DOI: 10.22034/isj.2025.464608.2191

International Studies Journal (ISJ)
Vol. 22, No. 3 (87), Winter 2025
Reseived Date: 2024/8/9
Accept Date: 2025/3/2
Article Type: Original Research
PP: 219-234

فصلنامه مطالعات بین‌المللی
سال ۲۲، شماره ۳ (۸۷)، زمستان ۱٤۰٤
تاریخ دریافت: ۱٤۰۳/٥/۱۹
تاریخ پذیرش: ۱٤۰۳/۱۲/۲
نوع مقاله: علمی- پژوهشی
صفحات: ۲۳٤-۲۱۹

حملات سایبری تروریستی در چارچوب دفاع مشروع

دکتر احسان صادقی‌پور* - دکتر محمود گنج‌بخش**

چکیده

در دو سال اخیر سازمان تروریستی مجاهدین خلق به واسطه فاصله سرزمینی قابل توجه، با رخنه در خلاءهای محیط سایبر در پی حملات سایبری به زیرساخت‌های دولتی برآمده است. بدیهی است که دفاع در برابر بازیگران غیردولتی حداقل در برخی مواقع قانونی است. اما ظهور گونه‌های جدید تروریسم مثل تروریسم سایبری که ممکن است به یک‌باره صلح و امنیت بین‌المللی را به مخاطره بیندازد موجب گردیده است که حقوق بین‌الملل از وضع قواعد جدید متناسب با فضای سایبری عقب بماند. سؤالی که در این تحقیق مطرح می‌گردد این است که در راستای اعمال صلاحیت و تأمین منافع ملی حیاتی، تفسیر مناسب از منشور ملل متحد در امکان سنجی توسل به دفاع مشروع از سوی ایران در برابر حملات سایبری سازمان مجاهدین خلق چیست؟ در پاسخ به این مسأله از روش تحقیق توصیفی-تحلیلی با استفاده از ابزار کتابخانه‌ای بهره گرفته شده است. بنابراین پس از بررسی، پژوهش حاضر نتیجه می‌گیرد که حملات سایبری سازمان مجاهدین خلق فعلاً به نقطه لازم برای توسل به دفاع مشروع نرسیده است.

کلیدواژگان

حمله سایبری، سازمان مجاهدین خلق، منافع ملی حیاتی، دفاع مشروع، جمهوری اسلامی ایران.

مقدمه

تعداد و تأثیر کنشگران غیردولتی خصوصاً از دهه ۱۹۹۰ افزایش یافته است. باید توجه داشت که تروریست های مدرن، سلاح های مختلف در اختیار داشته و از زبان زور برای توجیه اعمالشان استفاده می‌کنند. به عبارت دیگر اقدامات مسلحانه گروه های غیردولتی هم می‌تواند همانند اقدامات مسلحانه دولت‌ها به عنوان حمله مسلحانه در نظر گرفته شود. 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 زده‌اند. به این ترتیب از نظر سنتی حمله مسلحانه فقط به حملاتی که از جانب

* دکتری تخصصی حقوق بین‌الملل عمومی، مدرس دانشگاه.
** استادیار گروه اقتصاد و بانکداری اسلامی، دانشکده اقتصاد، دانشگاه خوارزمی، تهران، ایران./ نویسنده مسئول / ایمیل: ganjbakhsh@khu.ac.ir

Article Link: https://www.isjq.ir/article_234996.html
Online ISSN: 2676-5136 Print ISSN: 2045-1735

دولت‌ها صورت می‌گرفت اطلاق می‌شد اما به‌رسمیت شناختن این مطلب که اعمال کنشگران غیردولتی می‌تواند حمله مسلحانه تلقی شود، یقیناً تحولی انقلابی در حقوق بین‌الملل است. پس با توجه به آنچه در ماده ۵۱ و همچنین بند ۷ از ماده ۲ منشور ملل متحد آمده است، ضرورت دارد تا حملات سایبری مجاهدین خلق پیرامون مفهوم حمله مسلحانه به‌عنوان یک عنصر اساسی در حوزه صلاحیت ملی و بحث دفاع مشروع مورد تأمل و بررسی قرار گیرد. براساس فرضیه این تحقیق به‌نظر می‌رسد در خصوص حملات سایبری گروه تروریستی مزبور فعلاً به نقطه لازم در به‌مخاطره انداختن منافع ملی حیاتی نرسیده است. اما چنانچه در آینده شدت حملات به حد مفهوم حمله مسلحانه برسد، براساس اصل صلاحیت ملی در دفاع از منافع ملی حیاتی این حق برای جمهوری اسلامی ایران مسلم خواهد بود. این پژوهش به واکاوی ماهیت حملات سایبری سازمان مجاهدین خلق از منظر حقوق بین‌الملل (توسل به‌زور) می‌پردازد. بر این اساس ابتدا تعریفی از تررویسم سایبری[1] ارائه می‌شود، سپس حملات سایبری از منظر قاعده منع توسل به‌زور مورد تحلیل قرار می‌گیرد. همچنین به طور ویژه، حملات سایبری مجاهدین خلق از نگاه ماده ۵۱ منشور ملل متحد مورد ارزیابی قرار می‌گیرد و در نهایت چگونگی انتساب حملات تروریستی به دولت‌ها بررسی می‌شود.

۱- پیشینه تحقیق

نعمت پور و همکاران (۱۴۰۲) در مقاله‌ای با عنوان «مسؤلیت دولت‌ها در مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور» بیان می‌دارد از آن جایی که زیرساخت‌های حیاتی نقش بسیار مهمی در حیات اقتصادی، امنیتی یک دولت ایفا می‌کنند، برخی از دولت‌ها برای این که مستقیماً وارد مخاصمه با کشور هدف نشوند، سعی می‌کنند با توسل به گروه‌های تروریستی نیابتی یا بدون گذاشتن اثری از خود بیشتر خسارت را به آن کشور وارد نمایند. بنابراین، مقاله حاضر با تمرکز بر حملات تروریستی به زیرساخت‌های حیاتی یک کشور سعی در تبیین مسؤلیت دولت‌ها در زمینه حمایت از گروه‌های تروریستی دارد (نعمت پور و همکاران، ۱۴۰۲: ۱۷۱)؛(Nematpour et.al., 2023: 171).

شریفی طرازکوهی و پیری (۱۳۹۱) در مقاله «منافع ملی حیاتی در پرتو آراء قضایی بین‌المللی» به این نتیجه رسیده است که: دفاع در برابر حملات سایبری با استناد به منافع ملی در رویه قضایی بین‌المللی پذیرفته نیست و نمی‌توان این اقدام را بر اساس حقوق بین‌الملل دفاع مشروع محسوب کرد (شریفی طراز کوهی و پیری، ۱۳۹۱: ۳۵)؛(Sharifi Taraz Kuhi & Piri, 2012: 35).

