Volume 6. Issue 11. Spring 2023. Pages 55 to 73.

Research Paper

Cyberspace and the Challenges of International Law in the Face of Cyber Attacks

Ali Rostami Far*[1]

[1] Department of International Law and Relations, Faculty of International College, Qeshm Islamic Azad University

10.22080/JPIR.2023.23733.1292

Received:
August 27, 2022
Accepted:
September 8, 2023
Available online:
February 10, 2024

Keywords:
International Security, International Politics, Cyberspace, Cyber Attacks, Information Warfare

Abstract

Today, many critical infrastructures in the fields of energy, health, transportation (sea, air, land and even outer space) and telecommunications are highly dependent on computer systems and internet networks, Such a platform has changed the concepts of armed attacks and force as hostile states conduct their hostile operations in cyberspace, In some cases, these attacks destroy the infrastructure of a country, and the destructive effects of such actions will be far more than military operations, Therefore, the importance of developing international mechanisms is an inevitable necessity, The question is, based on which propositions do the current rules governing international relations make it possible to deal with subversive operations? And does international law have the capacity to identify cyber-attacks as an example of resorting to force or not? It seems that the answer to the questions depends on the analysis of the existing international realities, Until now, binding international rules have not been established in this field, and governments only respond to these operations based on the principle of legitimate defense, However, there is no rule in the issue of compensation for damages and dividing the boundary between legitimate and illegitimate actions and it is difficult to identify cyber-attacks as an example of force, In this article, the author tries to analyze a logical and descriptive interpretation of the rules of international law, the application of the said rules, focusing on the instrumental, goal-oriented and effect-oriented approach in the cyber space.

*Corresponding Author: Ali Rostami Far
Address: Qeshm Islamic Azad University
Email: arq119@yahoo.com
Tel: 07635243755

دوره ۶. شماره ۱۱. بهار ۱۴۰۲. صفحات ۵۵ تا ۷۳.

علمی

فضای مجازی و چالش‌های حقوق بین‌الملل در مواجهه با حملات سایبری

علی رستمی فر[1]*

[1] استادیار گروه حقوق و روابط بین الملل دانشکده بین الملل دانشگاه آزاد اسلامی قشم

10.22080/JPIR.2023.23733.1292

تاریخ دریافت:
۰۵ شهریور ۱۴۰۱
تاریخ پذیرش:
۱۷ شهریور ۱۴۰۲
تاریخ انتشار:
۲۱ بهمن ۱۴۰۲

چکیده

امروزه بسیاری از زیرساخت‌های حیاتی در زمینه‌های انرژی، سلامت، حمل‌ونقل (دریایی، هوایی، زمینی وحتی فضای ماورای جو) و مخابرات، به سیستم‌های رایانهای و شبکه‌های اینترنتی وابستگی شدید دارند، چنین بستری مفاهیم حملات مسلحانه و زور را تغییر داده؛ زیرا دولت‌های متخاصم عملیات خصمانه خود را در فضای سایبری انجام می‌دهند، این حملات در برخی موارد زیرساخت‌های یک کشور را نابود می‌کند و آثار مخرب چنین اقداماتی به مراتب بیشتر عملیات نظامی خواهد بود. ازاینرو اهمیت تدوین سازوکارهای بین‌المللی ضرورتی اجتنابناپذیر می‌باشد، پرسش این است که قواعد فعلی حاکم بر روابط بین‌المللی با تکیه بر کدام گزاره‌ها امکان مقابله با عملیات خرابکارانه را می‌دهد؟ و قواعد حقوق بین‌الملل ظرفیت این را دارد که حملات سایبری را به عنوان مصداق توسل به زور شناسایی کند یا خیر؟ به نظر می‌رسد پاسخ به پرسش‌های مطروحه در گرو تحلیل واقعیت‌های موجود بین‌المللی است. تاکنون قواعد الزامآور بین‌المللی در این زمینه وضع نشده و دولت‌ها تنها براساس اصل دفاع مشروع پاسخ‌های لازم را به این عملیات می‌دهند. اما در موضوع جبران خسارات و تفکیک مرز اقدامات مشروع و غیرمشروع هیچ قاعده‌ای وجود ندارد وآنگهی شناسایی حملات سایبری به عنوان مصداق زور دشوار می‌باشد. نگارنده در این مقاله سعی دارد تفسیری منطقی و توصیفی از قواعد حقوق بین‌الملل، کاربرد قواعد مذکور با تمرکز بر رویکرد ابزارگرا، هدفگرا و اثرگرا در فضای سایبری تحلیل نماید.

کلیدواژه ها:
امنیت بین‌الملل؛ سیاست بین‌الملل؛ فضای سایبری؛ حملات سایبری؛ جنگ اطلاعاتی.

* **نویسنده مسئول:** علی رستمی فر
آدرس: دانشگاه آزاد اسلامی قشم
ایمیل: arq119@yahoo.com
تلفن: ۰۷۶۳۵۲۴۳۷۵۵

۱ مقدمه

حملات سایبری می‌توانند اهدافی مانند سایت‌های دولتی یا رسانه‌ای، سیستم‌های رایانه‌ای بیمارستانی، زیرساخت‌های حمل‌ونقل یا حتی سایت‌های تولید صنعتی یا هسته‌ای را هدف قرار دهند. وابستگی شدید و فزاینده جوامع مدرن به شبکه‌ها و سیستم‌های رایانه‌ای و اختلال در سیستم‌های اصلی رایانه‌ای، عملکرد صحیح این سیستم‌ها را با آسیب مواجه می‌کند. هرچند تاکنون هیچ حمله سایبری نقش عمده‌ای در زمینه ایجاد درگیری یا آسیب جدی به کشورمان وارد نکرده است؛ اما وابستگی بسیاری از کشورها به زیرساخت‌های فناوری اطلاعات از یک طرف و آسیب‌پذیری برخی سیستم‌ها از سوی دیگر، فرضیه حملات سایبری در مقیاس بزرگ را به طور فزاینده‌ای گسترش داده است. ازاین‌رو پیامدهای چنین حملاتی، به دور از محدود شدن به دنیای مجازی، می‌تواند قابل توجه و تأثیر شگرفی بر یک کشور و جمعیت آن داشته باشد (برهان، ۲۷:۱۳۹۹). آمریکا خود از بنیان‌گذاران حملات سایبری به کشورهای دیگر از جمله ایران بوده؛ اما در سال‌های گذشته به دلیل وابستگی شدید به شبکه اینترنت به‌شدت در برابر همین حملات، آسیب‌پذیر نشان داده است. سال ۲۰۱۱ کاخ سفید سندی از یک راهبرد ملی آمریکا منتشر کرد که در آن، استفاده از زور نظامی در پاسخ به حملات سایبری مجاز شمرده شده بود. (عابدی،۱۴۰۲)، بسیاری از کارشناسان و تحلیل‌گران حوزه امنیت، بر این باورند که پایان یافتن دوران جنگ سرد نه‌تنها منجر به امن‌تر شدن جهان نشده است، بلکه به وجود آمدن چالش‌های امنیتی غیرنظامی جدیدی همچون تخریب محیط زیست، رفاه اقتصادی، سازمان‌های جنایی بین‌المللی و مهاجرت گسترده افراد، امنیت جهانی را با چالش‌های جدی‌تری نسبت به گذشته مواجه ساخته است. تحلیل‌گران بر این باورند که اهمیت این مسائل جدید نه‌تنها بازاندیشی در تهدیدهای امنیتی، بلکه تجدیدنظر درباره خود مفهوم امنیت را ضروری می‌سازد (خلیلی پور رکن آبادی، ۱۷۸:۱۳۹۱).

اعمال حقوق جنگ نسبت به حملات سایبری به‌شدت برانگیز است (آهنی آمینه،۱۲۸:۱۳۹۳)و عمده‌ترین سند بین‌المللی یعنی معاهده ژنو در این خصوص سکوت اختیار نموده است. اما امروزه درگیری‌های بین دولت‌ها، دیگر منحصر به جنبه فیزیکی و لشکرکشی نظامی نخواهد بود؛ بلکه در فضای مجازی رخ خواهد داد. در سال‌های اخیر مفهوم فضای سایبری به مثابه میدان جنگ دچار تحولات چشمگیری شده است (حراست ارشاد). این همان چیزی است که برخی آن را «جنگ سایبری» می‌نامند. حملات سایبری به برخی از سایت‌های هسته‌ای صلح‌آمیز ایران، بر اساس گزارش‌های کارشناسی انجام‌شده، یکی از حملات سایبری پیچیده بوده که توسط یک بدافزار به نام ویروس استاکس نت[۱] انجام شده است و این ویروس وظیفه داشته عملیات غنی‌سازی اورانیوم را تا ۲۳ درصد در یک دوره تقریباً ۱۲ ماهه کاهش دهد. البته این‌ها فقط جنبه تخمینی داشته‌اند و با توجه به ماهیت بسیار استراتژیک استاکس نت، به نظر نمی‌رسد این رقم با حمله ویروس به دست آمده باشد (پارسا،۱۳۸۹). اگرچه این آسیب محدود و نسبتاً سریع ترمیم شد، اما استاکس‌نت نشان داد که یک حمله سایبری پیچیده می‌تواند صدمات قابل توجه و طولانی‌مدتی به‌ویژه به زیرساخت‌های بنیادی و اصلی وارد و به اصطلاح «بحران» ایجاد کند. از طرفی اصطلاحات «جنگ سایبری»، «حمله سایبری»، نیز به موقعیت‌های درگیری اشاره می‌کند. هرچند در حقوق بین‌الملل در خصوص موضوع مطروحه و تطبیق مصادیق آن با منشور ملل متحد اتفاق نظری وجود ندارد (المجذوب،۸۱۴:۲۰۱۸) و از طرفی دیگر معاهدات بین‌المللی مکانیسم مناسبی برای چنین اقداماتی به طور جامع پیش‌بینی نکرده‌اند (صبرینه،۱۱۲:۲۰۱۵). به طورکلی تنها دو استثناء پذیرفته شده برای ممنوعیت توسل به زور وجود

[۱] Stuxnet

دارد که عبارت‌اند از: ۱-اقدامات انجام‌شده بر اساس قطع‌نامه شورای امنیت سازمان ملل متحد مطابق با فصل هفتم منشور سازمان ملل متحد، از جمله اقدامات مسلحانه انجام‌شده توسط سازمان‌های منطقه‌ای تحت به اصطلاح موافقت‌نامه‌های منطقه‌ای با مجوز یا موافقت شورای امنیت سازمان ملل؛ ۲-دفاع مشروع انفرادی یک دولت و دسته-جمعی چندین دولت باشد (عید کشایش،۱۴۰۲:۹۰)، لذا ضرورت‌های جهانی و امنیت بین‌المللی و پایداری موضوعات بایستی به گونه‌ای باشد که دولت‌ها با اجماع در راستای خطرات توسعه موارد فوق چاره-جویی نمایند.

