Journal of Islamic Human Rights
Volum 1, Consecutive Number 1, 2024
Journal Homepage: https://islamichumanrights.ir/

The Necessity of Considering Cyber-Technology Terrorism as Territorial Aggression in the Light of the International Human Rights System

Leila Mirbod[1*], MohammadMehdi Seyed Nasseri[2]

1. PhD Student in Public International Law, Islamic Azad University, Tehran Science and Research Unit, Tehran, Iran. Leila_mirbod@yahoo.com

2. Researcher in Medical Ethics and Law Research Center, Shahid Beheshti University of Medical Sciences, Tehran, Iran.

Abstract

In the modern era, legal challenges concerning family law, particularly in social, economic, and political contexts, have evolved into complex issues. This article examines the legal challenges facing families in this era and aligns them with the Declaration of Human Rights in Islam. The study begins by analysing the fundamental concepts of family law and its role in shaping individual and social identity. Subsequently, it scrutinises legal challenges such as imbalances in familial rights, gender inequalities, and difficulties arising from economic and social transformations. Adopting a qualitative methodology and employing content analysis, the article aims to demonstrate how Islamic human rights can contribute to improving the status of families and addressing their challenges. The findings suggest that the Declaration of Human Rights in Islam offers viable solutions to existing issues, emphasising principles of justice and equity to strengthen the foundation of families. Ultimately, the article concludes that adherence to Islamic principles in family law can pave the way for enhancing the condition of families in the contemporary age.

Keywords: Cyber Terrorism, Aggression, Human Rights, United Nations Charter, Resort to Force

- Mirbod L., Seyed Nasseri, M M. (2024). The Necessity of Considering Cyber-Technology Terrorism as Territorial Aggression in the Light of the International Human Rights System, *Journal of Islamic Human Rights*, 1(1), 1-26.

مجله حقوق بشر اسلامی
دورۀ اول ـ شمارۀ اول ـ ۱۴۰۳
صفحات ۱-۲۶ (مقاله پژوهشی)
تاریخ: دریافت ۱۴۰۳/۰۸/۱۵ـ پذیرش ۱۴۰۳/۱۰/۰۱ ـ انتشار ۱۴۰۳/۱۱/۰۱

بایسته‌های تلقی تروریسمِ سایبر - تکنولوژی به مثابه تجاوزِ سرزمینی در پرتو نظام حقوق بین‌الملل بشر

لیلا میربد[۱*]، محمدمهدی سیدناصری[۲]

۱. دانش‌آموخته دکتری حقوق بین‌الملل عمومی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران، تهران، ایران.
Leila_mirbod@yahoo.com
۲. پژوهشگر مرکز تحقیقات اخلاق و حقوق پزشکی دانشگاه علوم پزشکی شهید بهشتی، تهران، ایران.

چکیده

در عصر نوین، چالش‌های حقوقی خانواده به‌ویژه در زمینه‌های اجتماعی، اقتصادی و سیاسی، به معضلات پیچیده‌ای تبدیل شده است. این مقاله به بررسی چالش‌های حقوقی خانواده در این عصر و تطابق آن با اعلامیه حقوق بشر اسلامی می‌پردازد. در این تحقیق، ابتدا به تحلیل مفاهیم بنیادی حقوق خانواده و نقش آن در تکوین هویت اجتماعی و فردی پرداخته می‌شود. سپس، چالش‌های حقوقی نظیر عدم توازن در حقوق خانوادگی، نابرابری‌های جنسیتی، و مشکلات ناشی از تحولات اقتصادی و اجتماعی به دقت بررسی می‌شود. مقاله با هدف نشان دادن اینکه چگونه حقوق بشر اسلامی می‌تواند به بهبود وضعیت خانواده و حل چالش‌های آن کمک کند، روش‌شناسی کیفی را انتخاب کرده و از تحلیل محتوایی استفاده می‌کند. یافته‌ها نشان می‌دهند که اعلامیه حقوق بشر اسلامی می‌تواند راهکارهایی برای رفع چالش‌های موجود ارائه دهد و با تأکید بر اصول عدالت و انصاف، موجب تقویت بنیان‌های خانواده شود. در نهایت، مقاله به این نتیجه می‌رسد که توجه به اصول اسلامی در حقوق خانواده می‌تواند زمینه‌ساز بهبود وضعیت خانواده‌ها در عصر جدید باشد.

کلیدواژه: تروریسم سایبری، تجاوز، حقوق بشر، منشور سازمان ملل متحد، توسل به زور

- میربد، لیلا؛ سیدناصری، محمدمهدی. (۱۴۰۳). بایسته‌های تلقی تروریسمِ سایبر - تکنولوژی به مثابه تجاوزِ سرزمینی در پرتو نظام حقوق بین‌الملل بشر، مجله حقوق بشر اسلامی، ۱(۱)، صفحات ۱-۲۶.

مقدمه

یکی از بدیهی‌ترین حقوق شناخته‌شده بشر، حق آزادی و امنیت است و بالتبع، بخشی لاینفک از اسناد حقوق بشری محسوب می‌گردد. دولت‌ها نیز همواره علاوه بر اسناد جهانی و منطقه‌ای در قوانین داخلی خود، بر لزوم شناسایی و احترام به این حقوق تأکید دارند. با این حال سایبر تروریسم که گونه‌ای نوین از تروریسم بین‌المللی بوده و تهدیدی جدی برای بشریت محسوب می‌شود، موجب شده است که دولت‌ها محدودیت‌هایی را جهت تأمین این حقوق به وجود آورند؛ بدین‌معنا که همه اشخاص با بهره‌مندی از آزادی، در برابر دخالت‌های غیرقانونی و خودسرانه، مصون هستند. این مصونیت در زمینه تعقیب کیفری و نیز دیگر حوزه‌ها که دولت بر آزادی افراد، تأثیر می‌گذارد، قابل اعمال است. بخشی از تلاش‌های دولت برای مبارزه با تروریسم، عملاً منجر به اتخاذ اقداماتی می‌شود که بر حق آزادی افراد، تأثیرگذار است. برای نمونه می‌توان به اصول محاکمه در جرایم تروریستی، مشتمل بر مقررات مرتبط با قرار تأمین و نگهداشت افراد در بازداشت تا شروع محاکمه اشاره کرد (۱). از سوی دیگر، شروع هزاره سوم میلادی با اَشکال جدیدی از تروریسم بین‌المللی همراه بوده است. کوفی عنان، دبیرکل پیشین سازمان ملل در گزارش خود با عنوان «ما مردمان در آستانه هزاره سوم میلادی»، دو نوع رهایی عمده را برای مردمان جهان مطرح کرد: رهایی از خواسته و رهایی از ترس؛ به این امید که پیامدهای کوشش‌های بین‌المللی بتواند موجب رهایی از خواسته‌ها و نیازهای بشر ـ که ابعاد اقتصادی، اجتماعی، سیاسی و فرهنگی دارد ـ و رهایی مردم از ترس و خطر جنگ بشود. به نظر می‌آید که در حال حاضر، ترس از وقایع تروریستی، بیشتر از هر ترس دیگر در عرصه بین‌المللی وجود دارد. اگرچه مبارزه جامعه جهانی علیه تروریسم، پیش از تأسیس سازمان ملل آغاز شد، تردیدی نیست که با وقوع حوادث یازدهم سپتامبر ۲۰۰۱ علی‌رغم ابهامات موجود، پس از تجربه شیوه جدیدی از نقض قواعد بنیادین حقوق بشر، رویکرد دولت‌ها نیز در مبارزه با تروریسم، دچار تغییرات اساسی شد، چرا که دولت‌ها دریافتند حتی در مسافرت هوایی، تروریست‌ها با استفاده از فضای مجازی به راحتی امکان اطلاع از تعداد نفرات و مشخصات مسافرین پرواز، کنترل و هدایت هواپیما و ... را خواهند داشت (۲). لذا ابهاماتی را در سطح جوامع مطرح ساخت که آیا واقعاً امکان وقوع حوادث تروریستی از طریق فضای مجازی (سایبرتروریسم) وجود دارد؟ عکس‌العمل دولت‌ها در مقابل اقدامات احتمالی سایبر تروریسم که منجر به نقض تعهدات حقوق بشری می‌شود، با

چه ماهیت حقوقی توجیه‌پذیر است؟ پاسخ منطقی به سؤالات یاد شده، مستلزم شناختی جامع از سایبر تروریسم و حقوق و تکالیف دولت‌ها برای مبارزه با این پدیده در پرتو قواعد حقوق بشری است. این مقاله به شیوه توصیفی ـ تحلیلی با استفاده از منابع کتابخانه‌ای نگارش یافته است و در نوسان رویکرد و استدلال، در پی پاسخ به این پرسشی بوده است که، شرایط و بایسته‌های تلقی تروریسم سایبری به مثابه توسل به زور و تجاوز چه مواردی است و از رهگذر تفاوت رویکردهای تابعان حقوق بین‌الملل، چگونه توجیه‌پذیر است.

۱. مبانی حقوقِ مخاصمات مسلحانه در فضای سایبر در جهان آنلاین

همان‌گونه که در جنگ‌های نظامی، سلاح‌های سخت‌افزاری، موجودیت دولت هدف را مورد حمله قرار می‌دهند؛ در حملات سایبر نیز فناوری نوین رایانه‌ای، ماشین دولت، نهادهای مالی و زیرساخت‌های حیاتی در بخش‌های انرژی، حمل و نقل و سرانجام روحیه و عزم ملی را هدف حملات خود قرار می‌دهند.

تروریسم به هر شکل و شیوه‌ای که باشد، چه در زمان جنگ و چه در زمان صلح منع شده است و حتی ضرورت نظامی نمی‌تواند اقدامات تروریستی را توجیه کند. شناسایی تروریسم به‌عنوان یک جنایت بین‌المللی یکی از پیامدهای ممنوعیت آن است. (۳) تروریسم در زمان جنگ اگرچه ممنوع است اما اتفاق می‌افتد، بنابراین تابع حقوق مخاصمات مسلحانه و نیز حقوق بشردوستانه بین‌المللی است. بنابراین در شناسایی ضرورت مبارزه بین‌المللی با آن دو هر دو بعد قضیه قابل توجه است. تروریسم سایبری در شیوه انجام گاهی با مخاصمه مسلحانه پیوند می‌یابد یعنی در خلال یک مخاصمه کلاسیک اتفاق می‌افتد و از سوی دیگر در مبارزه با عوامل آن باید حقوق بشردوستانه و قواعد آن اعمال گردد.