نوری کاتاگیری (۲۰۲۱) در مقاله «چرا حقوق و هنجارهای بین‌المللی در زمینه جلوگیری از حملات سایبری غیردولتی کم‌کاری می‌کنند» تأکید می‌ورزد که چرا حقوق و هنجارهای بین‌المللی نتوانسته‌اند فضای مجازی را آرام نگه دارند. بیان می‌کند عمده مشکل از ناتوانی آن‌ها در رسیدگی به آنچه بازیگران غیردولتی، مانند هکرها و شرکت‌های فناوری در فضای سایبری انجام می‌دهند، ناشی می‌شود. حقوق بین‌الملل که توسط مقامات دولتی دهه‌ها پیش با تمرکز شدید بر دولت‌ها به‌عنوان

[1]. Cyber terrorism

بازیگران اصلی سیاست بین‌الملل ایجاد شد، با تسلط بازیگران غیردولتی به‌عنوان اپراتورهای واقعی فضای سایبری ناسازگار است (Katagiri, 2021: 1).

سارا پانگرازی (۲۰۲۱) در مقاله «دفاع مشروع در برابر حملات سایبری؟ دفاع دیجیتالی و جنبشی با توجه به ماده ۵۱ منشور ملل متحد» تحلیل می‌کند که حقوق بین‌الملل چگونه در مورد حملات سایبری اعمال می‌شود. حملات سایبری یکی از مبرم‌ترین مسائلی است که جامعه بین‌المللی دولت‌ها با افزایش تهدیدات ناشی از آن مواجه هستند. زیرا زیرساخت‌های حیاتی به‌طور فزاینده‌ای به سیستم‌های دیجیتالی وابسته هستند که این امر دولت‌ها را در برابر چنین حملاتی آسیب‌پذیر می‌کند. در خاتمه نویسنده بیان می‌دارد که توسعه حق جنگ از طریق گسترش دامنه ماده ۵۱ منشور ملل متحد در تضاد با هدف واقعی منشور ملل متحد، که ترویج صلح در میان ملت‌ها است، خواهد بود (Pangrazzi, 2021: 4).

۲- چارچوب مفهومی و مبانی نظری

با توجه به گسترش فضای مجازی کشورها منافع ملی خود را در همه ابعاد بازنگری نموده‌اند. رسانه‌های نوین همانند اینترنت از چنان ظرفیتی برخوردارند که سبب حفظ و پیشبرد منافع ملی کشور در سطح داخلی و بین‌المللی می‌شوند. در بعد داخلی گسترش فضای مجازی به افزایش مشارکت مردم، آگاهی بخشی، شفافیت در همه مسایل منتهی می‌گردد. ...در سطح بین‌المللی ارتقای امنیت ملی، کاهش آسیب پذیری، حضور فعال در تحولات و مسایل بین‌المللی، ترویج هنجارها و هویت خود در سطح جهانی از آثار مثبت رسانه های نوین می‌باشد... (متقی و شاهوردی، ۱۴۰۱: ۱۲۵)؛ (Mottaqi & Shahvardi, 2022: 125).

حملات سایبری از نتایج منفی گسترش فضای مجازی می‌باشد که ممکن است همه منافع ملی دولت را در معرض خطر قرار دهد. هرچند یکی از مبهم ترین مفاهیم در حقوق بین‌الملل، بحث منافع ملی حیاتی دولت‌هاست که قدمتی به بلندای خود دولت- ملت دارد و هر کشوری بنا به موقعیت و شرایط خود تعبیر خاصی از آن مطرح می‌نماید. اما رویه قضایی بین‌المللی در تعارض بین منافع ملی حیاتی دولت‌ها با نظم حقوقی بین‌المللی، نظم حقوقی را ترجیح داده و مقدم داشته است. دولت‌ها به‌طرق مختلفی با استناد به منافع ملی به‌عنوان یک سپر در مقابل موازین حقوقی و ساز وکاری برای فرار و رهایی از تعهدات قانونی، محدودیت‌هایی بر قواعد حقوق بین‌الملل اعمال و در عین حال اقدامات خودشان را قانونی و منطبق باحقوق بین‌الملل جلوه داده‌اند. به‌عنوان نمونه دیوان بین‌المللی دادگستری در پاراگراف ۷۸ از رأی خود در پرونده سکوهای نفتی ایران اعلام کرد که اقدامات آمریکا در تخریب سکوهای نفتی ایران را نمی‌توان به‌عنوان تدبیری ضروری برای حمایت از منافع اساسی امنیتی ایالات متحده بر اساس بند ۱ (د) ماده ۲۰ معاهده مودت، آن‌گونه که در پرتو حقوق بین‌الملل توسل به زور تفسیر می‌شود توجیه کرد، چون این اقدام توسل به‌زور بوده و نمی‌توان آن را بر اساس حقوق بین‌الملل دفاع مشروع از نوع اقدامات پیش‌بینی شده، محسوب کرد. در منشور ملل متحد موضوع قلمرو اختصاصی (منافع ملی) طی بند ۷ ماده ۲ به صورت صلاحیت ملی و به‌عنوان یکی از اصول سازمان ملل درآمد. منافع ملی، به دلیل انکار وجود جامعه جهانی و نادیده انگاشتن

منافع سایر جوامع، با سوءاستفاده گروه های حاکم و ذینفع همراه است. ...اما دیوان در نظریه مشورتی سال ۱۹۹۶ خود درمورد قانونی بودن تهدید یا توسل به سلاح های هسته‌ای، وقتی به منافع ملی حیاتی کشورها می‌رسد، پیشرفت حقوقی قرن بیستم را کنار می‌گذارد و بر مقررات منشور ملل متحد که خود رکن قضایی اصلی آن است، توجهی نمی‌کند و رویکرد واقعگرایی سیاسی را ترجیح می‌دهد... (شریفی طرازکوهی و پیری، ۱۳۹۱: ۲۹ و ۹)؛(Sharifi Taraz Kuhi & Piri, 2012: 9 & 29). البته گاهی منافع ملی بدون حمله و از طریق کمک‌های بشردوستانه تامین می‌شود. ...از اواخر دهه ۲۰۱۰، ژاپن به‌شکل رسمی عنوان داشت که برای حفاظت از منافع ملی خود کمک‌های خارجی ارائه خواهد کرد. هرچند که ژاپن این هدف را از سال ۱۹۶۹ اعلام کرده بود... (Hoshiro, 2024: 480). با عنایت به بند ۷ از ماده ۲ منشور ملل متحد، منافع ملی حیاتی هر کشوری جز صلاحیت داخلی آن کشور است و اعضا ملزم نیستند آن را تابع مقررات منشور نمایند البته تفسیر این بند نبایستی مغایر با اقدامات قهری مندرج در فصل هفتم باشد. به این‌ترتیب آیا دولت قربانی یا در معرض حمله تروریستی سایبری حق دارد به‌جهت دفاع مشروع از خود به عاملان حمله در کشور خارجی حمله کند؟