هرچند به رغم خطرات پیش‌گفته و آثار مخرب حملات سایبری بر حیات سیاسی، اجتماعی، امنیتی و حتی اقتصادی یک کشور تاکنون هیچ معاهده یا مجموعه قواعد الزام‌آوری در این خصوص وجود ندارد که تعیین نماید کشورها چه رفتاری را بایستی در فضای مجازی اتخاذ کنند و عدم ضمانت اجراهای مسؤولیت‌آور، مانع از اعمال قواعد بین‌المللی شده است، اما واقعیت این است که حقوق بین‌الملل عمومی برای رسیدگی به مشکلات مختلف در سطح جهانی بایستی راهکاری را تدوین نماید تا منافع ملی همه اعضای ملل متحد تأمین گردد. ازاین‌رو به نظر می‌رسد تفسیر برخی از قواعد مربوط به درگیری در جنگ، قوانین حاکم بر رفتار جنگی، نحوه کنترل و کاهش تنش‌های فیزیکی قابلیت انطباق با مصادیق حملات سایبری را دارند (احمدی،۱۳۹۳:۵۸)، گرچه این دسته قواعد برای حملات نظامی وضع شده‌اند و از بسیاری جهات با عملیات در فضای سایبری با عملیات جنگی «سنتی» متفاوت هستند، اما با تفسیر منطقی این قواعد و تسری آن به برخی از موقعیت‌ها، قواعد موجود امکان پاسخ‌گویی حداقلی برای کشور مهاجم یا گروه‌های هکری خواهد داشت.

لذا این موضوع منجر به طرح این سؤال می‌شود که چگونه می‌توان قوانین بین‌المللی را در فضای مجازی اعمال و پیامد حملات سایبری را کنترل نمود؟ ابتدا ضرورت دارد دقیقاً تعریف شود حملات سایبری چیست و با چه ابزارهای فنی اجرا می‌شوند، حملات سایبری در چه مواردی از نظر حقوق بین‌الملل مشروع و در کدام موارد غیر مشروع تلقی می‌گردد. دولت قربانی یک حمله سایبری در پاسخ به حملات سایبری می‌تواند چه واکنش‌هایی اتخاذ کند و چه سازوکارهایی را می‌توان در آینده به منظور ایجاد چارچوب قانونی پایدارتر در فضای سایبری پیشنهاد داد. امروزه حملات سایبری و به طور کلی اصطلاحات سایبر و جنگ سایبری در رسانه‌ها، برای توصیف پدیده‌های بسیار متفاوتی استفاده می‌شود که ارتباط چندانی با «جنگ» ندارند. برخی از اندیشمندان در تفسیر، جنگ سایبری را اغلب با اصطلاحات «جنگ اطلاعاتی» یا «جنگ رایانه‌ای»، «حمله سایبری» یا «حمله رایانه‌ای» یا حتی «جنایت سایبری» تحلیل می‌کنند. اما به دلیل فقدان اجماع در مورد مؤلفه‌های فوق، توافق بر سر یک تعریف یکسان و مشترک از این اصطلاحات دشوار است. اما وجه مشترک این مفاهیم در اصطلاحات مختلف، اصطلاح «سایبر» است و کلیه این موارد به فناوری‌های اطلاعاتی جدید، رایانه‌ها، «واقعیت مجازی» و اینترنت ارتباط می‌یابد. بنابراین حملات سایبری، جنگ سایبری یا حتی جرایم سایبری در جایی اتفاق می‌افتد که معمولاً «فضای سایبری» نامیده می‌شود (خاکپور،۱۴۰۰:۶۷) و با توجه به این گزاره، فضای مجازی را می‌توان شبکه‌ای جهانی و به هم پیوسته از اطلاعات، زیرساخت‌های ارتباطی از جمله اینترنت، شبکه‌های مخابراتی، سیستم‌های رایانه‌ای و اطلاعات موجود در آن‌ها توصیف کرد (ملزر،۲۰۱۱:۴).[۱] به نظر می‌رسد فقدان مقررات خاص بین‌المللی موجبات بی‌نظمی بین‌المللی از یک طرف و توسعه حملات سایبری را افزایش داده است. از طرفی فقدان اجماع بین‌المللی در خصوص شناسایی حملات سایبری به عنوان توسل به زور که در منشور ملل متحد بیان شده است، بر پیچیدگی و دشواری

[۱] Melzer

مفاهیم افزوده است. به همین مناسبت برای تحلیل موضوعات مطالب نگارش حاضر با تناسب منطقی در بندهای زیر به تحلیل موضوعات می‌پردازد.

۲ نگرش کلی به مفهوم فضای مجازی و امنیت

فضای مجازی تلفیقی از اجزای فیزیکی (مانند زیرساخت‌ها) و اجزای غیر فیزیکی (مانند اطلاعات و داده‌های موجود در این زیرساخت‌ها) هستند و از این جهت، فضای مجازی با چهار حوزه سنتی که در حقوق بین‌الملل مانند زمین، دریا، هوا و فضا تدوین شده، متفاوتند. زیرا فضای سایبری مانند زمین، دریا، هوا و فضا می‌تواند صحنه بسیاری از عملیات‌ها به نام‌های «عملیات رایانه‌ای» یا «عملیات سایبری» باشند. اما وجه اشتراک فضای مجازی با فضاهای مطروحه در حقوق بین‌الملل این است که این اصطلاح شامل عملیات تهاجمی و تدافعی می‌شود؛ چراکه عملیات سایبری به‌کارگیری قابلیت‌های سایبری با هدف اصلی دست‌یابی به اهداف در فضای سایبر یا از طریق آن تعریف می‌شود (اشمیت،۲۰۱۷)[1] با این توصیف سوء استفاده از فضای مجازی ممکن است به طور خاص با هدف انتشار اطلاعات با هدف تبلیغات، سرقت اطلاعات حساس، رمز عبور یا اسرار تجاری، بدون اینکه کاربر شبکه یا سیستم رایانه‌ای از آن آگاه باشد، اتفاق بیفتد. در این گونه موارد، بهره‌برداری سایبری با شکل مدرن جاسوسی مطابقت دارد. اگرچه جاسوسی در اکثر کشورها غیر قانونی تلقی می‌شود، اما هیچ یک از اصول حقوق بین‌الملل به صراحت چنین عملی را منع نکرده‌اند (جروایس،۲۰۱۲:۵۳۳)[2]

با توصیفات فوق حملات سایبری و عملیات دفاع سایبری، عملیات هستند که فراتر از بهره‌برداری صرف از فضای مجازی و سایبر صورت می‌پذیرد و در اکثر موارد با قصد خصمانه همراه است. لذا هدف از این عملیات مختل کردن یا از بین بردن اطلاعات موجود در سیستم‌ها و شبکه‌های کامپیوتری یا خنثی کردن عملکرد مطلوب و ایجاد اختلال و کنترل نامطلوب شبکه‌ها و سیستم‌های یک کشور است. بر پایه گزاره‌های فوق، اصطلاح حملات سایبری به عملیات در مقیاس کوچک مانند جرایم سایبری و تروریسم سایبری و به عملیات با پیامدهای جدی‌تری که مورد اخیرالذکر عملیات «جنگ سایبری» است، اطلاق می‌گردد.

پس از جنگ جهانی دوم و توسعه فناوری‌های الکترونیکی و در نیمه دوم قرن بیستم، بین روسیه و ایالات متحده امریکا، ژاپن، آلمان، فرانسه، بریتانیا، چین و سایر کشورها رقابت تنگاتنگی در توسعه ابزارهای الکترونیکی انجام گرفته است که نتیجه آن توسعه سیستم‌های تسلیحاتی الکترونیکی بوده است. در ایران نیز استفاده از فناوری‌های مدرن سیستم‌هایی برای دسترسی کنترل از راه دور نیز توسعه خاصی یافته است (بانکس وکویلان،۲۰۰۰:۲)، البته اهداف کشورمان از توسعه فناوری در راستای صلح‌آمیز و دفاعی می‌باشد. هرچند اکثر کشورها و دولت‌ها قابلیت‌های سایبری را ابزاری برای کنترل نفوذ منطقه‌ای و دست‌یابی به دستاوردهای استراتژیک، سیاسی، مالی و اقتصادی می‌دانند (سراج،۱۳۹۹:۳۷) لذا براساس مؤلفه‌های جدید، استفاده از روش‌های سنتی نظامی و دیپلماتیک، دیگر تنها ابزار رقابت منطقه‌ای و جهانی کشورها محسوب نمی‌گردد و فناوری‌های الکترونیکی و سایبری، گزاره‌های قدیمی نفوذ و رقابت کشورها را تقلیل داده‌اند. هرچند تغییر روش‌های سنتی دشوار و نیاز به زمان طولانی دارد؛ اما تحولات به نحو چشمگیری رویکردهای گذشته را تغییر داده است (عثمان،۲۰۱۷:۱۷). بر این اساس، فضای الکترونیک به عرصه جدیدی از درگیری‌های نوین و نفوذ منطقههای و جهانی تبدیل شده است؛ زیرا جنگ‌های الکترونیکی در شبکه‌های ارتباطی و اطلاعاتی فراتر از مرزهای سنتی حاکمیت دولت‌ها صورت می‌پذیرد (کیانا و هاشمی،۱۳۸۳:۹۰) و این

[1] Schmitt

[2] Gervais

فرآیند به مرور زمان بی‌اعتمادی بین دولت‌ها را ایجاد می‌کند.