حقوق مخاصمات مسلحانه[1]، حقوق حاکم در زمان جنگ است که برخی حقوقدانان آن‌را مرادف حقوق بشردوستانه دانسته‌اند و حاصل تجمیع حقوق لاهه[2]، در باب قواعد و آداب جنگ زمینی، حقوق و تکالیف متخاصمان، استفاده از ابزار و روش‌های جنگی و حمایت از افراد و اموالی است که در درگیری‌ها مورد آسیب قرار خواهند گرفت، کنوانسیون‌های ژنو ۱۹۴۹ و پروتکل‌های الحاقی ۱۹۷۷ در مورد بهبود شرایط مجروحان و

1. Jus in bello

۲. کنوانسیون‌های ۱۸۹۹ و ۱۹۰۷ لاهه

بیماران نیروهای مسلح در میدان نبرد، بهبود شرایط مجروحان، بیماران و کشتی شکستگان نیروهای مسلح در دریا، رفتار با اسرای جنگ، حمایت از غیر نظامیان در زمان جنگ و حمایت از قربانیان مخاصمات مسلحانه بین‌المللی و غیر بین‌المللی، حقوق عرفی و رویه قضایی است(۳).

اما در حوزه سایبر دستورالعمل غیر الزام‌آوری با نام تالین[1] وجود دارد که توسط گروه متخصصان مستقل بین‌المللی درباره حقوق بین‌المللی قابل اعمال در زمان درگیری‌های سایبری به ابتکار ناتو تدوین گردیده است. این دستورالعمل حاوی هنجارهای قابل اعمال حقوق مخاصمات مسلحانه کلاسیک در فضای سایبر است. تالین اگرچه یک سند رسمی نیست و حتی نظریات رؤسای ناتو را نیز بیان نمی‌کند اما از آنجایی که نظر متخصصان مشهور این فن بوده و از منابع حقوق بین‌الملل و دستورالعمل‌های نظامی دولت‌ها استفاده نموده است، به‌عنوان یک دستورالعمل نظامی در سیاست اجرایی و نظامی اعضای ناتو به کار می‌رود. از سوی دیگر به‌عنوان دکترین و نظریه علمای حقوق سایبر به‌عنوان منبع فرعی و ثانویه در حوزه سایبر کارایی دارد.

حقوق مخاصمات مسلحانه هنگامی منصه‌ای برای ظهور می‌یابند که مخاصمهٔ مسلحانه‌ای در حال وقوع باشد. تروریسم سایبری به هر حال نوعی از حمله سایبری است که در صورتی که به سطح مخاصمه برسد، عنوان جنگ سایبری را خواهد یافت. کمیته بین‌المللی صلیب سرخ دو دسته مخاصمه مسلحانه را مورد شناسایی قرار داده است، یکی بین دولتی که مخاصمه بین‌المللی خوانده شده و دیگری میان نیروهای غیردولتی و دولتی و یا میان گروه‌های مسلحانه غیردولتی با یکدیگر. پرسش اصلی این است که آیا با توجه به ماهیت اقدامات تروریستی و نیز ویژگی‌های فضای سایبر، حقوق مخاصمات مسلحانه در حملات سایبری کاربرد دارد؟ در قضیه مشورتی در مورد مشروعیت تهدید یا کاربرد سلاح هسته‌ای، دیوان با تکیه بر شرط مارتنس[2] مندرج در مقدمه کنوانسیون ۱۹۰۷ لاهه بیان داشته است که حتی اگر موضوع شامل مباحث مندرج در این کنوانسیون نباشد، به هر حال نظامیان و غیر نظامیان تحت حمایت اصول حقوق بین‌الملل عرفی، حقوق بشردوستانه و وجدان عمومی خواهند بود. بنابراین حتی اگر مخاصمه شامل شرایط مندرج در کنوانسیون نباشد، اصول حقوق بشردوستانه در فضای سایبر بدان تسری خواهد یافت (۴).

1. Tallinn manual
2. Martens clause

حملات فیزیکی و سایبر از برخی جهات به‌طور کامل شبیه به هم هستند؛ برای نمونه هدف اصلی در جنگ هر نوع وارد آوردن ضرر و زیان به دشمن است و روش اصلی در جنگ قاعدتاً تصاحب منابع دشمن خواهد بود. نقاط افتراق جنگ سایبر نسبت به سایر مخاصمات را می‌توان به صورت زیر دسته‌بندی نمود:

۱. حمله از راه دور: نخستین تفاوت جنگ سایبر با دیگر جنگ‌ها به‌ویژه جنگ فیزیکی و حقیقی، قابلیت طراحی، اجرا و نتیجه‌گیری از راه دور است.

۲. دشواری در شناسایی و ردیابی: به سبب خصایصی که در پروتکل‌های ارتباطی در فضای سایبر وجود دارد، در عمل شناسایی و ردیابی منبع اصلی حمله و مهاجم اصلی، بسیار دشوار و گاه ناممکن است.

۳. تهدید سه جنبه امنیت: در جنگ سایبر، هر سه جنبه امنیت (امنیت، ایمنی و پایداری)، می‌تواند مورد تهدید قرار گیرد.

۴. اندازه هدف: در جنگ‌های فیزیکی اغلب به دنبال تخریب مناطق جغرافیایی بزرگ‌تر هستند، ولی در جنگ سایبر باید اهداف مهم و اساسی «از نظر سایبری و نقش آن‌ها» را هدف قرار داد. این اهداف ممکن است از نظر فیزیکی بسیار ناچیز باشند ولی نقش بزرگی ایفا می‌کنند.

۵. انتشار حمله: حمله سایبری می‌تواند به سادگی از چندین منبع صورت پذیرد. در حالی که هدایت و راهبری حمله‌های فیزیکی که از چندین محل آغاز می‌شوند، بسیار دشوار است.

۶. هزینه: بی‌تردید هزینه جنگ فیزیکی از جنگ سایبر بیشتر است و این خصوصیتِ بارز فضای سایبر است که عوامل و عناصر آن در دسترس‌تر و ارزان‌تر هستند.

۷. مسئولیت‌پذیری: از آنجا که قوانین مدوّن و مشخص بین‌المللی برای مبارزه و ایجاد دعاوی سایبری وجود ندارد، کشورها به سادگی از زیر بار مسئولیت حملات سایبری خود شانه خالی می‌کنند. (۵)

در موضوع حمله سایبری و مخاصمه مسلحانه سه وضعیت قابل تفکیک است اول: حملات شبکه‌ای صرف همچون حمله استاکس نت در سال ۲۰۰۹ به تأسیسات هسته‌ای ایران، اگرچه تنها شایعاتی مبنی بر از کارافتادن ۱۰۰۰ سانتریفیوژ IR-1 وجود دارد، اما هیچ گزارشی از خسارت احتمالی آن موجود نیست. گزارش‌های فنی پس از بررسی این بدافزار اعلام کردند که فرمان بدافزار باعث تخریب تأسیسات هسته نمی‌شده بلکه قصد کنترل و

ایجاد اخلال در عملکرد تاسیسات را داشته است. بنابراین معیاری که پیکته و دیوان بین‌المللی کیفری در قضیه تادیچ برای شروع مخاصمه مسلحانه ارائه نموده‌اند[۱]، در این حملات از آنجایی که هدف تخریب یا صدمه فیزیکی به اموال دولتی بوده است مقدمه‌ای برای شروع مخاصمه مسلحانه تلقی می‌شوند. آن چه در حمله به گرجستان در ۲۰۰۸ رخ داد، به‌عنوان اولین مخاصمه مسلحانه سایبری شناسایی شده است (۵).

وضعیت دوم مربوط به زمانی است که حمله تروریستی در جریان یک مخاصمه فیزیکی رخ دهد، مسئله مهم قابلیت انتساب حمله است. چنانچه وقوع حمله مسلحانه محرز باشد، آن حملاتی که به‌طور مستقیم با عملیات نظامی ارتباط پیدا می‌کنند، مشمول قواعد حقوق مخاصمات خواهند بود.

و وضعیت سوم مربوط به زمانی است که استفاده از سلاح متعارف در حملات شبکهٔ رایانه‌ای به حدی نیست تا یک درگیری مسلحانه قلمداد شود اما وسعت و شدت حملات سایبری این وضعیت را فراهم می‌کند. یعنی به مثابه پشتیبانی از حملات متعارف تلقی می‌گردد. به‌عنوان مثال حمله متعارف کوچک علیه یک کلان شهر اگر همراه با قطع برق آن باشد، اثرات ناشی از حمله را چندین برابر می‌کند.

بنابراین اگرچه بحث ما فارغ از جنگ سایبری است اما از آنجا که این امکان وجود دارد که هم زمان با یک مخاصمه فیزیکی، تروریسم سایبری نیز به‌عنوان یک تاکتیک جنگی در شرف انجام باشد قابلیت انطباق مفاهیم کلاسیک حقوق مخاصمات در این باره خالی از فایده به نظر نمی‌رسد. از طرف دیگر اصطلاح مخاصمه مسلحانه در هیچ کنوانسیون یا پروتکلی تعریف نشده است و می‌تواند به وضعیت‌های متفاوتی میان طرفین درگیر به شرط سلاح تلقی شدن ابزار جنگ تسری یابد (۶).

۱-۱. اصل عدم مداخله در فضای سایبری

هر حمله سایبری که به سطح حمله مسلحانه برسد چه در حوزه حقوق مخاصمات مسلحانه و چه در بحث تروریسم سایبری، از سه منظر قابل بررسی است: از منظر اصل عدم توسل به

۱. ژان پیکته هرگونه اختلاف میان دو دولت که منجر به مداخله نیروهای نظامی شود را یک مخاصمه مسلحانه دانسته صرف نظر از اینکه چه مدت به طول انجامد یا چه میزان تلفات برجا گذارد. البته شعبه استیناف دادگاه بین‌المللی برای یوگسلاوی سابق در قضیه تادیچ مخاصمه مسلحانه را توسل به قوای مسلح بین دو دولت یا خشونت طولانی مدت میان مقامات حکومتی و گروه‌های سازمان‌یافته نظامی یا بین دولت و این گروه‌ها می‌داند.