هر چند هنوز هم اذهان عمومی از تروریسم همان برداشت کلاسیک را دارد اما واضح است که تروریسم امروزه آن‌قدر بسط یافته است که همراه با تحولات جوامع، دگرگون شده و هر روز شکل جدیدی از خود ارائه دهد. دسترسی تروریست‌ها به سلاح‌های کشتارجمعی و بهره‌برداری از امکانات دنیای مدرن نمایانگر نیاز جامعه بین‌المللی برای انطباق خود با آن‌هاست. به واقع 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. این تغییرات سبب شده است تا اقدامات تروریستی طی دهه‌های اخیر توسعه جغرافیایی بیشتری یابد و با افزایش چشمگیر آن‌ها، ترس و 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 جدید در حال گسترش است. تروریسم سایبری از جدیدترین مصادیق آن می‌باشد که از تلاقی اعمال تروریستی و فضای سایبر پا به عرصه وجود نهاده است. پر واضح است که «یکی از مهمترین منابع قدرت در هزاره سوم فضای سایبری و فناوری‌های مرتبط با آن می‌باشد» (Li & Liu, 2021: 8184). به‌عبارتی ظرفیت‌هایی که فضای سایبر برای جامعه بشری به ارمغان آورده نه فقط باعث گردیده تعدادی از بازیگران غیردولتی از این پتانسیل برای مقاصد سیاسی خود سوءاستفاده نمایند بلکه این ظرفیت به صعوبت امر مبارزه با تروریسم و پیشگیری از آن افزوده است. «تاریخ اخیر بشر نشان می‌دهد که تروریسم سایبری و تهدید آن تقریباً به‌طور کامل از نبرد مستقیم نظامی در جهان معاصر پیشی گرفته است»(Asekhauno & Okojie, 2024: 2)، «چرا که عواقب یک حمله سایبری می‌تواند شدید باشد، به‌لحاظ این که احتمال ضربه اقتصادی، آسیب به اعتبار و ثبات یک کشور و حتی تلفات جانی ناشی از تروریسم سایبری وجود دارد» (Leu et.al, 2023: 120). باید توجه داشت که در همه‌جا به نتیجه خشونت یعنی ایجاد وحشت توجه شده است. اگر این استدلال را بپذیریم، متوجه خواهیم شد که تروریسم سایبری نسبت به تروریسم فیزیکی دارای ترس و وحشت بسیار فزاینده‌تری است.

لذا این پژوهش بر این نظریه استوار است که طی سال‌های اخیر با گسترش چشمگیر حملات مسلحانه تروریستی و لزوم تأمین منافع ملی حیاتی، عملکرد دولت‌ها و رویه‌ی بین‌المللی حاکی از پذیرش حق دفاع مشروع کشورها علیه حملات تروریستی از جانب بازیگران غیردولتی می‌باشد. «دنیستین معتقد است که به موجب منشور لازم نیست حمله مسلحانه توسط یک کشور خارجی صورت بگیرد. بنابراین امکان حمله مسلحانه توسط بازیگر غیردولتی نیز وجود دارد. قاضی هیگینز نسبت به قسمتی از نظر مشورتی دیوان در قضیه دیوار حائل که اظهار داشته‌اند: ماده ۵۱ منشور ملل متحد، وجود حق ذاتی دفاع مشروع را در حمله مسلحانه کشوری علیه کشور دیگر به‌رسمیت می‌شناسد، انتقاد نموده و بیان می‌دارد در عبارات ماده ۵۱ منشور چیزی در خصوص این که مقرر کرده باشد دفاع مشروع فقط زمانی جایز است که انحصاراً حمله مسلحانه از سوی دولت رخ داده باشد، دیده نمی‌شود» (سعیدی، ۱۳۹۷: ۴۱-۳۹)؛(Saeidi, 2018: 39-41). پر واضح است تسلیحات مورد استفاده در حمله مسلحانه دستخوش تغییرات چشمگیر گردیده است. این تغییرات در نتیجه تغییر اساسی اوضاع و احوال و نوع و برد تسلیحات به وجود آمده است. استفاده از هواپیمای غیرنظامی که حامل مسافرین غیرنظامی می‌باشد می‌تواند به‌جای اهداف تجاری نتیجه معکوس داشته باشد و به‌عنوان سلاح کشتار جمعی به‌کار رود. علاوه بر این حملات متعددی از جمله حملات سایبری و جنگ اطلاعاتی که به لحاظ فنی در آن از سلاح نظامی استفاده نمی‌شوند هم ممکن است به‌عنوان حمله مسلحانه طبق ماده ۵۱ تلقی گردند. بدین ترتیب به‌نظر می‌رسد در صورتی که حملات سایبری پتانسیل تخریب در حد یک حمله مسلحانه را داشته باشند، مسلحانه فرض شده و دولت قربانی از حق دفاع مشروع برخودار خواهد بود. با این اوصاف در خصوص حملات سایبری سازمان مجاهدین خلق بین سال‌های ۲۰۲۳-۲۰۲۱ علیه ایران، از آن جایی که حملات مذکور به مفهوم حمله مسلحانه مندرج در ماده ۵۱ منشور نرسیده است، بنابراین استناد به حق دفاع مشروع منتفی است.

۳- تاریخچه

گفته می‌شود در «سال ۲۰۰۷ هکرهای روسی از طریق یک حمله سایبری باعث شدند که کامپیوترهای دولتی کشور استونی به‌طور موقت از کار بیفتند. متعاقباً در سال ۲۰۰۸ روسیه دوباره از حملات سایبری برای تکمیل نبرد فیزیکی علیه گرجستان استفاده نمود که این بار تعداد زیادی از وب سایت های دولتی (از جمله وزارت امور خارجه) این کشور را از کار انداخت» (بشیری، ۱۳۹۴: ۶۵)؛ (Bashiri, 2015: 65).

مورد دیگر در سال ۲۰۱۰، استاکس‌نت به‌عنوان کرم صنعتی که با هدف حمله سایبری به تأسیسات هسته ای نظنز و در نهایت، تأخیر در راه اندازی نیروگاه اتمی بوشهر طراحی و منتشر شده بود. «بنا به اظهارات مقامات جمهوری اسلامی ایران صرفاً مانع چرخش سانتریفیوژها در سرعت استاندارد و معمول شده و در نتیجه مانع غنی سازی اورانیوم شد. البته گزارش هایی هم وجود داشتند که میزان آسیب‌های وارد شده توسط استاکس‌نت را فراتر از ادعاهای مقامات رسمی ایران تخمین زدند. علی رغم واکنش‌های مختلف در راستای محکومیت این حمله، متأسفانه موضع حقوقی محکم و شفافی در این خصوص اتخاذ نشد»(اصلانی، ۱۳۹۴: ۲۴۱-۲۳۸)؛(Aslani, 2015: 238-241).