۳ جرایم سایبری

هرچند جرایم سایبری یکی از مفاهیمی است که از تعریفی جهانی بی‌بهره است، اما بسیاری از کشورهای امضاکننده کنوانسیون بوداپست تعریفی را که کنوانسیون بیان کرده پذیرفته‌اند. این کنوانسیون تحت حمایت شورای اروپا در سال ۲۰۰۱ تصویب و در سال ۲۰۰۴ لازم‌الاجرا شده است. در این راستا به‌ویژه با هدف تقویت همکاری بین دولت‌ها در مبارزه با جرایم سایبری از دولت‌ها می‌خواهد که «آسیب‌رسانی عمدی و غیر قانونی که شامل پاک کردن، زوال، تغییر یا حذف داده‌های رایانه‌ای و هرگونه اعمال عمدی و بدون مجوز برای عملکرد یک سیستم رایانه‌ای و انتقال، آسیب، پاک کردن، زوال، تغییر یا حذف داده‌های رایانه‌ای» را جدی گرفته و به عنوان جرم کیفری در قوانین خود جرم‌انگاری نمایند. لذا کنوانسیون مذکور از جهت جرایم سایبری، کلاهبرداری اینترنتی، دزدی دریایی، سرقت آثار سمعی، بصری و غیره را پوشش می‌دهد. ازاین‌رو با توجه به اینکه عملیات هماهنگ انجام شده از طریق فضای سایبری، با استفاده از سیستم‌های اطلاعاتی و ارتباطی منجر به اختلال در عملکرد یا تخریب سیستم‌ها و شبکه‌های رایانه‌ای می‌گردد، این فرآیند می‌تواند رفاه، امنیت و ثبات کشورها را تهدید کند؛ لذا جرم‌انگاری آن در سطح ملی و بین‌المللی می‌تواند پیامدهای مخرب چنین اقداماتی را کنترل نماید.

مجمع عمومی سازمان ملل متحد، در گزارش سال ۲۰۰۳، ۲۰۱۰، ۲۰۱۵ خطرات فضای سایبری را یادآوری می‌نماید و در قطع‌نامه سال ۲۰۱۳ متذکر می‌گردد: «حقوق بین‌الملل و به‌ویژه منشور سازمان ملل متحد برای حفظ صلح و ثبات در فضای بین‌المللی قابل اجراست.» (سازمان ملل متحد،۷:۲۰۱۹)[1]، در راستای اهمیت خطرات در سومین گزارش که در سال ۲۰۱۵ تهیه شده موارد سابق را به صورت مبسوطتر بیان می‌کند و در گزارش فوق به صراحت بیان می‌کند، منشور باید در مورد فناوری اطلاعات و ارتباطات اعمال شود و دولت‌ها نیز باید به اصول اصلی آن در فضای سایبری احترام بگذارند.

بر پایه گزاره‌های فوق، اصول مختلفی که دولت‌ها متعهد به رعایت آن‌ها شده‌اند به عنوان «اهمیت محوری» توصیف شده‌اند. این اصول عبارت‌اند از تساوی حاکمیتی کشورها، حل و فصل اختلافات با ابزارهای مسالمت‌آمیز، احترام به حقوق بشر و آزادی‌های اساسی، چشم‌پوشی از تهدید و استفاده از زور علیه تمامیت ارضی یا استقلال سیاسی هر کشوری به هر روش دیگری که با این مؤلفه‌ها مغایرت داشته باشد. لذا مجمع عمومی تأکید می‌ورزد دولت‌ها در این فرآیند با توجه به اهداف سازمان ملل متحد و اصل عدم مداخله در امور داخلی سایر کشورها گام‌های اساسی و سازنده بردارند (کاخ سفید،۹:۲۰۱۱).[2] حال اگر حملات سایبری با ضمانت اجراهای بین‌المللی همراه نباشد، فضای سایبری به جای اینکه بستر امن باشد، تهدیدی جهانی علیه صلح و امنیت جهانی خواهد بود. به همین دلیل حقوق بین‌الملل بایستی مسؤولیت‌های حقوقی دولت‌ها را در روابطشان با یکدیگر و روابطی که این کشورها ممکن است با افرادی که در قلمروشان زندگی می‌کنند، تعریف کنند.[3] زیرا کنوانسیون‌های بین‌المللی مختلف، حقوق بین‌الملل عرفی و همچنین اصول کلی حقوق بین‌الملل، منشور سازمان ملل متحد، یکی از ستون‌های حقوق بین‌الملل و اصول اصلی روابط بین‌الملل می‌باشند که قواعد مربوط به قانونی بودن استفاده از زور را تدوین می‌کنند، به همین مناسبت الزامات بین‌المللی بایستی در فضای سایبری قابل

[1] United Nations
[2] White House
[3] https://www.un.org/fr/sections/what-we-do/uphold-international-law/

اجرا باشد و ضرورت دارد این توافقات با معاهدات دیگری تکمیل شوند که حاوی قوانین مربوط به قانونی بودن اعمال دولت‌ها بر اساس حقوق بین-الملل و همچنین قواعد حقوق بین‌الملل عرفی است.

هرچند موارد فوق ماهیت بازدارندگی حقوق بین‌الملل را بازگو می‌کند و تضمینی بر صلح و امنیت جهانی بوده اما اقدامات برخی از دولت‌ها با نقض قواعد بین‌المللی به مخاطره نیفتد و از طرفی ابهام در مفاهیم و ماهیت حملات سایبری تطبیق حملات سایبری با اصل منع زور مندرج در بند ۴ ماده ۲ منشور ملل متحد و همچنین مفهوم تجاوز مسلحانه را دشوار می‌سازد؛ زیرا حمله‌ای که به معنای استفاده از زور یا حمله مسلحانه بر اساس قوانین بین‌المللی غیرقانونی تلقی می‌گردد، با مندرجات بند مذکور قابلیت انطباق نداشته و به همین دلیل ضرورت دارد خلأهای موجود در مورد حملات سایبری بر اساس قواعد جدید حقوق بین‌الملل سازمان‌دهی و بازتعریف گردند، یا با اصلاح مفاد ماده ۲ منشور و تسری حملات سایبری به عنوان نقض اصل عدم مداخله یا به طور کلی‌تر نقض حاکمیت دولت‌ها، غیرقانونی تلقی گردند.

۴ حملات سایبری به عنوان نقض اصل منع توسل به زور

بند ۴ ماده ۲ منشور سازمان ملل متحد یکی از مهم‌ترین مفاد این معاهده و به‌ویژه حقوق بین‌الملل است که به صراحت بیان می‌کند، اعضای سازمان در روابط بین‌الملل خود از توسل به تهدید یا استفاده از زور، چه علیه تمامیت ارضی یا استقلال سیاسی هر کشوری، یا از هر طریق دیگری که با اهداف سازمان ملل متحد ناسازگار باشد، خودداری کنند، دیوان بین‌المللی دادگستری در پرونده مربوط به فعالیت‌های نظامی و شبه نظامی در نیکاراگوئه یادآور شده است که توسل به هر اقدامی که نقض حاکمیت یک کشور باشد غیرقانونی و به مثابه نقض منشور می‌باشد. امروزه تفسیر اصل مذکور نیز ارزش عرفی پیدا کرده است و ازآنجایی‌که امکان نقض اصل مذکور در فضای سایبری نیز وجود دارد، لذا تجزیه و تحلیل اینکه یک عملیات سایبری می‌تواند به منزله استفاده از زور موضوع بند ۴ ماده ۲ تلقی گرددیا خیر نیاز به بررسی دارد.

۵ مفهوم زور در حقوق بین-الملل

مفهوم زور، در ماده ۲ منشور تعریف نشده و هیچ تفسیر واحدی از مفهوم زور در جامعه بین‌المللی توسط حقوقدانان ارائه نگردیده است، بنابراین این اصطلاح نیاز به تفسیر دارد، در زمینه تفسیر مفاد یک معاهده، اشاره به کنوانسیون وین[1] در مورد حقوق معاهدات ۱۹۶۹ مفید می‌باشد؛ زیرا کنوانسیون مذکور در مواد ۳۱ تا ۳۳ قواعد تفسیری خود را ارائه نموده است. اگرچه کنوانسیون مذکور به تصویب جهانی و کلیه اعضای سازمان ملل متحد نرسیده، اما پس از تصویب منشور سازمان ملل متحد لازم‌الاجرا شده است. اما در حقوق بین‌الملل عموماً اکثر مقررات این معاهده، به‌ویژه مواد مربوطه کنوانسیون، قواعد معتبری را تشکیل می‌دهند و به همین مناسبت قواعد فوق ارزش عرفی پیدا کرده‌اند. ماده ۳۱ کنوانسیون وین یک قاعده کلی را ارائه می‌دهد که معاهدات باید «بر اساس معنای معمولی

[1] کنوانسیون وین در مورد حقوق معاهدات معاهده‌ای است که حقوق بین‌الملل عرفی در مورد معاهدات را بیان می‌کند. تدوین این کنوانسیون از سال ۱۹۴۹ در دستور کار کمیسیون حقوق بین‌الملل قرار گرفت و متن نهایی آن در سال ۱۹۶۶ در این کمیسیون تصویب شد و در ۲۲ مه ۱۹۶۹ در کنفرانسی با شرکت نمایندگان ۱۱۰ کشور در وین تصویب شد و از ۲۷ ژانویه ۱۹۸۰ (یک ماه پس از تسلیم ۳۵مین سند الحاق یا تصویب) قوت اجرائی یافت. بیشتر کشورها، چه آن‌ها که به این معاهده پیوسته باشند و چه دیگر کشورها، فضل تقدم آن را به عنوان «معاهده معاهدات» مورد تأیید قرار می‌دهند. کنوانسیون وین در سطح گسترده‌ای به یک راهنمای معتبر برای ایجاد و اجرای معاهدات تبدیل شده است.

که به مفاد معاهده در متن آن‌ها و در پرتو موضوع و هدف آن داده می‌شود» تفسیر شوند.

علیرغم توصیفات فوق در چارچوب حقوق بین‌الملل، مفهوم تنش با توجه به تعبیری که از اصطلاح «زور» می‌شود نسبتاً گسترده است و می‌تواند به‌کارگیری زور، تسلیحات و نیروی اقتصادی یا سایر اقدامات محدودکننده را نیز شامل گردد (زروقه،۲۰۱۹:۱۰۱۷). لذا با توجه به موارد فوق و ازآنجایی‌که نمی‌توان با قاطعیت دامنه آن چه را که اصطلاح دامنه «زور» را شامل می‌شود، به‌درستی از مفاد فوق تفسیر نمود، ضرورت دارد نحوه استفاده از این واژه را در معاهده مورد بررسی قرار داد و موضوع و هدف آن را تفسیر نمود.