زور (بند ۴ ماده ۲ منشور سازمان ملل متحد)، توسل به قطعنامه تعریف تجاوز و اصل منع مداخله (قطعنامه ۳۶/ ۱۰۳ سال ۱۹۸۱ مجمع عمومی سازمان ملل متحد). اگرچه در حقوق بین‌الملل کلاسیک بیشتر بحث بیشتر بر سر حق مداخله بوده است آن هم این به علت که تنها راه دفاع در برابر تجاوز به حقوق یک دولت به‌شمار می‌آمده و نیز از آن به‌عنوان ابزاری برای پیشبرد منافع ملی استفاده می‌شده، اما امروزه هم مداخله مستقیم و هم غیر مستقیم مانند فشارهای سیاسی یا اقتصادی طبق اسناد متعددی ممنوع است (۶).[۱]

حمله سایبری می‌تواند اصل عدم مداخله را نقض نماید. حملاتی که در قالب تروریسم سایبری صورت می‌گیرد، مصداقی از نقض اعلامیه عدم مداخله مجمع عمومی مورخ[۲] ۱۹۸۱ است. در بند سه از پاراگراف اول بیان شده که «حق مردم و دولت در آزادی دسترسی به اطلاعات، حق توسعه سیستم‌های اطلاعاتی و رسانه‌های جمعی و استفاده از رسانه‌های اطلاعاتی بدون مداخله و با این هدف که مانع اقتصادی، سیاسی و فرهنگی خود را توسعه دهند». مطابق با ماده ۳۲ قطعنامه منشور حقوق و تکالیف اقتصادی دولت‌ها نیز هیچ کشوری حق استفاده ابزاری از امکانات سیاسی، اقتصادی و ... را به منظور دستیابی به اعمال حق حاکمیت خود ندارد.(۷)

لذا می‌توان گفت حتی اگر تروریسم سایبری را مصداقی از توسل به زور یا حمله مسلحانه ندانیم، بدون شک نقض اصل منع مداخله خواهد بود. شاید بهترین مصداق حملات تروریسم سایبری در قالب جاسوسی سایبری قابل بررسی باشد. در این نوع از حمله، اطلاعات امنیتی بدون اجازه از دارنده اطلاعات اخذ می‌شود. این داده‌ها می‌تواند، اطلاعات شخصی یا اطلاعات طبقه‌بندی شده متعلق به افراد، رایانه‌ها، رقبا، گروه‌ها و دولت‌ها باشد. این سری اقدامات برای منافع اقتصادی، سیاسی یا نظامی توسط دشمن و با استفاده از روش‌های غیرقانونی اینترنتی همچون هک کردن و ترفندهای نرم افزاری شامل اسب تروجان و اسپای ویر[۳] صورت می‌پذیرد.

---

۱. اعلامیه ۱۹۸۱ سازمان ملل متحد مربوط به عدم پذیرش دخالت و مداخله در امور داخلی دولت‌ها (قطعنامه شماره ۳۶/۱۰۳)، کنفرانس ۱۹۳۶ بوئنوس آیرس، قطعنامه ۲۱۳۱ مجمع عمومی ۱۹۶۵، ماده ۳۲ قطعنامه منشور حقوق و تکالیف اقتصادی دولت‌ها ۱۹۷۴.

2. Declaration of inadminissiblity of intervention in the domesic affaires of satets and the protection of their independence and soverienty

3. spyware

هرچند جاسوسی در حقوق بین‌الملل منع نشده است اما اقدام به جاسوسی ممکن است مشمول اصل منع مداخله در امور داخلی دولت‌ها شود. این ممنوعیت چند استثنا دارد. به‌عنوان مثال در زمانی که این عمل در چارچوب عمل متقابل صورت گیرد و یا در راستای احقاق قواعد آمره همچون حق تعیین سرنوشت مردم یک کشور صورت گیرد قانونی خواهد بود. جاسوسی همچنین در زمان جنگ و صلح متفاوت است. در حالی که جاسوسی در زمان جنگ جاسوس را تبدیل به یک مبارز می‌کند که در صورت دستگیری از امتیازات اسیر برخوردار می‌شود (مانند منع اعدام)، جاسوسی در زمان صلح اقدامی علیه امنیت ملی تلقی می‌شود که ممکن است به حکم اعدام نیز منجر شود. توماس وینگ فیلد معتقد است که کنوانسیون روابط دیپلماتیک وین جاسوسی در روابط میان دولت‌ها در زمان صلح را به رسمیت شناخته است. اعمال قواعد مربوط به جاسوسی در فضای سایبر مورد بحث زیادی قرار گرفته است. جاسوسی از سوی بازیگران غیردولتی همچون سایت‌های اینترنتی در صورتی که با اطلاع دولت میزبان صورت گیرد می‌تواند موجبات طرح مسئولیت بین‌المللی دولت حامی را مطرح نماید. دو مورد شناخته شده از جاسوسی دولتی در فضای سایبر عبارتند از مارپیچ شب مهتابی و باران تیتان. برخی نیز معتقدند جاسوسی اینترنتی متفاوت از جنگ اطلاعاتی است و در حوزه مخاصمه قرار نمی‌گیرد.(۸)

طبق دستورالعمل تالین اگر چنین عملیات‌های سایبری برای از میان بردن دولت انجام شوند (و مجوز خود را نیز براساس قوانین بین المللی کسب نکرده باشند)، این عملیات ممکن است به‌عنوان نوعی «مداخله» ممنوعه[1] یا «استفاده ممنوعه از قدرت» تلقی گردد (قواعد ۱۰ تا ۱۲). یک فعالیت سایبری که به‌عنوان یک «حمله مسلحانه» شناخته می‌شود و موجب امکان استناد به حق دفاع مشروع فردی یا جمعی شود. (قاعده ۱۳). اقداماتی که بیانگر حمله مسلحانه نبوده اما به هر حال تخطی از قوانین بین‌المللی محسوب می‌گردند نیز ممکن است منجر به اقدامات متقابل از سوی دولت گردند (قاعده ۹). اقدامات تأیید شده و مجاز از سوی شورای امنیت بر اساس فصل هفت منشور سازمان ملل متحد (قاعده ۱۸) شامل عملیات سایبری، تخطی از حاکمیت نیست.[2]

۱. منشور سازمان ملل متحد، بند ۱ ماده ۲.

۲. بندهای ۱، ۴، ۶ و ۷ قاعده ۱، دستورالعمل تالین

۲-۱. مفهوم تجاوز و ممنوعیت توسل به زور در فضای سایبر و نقض حقوق بشر

آنچه در بند ۴ ماده ۲ منشور به‌عنوان خودداری از توسل به زور علیه تمامیت ارضی و استقلال سیاسی آمده است، توسط دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه علیه آمریکا نیز به‌عنوان اصول بنیادین حقوق بین‌الملل شناسایی شده و توسط کمیسیون حقوق بین‌الملل نیز واجد وصف قاعده آمره می‌باشد در روابط دولت‌های عضو سازمان ملل ممنوعیت دارد. بنابراین اگر توسط کنشگران غیردولتی اتفاق افتد، خارج از مندرجات منشور خواهد بود. معنای دقیق زور هیچ‌گاه توسط دیوان یا مجمع عمومی سازمان ملل تعریف نشده است. اما دیدگاه اغلب حقوقدانان این است که این بند از ماده ۲ ناظر به کاربرد زور در بعد نظامی آن است. در ماده ۴۴ نیز منظور از زور را در اقدامات شورای امنیت از سایر اقدامات مربوط به قطع روابط اقتصادی، پستی، مخابراتی، رادیویی و دیپلماتیک مندرج در ماده ۴۱، جدا کرده است. با توجه به این دو ماده و نیز پاراگراف ۷ مقدمه منشور، اگر قرار بود این مواد معنایی فراتر از زور نظامی را مد نظر داشته باشند، قطعاً در مقدمه برای حفظ یکپارچگی داخلی، اصطلاح مسلحانه ذکر نمی‌شد.[۱] اما باید دید با توجه به مفهوم نوین سلاح آیا می‌توان استفاده از بدافزارهای سایبری را مصداق سلاح دانست و در صورت رسیدن اقدامات سایبری به سطح حمله مسلحانه آن را مصداق توسل به زور دانست؟ ژان پیکته هرگونه اختلاف میان دو دولت که منجر به مداخله نیروهای نظامی شود را یک مخاصمه مسلحانه دانسته صرف نظر از این که چه مدت به طول انجامد یا چه میزان تلفات برجا گذارد. البته شعبه استیناف دادگاه بین‌المللی برای یوگسلاوی سابق در قضیه تادیچ مخاصمه مسلحانه را توسل به قوای مسلح بین دو دولت یا خشونت طولانی مدت میان مقامات حکومتی و گروه‌های سازمان‌یافته نظامی یا بین دولت و این گروه‌ها می‌داند. (۹). می‌توان گفت که میان درجه خشونتی که برای وقوع مخاصمه مسلحانه بین‌المللی و داخلی لازم است تمایز وجود

---

۱. منظور تدوین‌کنندگان منشور از واژه زور در سال ۱۹۴۵، با توجه به عدم تعریف تجاوز، زور نظامی و مسلحانه است آن هم با استفاده از سلاح‌های سنتی که به شیوه‌های مرسوم مورد استفاده قرار می‌گرفته است. در کارهای مقدماتی ماده ۲، نظر نماینده آمریکا بر این بوده است که در آینده انواع مختلفی از تجاوز وجود خواهد داشت که با توجه به عبارت تهدید صلح تحت لوای منشور قرار می‌گیرد. این امر نماد این است که در آن روزگار تصوری که از زور وجود داشته یک تهدید مسلحانه خاص بوده و سایر موارد تحت عنوان کلی تهدید علیه صلح در مواد ۳۹ و مواد مربوطه در فصل ۷ مورد بحث قرار گرفته‌اند. رک: فصل دوم کتاب جنگ سایبری

دارد. اما هر دو نوع مخاصمه نیازمند به‌کارگیری نیروی نظامی، زور و حمله مسلحانه است که البته در حقوق بین‌الملل بر سر تعاریف آن‌ها اجماع وجود ندارد.