به هر حال در واکنش به حمله سایبری هر چند رویه و عملکردی از کشورها در قالب دفاع مشروع وجود ندارد ولی برخی از کشورها حق دفاع مشروع در برابر این گونه حملات را برای خود پیش بینی کرده‌اند. برای نمونه ایالات متحده آمریکا در صورت وقوع حملات سایبری علیه آمریکا حق دفاع مشروع مندرج در ماده ۵۱ منشور ملل متحد را برای خود محفوظ دانسته است.

٤- فضای سایبر در خدمت تروریسم: مسأله تعریف

تروریسم اصطلاحی است که عموماً برای توصیف استفاده از خشونت به منظور دستیابی به اهداف سیاسی، فکری یا اجتماعی استفاده می‌شود و شامل اقداماتی به عنوان حمله به غیرنظامیان و اماکن عمومی با هدف گسترش ترس و به دست آوردن کنترل است. اما شکی نیست در مورد تعریف پدیده «تروریسم سایبری به مانند تروریسم اجماع تعریف بین کارشناسان این حوزه وجود ندارد» (فضائلی، ۱۴۰۲: ۱۱۵)؛(Fazaeli, 2023: 115) و همچنان واژه ای بحث برانگیز است. «اصطلاح تروریسم سایبری را اولین بار محقق ارشد مؤسسه امنیت و اطلاعات کالیفرنیا باری کالین،[1] به‌کار برد»(رزمخواه، ۱۴۰۲: ۵)؛(Razmkhah, 2023: 5). «دوروتی دنینگ[2] استاد علوم رایانه‌ای در سال ۲۰۰۱ تروریسم سایبری را چنین تعریف می نماید: حملات غیرقانونی و تهدید علیه رایانه ها، شبکه و اطلاعات به منظور ارعاب مردم و حاکمیت برای پیشبرد اهداف سیاسی و اجتماعی می‌باشد»(امیرلی و ثقفی، ۱۳۹۸: ۳۹۵)؛ (Amirli & Saghafi, 2019: 395).

در تعریف دیگر گفته شده است که «تروریسم سایبری شامل استفاده از اینترنت و فناوری اطلاعات از طریق ایجاد ترس و تلفات جانی برای منافع سیاسی و ایدئولوژیک است» (Sharma, 2024: 824). به واقع «آنچه که تروریسم سایبری را از سایر حملات سایبری مانند جرایم سایبری متمایز می کند، قصد صریح برای بی ثبات کردن جوامع است که اغلب در تعقیب اهداف سیاسی است، نه صرفاً منافع مالی یا تعقیب اهداف اجتماعی یا اخلاقی»(Iftikhar, 2024: 2). در مفهوم تروریسم نوین اگرچه هدف نهایی و اصلی ترور دستیابی به امیال و خواسته های سیاسی می‌باشد ولی علاوه بر ابزارهای نظامی از ابزار و روش های متفاوت غیر نظامی هم استفاده می‌شود. این رویدادها نشان می‌دهند که اینترنت به یک ابزار جنگ مجازی برای تروریست‌ها تبدیل شده است. در واقع در قرن حاضر شیوه‌های جدیدی از سوی بازیگران غیردولتی برای آسیب‌رسانی 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 هر حال، تروریسم مفهومی است که در دنیای امروز جهانی شده و از این پس، محدودیت‌های بین‌المللی را برنمی تابد.

---

[1]. Barry Collin

[2]. Dorothy E. Denning

٤-١- حملات سایبری و نقض قاعده منع توسل به زور مندرج در منشور ملل متحد

منشور ملل متحد در بند ۴ ماده ۲ تصریح می‌دارد: کلیه اعضا در روابط بین‌المللی خود از کاربرد یا تهدید به‌کاربرد 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. مسأله ای 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 به‌زور را اعلام می‌کند، ممنوعیتی که در عین ابهام، بی پروا است و طبیعت پیچیده ی آن مهیای تحلیل های مختلف است. فقدان تعریف مشخص منجر به اختلاف نظر مابین حقوقدانان برای تعریف این اصطلاح شده است، که «عده ای زور را به‌عنوان هر اقدامی توسط یک دولت در نقض هنجارهای حقوق بین‌الملل همان طور که در منشور سازمان ملل متحد و سایر کنوانسیون های بین‌المللی بیان شده است، تعریف کرده‌اند» (Al-fahdawi, 2024: 96).

در مقابل برخی معتقدند واژه زور ناظر به حالت نظامی و مسلحانه است. به نظر می‌رسد این مقرره آنچنان گسترده است که اجبار نظامی و غیرنظامی را در بر می‌گیرد. با این وصف، حملات سایبری که دارای آثاری شبیه سلاح‌های نظامی هستند نبایستی مورد مجادله قرار بگیرد. دیوان بین‌المللی دادگستری در نظر مشورتی خود در خصوص مشروعیت تهدید یا استفاده از سلاح‌های هسته ای، 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 به‌زور، صرف نظر از سلاح مورد استفاده اعمال می‌شوند» (ICJ Reports, 1996: para 39). فرقی نمی‌کند که روش مورد استفاده در حمله، متعارف یا سایبری باشد، «مسأله اساسی آسیب ناشی از حمله است که تهدیدی برای امنیت بین‌المللی و حاکمیت دولت است» (Alkharman et.al, 2024: 861). «به‌طور خاص، سخت افزار، نرم افزار و کد های حمله از طریق شبکه رایانه، سلاح‌هایی هستند که می‌توانند از طریق انتقال جریان داده ها به ایراد خسارت منجر شوند» (شایگان و صفوی کوهساره، ۱۳۹۷: ۴۲۶)؛(Shaygan & Safavi Kohsare, 2018: 426). ...بنابراین، لزومی ندارد تسلیحات مذکور برای اهداف تهاجمی ساخته شده باشند و یا دارای آثار انفجاری باشند... (ICJ Reports, 1986: para 228).

اما باید توجه داشت که مفهوم حمله مسلحانه به صورت نامحدودی توسعه پیدا نکند. در صورت ارائه تفسیر نامحدودی از مفهوم مسلحانه، اصل ممنوعیت توسل به‌زور محدود خواهد شد. بنابراین باید عبارت حمله مسلحانه در چارچوب خاصی تعریف شود. به‌نظر می‌رسد ماده ۵۱ منشور در مورد معنای حمله مسلحانه انعطاف پذیرتر شده و شامل تهدید یا اجبار توسط ابزارهایی از جمله رایانه که رسماً به‌عنوان ابزارهای نظامی مطرح نیستند، بشود. ...با این وجود، ابزارهای مذکور حداقل باید همانند سلاح‌های نظامی استفاده شده و موجب خسارات محسوس به اموال یا مرگ افراد گردد... (Stahn, 2004: 35). از این رو در سال ۱۹۴۵ منشور ملل متحد نه تنها جنگ تجاوزکارانه، بلکه هرگونه تهدید یا استفاده از زور را نیز منع می‌کند. بنابراین منشور ملل متحد جهت توسل به‌زور دو ساز و کار را به‌رسمیت شناخته است، اول امنیت جمعی بر مبنای ماده ۳۹ و مواد بعد از آن دوم دفاع مشروع فردی

یا جمعی بر مبنای ماده ۵۱. با این استدلال اگرچه جهان شمولی شناسایی و پذیرش منع توسل به‌زور و اهمیت نظری و عملی آن موجب شده آن را در زمره قواعد آمره حقوق بین‌الملل به شمار آورند اما در بعضی از موارد استفاده از زور می‌تواند مشروع باشد و بدیهی است هدف دفاع مشروع صرفاً دفع تجاوز دشمن است.