اصطلاح زور در مقدمه منشور و برخی از مواد بیان شده است، اما هیچ گونه تعریفی از واژه زور در منشور ملاحظه نمی‌گردد. در مقدمه فقط به منع توسل به زور اشاره شده و صرفاً یک سری الزاماتی را برای کشورها تعیین می‌کند تا از استفاده از «نیروی تسلیحات» اجتناب کنند. اما ماده ۴۱ منشور از نیروی مسلح صحبت می‌کند. حال با توصیفات فوق این سؤال مطرح می‌شود که آیا واژه «زور» در ماده ۲ بایستی مانند مقدمه و ماده ۴۱ تقسیر شود؛ زیرا ماده ۲ استفاده از زور در قالب توسل به نیروی «نظامی» می‌داند یا برعکس، فقدان توسل به نیروی «نظامی» با تفسیر موسع از مفهوم «زور» در بند ۴ ماده ۲، مفهوم مذکور می‌تواند قابلیت تسری به اجبار سیاسی یا اقتصادی و حملات سایبری را داشته باشد.

با توصیفات فوق تفاسیر سیستمی، موسع، مضیق و منطقی می‌توان از موضوع فوق ارائه نمود. رویکرد اول رویکردی سیستمی به موضع دارد؛ زیرا با تفسیر سیستمی استدلال می‌کند منظور از زور در بند ۴ ماده ۲ توسل به نیروی مسلح بوده و کلیه مظاهر دیگر از مصادیق زور محسوب نمی‌گردند. این تفسیر از وحدت ملاک بند هفتم مقدمه منشور قابل استنباط می‌باشد؛ زیرا بند مذکور بیان می‌دارد: «از نیروی نظامی جز در جهت منافع مشترک استفاده نمی‌شود» (اشمیت،۱۹۹۹:۹۰۴)[1]، آلبرشت راندلژوفر تأکید می‌کند اگر هدف بند ۴ ماده ۲ منع اجبار اقتصادی یا سیاسی باشد، دیگر هیچ ابزار قانونی برای اعمال فشار بر دولت دیگری که برخلاف قوانین بین‌المللی عمل می‌کند، وجود نخواهد داشت (نولت وراندلژوفر،۲۰۲۰:۱۱۸).[2] به نظر می‌رسد این تفسیر با واقعیت‌های بین‌المللی و منشور سازگارتر بوده؛ زیرا تفسیر هر معاهده، قانون، کنوانسیون و هر قراردادی بایستی با توجه به موضوع و هدف آن تفسیر گردد، با این قرائت، برای تحلیل هدف منشور، مقدمه، مقررات مندرج در متن آن با توجه به ارتباط بندهای آن با یکدیگر تفسیر گردند. رویکرد دیگر، رویکرد موسع است، بنابراین مقدمه باید موسع‌تر از عبارات مندرج در مقرراتی که بدنه معاهده را تشکیل می‌دهند، تفسیر شوند؛ زیرا مفاد منشور برای تحقق آرمان‌های مقدمه طراحی شده است و ازآنجایی‌که مقدمه صریحاً به استفاده از زور در قالب توسل به نیروی نظامی اشاره می‌کند، بند ۴ ماده ۲ را نمی‌توان به طور گسترده‌تر تفسیر کرد، به نحوی که شامل اجبار اقتصادی یا سیاسی باشد. برخی از نویسندگان با انتقاد از رویکردهای فوق اعتقاد دارند که مفاد منشور بایستی به صورت مضیق تفسیر نمود، ازاین‌رو در تفسیر مضیق و تحت‌اللفظی مفاد بند ۴ ماده ۲ این موضوع ملاک قرار گیرد که تهیه‌کنندگان منشور عمداً ترجیح داده‌اند به نیروی نظامی اشاره نکنند تا به ممنوعیت استفاده از زور دامنه وسیع‌تری بدهند، حال اگر نویسندگان منشور قصد اشاره به استفاده از نیروی نظامی را داشتند، قطعاً واژه نیروی نظامی را در بند ۴ ماده ۲ به صراحت قید می‌کردند. علیرغم جذابیت تفسیر فوق، این رویکرد مورد پذیرش تدوین‌کنندگان منشور قرار نگرفته است؛ زیرا در طول کنفرانس سانفرانسیسکو در سال ۱۹۴۵ که طی آن منشور تدوین شد، برخی از کشورها پیشنهاد کردند که اجبار

[1] Schmitt

[2] Nolte/Randelzhofer

اقتصادی به عنوان استفاده از زور در متن گنجانده شود، اما در نهایت این متن تصویب نشده و مجدداً در سال ۱۹۷۰، در جریان مذاکرات مربوط به تهیه پیش‌نویس قطع‌نامه مجمع عمومی سازمان ملل متحد در مورد روابط دوستانه و همکاری بین کشورها، این سؤال مجدداً مطرح شد که آیا اصطلاح زور شامل کلیه اشکال فشارها از جمله فشارهایی که با ماهیت اقتصادی یا سیاسی بر یک کشور تحمیل می‌گردد یا تأثیر بر تهدید تمامیت ارضی یا استقلال سیاسی یک دولت دارد می‌گردد یا خیر؟ در نهایت پاسخ منفی داده شد و محدودیت اقتصادی در اصل عدم مداخله گنجانده شد.[1] بنابراین، حتی اگر «زور» در مفهوم بند ۴ ماده ۲ به طور دقیق تعریف نشده باشد، شامل اجبار اقتصادی و سیاسی نمی‌شود. اما تفسیر دیگر مبتنی بر رویکرد منطقی به موضوعات بین المللی است و اعتقاد دارد وجود این استدلال‌ها، قاعده تفسیر کلی مندرج در ماده ۳۱ کنوانسیون وین برای تصمیم‌گیری بین تفسیر مبسوط و تفسیر محدود کافی نبوده و بهتر است که به اسناد تفسیری تکمیلی پیشنهاد شده در ماده ۳۲ کنوانسیون وین استناد شود. زیرا علیرغم قرابت نزدیک بین مرزهای اصطلاح «زور» در بند ۴ ماده ۲ با مرزهای عبارت «تجاوز مسلحانه» در ماده ۵۱ منشور، اما اصطلاح «زور» در منشور با هم انطباق ندارند (دینیس،۲۰۱۴:۴۷).[2] بنابراین، دیوان بین‌المللی دادگستری، در حکمی درباره فعالیت‌های نظامی و شبه‌نظامی در نیکاراگوئه، اعلام کرد که آموزش، تأمین تسلیحات یا هر نوع حمایت دیگری ممکن است به منزله استفاده غیرقانونی از زور باشد که فراتر از استفاده صرف از نیروی مسلح است. همان طور که دیوان بین المللی دادگستری در نظر خود در مورد قانونی بودن تهدید یا استفاده از سلاح‌های هسته‌ای اعلام کرد، ممنوعیت استفاده از زور «صرف نظر از سلاح‌های مورد استفاده» قابلیت تحقق دارند و در این مورد نمی‌توان صرفاً به توسل به نیروی نظامی به عنوان مصداق زور اکتفا نمود (مور،۲۰۱۰:۲۲۶).[3] با این تفسیر استفاده از سلاح‌های رایانه‌ای نیز مانند استفاده از سلاح‌های متعارف، شیمیایی یا بیولوژیکی می‌تواند به منزله استفاده از زور تلقی گردد و یک ارتباط منطقی بین مصادیق زور فراهم می‌گردد. اگر با نگرشی به فلسفه منشور نگاه شود، امروزه با توجه تغییر نحوه تجاوز و مداخلات و پیشرفت تکنولوژی، نگرش به واژه زور با قالب سنتی امکانپذیر نمی‌باشد؛ زیرا دولت امریکا در مورد شهادت سردار قاسم سلیمانی در عراق و دکتر فخری زاده در دماوند از این نوع سلاح‌ها استفاده نموده که خود از مصادیق استفاده از زور می‌باشد.

۶ حملات سایبری به عنوان مصادیق استفاده از زور

ازآنجایی‌که واژه «استفاده از زور» بایستی مستقل از نوع تسلیحات مورد استفاده مورد توجه و تحلیل قرار گیرد، این تغییر نگرش موجب شده، تفاسیری که از زور ابراز می‌گردد با رویکردهای جدید بازشناسی شوند و از طرفی در نگرش‌های تحلیل مفهوم زور، اشکال این مفهوم بایستی با تحلیل واقعی تفسیر شوند؛ زیرا عملیات سایبری از نظر تئوری، به استفاده از زور شباهت دارد.

هرچند نمی توان نتیجه گرفت که یک حمله سایبری همیشه به معنای استفاده از زور می باشد؛ زیرا این حملات می‌توانند با وسایل و در مقیاسی متفاوت انجام شوند. بنابراین تجزیه و تحلیل حملات سایبری بایستی مورد به مورد صورت پذیرد. از تفاسیر متفاوت دیوان بین‌المللی دادگستری یا مجمع عمومی سازمان ملل متحد دو نتیجه گرفته می‌شود. اول اینکه، اجبار اقتصادی یا سیاسی به معنای استفاده از زور مندرج در بند ۴ ماده ۲ نمی-

[1] Résolution 26/25 (XXV) de l'Assemblée générale relative aux principes du droit international touchant les relations amicales et la coopération entre Etats conformément à la Charte des Nations Unies du 24 octobre 1970.

[2] Dinniss
[3] Mohr

باشد. دوم اینکه، استفاده از نیروی نظامی به معنای استفاده از زور به معنای استفاده از زور مندرج در بند ۴ ماده ۲ می‌باشد. حال با توجه به تفسیر متناقض می‌توان حمله سایبری را از مادیق زور تلقی نمود یا خیر، در خصوص حملات سایبری به عنوان استفاده از زور سه نظریه از جانب متخصصین حقوق و روابط بین‌الملل ارائه شده است، رویکرد اول، رویکردی ابزارگرا یا مبتنی بر ابزار به موضوع دارد، رویکرد دوم مبتنی بر هدف بوده و اهداف را مورد بررسی قرار می دهد و رویکرد سوم رویکرد مبتنی بر پیامدهاست.