۳. تجاوز در فضای سایبر از منظر حقوق بشر و حقوق بین‌الملل بشردوستانه

یکی از نکاتی که امروزه در باب حملات سایبری مورد توجه است، مسئله توسعه مفهوم توسل به زور و احراز تجاوز است. ادبیات حقوقی معاصر در حال تغییر مسیر از نبردهای نظامی و سنتی به حوزه فضای نرم افزاری است. اما تلقی منشور از ملل متحد طبق بند ۴ ماده ۲ منشور، توسل به زور ناظر بر اقدامات نظامی است (۹) و جنگ نیز اساساً در قالب همین ممنوعیت قرار می‌گیرد، لذا اقدامات مربوط به دفاع مشروع و اقدامات قهری شورای امنیت در همین چارچوب استثناء تلقی می‌شود. بنابراین تفسر موسع از توسل به زور می‌تواند خلاف جهتی که به تدوین منشور انجامیده تلقی شود. اما از سوی دیگر، برخی حقوقدانان حمله سایبری را مصداق توسل به زور دانسته‌اند. با توجه به شناسایی بین‌المللی تهدیدات سایبری، که می‌تواند آسیب‌های فیزیکی تهدید کننده امنیت ملی وارد نماید، دولت‌ها برای واکنش به این تهدیداتی که نقاط ضعف آن‌ها را هدف قرار می‌دهند، در ارتش‌های خود واحدهای سایبری ایجاد کرده‌اند. اقداماتی همچون حمله سایبری به استونی در ۲۰۰۷ میلادی، عملیات تروریسم سایبری هم زمان روسیه در زمان درگیری با اوستیای جنوبی در ۲۰۰۸، حملات سایبری چین به آمریکا، هند، بریتانیا و کانادا، از آنجایی که مسئله انتساب اقدامات صورت گرفته به دولت‌های متهم به چنین اقداماتی هرگز ثابت نشد، این اقدامات نیز توسل به زور تلقی نگردید.

اما آمریکا در سال ۲۰۰۲ اعلام کرد که در پاسخ به حملات سایبری از هر وسیله مقتضی ازجمله حمله نظامی استفاده خواهد کرد. این امر در دستورالعمل محرمانه بوش برای تهیه رهنمودهای ملی آمریکا در این زمینه که چه زمانی و چگونه حملات سایبری خود را علیه شبکه‌های رایانه‌ای دشمن اغاز کند، در بیانه وزیر امور خارجه که بیان نمود، تروریست‌ها و دولت‌هایی که در حملات سایبری علیه امریکا شرکت می‌کنند باید نتایج و تبعات آن را بپذیرند و نیز در بحث استراتژیک معاون وزیر دفاع، در اینکه ممکن است استراتژی دفاعی فعال آمریکا شامل حملات پیش‌دستانه علیه شبکه‌های رایانه‌ای دشمن شود، هویداست.

روسیه نیز با اعلام این مسئله که استفاده از جنگ اطلاعاتی صرف نظر از تلفات را به‌عنوان مراحل غیر نظامی یک مخاصمه در نظر خواهد گرفت و به حق استفاده از

سلاح‌های هسته‌ای در وهله نخست علیه سلاح‌ها و نیروهای این جنگ اطلاعاتی و در مرحله بعد علیه خود دولت متجاوز متوسل می‌شود. (۱۰)

اما در ناتو به ویژه در مورد حمله به استونی، رویکرد محافظه کارانه‌ای اتخاذ شده است. قانون حاکم بر دفاع سایبری در داخل ساختار ناتو ماده ۴ اساسنامه بوده و بدین شکل است که دولت‌های عضو می‌توانند با یکدیگر مشورت‌هایی در مورد حملات سایبری انجام دهند اما موظف نیستند که به یکدیگر در راه دفاع سایبری کمک‌رسانی نمایند. این در حالی است که طبق ماده ۵ اساسنامه این سازمان در مورد تجاوز به یک کشور از اعضای سازمان، وظیفه دفاع جمعی مقرر گردیده است. دفاع سایبری عمدتاً در معنای یک مسئولیت ملی باقی مانده است، اما ناتو تلاش‌هایی را برای ایجاد ساختارهایی برای مشاوره در این باب انجام داده است، اگرچه این رویکردها در باب مشورت، فقط در حد یک بحث صرف باقی مانده است؛ اما این رویکرد همچنان در ناتو دیده می‌شود که بحث حملات سایبری را در مفهوم تجاوز دانسته و باتوجه به ماده ۵ اساسنامهٔ خود دفاع جمعی در مقابل آن را مجاز شمارد. اما آنچه مهم است بحث شناسایی مهاجم در این فضا است چرا که همان‌طورکه گفته شده است چون شناسایی منبع هجوم در این فضا کار دشواری است لذا نسبت دادن آن به یک دولت سخت و در مواردی غیرممکن خواهد بود، چرا که مرز در این فضا رنگ باخته است. در نظریات علمای حقوق نیز در این مورد اختلاف نظرهای عمیقی وجود دارد، افرادی همچون بران لی و دنیستین از دیدگاه پوزیتویسم حقوقی رویکردی مضیق گرا اتخاذ نموده‌اند. یورام دنیستین، رویکردی نیتجه محور را اتخاذ نموده است و بیان می‌کند: «نتایج خشونت‌آمیز کلید حل تعریف حملات مسلحانه هستند. از دیدگاه حقوقی دلیلی ندارد که میان ابزارهای فعال و الکترونیکی حمله، تمایز قائل شویم. حمله رایانه‌ای، تا زمانی که نتایج مشابهی به بار آورند، می‌توانند به‌عنوان حمله مسلحانه تلقی گردند. اگر رابطه علت و معلول میان حملات شبکه رایانه‌ای و نتایج خشونت باری وجود داشته باشد، مهم نیست که اثرات با فناوری به وجود آمده یا نه» (۱۱) این رویکرد به هر حال به قواعد ایجاد شده توسط جامعه بین‌المللی نظر دارد مقرر می‌کند که هر چیزی خارج از این ممنوعین قرار بگیرد قانونی است. ارزیابی کمی و کیفی یک رویکرد نتیجه محور دشوار است و نیز یک معیار هنجاری جدید ایجاد می‌کند که براساس آن شاید بتوان فشار اقتصادی و سیاسی را نیز نوعی حمله در نظر گرفت. اما به هر حال اهمیت جنگ‌های آینده آنقدر زیاد هست که باید در مفهوم سلاح به معنای سنتی آن تجدید نظر نمود. از

سوی دیگر حقوق دانانی مانند مک دوگال و مایکل رایزمن تفسیر موسعی از سلاح ارائه می‌نمایند. مک دوگال زور را میزانی از فشار و خشونت فوق العاده دانسته که در ابعاد فراملی اعمال می‌شود. رایزمن معتقد است توسل به زور تاحدی از مجوز حقوق بین‌الملل برخوردار است. در توجیه قانونی بودن نوعی از فشار خاص باید به این پرسش پاسخ داده شود که آیا این عمل خاص، با هر توجیهی که باشد، موجب ارتقاء نظم جهانی می‌شود یا تضعیف آن. این رویکرد زمینه محور نیز با انتقادات جدی مواجه است. زیرا هیچ‌گونه حقوق عینی که بیانگر ضرورت‌های اجتماعی یا مکانیزم های همبستگی که توصیف‌کننده جامعه بین‌المللی باشد، وجود ندارد.[۱]

این رویکرد که ساختاری موسع دارد دلالت دارد بر اینکه تمام انواع فشار در یک سلسله مراتب قرار دارند و حاصل آن‌ها برهم زدن نظم اجتماعی است. اما موضع انفرادی برخی دولت‌ها مؤید تفسیری موسع‌تر است؛ مانند موضع ایران که در سال ۱۹۵۳ با ارائه نامه‌ای به سازمان ملل اعلام نمود که هرگونه اقدامی که با هدف حمله نظامی یا برای به خطر انداختن استقلال دولت صورت گیرد «تجاوز» تلقی خواهد نمود. مشکل دیگر این است که بند ۴ ماده ۲ منشور صحبت از دولت عضو می‌کند در حالی که در فضای سایبر با بازیگران غیردولتی روبه‌رو هستیم. بنابراین تجاوز نه‌تنها علیه تمامیت ارضی مصداق پیدا می‌کند که شامل نقض استقلال سیاسی نیز می‌شود. بنابراین باید دید حمله سایبری در چه سطحی استقلال سیاسی کشور را تهدید می‌کند. به نظر می‌رسد حمله به زیرساخت‌ها گرجستان و از کار انداختن برخی زیرساخت‌های مهم آن نمونه‌ای از نقض استقلال سیاسی باشد.

در قطعنامه تعریف تجاوز، قطعنامه از تجاوز تعریف مرکبی به دست می‌دهد؛ تعریفی کلی همراه با فهرستی از اقدامات منع شده. مطابق با ماده ۱: «تجاوز عبارت است از کاربرد نیروهای مسلح توسط یک دولت علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولتی دیگر یا کاربرد آن از دیگر راه‌های مغایر منشور ملل متحد، آنچنان‌که در این تعریف آمده است» اگرچه در زمان مذاکرات بسیاری از دولت‌ها معتقد به درج سایر اشکال تجاوز مانند اقتصادی یا ایدئولوژیک نیز بودند اما نهایتاً کاربرد زور توسط نیروهای مسلح مد نظر قرار گرفت. اما در ماده ۴ به شورای امنیت آزادی عمل داده شد تا موارد دیگری را نیز در

۱. برای مطالعه بیشتر رجوع کنید به:

Corten, Olivier, The controversies over the customary prohibition of the use of force: A methodological debate, 2005, 16 EJIL 803.

صورت اقتضا حتی اگر مستلزم استفاده از نیروهای مسلح نباشد، تجاوز قلمداد کند. بنابراین اگر حمله تروریستی سایبری از سوی عوامل دولتی یا منتسب به دولت واقع شوند و به آستانه حمله مسلحانه برسند، می‌توانند استقلال سیاسی یک دولت را خدشه‌دار نموده و مصداق عمل تجاوز به حساب آیند.

