Birjandi, F., Ghasemi, Z. (2018). The challenges of

modern terrorism from the perspective of international humanitarian law. *Afaq Journal of Humanities*, (23), 65-81. **(In Persian)**

22. Martínez Esponda, P. (2023). Norm-instability as a Strategy in International Lawmaking: The Case of Self-defence against Non-state Actors. *The Many Paths of Change in International Law*. 69-88. doi: doi.org/10.1093/oso/9780198877844.003.0003
23. Melzer, N. (2011). Cyberwarfare and international Law. *UNIDIR*. 1-38.
24. Mohebbi, M., Shafiei, A. (2017). Evolution of the concept of self-defence: international law and non-state actors. *Legal Research Quarterly*, 21(81), 113-89. doi: 10.22034/jlr.2018.120863.1134. **(In Persian)**
25. Momtaz, J., Saberi Ansari, b. (2012). The effect of the subsequent procedure of governments on the principle of prohibition of threats and resorting to force. *Strategy Quarterly*, 21(2), 175-204. **(In Persian)**
26. Mousavi, S., Hatami, M. (2006). Preemptive self-defence in international law. *Journal of Faculty of Law and Political Sciences*, 72(0), 324-303. **(In Persian)**
27. Nematpour, A., Taghizadeh Ansari, M., Bebri Gonbadi, S. (2021). Dealing with terrorist attacks on the critical infrastructure of a country in the rules of international law. *International Studies Quarterly*, 18(3), 165-185. doi: 10.22034/isj.2022.301984.1573. **(In Persian)**
28. Nematpour, A., Taghizadeh Ansari, M., Bebri Gonbadi, S. (2023). The responsibility of governments in dealing with terrorist attacks on the critical infrastructure of a country. *International Studies Quarterly*, 19(4), 171-187. doi: 10.22034/isj.2023.365506.1912. **(In Persian)**
29. Noandish. (2021). Cyber attack on the website of the Ministry of Guidance and the display of images of the group of hypocrites. *Noandish news-analytical database*, at: https://noandish.com/fa/news/138788/%D8%AD%D9%85%D9%84%D9%87 **(In Persian)**
30. Plasaeidi, P., Ranjbarian, A. (2022). Critical reading of the concept of collective security in the current international system. *Public Law Studies Quarterly*, Volume 52(4), 1717-1737. doi: 10.22059/JPLSQ.2020.289395.2175 **(In Persian)**
31. Qanbarlu, A. (2018). National Security: Concept, Theory, and Practice. *Applied Politics Quarterly*, 1(1), 41-67. **(In Persian)**
32. Qasemi, A., Barin Chaharbakhsh, w. (2012). Cyber attacks and international law. *Judiciary Law Journal*, (78), 115-145. **(In Persian)**

33. Ramehr, A. (2006). A study of the concept of national security. *Quarterly Journal of Military Sciences and Technologies*, 3(5), 33-25. **(In Persian)**
34. Razmkhah, N. (2023). Criticism of the draft law of the European Union in harmonizing the laws governing artificial intelligence, from the perspective of dealing with cyber terrorism. *Public Law Studies Quarterly*, 1-27. doi: 10.22059/jplsq.2022.343006.3086. **(In Persian)**
35. Sahraei, M. (2009). Legitimacy of use of force in the fight against terrorism. *Foreign Policy Quarterly*, 23(4), 1115-1136. **(In Persian)**
36. Scharf, P., Sterio, M., Williams, P. (2020). *Use of Force in Self-Defense against Non-State Actors* In: *The Syrian Conflict's Impact on International Law.* London: Cambridge University Press. doi: https://doi.org/10.1017/9781108863650.005.
37. Scobbie, I. (2020). self—defence as an exception to the prohibition on the use of force. *Oxford University Press*. 149-178. doi: doi.org/10.1093/oso/9780198789321.003.0009.
38. SC/Res/2249. (2015). (threats to international peace and security caused by terrorist acts) at: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2249.pdf.
39. Sepehr, H. (2005). The reaction of the Security Council to the procedure of governments in the fight against international terrorism. *Strategy Quarterly*, 13(2), 338-335. **(In Persian)**
40. Sharifi, M. (2003). Evolution of the concept of self-defence in international law with emphasis on developments after September 11, 2001. *Foreign Policy Quarterly*, 17(1), 91-112. **(In Persian)**
41. Stark, R. (1999). *cyber Terrorism: Rethinking New Technology*. Department of Defence and Strategic Studies.
42. The U.S. Army Training and Doctrine Command. (2016). Threat tactics report: islamic state of Iraq and the levant. *U.S. Army Training and Doctrine Command*. 1-44.
43. Voice of Iran. (2021). What is the story of radio and television hacking?. *Voice of Iran news base*, at: https://sedayiran.com/fa/news/271584/%D9%85%D8%A7%D8%AC%D8%B1%D8%A7% **(In Persian)**
44. YOUNG, S. (2022). Contesting Subjects: International Legal Discourses on Terrorism and Indigenous Peoples' Human Rights. *Asian Journal of International Law*, 13(2). 273-293. doi: https://doi.org/10.1017/S2044251322000534.
45. Zarif, M. Ahani Amine, M. (2012). Preemptive self-defence of the legitimacy of the use of force in international relations. *International Political Research Quarterly*, (12), 41-

82. **(In Persian)**

46. Zavarei, M., Salimi, P. (2022). Applying the principle of universal jurisdiction to crimes against cyber security in international aviation. *Journal of Legal Research*, 21(52), 89-65. doi: 10.48300/jlr.2021.299970.1741. **(In Persian)**