رویکرد اول یا ابزارگرا تمرکز بر حمله دارد. طرفداران این رویکرد اعتقاد دارند اگر حملات سایبری ویژگی‌های فیزیکی را که به طور سنتی با یک عملیات نظامی مرتبط است، نشان دهند، عملیات سایبری معنای استفاده از زور را خواهد داشت. اما قرائت دوم معتقد است هنگامی که زیرساخت‌های ملی حیاتی هدف قرار گیرد، این عملیات به معنای استفاده از زور تلقی می‌شود و نهایتاً رویکرد سوم پیامدهای حمله را به عنوان یک کل در نظر می‌گیرد و به دنبال تجزیه و تحلیل این است که آیا اثرات عملیات به اندازه کافی جدی بوده که آن را به عنوان استفاده از زور واجد شرایط ارزیابی کند. لذا با توجه به اهمیت موضوع توصیف و تحلیل هریک از رویکردها ضروری می‌باشد.

۷ رویکرد ابزارگرا

رویکرد ابزارگرا یک تفسیر وسیع از ابزار دارد؛ لذا در این راستا ابزاری را در نظر می‌گیرد که توسط آن یک دولت به استفاده از زور متوسل می‌شود. قرائت طرفداران فوق این است که یک کشور ممکن است به مدد نیروی اقتصادی، دیپلماتیک/سیاسی یا مسلح، به عملیات نظامی متوسل شود (بناتر،۲۰۰۹:۳۸۸).[1] از نظر ابزارگراها یک عملیات تنها زمانی به عنوان استفاده از زور مشمول بند ۴ ماده ۲ می‌گردد که دارای ویژگی فیزیکی و نظامی باشد. اینان اجبار سیاسی یا اقتصادی را از شمول بند ۴ ماده ۲ منشور مستثنی می‌کنند، این رویکرد بر ابزارهای مورد استفاده متمرکز است و بیشتر به استفاده از سلاح‌های نظامی سنتی توجه دارد. گرچه با یک سری پیش‌فرض‌هایی گرچه محدود برخی از عملیات سایبری را به عنوان استفاده از زور شناسایی می‌نماید، اما هیچ تعریف دقیقی از ماهیت نظامی یک عملیات و به‌خصوص که تکنیک‌های مورد استفاده که به‌سرعت در حال تغییر هستند، اشاره نمی‌کند (نگوین،۲۰۱۳،۱۱۱۸).[2] امروزه تحت تأثیر تنوع تکنیک‌های نظامی و توسعه فناوری‌های نظامی یک تغییر نظری در رویکرد ابزارگرا ایجاد کرده است (حیدری نسب،۱۴۰۰:۱۴۳) و برخی از نویسندگان پیشنهاد می‌کنند با توجه به اینکه ماهیت نظامی حملات سایبری دارای همان تکنیک استفاده از زرادخانه ارتش یک دولت بوده؛ لذا این موارد بایستی به عنوان مصادیق زور فرض شوند. این تغییر نگرش موجب گردیده بسیاری از دولت‌ها واحدهای دفاع سایبری تحت عنوان ارتش سایبری را تحت نظر نیروهای مسلح ایجاد کنند تا در صورت حملات سایبری از طریق ابزارهای سایبری تخصصی از خود دفاع دارند، بنابراین می‌توان گفت که عملیات سایبری می‌تواند جنبه نظامی داشته باشد.

علیرغم توصیفات فوق، برخی از نویسندگان معیار دوم را اضافه می‌کنند که مربوط به ماهیت فیزیکی عملیات است، از نظر اینان ویژگی فیزیکی یک عملیات به طور کلی به معنای تولید یک موج ضربه‌ای و یک اثر انفجاری است. بر اساس این رویکرد، یک حمله سایبری به‌تنهایی و در صورتی که هیچ موج ضربه و اثر انفجاری به دنبال داشته باشد، نمی‌تواند به منزله استفاده از زور باشد، زیرا فاقد ویژگی فیزیکی مرتبط با اجبار نظامی است. اینان با تفکیک عملیات با ماهیت انفجاری از غیرانفجاری اعتقاد دارند، یک حمله سایبری که از طریق استفاده از کدهای رایانه‌ای صورت می‌گیرد که به اندازه کافی شبیه سلاح‌های متعارف نبوده و ویژگی فیزیکی

[1] Benatar

[2] Nguyen

مرتبط با اجبار نظامی را ندارند (هالیس،۲۰۰۷:۱۰۴۱). زیرا یک حمله سایبری به خودی خود باعث آسیب فیزیکی انفجاری نمی‌شود، حتی اگر علت انفجار و با هدف از کار انداختن سیستم‌های رایانه‌ای صورت گرفته باشد. این رویکرد نظریه خود را با این واقعیت تقویت می‌کند که ماده ۴۱ منشور سازمان ملل متحد قطع کامل یا جزئی روابط از طریق تلگراف، رادیو و سایر وسایل ارتباطی را از شمول توسل به زور مستثنی کرده است، انتقادات وارده به نظریات طرفداران رویکرد ابزارگرا موجب شده، تئوری‌پردازان ابزارگرای جدید با اتکا بر آمیزه‌های رویکرد ابزارگرا و واقع‌گرایی، مفروضات سابق خود را تعدیل کنند و ابراز دارند اگر استفاده از حملات سایبری شبیه به استفاده از سلاح‌های نظامی باشد، هرچند ماهیت فیزیکی آن را نداشته باشد، مانع از تعمیم استناد به زور در مفهوم بند ۴ ماده ۲ منشور نخواهد بود. اما انتقاد اصلی به قرائت رویکرد ابزارگرا این است که موارد و مصادیق زور را بیش از حد محدود و به طور غیر ضروری برخی از حملات سایبری را از مصادیق زور مستثنی و آن را مشروط به ماهیت فیزیکی عملیات می‌کند. لذا با توجه به تحول مفهوم زور نمی‌توان کلیه عملیات سایبری را که با هدف خارج کردن شبکه‌ها و سیستم‌های رایانه‌ای خاص بدون ایجاد آسیب مستقیم می‌گردند و حیات سیاسی، اقتصادی، نظامی و حاکمیتی دولت را مورد تعرض قرار می‌دهند، از زور مستثنی کرد و صرفاً به حملاتی بسنده نمود که می‌تواند به طور غیر مستقیم باعث آسیب فیزیکی، مانند انفجار شود. هرچند برخی از عملیات سایبری درواقع به استفاده از تکنیک‌های نظامی شباهت دارند. هرچند برخی دیگر از حملات مشابهت به عملیات نظامی ندارد؛ اما به مراتب مخرب‌تر از حملات نظامی بوده و حاکمیت اقتصادی سیاسی دولت‌ها را هدف و تعرض قرار دهند و بایستی با استناد به مفاد منشور به عنوان مصادیق زور مورد شناسایی قرار گیرند. گرچه به‌سختی می‌تواند شبیه به یک عملیات نظامی باشد.

[1] Hollis

ازآنجایی‌که این رویکرد فقط ماهیت نظامی و فیزیکی یک عملیات را در نظر می‌گیرد و بسیاری از حملاتی را که عواقب جدی ایجاد می‌کنند استثنا می‌کند، اما با وجود این، ایجاد تمایز براساس جدیت پیامدها به منزله استفاده از رویکرد مبتنی بر پیامد در کلیه موارد قابلیت تعمیم نخواهد داشت. به عنوان مثال حمله استاکس‌نت به منزله استفاده از زور است؛ زیرا این عملیات با استفاده از یک ویروس رایانه‌ای و نه با موشک یا سلاح معمولی انجام شده است و موجبات موج انفجاری شده اما اگر رویکرد کلاسیک ابزارگرایی مناط قرار گیرد، چنین حمله سایبری از مصادیق زور محسوب نخواهد شد.

۸ رویکرد مبتنی بر هدف

قرائت رویکرد مبتنی بر هدف یک عملیات سایبری را زمانی که هدف آن نفوذ به سیستم‌های زیرساخت ملی و حیاتی باشد، استفاده از زور تلقی می‌گردد، حتی اگر عملیات آسیب جدی به این سیستم‌ها وارد نکند (هالیس،۱۰۴۱)، برخی از نویسندگان همچنین از رویکرد مسؤولیت سخت سخن می‌گویند. قرائت مذکور با این ایده توجیه می‌شود که امروزه عملکرد صحیح این زیرساخت‌ها در جوامع مدرن به طور خاص به سیستم‌های رایانه‌ای وابسته بوده و عملیاتی که با ابزارهای غیرنظامی به معنای کلاسیک مانند حملات سایبری انجام می‌گردد، این امکان را فراهم می‌نماید تا آسیب‌های قابل توجهی به زیرساخت‌ها وارد گردد؛ زیرا حملات سایبری زیرساخت‌های حیاتی یک کشور را تضعیف کند. بر خلاف رویکرد ابزارگرا، رویکرد مبتنی بر هدف صرفاً عملیات بسیار گسترده و محدود را واجد ماهیت زور می‌داند. هرچند برخی از عملیات که زیرساخت‌های حیاتی را هدف قرار دهند و اثراتی در مقیاس بزرگ ایجاد نمی‌کند، مشمول توسل به زور خواهند شد.

لذا عملیات سایبری با هدف غیر قابل دسترس کردن خدمات دولتی خاص و وب‌سایت‌های یک کشور حتی برای چند دقیقه بایستی به عنوان

استفاده از زور شناخته شوند. هرچند این وب‌سایت بلافاصله پس از آن دوباره به طور معمول عمل کنند. با توجه به رویه‌های فعلی دولت‌ها در حقوق بین‌الملل و نظر اکثر حقوقدانان، چنین عملیاتی از درجه ثقل کافی برای شمولیت استفاده از زور در معنای بند ۴ ماده ۲ برخوردار نبوده، زیرا هیچ تعریفی از آن چه که زیرساخت ملی حیاتی را تشکیل می‌دهد در حقوق بین‌الملل وجود ندارد. اما زیرساخت‌های حیاتی و ملی به طور کلی به زیرساخت‌هایی اطلاق می‌گردند که تخریب آن‌ها می‌تواند تأثیر جدی بر امنیت، اقتصاد ملی یا سلامت عمومی یک کشور داشته باشد. به‌ویژه در صورتی که بخش‌های انرژی، تأمین آب، بانک‌داری، حمل‌ونقل و ارتباطات مورد هدف قرار دهند. با اتخاذ رویکرد مبتنی بر هدف، موارد بسیاری از حملات سایبری می‌توانند مشمول استفاده از زور واجد تلقی شوند و دلیل این امر نیز مبتنی بر این است که منطقه هدف توسط دولت قربانی به عنوان یک ضرورت حیاتی در نظر گرفته شده است. یکی از انتقادات وارده به رویکرد مبتنی بر هدف این است که دامنه و مفهوم یک عملیات را به عنوان استفاده از زور را بیش از حد توسعه می‌دهد و این امر خطرات تشدید تنش بین روابط بین کشورها را به دنبال دارد.