نهایتاً می‌توان گفت اگر یک حمله سایبری به‌طور مستقیم یا غیر مستقیم منجر به مرگ، جراحت و تخریب اموال گردد، می‌تواند مصداق به‌کارگیری نیروی نظامی باشد. از سوی دیگر مداخله نیروهای نظامی یک دولت پیش شرط وقوع مخاصمه مسلحانه است. امروزه با به‌کارگیری بسیاری از سلاح‌های فوق مدرن ممکن است نیروهای نظامی تنها عامل درگیر در یک مخاصمه نباشند. نکته دیگر برای احراز تجاوز توسط حملات سایبری این است که به شکل مداوم و مستمر علیه زیرساخت‌های حیاتی یک کشور صورت گرفته که در آن درجه‌ای از سازمان‌یافتگی وجود داشته باشد. در سطح بین‌المللی اقدامات تروریستی منتسب به یک دولت ممکن است منجر به یک مخاصمه مسلحانه میان آن دولت و دولتی که هدف قرار گرفته است بشود، اما هنگامی که هیچ دولتی در شکل‌گیری اقدام تروریستی دخیل نباشد، به موجب ماده ۳ مشترک کنوانسیون‌های ژنو یا پروتکل الحاقی دوم، اگر گروه تروریستی سازمان یافته باشد و اقدامات نیز به شکل مداوم و خشونت‌بار باشد، ممکن است باعث وقوع مخاصمه غیر بین‌المللی گردد. در صورتی که گروه تروریستی چنین معیارهایی را نداشته باشند، اقدامات صورت گرفته در قالب جرم در نظام حقوق داخلی مورد رسیدگی قرار خواهد گرفت. (۱۲)

٤. اصل منع توسل به زور در منظومه حقوق بشر

دیوان بین‌المللی دادگستری در نظریه مشورتی مربوط به سلاح‌های هسته‌ای طبق بند ۲ ماده ۴ منشور ملل متحد اعلام کرده است که عنوان استفاده از زور برای، «هر استفاده‌ای از زور، بدون توجه به سلاح استفاده شده» به کار می‌رود. گروه کارشناسان بین‌المللی تدوین‌کننده دستورالعمل تالین به اتفاق آرا توافق کرده‌اند که این حکم بازتاب دقیقی از حقوق بین‌الملل عرفی است. طبق قاعده ۱۰ از دستورالعمل تالین، عملیات سایبری که تهدید یا استفاده از زور بر ضد تمامیت ارضی یا استقلال سیاسی هر دولت را تشکیل می‌دهد یا به هر روشی دیگر، با اهداف سازمان ملل در تناقض است، غیر قانونی است. بند ۲ ماده ۴ منشور سازمان ملل مقرر می‌کند که «کلیه اعضای سازمان ملل باید در ارتباطات بین‌المللی شان از

تهدید یا استفاده از زور بر ضد تمامیت ارضی یا استقلال سیاسی هر دولتی، یا به هر روش دیگری که با اهداف سازمان ملل متناقض است» خودداری کنند، ممنوعیت بدون شک هنجاری از حقوق بین‌الملل عرفی است. به علاوه کارهای مقدماتی منشور سازمان ملل این مسئله را روشن می‌کند که ارجاع به بند ۲ ماده ۴ برای تهدید یا استفاده از زور که با اهداف سازمان ملل در تناقض است، قصد ایجاد فرض غیرقانونی بودن هر تهدید یا استفاده از زور را داشته است. به بیان دیگر حتی اعمالی که بر ضد هریک از تمامیت ارضی یا استقلال سیاسی یک دولت هدایت نشده‌اند می‌توانند اگر با اهداف سازمان ملل متناقض هستند ممنوع تلقی شوند. عملی برای اینکه واجد شرایط استفاده از زور باشد، لزوماً نیازی نیست که توسط نیروهای مسلح یک دولت انجام گیرد. به‌عنوان مثال، روشن است که یک عملیات سایبری که به‌عنوان استفاده از زور واجد شرایط است ممکن است توسط عاملان اطلاعاتی یک دولت یا پیمانکار خصوصی که قابل انتساب به دولت است، انجام شود. موضوع قابل ملاحظه دیگر بحث مداخله و ممنوعیت آن است. روشن است که تمام دخالت‌های سایبری به‌طور خودکار حقوق بین‌الملل مربوط به ممنوعیت مداخله را نقض نمی‌کنند. بنابراین موضوع «دخالت محض و ساده نیست». همان‌طورکه توسط دیوان در دعوای نیکاراگوئه علیه آمریکا گفته شده است «مداخله زمانی که از روش‌های تهدید و اجبار استفاده کند غیر قانونی است» بنابراین جاسوسی سایبری که فاقد عنصر اجبار است، فی نفسه قاعده کلی عدم مداخله را نقض نمی‌کنند. اما نفوذ به سیستم‌های دولت دیگر اصل عدم مداخله را نقض می‌کند. به شرطی که این نفوذ مستلزم نقض پروتکل‌های امنیت سیستم باشد[1]. بنابراین استفاده از استاکس نت نقض اصل عدم مداخله تلقی می‌گردد (۱۲).

در مورد عملیات سایبری که به آستانه استفاده از زور نمی‌رسند، تشخیص آن‌ها به‌عنوان نقض اصل عدم مداخله سخت‌تر است. بنابراین تهدید و اجبار بیش از حد دخالت سیاسی است. زمانی که چنین اعمالی توسط ابزارهای سایبری انجام یا تسهیل می‌شوند، مداخله تلقی می‌گردند، همچون موضوع دستکاری انتخابات یا افکار عمومی در آستانه انتخابات به وسیله ابزارهای سایبری. بنابراین واضح است که هر شکلی از دخالت اقتصادی یا سیاسی اصل عدم مداخله را نقض می‌کند (۱۳). قاعده شماره ۱۱ دستورالعمل تالین استفاده از زور را در عملیات سایبری منوط به مقیاس و اثرات آن در مقایسه با عملیات غیر سایبری که به

۱. مثل شکستن فایروال‌ها یا رمز عبور

سطح استفاده از زور می‌رسند، دانسته است. گروه کارشناسان بین‌المللی تدوین‌کننده این دستورالعمل معتقدند، منشور سازمان ملل هیچ معیاری ارائه نمی‌دهد که با آن تعیین شود چه زمانی یک عمل به استفاده از زور می‌رسد، بنابراین در بحث‌های مربوط به آستانه مناسب برای استفاده از زور این گروه به رأی نیکاراگوئه علیه امریکا استناد جسته‌اند که در آن دیوان اعلام کرده است که «مقیاس و اثرات» باید در زمان تعیین اینکه آیا اعمال ویژه‌ای به «حمله مسلحانه» می‌رسد یا خیر مورد توجه قرار بگیرند. به بیان دیگر عبارت مقیاس و اثرات، اصطلاحی مختصر است که فاکتورهای کیفی و کمی را برای تحلیل در تعیین اینکه آیا عملیات سایبری به‌عنوان استفاده از زور واجد شرایط است یا خیر در نظر می‌گیرد.

اگرچه هیچ تعریف یا معیار معتبری برای تهدید یا استفاده از زور وجود ندارد اما دسته‌های معین از عملیات سایبری استفاده از زور تلقی نمی‌شوند. در ۱۹۴۵ در کنفرانس سانفرانسیسکو، دولت‌ها با پیشنهاد در نظر گرفتن فشار اقتصادی به عنوان زور مخالفت کردند. این موضوع بیست و پنج سال بعد طی فرآیندهایی که منجر به اعلامیه مجمع عمومی در ارتباط با روابط دوستانه شد، مجدداً پیش آمد. این پرسش که آیا «زور» شامل «هر نوع فشار، ازجمله فشارهای سیاسی و اقتصادی که اثر تهدیدکننده برای تمامیت ارضی و استقلال سیاسی هر کشور دارد» است با جواب منفی پاسخ داده شد. بر این اساس «زور» هر آنچه که باشد، یک اجبار اقتصادی یا سیاسی صرف نیست. عملیات سایبری که با این فعالیت‌ها مرتبط است، استفاده ممنوعه از زور تلقی نمی‌شوند. به‌عنوان مثال، عملیات غیرتخریبی روانی سایبری که منحصراً برای تضعیف اعتماد به نفس دولت و یا اقتصاد به کار برده می‌شود، به معنی استفاده از زور و قدرت نیست. علاوه بر این، مطابق با نظر دیوان در پروندهٔ نیکاراگوئه، صرف تأمین بودجه چریک‌های درگیر در عملیات علیه دولت دیگر به آستانه تعریف استفاده از زور نمی‌رسد. درنتیجه، برای مثال، تأمین مالی یک گروه هکر که منجر به عملیات سایبری به‌عنوان بخشی از یک شورش می‌شود، استفاده از زور نیست. از سوی دیگر استفاده از قدرت صرفاً به دخالت ارتش و سایر قوای نظامی یک کشور نیاز ندارد. در پرونده مزبور، دیوان تشخیص داد که مسلح کردن و آموزش یک گروه چریکی که در خصومت علیه یک دولت دیگر به کار می‌رود به معنای استفاده از زور است. درنتیجه، فراهم کردن نرم‌افزارهای مخرب و دادن آموزش‌های لازم به یک گروه مسلح

برای استفاده از آن در حملات سایبری علیه دولت‌های دیگر نیز به‌عنوان استفاده از زور در نظر گرفته می‌شود (۱۴).

نهایتاً باید گفت: در تشخیص اینکه آیا یک عمل «استفاده از زور» است یا خیر، بهتر است که مفهموم حملهٔ مسلحانه را بدانیم: آستانه‌ای است که در آن یک دولت ممکن است به صورت قانونی از زور برای دفاع از خود استفاده کند. درنتیجه، هرگونه عملیات سایبری که از نظر مقیاس‌ها و اثرات ذکر شده که به سطح «حمله مسلحانه» برسد، و آن‌هایی که توسط یک کشور هدایت می‌شوند یا قابل نسبت دادن به یک کشور هستند، به‌عنوان «استفاده از زور» در نظر گرفته می‌شوند. اعمالی که مردم را مجروح می‌کنند یا می‌کشند به روشنی استفاده از زور هستند. امریکا در استناد به دفاع مشروع در برابر حملات ترویست‌های سایبری، در قالب اقدام نظامی به همین مسئله استناد نموده است (۱۴).