٤-۲- رابطه حملات سایبری سازمان مجاهدین خلق با حق ذاتی دفاع مشروع

برخی حقوقدانان همچون ...آنتونیو کاسسه و جورجیو گاجا باور دارند که حق دفاع مشروع مربوط به مخاصمه دولت با دولت است و در اقدامات تروریستی نمی‌توان به آن استناد کرد... (Cassese, 2001: 996). اما باید اظهار داشت ماده ۵۱ منشور هیچ اشاره ای نکرده است که چه کسانی باید مرتکب حمله مسلحانه شده باشند. ...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. 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 بدین ترتیب در مقابل آن حق دفاع مشروع به وجود می‌آید، که چنین روندی می‌تواند منجر به شکل‌گیری قاعده عرفی بین‌المللی باشد. در برخی مواقع بازیگران غیردولتی با استفاده از امکاناتی که محیط سایبر در اختیار آن‌ها قرار داده بدون اینکه گلوله ای شلیک شود اعمالی را مرتکب می‌شوند که خسارات ناشی از آن بسیار بالاتر از خسارات جنگ‌های مسلحانه است. بنابراین پرسشی که مطرح می‌شود این است که کشور قربانی توسل به زور سایبری در صورت تلقی چنین حمله ای به‌عنوان یک حمله مسلحانه، می‌تواند به دفاع مشروع متوسل شود؟ برداشت حداقلی از مفهوم حمله مسلحانه در عصر تروریسم نوین به سختی قابل پذیرش است. ابزارهای به‌کار رفته حملات ۱۱ سپتامبر سلاح‌های متعارف نبوده، بلکه هواپیماهای غیرنظامی بودند. بنابراین ابزارهای نامعمول و غیرمتعارف جنگی از حوزه ماده ۵۱ منشور ملل متحد مستثنی نمی‌شوند. نکته قابل توجه در خصوص نبرد سایبری این است که «برخی حملات در فضای سایبر را باید در درجه ای پایین تر از جنگ قلمداد کرد چرا که از شدت کمتری برخوردارند» (Cornish et.al., 2010: 10).

در آوریل ۲۰۰۷ تعدادی از تارنماهای مهم نهاد های دولتی کشور استونی مورد حمله سایبری قرار گرفتند 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 اندازه ای طول نکشیدند که بخواهند تشکیل یک حمله مسلحانه بدهند» (قاسمی و نامدار، ۱۳۹۷: ۲۱۲)؛(Qassimi & Namdar, 2018: 212). در این جا هر حمله سایبری علیه شبکه رایانه‌ای هر ساختاری را نمی‌توان حمله مسلحانه سایبری دانست، به‌عبارتی مقوله زیرساخت‌های حیاتی نقش بسیار اساسی دارد. ... می‌توان مصادیق زیرساخت‌های حیاتی را به دسته‌های ذیل تقسیم نمود: جمعیت، انرژی، بانک مرکزی، ارتباطات، خدمات (از جمله خدماتی مالی، توزیع غذا و مراقبت‌های بهداشتی) حمل و نقل، تأسیسات هسته‌ای، ساختمان‌های دولتی، سدها، دارایی ها و اماکن تجاری، پایگاه‌ها و تأسیسات نظامی... (نعمت پور و همکاران، ۱۴۰۰: ۱۷۲)؛ (Nematpour et.al., 2021: 172).

از این حیث قطعنامه تعریف تجاوز مجمع عمومی سازمان ملل متحد اقداماتی از جمله اعزام دسته‌ها، گروه‌ها، نیروهای نامنظم یا مزدوران مسلح از جانب یک دولت علیه دولت دیگر را در صورتی به عنوان اقدام تجاوز می پذیرد که «دارای شدت معین همانند اقدامات مندرج در بندهای دیگر ماده ۳ باشد» (GA/Res/3314, 1994). در رویه قضایی بین‌المللی هم می‌توان مواردی در تأیید مسأله فوق پیدا کرد. دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه بیان داشت که ارسال دسته‌ها و گروه‌های مسلحانه به سرزمین دولت دیگر جهت انجام اقداماتی علیه آن «با توجه به معیار مقیاس و تأثیر به عنوان حمله مسلحانه در نظر گرفته می‌شود و با توجه به همین معیار نمی‌توان حوادث مرزی را به‌عنوان حمله مسلحانه علیه دولت دیگر در نظر گرفت» (ICJ Reports, 1986: para103).

شورای امنیت حملات تروریستی ۱۱ سپتامبر را به‌عنوان حمله مسلحانه تلقی کرد و با صدور قطعنامه های ۱۳۶۸ و ۱۳۷۳ حق دفاع را علیه آن به‌رسمیت شناخت. بدون شک یکی از مهمترین دلایل که شورا این حملات را به‌عنوان حمله مسلحانه در نظر گرفت معیار درجه و تأثیر این حملات بوده است زیرا شورا در مورد حملات تروریستی دیگر قبل از ۱۱ سپتامبر اقدام به شناسایی حق دفاع مشروع در پاسخ به آن نکرده بود. در خصوص موضوع مقاله مستنداتی در دست است که نشان می‌دهد سازمان مجاهدین خلق از خاک کشور آلبانی در دو سال اخیر اقدام به حملات سایبری علیه سازمان های دولتی و غیردولتی ایران کرده است مثل هک دوربین ها و وب سایت های شهرداری، شبکه های صدا و سیما، وب سایت های وزرات امور خارجه و نهاد ریاست جمهوری. ضمن پذیرش مسؤلیت این حملات از سوی این گروه، طبق گفته «منابع آلبانیایی پلیس این کشور سرورهایی از محل استقرار مجاهدین خلق کشف کرده‌اند که نشان می‌دهد که از طریق این تجهیزات کامپیوتری مرتکب حمله سایبری می‌شدند» (سفارت جمهوری اسلامی ایران در رم، ۱۴۰۲: ۲)؛ (Embassy of the Islamic Republic of Iran in Rome, 2023: 1).