۹ رویکرد مبتنی بر اثرات

رویکرد مبتنی بر اثرات مورد علاقه اکثر نویسندگان است و رویکرد مذکور توجهات حقوق‌دانان کشورهایی مانند ایالات متحده و گروهی از کارشناسان کتابچه راهنمای تالین را به خود معطوف نموده است، رویکرد مذکور بر این اصل استوار است که یک حمله سایبری اثراتی معادل استفاده از زور را دارد، زیرا با ابزارهای خاص زمینه تخریب اموال یا تهدید جان انسان‌ها را فراهم می‌کند و در این فرآیند خسارت‌های مالی به اموال و تهدیدات جسمانی، مرگ و آسیب شهروندان یک کشور را به همراه دارد که این امر می‌تواند از مصادیق استفاده از زور قلمداد گردد. از نظر نویسندگان کتاب راهنمای تالین، «عملیات سایبری زمانی استفاده از زور تلقی می‌گردد که ابعاد و اثرات آن با عملیات غیر سایبری که به سطح استفاده از زور می‌رسد، قابل مقایسه باشد» (اشمیت،۲۰۱۷: ۱۱)[1]. متخصصین روابط بین-الملل و حقوق بین‌الملل با توسل به قیاس، استدلال می‌نمایند عملیات سایبری در صورتی که اثراتی مشابه عملیات جنگی داشته باشد، استفاده از زور محسوب می‌گردد. لذا به باور طرفداران رویکرد مبتنی بر اثر، تحلیل تأثیرات حمله این امکان را فراهم می‌کند که عملیات خاصی را به طور نسبی به عنوان استفاده از زور قلمداد نمود؛ زیرا این امر به‌ویژه در مورد عملیاتی که باعث تخریب اموال یا مرگ افراد شود صدق می‌نماید. ازاین‌رو پیامدهای چنین حملات سایبری در برخی موارد از جمله حملات سایبری به راکتورهای سایت هسته‌ای، آسیب رساندن به سیستم‌های کنترل ترافیک هوایی یا باز کردن درب سدها که منجر به سیل شود، اثرات تخریبی آن از جنگ‌های مسلحانه به مراتب بیشتر خواهد بود.

رویکرد مبتنی بر اثرات با توجه به اینکه امکان حذف برخی عملیات را که پیامدهای بسیار اندک دارند به عنوان مفهوم استفاده از زور می‌دهد، طرفداران بیشتری نسبت به رویکردهای سابق‌الذکر دارد. گرچه بر اساس انگاره‌های فوق، مؤلفین کتاب راهنمای تالین، یک عملیات روانی و غیر مخرب را که با هدف تضعیف اعتماد عمومی به یک دولت یا یک اقتصاد می‌شود در برخی وضعیت‌ها به عنوان مصداق زور در نظر می‌گیرد، اما پیامدهای کلیه عملیات سایبری را که با هدف تضعیف دولت و سیستم اتخاذی دولت برای اداره اقتصاد کشور باشد از شمول عملیات سایبری از مصادیق زور مستثنی می‌کند. مفهوم مخالف این امر این است که عملیات مذکور بر اساس قوانین بین المللی قانونی فرض می‌شود؛ زیرا به آستانه استفاده از زور نمی‌رسد. به اعتقاد سیمونت، روش مبتنی بر اثرات، مناسب‌ترین روش در زمینه حملات سایبری می‌باشد و درواقع،

[1] Schmitt

«عمل تجاوز رایانه‌ای از این جهت منحصر به فرد است که گرانش آن به مکانیسم وقوع آن (نفوذ یک ویروس یا یک کرم در یک شبکه رایانه‌ای) نیست، بلکه پیامدهای بالقوه آن را که بر زندگی انسان‌ها یا جمعیت یک کشور تأثیرگذار باشد، در نظر می‌گیرد (سیمونت،۲۰۱۲:۱۲۴). [1]

به رغم کثرت طرفداران رویکرد اخیرالذکر اما رویکرد مذکور از ایرادات مصون نمانده باشد، عمده‌ترین ایراداتی که به این نظریه وارد شده این است که به اثراتی که عملیات سایبری ایجاد می‌کند، اهمیت زیادی می‌دهد و این ویژگی حملات سایبری را در نظر نمی‌گیرد که می‌تواند آسیب منحصر به فردی ایجاد کند که حملات سنتی نمی‌تواند ایجاد نماید. از این رو بر اساس رویکرد مبتنی بر اثرات، چنین حمله‌ای، هرچند می‌تواند هزینه‌های انسانی و مادی زیادی را به همراه داشته باشد، اما مشمول استفاده از زور بدان سیاق که در بند ۴ ماده ۲ منشور پیش‌بینی شده است، نخواهد بود. برخی از اندیشمندان با تحلیل اثرات یک حمله اعتقاد دارند یک حمله سایبری که نتواند اثرات مورد نظر را ایجاد کند، به عنوان استفاده از زور تلقی نخواهد شد (نگوین، همان:۱۱۲۲).

یکی از بارزترین انتقاداتی که به نظریه شده این است که این رویکرد فاقد بازدارندگی بوده؛ زیرا پاسخ مناسبی نسبت به اثرات ناخواسته حملات هسته‌ای پیش‌بینی و راهکار مناسب با توجه به شرایط فعلی جهان ارائه نمی‌کند. به همین استناد مورد انتقاد بسیاری از متخصصین حوزه امنیت بین‌المللی است.

اما با توجه به موارد فوق هر یک از رویکردها مزایا و معایبی دارند. اما رویکرد مبتنی بر اثرات همان طوری که در اعلامیه‌ها، گزارش‌ها بیان می‌گردد مورد توجه اکثر دکترین‌ها و دولت‌ها بوده؛ زیرا حداقل ایرادات به آن وارد شده و از این منظر به نظر می‌رسد متعادل‌ترین رویکردهای فعلی باشد. اگر حمله سایبری به معنای استفاده از زور تلقی گردد تاب این تفسیر را دارد که برابر بند ۴ توسط ماده ۲ ممنوع اعلام شود. با این توصیف زمانی که این اثرات برابر با اثرات یک عملیات انتحاری باشد، به عنوان استفاده از زور شناخته می‌شود. ازآنجایی‌که مفهوم زور شامل اجبار ساده سیاسی یا اقتصادی نمی‌شود، حملات سایبری که اثرات آن‌ها محدود به حوزه اقتصادی، سیاسی یا دیپلماتیک است، نباید به عنوان استفاده از زور تلقی شود. هرچند این اعمال لزوماً بر اساس قوانین بین‌المللی قانونی نیستند. اما تلقی نمودن مصادیق فوق به عنوان استفاده از زور، طیف وسیعی از گزینه‌ها و واکنش‌های متفاوت را به سهولت در اختیار دولت قربانی می‌گذارد (طلس،۲۰۱۹:۲۸۹).

۱۰ تحلیل حملات سایبری دارای آستانه جدیت

انتقادات وارده به نظریات فوق موجب گردیده برخی از حقوقدانان زور را به مفهوم تجاوز مسلحانه تحلیل کنند؛ زیرا حملات رایانه‌ای در مفهوم واقعی عملی است که لزوماً به منزله استفاده از زور تلقی می‌گردد. این دسته از اندیشمندان با استناد به رأی دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه اعتقاد دارند، مفهوم زور الزماً مساوی با به‌کارگیری نیروی نظامی نبوده، اما به رغم نگرش فوق اکثر حملات سایبری به سطح یک حمله مسلحانه نمی‌رسند. بنابراین در مواردی که حملات سایبری به آستانه حمله مسلحانه نرسد چگونه می‌توان این گونه اقدامات را به عنوان استفاده از زور شناخت. از تفسیر رأی دیوان در مورد فعالیت‌های نظامی و شبه‌نظامی در نیکاراگوئه، این استنباط می‌گردد که دیوان بین‌المللی دادگستری بین «جدی‌ترین اشکال استفاده از زور (آن‌هایی که تهاجم مسلحانه را تشکیل می‌دهند) و سایر روش‌های خفیف‌تر تمایز

[1] Simonet

قائل شده است.[1] بنابراین به نظر می‌رسد نوعی درجه‌بندی در همان دسته از اعمالی که به عنوان «استفاده از زور» شناخته می‌شوند، وجود دارد. با وجود این، اتفاق نظر در خصوص تمایز درجه-بندی‌های موجود بین دکترین و دولت‌ها اتفاق نظر وجود ندارد. به‌ویژه اینکه در پی این قضاوت، ایالات متحده اعلام کرده که هرگونه تفسیری را که تفاوت بین استفاده از زور و حمله مسلحانه و غیر آن باشد به رسمیت نمی‌شناسد؛ زیرا اگر اقداماتی به عنوان استفاده از زور تلقی گردد، این امر به یک دولت حق می‌دهد اقدامات متجاوز را با اقدامات دفاعی و نظامی پاسخ دهد.