اگر بپذیریم که براساس گفته پروفسور ایان برانلی، اقدامات آتی دولت‌های متعاهد بهترین راهنمای ما در معنای مفهوم زور است، این نتیجه حاصل می‌شود که: «تردید وجود ندارد، آنچه از این رویه فهمیده می‌شود این است که هرگونه استفاده ماهوی از نیروی نظامی مورد نظر بوده است».[۱]

اگرچه مفهوم توسل به زور معطوف به نیروی نظامی است اما تعریف نیروی نظامی تعریفی موسع است. این تفسیر موسع در معنای زور توسط دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه به این صورت بیان شده است که برخی اشکال حمایت غیر مستقیم نیز در زمره ممنوعیت توسل به زور قرار می‌گیرد. حکم دیوان بیان‌گر آن است که، اعمال ناقض اصل عدم مداخله به‌طور مستقیم و غیر مستقیم ممکن است مصداق نقض اصل منع توسل به زور باشد (۱۵). دیوان تأکید می‌کند که دولت‌ها باید از اقدامات تلافی جویانهٔ متضمن توسل به زور خودداری کنند. در این مورد دیوان برخی اعمال تجاوزکارانه غیر مستقیم را به‌عنوان توسل به زور البته از نوع خفیف آن در حقوق بین‌الملل در نظر گرفته است.[۲]

---

۱. در اسناد سازمان‌های بین‌المللی مانند ناتو و منشور سازمان کشورهای آمریکایی نیز اگرچه تعریفی از زور به عمل نیامده است اما از فشار سیاسی یا اقتصادی نیز به‌عنوان نوعی زور سخن به میان نیامده است.

۲. اگرچه برخی مفسران معتقدند دیوان در این قضیه تعریف زور را به فشار سیاسی و اقتصادی هم تعمیم داده است اما به نظر نمی‌رسد، که منظور دیوان از زور فراتر از نیروی نظامی و شبه نظامی باشد. اما این زور می‌تواند ازطریق ابزارهای غیر مستقیمی مانند نمایندگی به دولت استناد یابد. (هریسون دنیس،۱۳۹۴:۶۵)

این استدلال در مورد حملات سایبری کاربرد دارد. زیرا با توجه به ماهیت غیرمستقیم نتایج حاصل از آن‌ها این استدلال مطرح شده که نمی‌توان این حملات را در زمره انواع توسل به زور قلمداد نمود. به‌علاوه از آنجایی که دیوان در پرونده نیکاراگوئه بیان نموده است که بند ۴ ماده ۲، تنها بخشی از حقوق بین‌الملل عرفی در مورد اعمال زور است و منشور دربردارنده تمام مقررات مربوط به کاربرد زور در روابط بین‌المللی نیست. بنابراین باید به رویه دولت‌ها و دکترین نیز مراجعه کنیم. (۱۶) طبقه‌بندی مایکل اشمیت درباره اینکه چه نوعی از حملات سایبری توسل به زور است اهمیت دارد، ایشان شش معیار را برای تفکیک ارائه می‌دهند که عبارتند از: شدت عمل حمله سایبری[۱]، بی‌واسطه بون حمله سایبری[۲]، مستقیم بودن حمله، خاصیت تهاجمی داشتن حمله[۳]، قابلیت اندازه‌گیری داشتن

---

۱. شدت: وقایعی که به افراد یا اموال آسیب فیزیکی وارد می‌کنند به‌عنوان استفاده از زور طبقه‌بندی می‌شوند. آن‌هایی که رنجش یا ناراحتی کمی ایجاد می‌کنند، این‌گونه نخواهند بود بسیار محتمل است که یک عملیات سایبری، مانند هر عملیات دیگری که منجر به آسیب، نابودی، جراحت و مرگ می‌شود، به‌عنوان استفاده از زور در نظر گرفته شود. بدیهی است که شدت مهم‌ترین عامل در تحلیل ما است.

۲. در حالی که فاکتور فوریت بر جنبه‌های زمانی عواقب تمرکز دارد، بی‌واسطه بودن زنجیرهٔ بین علت و معلول را بررسی می‌کند. ارتباط سببی بین اعمال اولیه و اثرات آن تمایل دارند تا غیرمستقیم باشند؛ ممکن است هفته‌ها یا حتی ماه‌ها طول بکشد تا تحریم‌های اقتصادی اثر معناداری داشته باشند. در مقابل، در اعمال مسلحانه، علت و اثر ارتباط نزدیک‌تری دارند. برای مثال، یک انفجار، مستقیماً به انسان‌ها و اشیا آسیب می‌رساند. احتمال اینکه، عملیات سایبری که در آن علت و اثر به وضوح به یکدیگر مرتبط هستند، به‌عنوان استفاده از زور در نظر گرفته شوند بیشتر است.

۳. تهاجم به درجه‌ای از عملیات سایبری که کشور هدف یا سیستم‌های سایبری آن را تحت تأثیر قرار می‌دهد، مرتبط است. به‌عنوان یک قانون، هرچه یک سیستم سایبری هدف ایمن‌تر باشد، نفوذ به آن سخت‌تر می‌شود. برای مثال، نفوذ به یک سیستم ارتش که از نظر معیارهای رایج در سطح اطمینان ارزیابی (EAL7) قرار دارد، نسبت به آسیب‌پذیری یک سیستم منبع باز غیرمعتبر موجود در یک دانشگاه غیرنظامی یا کسب و کار کوچک، تهاجمی‌تر است. نام دامنه یک نشان‌دهندهٔ آشکار در فضای سایبر است و به همین علت ممکن است در ارزیابی میزان تهاجمی بودن یک عملیات مورد استفاده قرار گیرد. عملیات سایبری که به‌طور ویژه نام دامنه‌های یک کشور خاص را هدف می‌گیرند، نسبت به عملیاتی که نام دامنه‌هایی غیر از دامنه‌های خاص یک کشور مثل com را هدف می‌گیرند، تهاجمی‌تر در نظر گرفته می‌شوند. این فاکتور در زمینهٔ سایبری باید با احتیاط اعمال شود. به‌طور ویژه، استفاده از شبکه‌های کامپیوتری، یک ابزار فراگیر در جاسوسی مدرن است. اگرچه این روش بسیار تهاجمی است، اما جاسوسی سایبری به علت فقدان یک منع مستقیم در قانون بین‌الملل برای جاسوسی، به سطح تعریف «استفاده از قدرت» نمی‌رسد. بنابراین، اعمالی مثل مکانیسم‌های از کار انداختن امنیت سایبر برای وارد کردن ضربات کلیدی، علی‌رغم تهاجمی بودن به‌عنوان استفاده از زور در نظر گرفته نمی‌شوند. این بدان معنا نیست که اعمالی که برای فراهم آوردن زمینهٔ جاسوسی انجام می‌شوند، نیز استفاده از زور نیستند. برای مثال، یک نفوذ بدون اجازه به حریم هوایی ملی توسط یک هواپیمای نظامی به‌عنوان ابزاری برای جاسوسی سایبر می‌تواند به‌عنوان استفاده از قدرت تلقی شود.

حمله[۱] و مشروعیت یا غیر مشروع بودن احتمالی حمله[۲]. این طرح و معیارهای اشمیت، با تکنیک خاصی، این اجازه را می‌دهد تا با سنجیدن یکایک این معیارها به این نتیجه برسیم که فعل ارتکاب یافته توسل به زور است یا نه و بالطبع مقررات منشور سازمان ملل درباره آن قابل اعمال است یا خیر؟ درواقع رویکرد اشمیت بدین‌گونه است که تخریب حمله سایبری را با حمله مسلحانه قیاس نموده و حکم می‌دهیم و این مسأله نتیجه معیاری است که اشمیت با رویکرد نتیجه گرایانهٔ خود توسل به زور را در فضای سایبر تحلیل می‌نماید (۱۶).

در تدوین دستورالعمل تالین عامل فوریت[۳] و تهاجم توسط نیروهای مسلح و بحث مسئولیت صریح یا ضمنی دولت نیز مطرح شده است. البته این عوامل جامع نیستند و براساس شرایط موجود، کشورها فاکتورهای دیگر، مانند محیط غالب سیاسی، پیش‌بینی عملیات استفاده از زور در آینده، تشخیص حمله‌کننده، هرگونه ثبت عملیات سایبری از فرد حمله‌کننده، و ماهیت هدف (مثل زیرساخت‌های اساسی) را در نظر می‌گیرند. علاوه بر این، فاکتورها هماهنگ با یکدیگر عمل می‌کنند. به‌عنوان یک مثال، احتمال اینکه یک عملیات شدید که تنها باعث آسیب‌هایی مانند انکار موقت خدمات می‌شود، به‌عنوان توسل به زور در نظر گرفته شود، پایین است. در مقابل، برخی ممکن است با وجود قانونی بودن

۱. این فاکتور از تمایلات بیشتر کشورها برای نسبت دادن اعمال به‌عنوان استفاده از زور، در هنگام آشکار بودن عواقب، دلالت دارد. به‌طور سنتی، نیروهای مسلح عملیاتی که به‌عنوان توسل به زور در نظر گرفته می‌شود را انجام می‌دهند و اثرات این نوع عملیات به‌طورکلی قابل اندازه‌گیری است (مانند مورد ارزیابی خسارت جنگ). در حوزهٔ سایبر، ممکن است که عواقب کمتر آشکار باشند. درنتیجه، هرچه عواقب قابل سنجش‌تر و قابل تشخیص‌تر باشند، سنجش وضعیت برای یک کشور در هنگام تشخیص اینکه یک عملیات به سطح استفاده از زور رسیده است، راحت‌تر می‌شود. بر این اساس، احتمال اینکه یک عملیات سایبری که از جنبه‌های مختلف قابل ارزیابی است، به‌عنوان استفاده از زور در نظر گرفته شود نسبت به عملیاتی که فاکتورها در آن قابل اندازه‌گیری نیستند، بیشتر است.

۲. حقوق بین‌الملل به صورت کلی منع‌کننده است. اعمالی که منع نشده‌اند، مجاز هستند؛ فقدان معاهدهٔ صریح یا منع پذیرفته شده در مورد یک عمل، باعث قانونی بودن احتمالی آن می‌شود. برای مثال حقوق بین الملل، تبلیغات، عملیات روانی، جاسوسی یا وارد کردن فشار اقتصادی را منع نمی‌کند. درنتیجه، این اعمال و سایر اعمال مشابه قانونی هستند و با توجه به موارد گفته شده، احتمال اینکه این اعمال توسط کشورها به‌عنوان استفاده از قدرت در نظر گرفته شوند کمتر است.