این حقیقت که حملات سایبری فاقد شدت لازم نقض بند ۴ ماده ۲ تعبیر نمی‌شوند، به معنای مشروعیت آن‌ها نیست. حمله به سیستم کنترل حمل و نقل هوایی و یا اختلال در نیروگاه های اتمی می‌توان با اطمینان بیان نمود که خسارات مادی و تلفات جانی منتج از آن قابل پیش بینی بوده اما در مورد حمله به وب سایت های صدا و سیما یا چند وزارتخانه قدری ابهام وجود دارد. چرا که مطابق دکترین نتیجه محور فلسفه اصلی دفاع مشروع جلوگیری از ورود خسارت‌های مالی و جانی به یک کشور است. لکن جمهوری اسلامی ایران گزینه‌های حقوقی و سیاسی مختلفی را پیش رو دارد که می‌تواند برای دفاع از خود در برابر چنین حملاتی در آینده به این تدابیر متوسل شود.

٤-۳- ارتباط بین حمله تروریستی و یک دولت (قابلیت انتساب)

در ماده ۸ پیش نویس طرح مسؤلیت بین‌المللی کمیسیون حقوق بین‌الملل مقرر شده است که یک دولت در صورتی مسؤل اقدامات گروه‌ها می‌باشد که این گروه‌ها طبق دستور، هدایت یا کنترل آن دولت اقدام کرده باشند. نظر کمیسیون در این جا بیشتر با رأی دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه منطبق است. تأیید دولت نیز به‌عنوان عاملی در قابلیت انتساب مطرح می‌باشد. طبق رأی دیوان بین‌المللی دادگستری در قضیه کارکنان دیپلماتیک و کنسولی ایالات متحده در تهران، عمل یک گروه غیردولتی قابل انتساب به دولت خواهد بود چنانچه دولت آن عمل را تأیید کند به جای

این که اقداماتی علیه آن صورت دهد. این مسأله در ماده ۱۱ طرح کمیسیون حقوق بین‌الملل در مورد مسؤلیت دولت‌ها ۲۰۰۱ منعکس شده است. با این حال مسأله مسؤلیت بین‌المللی دولت‌ها ناشی از حملات سایبری بازیگران غیردولتی با چالش اساسی مواجه است. در حقیقت، فقدان مرز در فضای سایبری سبب شده است شناسایی منشأ حمله سایبری با دشواری هایی مواجه شود «اما بسیاری از کارشناسان بر این عقیده هستند که با اختصاص وقت و منابع کافی مسأله انتساب موثق حملات سایبری قابل حل است حداقل هنگامی که حملات با مقیاس بالا علیه زیرساخت‌های حیاتی صورت گیرد» (فرشاسعید و همکاران، ۱۴۰۰: ۲۱)؛(Farshasaid et.al., 2021: 21).

پر واضح است در مواردی که اعطای پناهندگی به مرتکبین اعمال تروریستی توسط یک دولت و همچنین از پوشش پناهندگی برای اقدام تروریستی در دولت متبوع یا سایر دولت‌ها استفاده شود، چنانچه دولت اعطا کننده، از این فعالیت‌ها مطلع باشد، یا حمایت و هدایت‌کننده این گونه اعمال باشد، و یا دستور آن‌ها را داده باشد، مسؤلیت بین‌المللی دولت اعطاکننده قابل تصور است. «در واقع، دولت‌ها از نظر حقوقی موظند نه تنها از ارائه کمک در حمایت از فعالیت‌های مسلحانه بازیگران غیردولتی علیه سایر دولت‌ها خودداری کنند، بلکه در حصول اطمینان از اینکه قلمرو آن‌ها توسط بازگیران غیردولتی برای چنین مواردی استفاده نمی‌شود، اهتمام لازم را به عمل آورند» (Preto, 2024: 49). در این زمینه، دولتی که میزبان یک سازمان تروریستی است، نمی‌تواند از حاکمیت خود به‌عنوان سپری برای بازدارندگی و جلوگیری از واکنش مسلحانه دولت قربانی استفاده کند. «بنابراین، ناتوانی یا عدم تمایل دولت‌ها برای جلوگیری از حملات تروریستی است که تمامیت ارضی آن‌ها را در معرض نقض توسط دولت قربانی قرار می‌دهد» (Henderson, 2024: 415). به‌طور کلی باید بیان داشت برای اثبات انتساب اقدام تروریستی به دولت بایستی یکی از معیارهای زیر وجود داشته باشد:

اول، دولت کنترل مؤثر بر فعالیت‌های تروریستی داشته باشد (ماده ۸ پیش نویس طرح مسؤلیت بین‌المللی). دوم، دولت به‌جای اتخاذ اقداماتی علیه اقدام تروریستی، آن را تأیید کرده باشد (ماده ۱۱ پیش نویس طرح مسؤلیت بین‌المللی). سوم، «دولت کنترل کلی بر فعالیت‌های تروریستی داشته باشد» (دادگاه کیفری یوگسلاوی سابق در قضیه تادیچ ۱۹۹۹ به این معیار اشاره کرده است (ICTY, 1999: Para137,145). معیار کنترل کلی برای توجیه اقدام علیه طالبان و القاعده در ۲۰۰۱ هم کفایت می کرد. شکی نیست که طالبان نقش مهمی در آموزش و حمایت عملیاتی القاعده داشت. «طالبان به تروریست‌های القاعده اجازه ایجاد پادگان های آموزشی در سرزمین افغانستان را داد و علی رغم تلاش های جامعه بین‌المللی، رژیم طالبان از تغییر سیاست خودداری کرد»(Tsagourias, 2024: 337). در حال حاضر تمایل آشکاری به این سمت وجود دارد که حتی یک دولت صرفاً به دلیل مأمن تروریست‌ها شدن، مسؤلیت خواهد داشت.

فرجام سخن

برای مدت قابل توجهی، جامعه بین‌المللی سعی کرد به تفسیری مبسوط از ممنوعیت توسل به‌زور، همراه با قرائتی کم‌وبیش محدود کننده از حق دفاع مشروع پایبند باشد. با این حال این تعادل شکننده

در دهه ۹۰ و به ویژه با حملات ۱۱ سپتامبر ۲۰۰۱ متحول شد. در حال حاضر رویه بین‌المللی حکایت از مشروعیت توسل به دفاع مشروع در برابر حملات تروریستی گروه‌های غیردولتی از سرزمین یک کشور ناتوان یا کشوری که حکومت آن در برابر اعمال گروه‌های غیردولتی حالت انفعالی داشته است، دارد. اگرچه در نبود نظام حقوقی کارآمد در خصوص فضای سایبری تردیدی نیست، لیکن آنچه مهم جلوه می‌کند، تلاش برای وام گرفتن اصول و قواعدی حقوقی از دیگر نظام‌های موجود حقوق بین‌الملل و سنجش میزان مشابهت آن‌ها با فضای سایبری است. و بیان کردیم یک حمله سایبری با توجه به نتایج و آثار آن یعنی شدت آسیب و تخریب ایجاد شده و البته وجود رابطه علت و معلولی بین حمله سایبری و خسارات به وجود آمده ارزیابی می‌گردد و در این چارچوب می‌تواند حمله مسلحانه تلقی شده و حق دفاع مشروع را در پی داشته باشد.