واقعیت این است که اکثریت دولت‌ها و نویسندگان این تفاوت را به رسمیت می‌شناسند و به این نتیجه می‌رسند که عملیاتی که به عنوان یک حمله مسلحانه در مفهوم ماده ۵۱ منشور ملل متحد شناخته می‌شود، لزوماً به منزله استفاده غیر قانونی از زور تلقی می‌گردد. از سوی دیگر در این زمینه با یک پارادوکس مواجه بوده؛ زیرا عملیاتی که به عنوان استفاده از زور شناخته می‌شود، لزوماً یک حمله مسلحانه نیست؛ اما این حق را برای دولت ایجاد می‌کند که در دفاع از خود واکنش نشان دهد. لذا تعریف تجاوز مسلحانه - مانند استفاده از زور - همچنان موضوع بحث در حقوق بین‌الملل است، به نظر می‌رسد اگر عملیاتی به اندازه کافی جدی باشد و منجر به تخریب اموال و یا ایجاد خسارت جانی شود، عموماً یک حمله مسلحانه تلقی می‌شود و در نتیجه مصداق استفاده از زور و یک حمله مسلحانه را خواهد داشت، به همین دلیل بر اساس روش مبتنی بر اثرات، حمله سایبری که اثرات مستقیم آن منجر به تخریب اموال و یا تلفات جانی انسانی می‌شود، مشمول استفاده از زور و حتی حمله مسلحانه در مفهوم ماده ۵۱ می‌شود. از طرفی دیگر مواد ۲ (بند ۴) و ۵۱ منشور ملل متحد کارکرد یکسانی ندارند. بند ۴ ماده ۲ اصل منع توسل به زور را صرفاً شامل تجاوز مسلحانه می‌داند. حال اگر حملات سایبری آستانه جدیت را داشته باشند، تشخیص اینکه یک کشور قوانین بین‌المللی را نقض کرده به سهولت صورت می‌پذیرد. هرچند ماده ۵۱ به دولت‌ها اجازه می‌دهد استفاده قانونی از زور را برای دفاع از خود مشروع بداند (لوتریونته،۲۰۱۲:۱۹).[2] برخی از عملیات سایبری قابلیت تشابه توسل به زور فراتر از محدودیت‌های اقتصادی یا سیاسی ساده را بدون اینکه به اندازه کافی جدی واجد وصف تهاجم مسلحانه باشند، دارا می‌باشند؛ زیرا این اعمال بسته به شرایطی قابلیت شناسایی به عنوان توسل به زور در معنای بند ۲ ماده ۲ را دارند و در مورد اعمال در فضای سایبری نیز صدق می‌کند. با این حال، فقدان اجماع بین‌المللی در مورد اینکه حملات سایبری به معنای توسل به زور بوده، نیل به یک تعریف واحد را دشوار می‌سازد. پرفسور اشمیت در این خصوص پیچیده‌ترین نظریه را ارائه کرده است و بر همین اساس در کتاب راهنمای تالین به معیارهای اشمیت اشاره شده و اشمیت با تحلیل‌های خود به این نتیجه می‌رسد که با تکیه بر برخی از نظریات می‌توان ابراز داشت که جامعه بین-المللی بایستی یک حمله سایبری را واجد شرایط زور قلمداد کند (اشمیت،۱۹۹۹:۹۱۶). اشمیت با با لحاظ معیارهای کیفی بین عملیاتی که ترجیحاً به عنوان اجبار اقتصادی یا سیاسی شناخته می‌شود و عملیاتی که به آستانه استفاده از زور می‌رسد، تمایز قائل می‌گردد. البته این‌ها معیارهای رسمی و تأیید شده نیستند، بلکه این زمینه را فراهم می‌سازد که بر تصمیم دولت‌ها تأثیر گذارند. با این قرائت عملیاتی به عنوان استفاده از زور توصیف می‌شود که دارای شرایطی باشند. بنابراین با در نظر گرفتن معیارهایی مانند: شدت، فوری بودن، مستقیم بودن حمله، درجه تهاجم، قابلیت اندازه‌گیری اثرات، ویژگی نظامی عملیات، درجه دخالت دولت و قانونی بودن احتمالی عملیات توجیه‌پذیر می‌گردد. اما در بین

[1] Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique), CIJ, Recueil 1986.

[2] Lotrionte

ملاک‌های فوق‌الذکر، شدت قطعاً مهم‌ترین ملاک است. لذا حمله سایبری که منجر به مرگ افراد یا تخریب زیرساخت‌های یک کشور می‌شود، بایستی به عنوان استفاده از زور مورد شناسایی قرار گیرد. درحالی‌که حمله‌ای که فقط باعث ایجاد نگرانی و مزاحمت صرف شود، به آستانه استفاده از زور نمی‌رسد از دامنه شمول زور مستثنی می‌گردند. لذا با اجتناب از افراط، می‌توان حمله‌ای را که پیامدهایی برای منافع حیاتی ملی داشته باشد، به عنوان استفاده از زور تلقی کرد و برای ارزیابی شدت حمله، باید وسعت، مدت و شدت آن را نیز در نظر گرفت.

ازآنجایی‌که لحاظ معیار شدت به سهولت قابلیت اعمال را نخواهد داشت، معیارهای دیگری که بر تصمیم یک دولت برای واجد شرایط بودن عملیات به عنوان استفاده از زور تأثیر می‌گذارند، عبارت خواهد بود از فوری بودن حمله. این مؤلفه‌ها بایستی بر تصمیم دولت تأثیر گذارد. نظر به اینکه شدت و فوریت پیامد یک عملیات را زودتر آشکار می‌سازد؛ زیرا این گزاره‌ها به دولت‌ها کمترین فرصت برای متوسل شدن به اقدامات صلح‌آمیز برای محدود کردن اثرات مضر آن می‌دهد. بنابراین، کشورها تمایل دارند تا یک حمله سایبری را که نتایج آن فوراً حاصل می‌گردد به عنوان استفاده از زور ارزیابی و آن را تهدید قریب الوقوع تلقی نمایند، علاوه بر موارد فوق ماهیت مستقیم حمله نیز بایستی در نظر گرفته شوند. ازاین‌رو فقدان واسطه حمله به موقتی بودن آن ارتباط می‌یابد، درحالی‌که مستقیم بودن به علیت بین عملیات و پیامدها ارتباط پیدا می‌نمایند، دستورالعمل تالین به تفصیل توضیح می‌دهد که در چارچوب اقدامات اجباری اقتصادی، مانند تحریم‌ها، عواقب آن بعد از چندین هفته یا حتی ماه‌ها احساس می‌شود. از سوی دیگر، عملیات نظامی کلاسیک اثرات آنی بیشتری دارند و حملات هوایی یا اعزام نیروی زمینی عواقب آن تقریباً فوری است. اما در برخی موارد تأثیرات مستقیم یک عملیات سایبری به مراتب بیشتر از حملات نظامی است. مضاف بر معیارهای فوق، معیار تهاجم، ماهیت هدف مورد نظر و اهمیت آن برای دولت قربانی یک عملیات سایبری را هم بایستی لحاظ نمود. ازاین‌رو هر چه هدف به سهولت انجام پذیرد، این قبیل موارد می‌تواند به عنوان تهدیدی برای دولت قربانی لحاظ گردند و امکان شناسایی آن به عنوان استفاده از زور وجود دارد. علاوه بر آن، عملیاتی که به این گونه انجام شود، تنها یک کشور را هدف قرار دهد، در مقایسه با عملیاتی که دولت‌های مختلف را بدون تفکیک هدف قرار می‌دهد، احساس تهدید را برای دولت‌های قربانی افزایش می‌دهد.

با اتکا بر معیارهای فوق می‌توان ابراز داشت زمانی که پیامدهای حملات سایبری آشکار باشد، معیار سنجش‌پذیری اثرات با واقعیت سنجیده می‌شود که دولت‌ها تمایل بیشتری به توصیف یک عملیات سایبری به عنوان استفاده از زور دارند. اما اعمال این معیار در فضای مجازی کمی دشوار به نظر می‌رسد. واقعیت این است که اگر عواقب حملات سایبری قابلیت اندازه‌گیری و شناسایی داشته باشد، احتمال بیشتری وجود دارد که به عنوان استفاده از زور شناخته شود. به عنوان مثال، اگر دولتی بتواند به طور دقیق میزان پیامد یک عملیات سایبری، تخریب داده‌ها، فایل‌های استخراج‌شده، تعداد سرورهای آسیب‌دیده و غیره را تعیین کند، اینکه عملیات سایبری به معنای استفاده از زور قابلیت شناسایی داشته باشد، ماهیت نظامی یک عملیات سایبری نیز نقش دارد؛ زیرا عملیات در این مورد شبیه یک حمله مسلحانه است که به منزله استفاده از زور است. زمانی که یک عملیات توسط ارتش یک کشور انجام شود، ویژگی نظامی خواهد داشت؛ زیرا ویژگی برخی از جنگ‌های سایبری این است که تخریب‌هایی به دنبال دارد که لزوماً همیشه همراه با کشتار نیست، اما عواقب جدی برای زیرساخت‌های حیاتی یک کشور به دنبال دارد. با این قرائت، تخریب وب‌سایت‌های یک کشور با حملات رگباری ویروس‌ها یا استفاده سلاح‌های مرگبار هدایت‌شونده با استفاده از فضای مجازی برای ترور شخصیت‌های یک کشور می‌تواند با

مفهوم زور در منشور قابلیت انطباق داشته باشند. تجربه شهادت دکتر فخری زاده و سایر ترورهایی از این دست نشان‌های بارز تروریستی سایبری هستند. علاوه بر این، افزایش تعداد مهاجمان و نقش حملات متقابل به گونه‌ای است که بیانگر وضعیت درگیری طولانی‌مدت بوده و این امر شناسایی ماهیت فضای مجازی را به عنوان قابلیت شناسایی مفهوم زور تسهیل می‌کند (شلوش،۲۰۱۸:۱۹۵). علاوه بر موارد فوق، معیار میزان مشارکت دولت راه‌اندازی کننده عملیات سایبری نیز نقش مهمی در این خصوص ایفا می‌کند،. هر چه دولت رهبری عملیات سایبری را عهده‌دار باشد و کمتر به «نمایندگان» یعنی واسطه‌ها متوسل شود، این فرآیند به دولت قربانی اجازه می‌دهد این عملیات را به عنوان استفاده از زور شناسایی کند (العربی،۲۰۱۸:۳۱). آخرین معیاری که باید رعایت شود، قانونی بودن مفروضات عملیات است. هرچند قواعد حقوق بین‌الملل ذاتاً برخی از اقدامات را منع کند، اما در برخی موارد برخی از اقدامات به صراحت توسط قواعد مذکور منع نشده‌اند و عدم ممنوعیت اصولاً در معنای جواز پاسخ متناسب دولت قربانی بوده و ازآنجایی‌که حقوق بین‌الملل صراحتاً و به طور کلی برخی از اقدامات مانند فشار ساده اقتصادی، تبلیغات، عملیات روانی یا جاسوسی را ممنوع نمی‌کند، چنین به ذهن متبادر می‌گردد که این دسته اقدامات از منظر حقوق بین‌الملل عموماً قانونی تلقی می‌شوند. بنابراین، عملیات سایبری را که پیامدهای آن معادل یکی از این مقوله‌های فوق باشد، بایستی قانونی تلقی نمود و از شمول استفاده از زور مستثنی گردند.