۳. فوریت: هرچه عواقب زودتر اتفاق بیفتند، کشورها فرصت کمتری دارند تا به دنبال حل مسالمت‌آمیز اختلافات باشند یا اثرات زیان‌بار آن را پیش بینی کنند. درنتیجه، کشورها به عواقب سریع توجه بیشتری نسبت به عواقب تاخیری یا کند نشان می‌دهند و احتمال اینکه یک عملیات سایبری که نتایج سریعی در پی دارد به‌عنوان استفاده از زور در نظر گرفته شود، نسبت به عملیاتی که هفته‌ها یا ماه‌ها طول می‌کشد تا به اثرات در نظر گرفته شده برسد، بیشتر است.

جاسوسی اقتصادی، یک عملیات سایبری شدید که اقتصاد را فلج کرده، به‌عنوان استفاده از زور در نظر بگیرند (۱۶).

بسیاری از معیارهایی که بیان گردید در حملات سایبری مورد تردید واقع می‌شود. به ویژه در مسئله تروریسم سایبری که فوریت نتایج قابل اندازه‌گیری نیست و ممکن است یک ویروس از زمان شروع به کار مدت زمان طولانی را صرف آسیب‌هایی نماید که حتی هیچ‌گاه کشف نگردد. همین ویژگی حملات سایبری در زمینه قابلیت اندازه‌گیری خسارت نیز وجود دارد. اگرچه تروریسم علیه جمعیت غیر نظامی اتفاق می‌افتد، اما در تروریسم سایبری، زیر ساخت‌های حیاتی یک کشور که ممکن است دولتی باشند نیز مورد حمله تروریست‌ها قرار می‌گیرند و آن هم امکان دارد با استفاده از رایانه‌هایی از داخل یک دولت صورت پذیرد. در فضای سایبر ممکن است تعیین اینکه حمله در کجا شکل گرفته و یا اینکه به شکل مخاصمه، حمله تروریستی و یا جرم داخلی بوده است، غیر ممکن باشد.[۱] این مسئله به ویژه در مورد صلاحیت محاکم در دعاوی مربوط به جرایم فرامرزی سایبری اهمیت دارد.

۵. مفهوم نوینی از سلاح و حمله مسلحانه و عصر جهانی شدن

تروریست‌ها، اقدامات خود را از طریق، بحران سازهای فضای سایبر که شامل، ویروس‌ها یا برنامه‌های خود همانندساز، برنامه‌هایی هستند، با هدف آلوده کردن سیستم‌های دیگر نوشته می‌شوند و معمولاً از طریق یک دیسکت و گاهی از طریق اینترنت یا شبکه‌های پست الکترونیک سرایت می‌کنند، صورت می‌دهند. بعضی ویروس‌ها ممکن است قادر به حمله به فایل‌های سیستم و ذوب کردن مادربورد یک رایانه، پاک کردن تمام داده‌های دیسک سخت و از کارانداختن رایانه باشند. عنکبوت‌های موتورهای جستجو و پالس‌های الکترومغناطیس می‌توانند دیسک سخت یک رایانه را ذوب کنند. کرم‌ها می‌توانند به یک سیستم دسترسی پیدا کنند اما نمی‌توانند در خارج از شبکه، برای مثال از طریق یک دیسکت، گسترش پیدا کنند. کرم‌ها در یک رایانه مقیم می‌شوند و فضای رایانه را اشغال می‌کنند تا آنکه سرعت رایانه کند شود یا از کار بیفتد. بمب‌های نرم افزاری[۲] که تعمداً زیانبار ساخته می‌شوند، اما مانند ویروس‌ها تکثیر نمی‌شوند. آن‌ها طوری طراحی شده‌اند

---

۱. مانند حملات قطع سرویس. در این حملات چند رایانه یک بات نت را به کار می‌گیرند و ردیابی رایانه کنترل کننده فرآیندی پیچیده و زمان بر است. مانند حملاتی که به استونی و گرجستان شد.

2. logic bomb

که طی یک دوره زمانی در رایانه غیرفعال باقی می‌مانند و سپس با سررسیدن تاریخی که در برنامه آن‌ها مشخص شده است منفجر می‌شوند.

بدافزار استاکس‌نت که مخفیانه به تأسیسات اتمی ایران وارد شده بود، باعث خرابی سانتریفوژهایی شد که در غنی‌سازی اورانیوم کاربرد داشت. مسئولیت حمله استاکس‌نت را کسی به عهده نگرفت، اما کارشناسان امنیت اینترنت اعلام کردند که اساساً چنین بدافزار پیچیده‌ای بدون حمایت یک یا چند دولت، قابلیت طراحی و اجرا نمی‌یافت. گمانه‌زنی‌ها در این مورد عمدتاً متوجه رژیم اسرائیل و آمریکا است که ایران را به تلاش برای دستیابی به توانایی تولید سلاح اتمی متهم می‌کنند، اما هیچ‌یک از این دو کشور مسئولیت استاکس‌نت را نپذیرفته‌اند (۱۷).

براساس دستورالعمل تالین اقداماتی که به کشتن و یا زخمی کردن اشخاص و یا آسیب رساندن و نابودی اشیاء بیانجامد، به روشنی مصداق استفاده از زور است مایکل اشمیت بر این باور است که تمامی محققانی که این گزارش را تهیه کرده‌اند، بر این موضوع توافق دارند که استفاده از ویروس «استاکس‌نت» علیه ساختارهای سایبری ایران در سال ۲۰۰۹ میلادی، استفاده از زور محسوب می‌شود بنابراین نوعی سلاح است. بدافزار یک سلاح آشکار است. ویروس‌ها و کرم‌ها می‌توانند سرعت سیستم را پایین آورند یا بر روی داده‌های هدف اختلال ایجاد کنند و یا یک سیستم عامل را به‌طور موقت غیرفعال نمایند. از دست دادن اطلاعات یا دستکاری آن‌ها ممکن است آثار و تبعات مالی و جانی زیادی در پی داشته باشد. بسیاری از اطلاعات مالی یا دولتی که به طور ذخیره شده در سیستم‌ها مورد استفاده قرار می‌گیرند و به اشتراک گذاشته می‌شوند، توسط سازمان‌های تروریستی جمع‌آوری شده و به سازمان قربانی آسیب قابل توجه وارد می‌کنند. این اطلاعات می‌تواند در قتل یا آدم‌ربایی مورد استفاده قرار گیردو یا در جهت باج‌گیری از افراد یا اخاذی از دولت‌ها و سازمان‌ها برای کمک به مقاصد جنایت کارانه استفاده شود. سرقت هویت به تروریست‌های سایبری این امکان را می‌دهد که به بانک‌ها، اسناد هویتی یا سیستم‌های کنترل دسترسی پیدا کنند. ابزارهایی مانند گوگل مپ می‌تواند اطلاعات ارزشمندی را در اختیار تروریست‌ها قرار دهد تا جایی که با استفاده از آن و تصاویر ماهواره‌ای، می‌توانند جزییات دقیق مناطق حساس را استخراج کنند.[۱]

۱. محمد نعیم نورخان متخصص کامپیوتر در پاکستانن در سال ۲۰۰۴ توانست با استفاده از امکانات اینترنتی تعداد و نمودار طبقات ساختمان‌ها در آمریکا را تخمین بزند.

بسیاری ازحملات سایبری غیر مستقیم انجام می‌شوند همچون دستکاری اطلاعات مربوط به جهت‌یابی ماهواره‌ای که باعث انحراف مسیر موشک‌ها می‌شود. همان‌طورکه دیوان هم در قضیه نیکاراگوئه کمک غیر مستقیم را توسل به زور قلمداد نموده است. بنابراین بسیاری از معیارهای ارائه شده از سوی اشمیت در فضای سایبر جهات حمله مسلحانه قلمداد کردن یک حمله کاربرد ندارد. اما معیاری که دیوان در قضیه مشورتی سلاح‌های هسته‌ای بیان نموده در مورد حملات شبکه رایانه‌ای نیز قابل اعمال است. به‌منظور اعمال حقوق منشور در مورد توسل به زور و حقوق قابل اعمال آن در مخاصمات مسلحانه، باید ویژگی‌های منحصر به فرد سلاح هسته‌ای مد نظر قرار گیرد. (Nuclear weapons case, para 36)

بنابراین می‌توان گفت حملات در فضای سایبر، اغلب غیر مستقیم انجام می‌شود، این غیر مستقیم بودن باعث مخفی ماندن مرتکب واقعی آن و نیز بالا رفتن خطر اقدامات متقابل علیه افراد بی‌گناه و نیز پدید آمدن مشکل قابلیت انتساب می‌شود. همان‌طورکه در مورد استفاده از رایانه کاخ کرملین در حمله به استونی، گروهی از میهن پرستان از آن به‌عنوان رایانه واسطه استفاده نموده بودند. غیرملموس بودن هم در هدف، تسلیحات و میزان آسیب از ویژگی‌های فضای سایبر است. در زمینه هدف می‌توان گفت اهداف حملات سایبری به دو نوع سیستم‌های اطلاعاتی و اطلاعات و نیز حملات با هدف آسیب به سخت‌افزار انجام می‌شود. بنابراین وقتی این حملات صرفاً اطلاعات را مدنظر قرار می‌دهند اهداف غیر ملموس خواهند بود. در تسلیحات در اینجا نیز ممکن است یک بدافزار دارای قابلیتی باشد که بتواند به‌عنوان سلاح در نظر گرفته شود که با توجه به جمع نظریات می‌توان ملاک میزان آسیب را برای آن در نظر گرفت و گفت: سلاح وسیله است که برای ایراد آسیب به اشخاص و اموال و کسب برتری در یک مخاصمه طراحی شده باشد (۱۷). بنابراین یک حمله سایبری در سه سطح ممکن است بررسی شود. یکی تهدید سایبری صرف، تروریسم سایبری و مخاصمه مسلحانه. بنابراین می‌توان گفت در موردی که حمله در سطح تهدید صرف است حقوق کیفری آن را به مثابه جرم رایانه‌ای در نظر خواهد گرفت اما وقتی حمله به سطح تروریسم برسد هم مسئله عاملان در انتساب مسئولیت بین‌المللی عمل متخلفانه بین‌المللی در قالب جنایت تروریسم و مسئله مداخله غیر قانونی مطرح می‌شود و اگر هم این حمله به سطحی مانند ویروس استاکس نت هم برسد وارد مفهوم مخاصمه مسلحانه خواهیم شد.