این که حملات سایبری مجاهدین خلق با توجه به نوع تأثیری که گذاشته نقض اصل ممنوعیت توسل به‌زور تلقی می‌شود، ظاهراً متقن نبوده چرا که حملات سایبری این گروه در حد حملات پراکنده به وبگاه‌های اینترنتی چند سازمان دولتی یا غیردولتی است. بنابراین حملات سایبری این گروه فعلاً در حدی نیست که در چارچوب مفهوم حمله مسلحانه بگنجد و منافع ملی حیاتی را به‌مخاطره اندازد. از طرف دیگر بنا به اظهارات مقامات رسمی ایران حمله مزبور هیچ گونه خسارات فیزیکی به‌همراه نداشته و از این رو نقض ممنوعیت توسل به‌زور در حقوق بین‌الملل تلقی نمی‌شود. البته سکوت رسمی، عدم پیگیری مسأله فوق در مجامع بین‌المللی و واکنش انفعالی جمهوری اسلامی ایران در قبال این حمله بررسی گزینه‌های موجود را عملاً عقیم می‌کند. بدون تردید حملات سایبری نه تنها معضلی سیاسی- امنیتی، بلکه چالشی حقوقی است. از این رو نقش آفرینی کمیسیون حقوق بین‌الملل به عنوان رکن حقوقی مجمع عمومی سازمان ملل متحد در تدوین چارچوب مؤثر حقوقی بین‌المللی در حوزه سایبر و ارتقاء همکاری‌های بین‌المللی و منطقه‌ای دولت‌ها برای مقابله با حملات سایبری می‌تواند در این خصوص راهگشا باشد.

منابع فارسی

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

۲. امیرلی، ح.، و ثقفی، ک. (۱۳۹۸). ارائه مدل مفهومی ارزیابی تهدیدات تروریسم سایبری. *فصلنامه امنیت ملی*، ۹(۳۳)، ۳۸۹-۴۲۴.

۳. بشیری، آ. (۱۳۹۴). *حمله سایبری و دفاع مشروع در حقوق بین‌الملل*. پایان‌نامه کارشناسی‌ارشد، قم: دانشگاه قم.

۴. 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

۵. سعیدی، ط. (۱۳۹۷). *تحولات حقوق بین‌الملل در زمینه دفاع مشروع علیه گروه‌های غیردولتی*. پایان‌نامه کارشناسی‌ارشد، صفادشت: دانشگاه آزاد اسلامی واحد صفادشت.
۶. سفارت جمهوری اسلامی ایران در رم. (۱۴۰۲). درگیری پلیس آلبانی در مقر منافقین در اجرای حکم دادگاه در بازرسی از کمپ به خاطر فساد، جرایم سازمان یافته و حملات سایبری. *تارنمای سفارت*، در: https://italy.mfa.gov.ir/portal/newsview/722684
۷. شایگان، ف.، صفوی کوهساره، س. (۱۳۹۷). عملیات سایبری به مثابه توسل به‌زور. *فصلنامه مطالعات حقوق عمومی*، ۴۸(۲)، ۴۱۹-۴۴۱. doi: https://doi.org/10.22059/jplsq.2017.237650.1546
۸. شریفی طرازکوهی، ح.، و پیری، ح. (۱۳۹۱). منافع ملی حیاتی در پرتو آراء قضایی بین‌المللی. *فصلنامه پژوهش حقوق عمومی*، ۱۴(۳۸)، ۹-۳۷.
۹. فرشاسعید، پ.، جلالی، م.، و گودرزی، م. (۱۴۰۰). ضرورت تدوین کنوانسیون بین‌المللی حملات سایبری. *فصلنامه مطالعات حقوقی*، ۱۳(۱)، ۲۰۵-۲۳۰. doi: 10.22099/jls.2021.33031.3370
۱۰. 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
۱۱. قاسمی، غ.، و نامدار، س. (۱۳۹۷). بررسی مفهوم دفاع مشروع در پرتو حملات سایبری با تأکید بر حمله استاکس‌نت به تأسیسات هسته ای ایران. *مجله مطالعات حقوقی*، ۱۰(۱)، ۱۹۹-۲۳۵. doi: 10.22099/jls.2018.23191.2178
۱۲. متقی، ا.، و شاهوردی، ص. (۱۴۰۱). جایگاه رسانه های نوین در پیشبرد منافع ملی در چشم انداز نظری. *فصلنامه مطالعات منافع ملی*، ۸(۲۹)، ۱۲۵-۱۴۸.
۱۳. نعمت پور، ا.، تقی‌زاده انصاری، م.، و 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
۱۴. نعمت پور، ا.، تقی‌زاده انصاری، م.، و ببری گنبدی، س. (۱۴۰۰). مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور در قواعد حقوق بین‌الملل. *فصلنامه مطالعات بین‌المللی*، ۱۸(۳)، ۱۶۵-۱۸۵. doi: 10.22034/isj.2022.301984.1573

English References

1. Al-Fahdawi, T. (2024). Cyber Warfare as a Use of Force against Third-Party Countries: The Perspective of International Law. *Groningen Journal of International Law*, 10(2), 91-102. doi: 10.21827/GroJIL.10.2.91-102
2. Alkharman, J., Drawsheh, S., Al-Khataybeh, M., Younes, Z., Darawsheh, N., & Alrashdan, H. (2024). Cyber Attacks and its Implication to National Security: The Need for International Law Enforcement. *Pakistan Journal of Criminology*, 16(3), 851-864. doi: https://doi.org/10.62271/pjc.16.3.851.864

3. Asekhauno, A., & Okojie, T. (2024). International Cyber Terrorism: A Global Apocalyptic 'Time-Bomb.' *African Education Indices*, 13(1).
4. Cassese, A. (2001). Terrorism is Also Disrupting Some Crucial Legal Categories of International Law. *EJIL*, 12(5), 993-1001.
5. Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). On Cyber Warfare. *A chatham House Report*. 1-49.
6. GA/Res/3314. (1974).
7. Henderson C. (2024). *The Use of Force and International Law*. Cambridge: Cambridge University Press, 2nd edition.
8. Hoshiro, H. (2024). Bringing the National Interest to the Forefront of Foreign Aid Policy: The Case of Japan. *Asian Survey*, 64(3), 480–513. doi:10.1525/as.2024.2064348
9. ICJ Reports. (1986). Military and Paramilitary Activities in and Against Nicaragua (Nicaragua V United states). at: https://www.icj-cij.org/node/100900.
10. ICJ Reports. (1996). on the Legality of the Threat or use of Nuclear weapons. at: Reportshttps://www.refworld.org/cases,ICJ,4b2913d62.html.
11. ICTY. (1999). Prosecutor V. Tadic.
12. Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science.* doi: 10.7717/peerj-cs.1772
13. Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity*, Volume 7, Issue 1. doi: https://doi.org/10.1093/cybsec/tyab009
14. Leu, D., Udroiu, C., Raicu, G., Gârban, H., & Șcheau, M. (2023). Analysis of some case studies on cyberattacks and proposed methods for preventing them. *Romanian Journal of Information Technology and Automatic Control*, 33(2), 119-134. doi: 10.33436/v33i2y202309
15. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186. doi: https://doi.org/10.1016/j.egyr.2021.08.126
16. 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
17. Pangrazzi, S. (2021). Self-defence Against Cyber Attacks? Digital and Kinetic Defence in Light of Article 51 UN-CHARTER. Policy Brief. *ICT for Peace Foundation*, Geneva.
18. Preto, R. (2024). A never-ending tug-of-war: The inherent right of self-defense against non-state actors. *e-Publica*, 11(2), 32-58. doi: 10.47345/v11n2art2