۱۱ نتیجه و پیشنهاد

نظریات ابراز شده در زمینه شناسایی حملات سایبری به عنوان مصادیق زور یا حمله نظامی با ایراد و انتقادات فراوانی همراه بوده و از طرفی اجماع بین‌المللی در این خصوص وجود ندارد. به عنوان نتیجه، می‌توان گفت، مدل اشمیت نسبت به مفاد منشور ظریف‌تر است؛ زیرا تمایز بین حملات مختلف را با توجه به شدت و اثرات غیر مستقیم آن‌ها در نظر می‌گیرد. لذا تجزیه و تحلیل مذکور این امکان را فراهم می‌سازدکه چه زمانی یک عملیات سایبری مصداق توسل به زور را دارا می‌باشد. اما استناد به این معیار با دشواری‌های خود همراه بوده و عمده‌ترین انتقاد وارده به مدل اشمیت اتکای بیش از حد بر معیارهای ذهنی است. لذا در راستای تضمین حقوقی پیامدها و آثار حملات سایبری گرایش بسیاری از نویسندگان و برخی از دولت‌ها بر تعریف مجدد مفهوم زور در زمینه سایبری است. از طرفی برخی از نظریات تمایل دارند با شناسایی حملات سایبری به منزله توسل به زور به اختیار دولت‌ها مضاعفی تفویض نمایند، اما اختیارات مضاعف و فقدان اجماع این خطر را ایجاد می‌کند که دولت هادی مقام دفاع و عملیات تدافعی اقداماتی را با گستردگی خاص دنبال نمایند و با تفسیر آن به عنوان توسل به زور فراتر از اقدامات تدافعی عملیات نظامی را انجام دهند و جهان را با بحران مواجه سازند. لذا این گزاره خطر تشدید مقابله از سوی دولت قربانی را توجیه و امکان سوء استفاده دولت مذکور را در پی خواهد داشت.

لذا پیشنهاد می‌گردد، برای ارائه یک چارچوب قانونی مؤثر برای شمولیت عملیات سایبری به عنوان توسل به زور، شدت پیامدهای یک حمله برای حاکمیت یک دولت و صلح و امنیت بین‌المللی در نظر گرفته شوند و مضاف بر این، بایستی اثرات برگشت‌پذیر یا غیرقابل برگشت یک حمله سایبری و همچنین هدف یک حمله را، بدون استفاده از رویکرد مبتنی بر هدف که عواقب را نادیده می‌گیرد، لحاظ نمود. بنابراین، یک حمله سایبری زمانی که هدف آن ایجاد آسیب فیزیکی در مقیاس بزرگ و غیرقابل برگشت با حمله به سیستم‌ها و شبکه‌های رایانه‌ای باشد که یک جامعه برای عملکرد مناسب خود به آن وابسته است، بایستی به عنوان مصداق توسل به زور شناسایی شود؛ زیرا کلیه عملیات سایبری این قابلیت را ندارند که آستانه استفاده از زور مندرج در بند ۴ ماده ۲ را داشته باشند. هرچند

به لحاظ عرف بین‌المللی، قابلیت تقبیح را داشته باشند. ازاین‌رو ضرورت دارد سازمان ملل متحد و شورای امنیت با توجه به اصل منع توسل به زور که در منشور ملل متحد بیان شده، قوانین حاکم بر فضای سایبری برای اتخاذ روشی مناسب برای به-کارگیری آن وضع کند، به‌طوری‌که کاربرد حوزه ارتباطات و انقلاب دیجتال به جای کاربرد آن در منازعات، درگیری‌ها و جنگ‌ها در خدمت رفاه کشورها به طور عام و مردم به طور خاص قرار گیرد.

منابع

احمدی، زهرا، ۱۳۹۳، جنگ سایبری، ادامه‌ای برای جنگ تن به تن، تهران: مؤسسه پارسا مبتکر گام اول، هوشمند تدبیر.

آهنی امینه، محمد، فتح اللهی، فاطمه زهرا، ۱۳۹۳، حقوق بین مدرن در مواجهه با جنگی پست مدرن (نبرد سایبری)، فصل‌نامه راهبرد، شماره ۱۲۱-۱۴۹:۷۲

اندیشکده برهان، ۱۳۹۹، ریشه‌های نفوذ: واکاوی راهبردها و اقدامات نظام سلطه در پیشبرد نفوذ فکری، تهران: انتشارات دیدبان.

العربی، شحاته، تصاعد التهدیدات الامنیه للشرکات التکنولوجیه الکبری، **اتجاهات الاحداث**، ابوظبی، العدد۲۸.

المجذوب، محمد، ۲۰۱۸، **الوسیط فی القانون الدولی العام**، المنشورات الحلبی الحقوقیه، بیروت الطبعه السابعه.

پارسا، علی، ۱۳۸۹، «سرانجام راز استاکس‌نت کشف شد: هدف تأسیسات غنی‌سازی اورانیوم نطنز». وبگاه وین بتا، در ۲۴ نوامبر ۲۰۱۰. و «روایتی تازه از حمله استاکس‌نت به تأسیسات هسته‌ای نطنز». BBC Farsi.۰۳-۰۹-۲۰۱۹. دریافت‌شده در ۰۳-۰۹-۲۰۱۹.

حیدری نسب، علیرضا، خاکریز دوازدهم (روایت جنگ و دفاع نرم)، تهران، انتشارات پیام آزادگان (وابسته به مؤسسه فرهنگی پیام آزادگان).

خاکپور، فریبرز، خزائی، علی، عنایتی، حمید، ۱۴۰۰، جنگ سایبری: مقدمه‌ای بر مناقشات در عصر اطلاعات، تهران، انتشارات نیروی پدافند هوایی آجا.

خلیلی پور رکن آبادی، نورعلی وند، یاسر، ۱۳۹۱، تهدیدات سایبری و تأثیر آن بر امنیت ملی، فصل-نامه مطالعات راهبردی، شماره۱۶۷:۵۶-۱۹۶

زروقه، اسماعیل،۲۰۱۹، القضاءالسیبرانی والتحول فی المفاهیم القوه والصراع، مجله العلوم القانونیه و السیاسه، جامعه محمد بوضیاف، الجزایر، المجلد ۱۰، العدد ۲

سراج، رضا، اخوان، محمدجواد، ۱۳۹۹، از جنگ نرم هوشمند تا نبرد محاسبات: بررسی رهیافت‌ها و راهبردهای غرب در جنگ نرم علیه انقلاب اسلامی، انتشارات دیدمان.

شلوش، نوره، ۲۰۱۸، القرصنه اللکترونیه فی الفضاء السیبرانی «التهدید المتصاعد لامن الدول»، **مجله مرکز بابل للدراسات الانسانیه**، المجلد ۸، العدد ۲ .

صبرینه، بن سعید، ۲۰۱۵، مایه الحق فی حرمه الحیاه الخاصه فی عهد التکنولوجیا"الإعلام والاتصال"، رساله دکتوراه العلوم فی العلوم القانونبه، جامعه الحاج اخضر-باتنه-الجؤایر

طلس، مصطفی،۲۰۱۹، ألاستراتیجیه السیاسیه العسکریه، ط ۲، **دارطلس للدراسات والترجمه والنشر.**

کیانا، هانیه، هاشمی، تقی، ۱۳۹۳، جنگ سایبری، تهران: انتشارات اخوان.

عابدی، سجاد، ۱۴۰۲، خبر آن‌لاین

عیدکشایش، سعید، ثریائی آذر، حسین، باقری، جهانگیر،۱۴۰۲، حق بر «دفاع مشروع» در قبال حملات سایبری با تأکید بر حملات ایالت متحده آمریکا، فصل‌نامه حقوقی فضای مجازی، شماره اول:۸۸-۱۰۰

عثمان، احمد زکی،۲۰۱۷، تأثیرات القدرات السیبرانیه فی الصراعات القایمیه، **مجله السیاسه الدولیه**، ملحق اتجاهات نظریه، العدد ۲۰۸، المجلد ۵۲، مصر.

Banks, H.& Quillan, R. Mc,2000, Electronic Warfare Test and Evaluation, Flight Test Techniques Series, researh and tachnology organization-

north atltntIc treaty organi

zition,Canada.

Benatar, Marco,2009, "Use of cyberforce: need for legal justification?", **Goettingen Journal of International Law** 1, 3, https://www.researchgate.net/ publica

tion/265194617

Dinniss, Heather Harrison, 2012,

"**Cyberwarfare and the laws of war**", Cambridge Studies in International and comparative Law, Cambridge University Press.

Gervais, Michael, 2012, "Cyberattacks and the law of war", **Berkeley Journal of International Law**, Vol. 30

Hollis, Duncan B, 2007, "Why states need an informational law for information operations", **Lewis & Clark Law Review,** Vol. 11.

Lotriónte, Catherine, 2012, «Cyber Operations: Conflict Under

International Law", **Georgetown Journal of International Affairs,** International Engagement on

Cyber: Establishing Norms and Improving Security, Published By: The Johns Hopkins University Press, https://www.jstor.org /stable/43134334.

Melzer, Nils, 2011, "**Cyberwarfare and international Law**", www.UNIDIR.com.

Mohr, Manfred, 2010, CIJ, **Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif**, C.I.J. Recueil, Cambridge University Press.

Nguyen, Reese, 2013, "Navigating jus ad bellum in the age of cyberwarfare", **California Law Review**, Vol. 101(4).

Nolte/Randelzhofer, 2020, «**The Charter of the United Nations: a**

Commentary", Vol. II (3rd edition), Article 2(4)

Schmitt, Michael N, 2017, **Tallinn Manual**, on the international law applicable to cyber operations, second edition, prepared by the

International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press.

Schmitt, Michael N, 1999, «Computer network attacks and the use of force in international law: Thoughts on a normative Framework, **Columbia Journal of Transnational Law**, Vol. 37.

Simonet, Lois, 2012, «L'usage de la force dans le cyberespace et le droit international», **Annuaire français de droit international**, Vol. 58.

Activités militaires et paramilitaires au Nicaragua et contre celui-ci (**Nicaragua c. Etats-Unis**

d'Amérique), fond, arrêt, CIJ,

Recueil 1986.

relations amicales et la coopération entre Etats conformément à **la Charte des Nations Unies** du 24 octobre 1970.

Résolution 26/25 (XXV) **de l'Assemblée générale relative aux principes du**

droit international touchant les, xford University Press.

White House, **International Strategy for Cyberspace**, May 2011.

https://ww.un.org/fr/sections/what-we-do/uphold-international-law