پس از آنکه حمله سایبری به حد یک مخاصمه مسلحانه رسید، یک نظام امنیتی بین‌المللی که شامل حقوق بشردوستانه بین‌المللی و حقوق بشر می‌شود به جریان می‌افتد. طرح سال ۲۰۰۰ برای کنوانسیون بین‌المللی جرم و تروریسم سایبری[1] که در دانشگاه استنفورد تهیه شده است، لزوم دستیابی به یک معاهده جامع ر این‌گونه بیان می‌دارد: «مجرمان سایبری نقطه ضعف‌های حقوق و رویه‌های دولتی لازم‌الاجرا را بیرون کشیده و به کلیه دولت‌ها خطراتی وارد می‌سازند که خارج از توانایی یک جانبه یا دو جانبه آن‌ها برای واکنش است. سرعت و پیچیدگی تکنولوژیک اقدامات سایبری، لزوم اتخاذ روندهای تنظیم شده و توافق شده برای همکاری در تحقیقات و واکنش به این تهدیدات و حملات را نشان می‌دهد.» ماده ۱۲ طرح پیش‌نویس استنفورد، تأسیس یک نهاد بین‌المللی جهت حفاظت از ساختار اطلاعاتی را پیشنهاد می‌دهد. مرکز دفاعی اینترنتی سایبری ناتو باید الگوی سازمانی برای ایجاد چنین نهادی باشد، که می‌تواند مرکز جهانی واکنش اضطراری سایبری نام بگیرد. طرح استنفورد عمل دولتی را استثناء کرده است و تنها به عمل افراد یا گروه‌ها اشاره دارد.

استاکس نت نشان داد که یک بدافزار پیچیده رایانه‌ای می‌تواند به مثابه یک سلاح عمل کند. البته این در مورد همه کرم‌ها یا ویروس‌ها قابلیت ندارد. جاسوسی سایبری و ممانعت از ارائه خدمات در قالب حمله سایبری قرار خواهند گرفت. «مایکل آنینی» و «جی.ای.ادوارد» در تعریف تسلیحات مجازی می‌گویند: «تسلیحات مجازی، تسلیحاتی است که گروه‌های تروریستی برای تخریب شبکه‌های رایانه‌ای و سرقت‌های مجازی در حجم بسیار کمتر از حجم فیزیکی آن‌ها به کار می‌برند، زیرا این تسلیحات دارای سیستم‌های بسیار پیچیده‌ای هستند. یکی از ویژگی‌های این نوع تسلیحات این است که تروریست می‌تواند توسط آن‌ها مرزهای بین‌المللی را سهل‌تر پشت سر گذارد». تسلیحات مجازی برای گروه‌های تروریستی سایبری، تابعی از نوع فعالیت آن‌هاست. بنابراین وقتی که فعالیت آن‌ها در یک فضای مجازی است، اجزای تسلیحات آن‌ها نیز بسته به فعالیتشان، مجازی است. می‌توان گفت ابزار مورد نیاز سایبرتروریست‌ها در همه دنیا مشترک بوده و شامل دستگاه رایانه شخصی و یک خط اینترنتی است که بتواند رایانه شخصی را به شبکه جهانی اینترنت متصل کند. ظهور اینترنت به‌عنوان یک ابزار جدید سریع و ارزان ارتباطی،

1 A Proposal for an International Convention on Cyber Crime and Terrorism, Stanford University, Aug. 2000.

عرصه‌های مختلف زندگی بشر را دچار دگرگونی کرد و از بسیاری جهات معنا و مفهومی جدید به ابعاد آن بخشید؛ بنابراین تروریست‌های سایبری، به جای بهره‌گیری از سلاح‌های رایج، بمب‌ها و موشک‌ها یا سایر ابزارهای معمول، از نرم‌افزارهای مخرب رایانه‌ای برای پیشبرد اهداف خود بهره‌گیری می‌کنند. ویروس‌ها، کرم‌ها، تروجان‌ها، اسپم‌ها، ایمیل بمبینگ، گوگل بمبینگ، هک و نفوذ رایانه‌ای و خرابکاری یا دستکاری‌های اینترنتی و شبکه‌ای، بخشی از ابزارهای تروریست‌های سایبری به شمار می‌رود. (۱۷)

نتیجه‌گیری

مفهوم تجاوز متناسب با زمان در حال تغییر و دگرگونی است. در گذشته حمله به حریم و قلمرو سرزمینی مصداق بارز تجاوز محسوب می‌شد ولی با تغییرات زندگی بشری ناشی از به‌کارگیری علوم و دانش و کاربرد تکولوژی‌های مدرن، مصادیق تجاوز نیز متفاوت شده است. امروزه به‌واسطه ظهور اینترنت و فضای مجازی مرزی برای فعالیت‌های انسانی وجود ندارد. اصل تمامیت ارضی در حقوق بین‌الملل بیانگر این است که سرزمین یک دولت هیچ‌گاه نباید مورد تجاوز، تهاجم یا تجزیه غیرقانونی قرارگیرد. جنگ سایبری به قصد و نیت سیاسی در جهت اخلال در امور حیاتی و زیربنایی و خدمات‌رسانی به شهروندان و هرگونه ایجاد خسارت به افراد غیرنظامی مصداقی از مفهوم تجاوز قلمداد می‌گردد. تروریسم سایبری را در فقدان تعریف مورد اجماع از تروریسم، می‌توان با توجه به عناصر و اهداف آن، ایراد خسارت فیزیکی یا اطلاعاتی به اموال و اشخاص در حمله به زیرساخت‌های حیاتی و ایجاد رعب و وحشت، جهت به زانو درآوردن دولت یا سازمان دولتی دانست. ادبیات حقوقی در حال تغییر از نبردهای سنتی به سایبری و توسعه مفهوم سلاح و احراز تجاوز است. اگرچه تلقی منشور از توسل به زور ناظر بر اقدامات نظامی است و تفسیر موسع از توسل به زور می‌تواند خلاف جهتی که به تدوین منشور انجامیده تلقی شود اما برخی حقوقدانان و دولت‌ها، این حملات را به مثابه تجاوز دانسته و پاسخ نظامی به آن را مجاز اعلام کرده‌اند. این مقاله به شیوه توصیفی ـ تحلیلی با استفاده از منابع کتابخانه‌ای نگارش یافته است و در نوسان رویکرد و استدلال، در پی پاسخ به این پرسشی بوده است که، شرایط و بایسته‌های تلقی تروریسم سایبری به مثابه توسل به زور و تجاوز چه مواردی است و از رهگذر تفاوت رویکردهای تابعان حقوق بین‌الملل، چگونه

توجیه‌پذیر است. بایسته‌ها می‌بایست پاسخ‌گوی دشواری معیارهای شناسایی مرتکب، انتساب حملات به دولت‌ها، ارتکاب توسط بازیگران غیردولتی و معیار مقیاس و نتایج حملات سایبری باشد. رسیدن حملات به آستانه حمله مسلحانه، توسل به قطعنامه تعریف تجاوز، که حاوی تعریفی کلی همراه با فهرستی از اقدامات منع شده علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولت است، را مطرح می‌نماید، در عین حال، ماده ۴ به شورای امنیت آزادی عمل داده تا موارد دیگری را نیز در صورت اقتضا، تجاوز قلمداد نماید. بنابراین اگر حمله تروریستی سایبری از سوی عوامل دولتی یا منتسب به دولت بوده و به آستانه حمله مسلحانه برسند، می‌توانند استقلال سیاسی یک دولت را خدشه‌دار نموده و مصداق عمل تجاوز به حساب آیند.

References

- Jafari, Ali Akbar; Nikrosh, Maleeha (2012). Soft war in the context of cyber threats and security solutions, Psychological Operations Quarterly. Year 9, 35: 46-31. [Persian]
- Shackelford, Scott j. (2009). "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", Berkley Journal of International Law (BJIL), Vol. 25, No. 3. last revised :12/2016
- The Legality of the Threat or Use of Nuclear Weapons Case. ICJ Rep (1996). Para 78.
- Charvat, J. (2012). Cyber Terrorism: A New Dimension in Battle space. https://ccdcoe.org/ sites/default.
- Hoisington, Matthew (2010), Cyber warfare and the Use of Force Giving Rise to the Right of Self-Defense, Boston College International and Comparative Law Review, Vol. 32.
- Ian Brownline, international law and the use of force by statea, Oxford university press, 1963.
- International Committee of the Red Cross (ICRC) (2008). How is the Term "Armed Conflict" Defined in International Humanitarian Law? fromhttp://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf#page=3&zoom=auto,0,822.
- Albright, D., Branna, P., & Walorand, C. (2011). Did Stuxnet take-out 1000 centrifuges at the Natanz enrichment plan? Institute for science and international security.
- Lynn III, William. j, defending a new domain- the pentagon cyber strategy, 2010, 89(5) Foreign affairs 97.
- TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (2013). Cambridge University Press.

- Yunos, Z., & Sulaman, S. (2017). Understanding Cyber Terrorism from Motivational Perspectives. Journal of Information Warfare, 16(4), 1–13. https://www.jstor.org/stable/26504114.
- Ambos, K. (2016). Individual Criminal Responsibility for Cyber Aggression. Journal of Conflict & Security Law, 21(3), 495-504.
- Ruys, T. (2018). Criminalizing Aggression: How the Future of the Law on the Use of Force Rests in the Hands of the ICC. European Journal of International Law, 29(3), , 887-917.
- Roshanaei, M (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. Journal of Computer and Communications, 9 (8), 80-102.
- McDougall, C. (2021). The Crime of Aggression under the Rome Statute of the International Criminal Court. 2nd edition, Cambridge University Press.
- Madubuike-Ekwe, J. N. (2021). Cyberattack and the Use of Force in International Law. Beijing Law Review, 12, 631-649.
- Horowitz, J. (2020). Cyber Operations under International Humanitarian Law: Perspectives from the ICRC. ASIL Insights.
- Heller, kj. (2020). Who Is Afraid of the Crime of Aggression?. Journal of International Criminal Justice,. 18(1), 2019-2031.
- Darcy, S. (2021). Accident And Design: Recognising Victims Of Aggression In International Law. International & Comparative Law Quarterly, 70(1), pp 103-132.