19. Sharma, M. (2024). Risks of Cyber Security Threats, Cyber Terrorism and Cyber Warfare. *Nanotechnology Perceptions*, 20(S13), 824-837. doi:10.62441/nano-ntp.v20iS13.51
20. Stahn, C. (2004). Nicaragua is Dead, long live Nicaragua, the Right of self-Defence Under Art. 51 UN charter and International Terrorism. doi:10.1007/978-3-642-18896-1_26
21. Tsagourias, N. (2024). The Use of Force Against Terrorist Attacks: The Two Facets of Self-Defence. *Saint Louis University Law Journal,* 68(2), 326-348.

Translated References to English

1. Al-Fahdawi, T. (2024). Cyber Warfare as a Use of Force against Third-Party Countries: The Perspective of International Law. *Groningen Journal of International Law*, 10(2):91-102. doi: 10.21827/GroJIL.10.2.91-102
2. Alkharman, J., Drawsheh, S., Al-Khataybeh, M., Younes, Z., Darawsheh, N., & Alrashdan, H. (2024). Cyber Attacks and its Implication to National Security: The Need for International Law Enforcement. *Pakistan Journal of Criminology*, 16(3), 851-864. doi: https://doi.org/10.62271/pjc.16.3.851.864
3. Amirli, H., & Saghafi, K. (2019). Presenting a conceptual model for evaluating cyber terrorism threats. *National Security Quarterly*, Volume 9(33), 389-424. **(In Persian)**
4. Asekhauno, A., & Okojie, T. (2024). International Cyber Terrorism: A Global Apocalyptic 'Time-Bomb.' *African Education Indices*, Volume 13, No. 1.
5. 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)**
6. Bashiri, A. (2015). *Cyber attack and self-defence in international law*. Master's thesis, Qom: Qom University. **(In Persian)**
7. Cassese, A. (2001). Terrorism is Also Disrupting Some Crucial Legal Categories of International Law. *EJIL*, 12(5), 993-1001.
8. Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). On Cyber Warfare. *A chatham House Report*. 1-49.
9. Embassy of the Islamic Republic of Iran in Rome. (2023). Clash of Albanian police in the headquarters of the hypocrites' in the implementation of the court order in the search of the camp for corruption, organized crimes and cyber attacks. *Embassy website*, at: https://italy.mfa.gov.ir/portal/newsview/722684 **(In Persian)**
10. Farshasaid, P., Jalali, M., & Gudarzi, M. (2021). The necessity of developing an international convention on cyber attacks. *Legal Studies Quarterly*, 13(1), 205-230. doi:

10.22099/jls.2021.33031.3370 **(In Persian)**

11. 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)**
12. GA/Res/3314. (1974).
13. Ghasemi, G., & Namdar, S. (2018). Examining the concept of Self-defence in the light of cyber attacks, emphasizing the Stuxnet attack on Iran's nuclear facilities. *Journal of Legal Studies*, 10(1), 199-235. doi: 10.22099/jls.2018.23191.2178 **(In Persian)**
14. Henderson C. (2024). *The Use of Force and International Law*. Cambridge: Cambridge University Press, 2nd edition.
15. Hoshiro, H. (2024). Bringing the National Interest to the Forefront of Foreign Aid Policy: The Case of Japan. *Asian Survey*, 64(3), 480–513. doi:10.1525/as.2024.2064348
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. ICTY. (1999). Prosecutor V. Tadic.
19. Iftikhar, S. (2024). Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science.* doi: 10.7717/peerj-cs.1772
20. Katagiri, N. (2021). Why international law and norms do little in preventing non-state cyber attacks. *Journal of Cybersecurity*, 7(1). doi: https://doi.org/10.1093/cybsec/tyab009
21. Leu, D., Udroiu, C., Raicu, G., Gârban, H., & Şcheau, M. (2023). Analysis of some case studies on cyberattacks and proposed methods for preventing them. *Romanian Journal of Information Technology and Automatic Control*, 33(2), 119-134. doi: 10.33436/v33i2y202309
22. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186. doi: https://doi.org/10.1016/j.egyr.2021.08.126
23. 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
24. Mottaqi, A., Shahvardi, P. (2022). The position of new media in advancing national interests in a theoretical perspective. *Quarterly Journal of National Interest Studies*, 8(29), 125-148. **(In Persian)**
25. 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)**

26. 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)**
27. Pangrazzi, S. (2021). Self-defence Against Cyber Attacks**?** Digital and Kinetic Defence in Light of Article 51 UN-CHARTER. Policy Brief. *ICT for Peace Foundation*, Geneva.
28. Preto, R. (2024). A never-ending tug-of-war: The inherent right of self-defense against non-state actors. *e-Publica*, 11(2), 32-58. doi: 10.47345/v11n2art2
29. 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)**
30. Saeidi, T. (2018). *Evolutions of international law in the field of self-defence against non-state groups*. master's thesis, Safadasht: Islamic Azad University, Safadasht branch. **(In Persian)**
31. Sharifi Taraz-Kuhi, H., & Piri, H. (2012). Vital National Interests in the Light of International Judicial Decisions. *Quarterly Journal of Public Law Research*, 14(38), 37-9. **(In Persian)**
32. Sharma, M. (2024). Risks of Cyber Security Threats, Cyber Terrorism and Cyber Warfare. *Nanotechnology Perceptions*, 20(S13), 824-837. doi:10.62441/nano-ntp.v20iS13.51
33. Shaygan, F., & Safavi Kohsare, S. (2018). Cyber operations as use of force. *Public Law Studies Quarterly*, 48(2), 441-419. doi: https://doi.org/10.22059/jplsq.2017.237650.1546 **(In Persian)**
34. Stahn, C. (2004). Nicaragua is Dead, long live Nicaragua, the Right of self-Defence Under Art. 51 UN charter and International Terrorism. doi:10.1007/978-3-642-18896-1_26
35. Tsagourias, N. (2024). The Use of Force Against Terrorist Attacks: The Two Facets of Self-Defence. *Saint Louis University Law Journal,* 68(2), 326-348.