فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱
وبگاه مجله: https://cyberlaw.maragheh.iau.ir
ISSN:2821-126X

Cyber Attacks from the Perspective of the Use of Force Stipulated Under International Law

Alireza Ansari Mahyari
Department of International Law, Assistant Professor, and Director of Graduate Studies, Najaf Abad Branch, Islamic Azad University, Najaf Abad, Iran
Zahra Sadat Hosseini
M.A., Department of International Law, Najaf Abad Branch, Islamic Azad University, Najaf Abad, Iran
Zahra.hosseini00@yahoo.com

DOI: 10.30495/CYBERLAW.2022.693895

Keywords:
Use of force ,
Cybercrime ,
Cyber-attacks ,
Cyber space ,
Armed conflict

Abstract

One of the most important issues of the international community has been the use of force and the changes and evolutions it has underwent. The use of force is one of the important rules of international law, which is mentioned in paragraph 4 of the Article 2 of the UN Charter. With the comprehensive growth and development of societies, the concept of resorting to force has changed and new dimensions have been created and new methods have been used by governments. One of these methods is cyberattacks. A cyberattack is an example of a new weapon the ability of which to damage, kill and physically destroy in cyberspace, has changed the concept of the use of force. In this study, the aim is to investigate cybercrime and cyberspace to clarify the nature of cyberattacks and the relationship between these attacks and the use of force. This research has achieved its results using descriptive-analytical method. It has been found out that the development of the field of communication has led to the spread of new attacks which occur in cyberspace and, because of the unique features that these attacks have, governments are very much willing in using these attacks. Furthermore, when these attacks are carried out on a large scale and target the vital infrastructure of the country the use of force has taken place indeed and that it makes no difference whether these infrastructures are damaged or not. The mere cyber-attack on these infrastructures is the use of force and is in conflict with the Principle of Prohibition of the Use of Force contained under paragraph 4 of Article 2 of the UN Charter. Cyber-attacks can be considered as resorting to force according to this article.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

حملات سایبری در پرتو توسل به زور از نگاه حقوق بین الملل

علیرضا انصاری مهیاری

استادیارو مدیر مقطع تحصیلات تکمیلی گروه حقوق بین الملل دانشکده حقوق، الهیات و معارف اسلامی، واحد نجف آباد، دانشگاه آزاد اسلامی، نجف آباد، ایران

زهرا سادات حسینی*

دانش‌آموخته حقوق بین‌الملل، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران

Zahra.hosseini00@yahoo.com

تاریخ دریافت : ۰۵ خرداد ۱۴۰۱ تاریخ پذیرش: ۰۳ مرداد ۱۴۰۱

چکیده

یکی از مسائل مهم جامعه بین المللی، توسل به زور بوده و تحولاتی را به خود دیده است.توسل به زور از جمله قواعد مهم حقوق بین‌الملل است که در بند ۴ ماده ۲ منشور به ممنوعیت این امر اشاره شده است. با رشد و توسعه همه جانبه جوامع، مفهوم توسل به زور نیز تغییر پیدا کرده و ابعاد جدیدی از آن ایجاد شده و روش‌های جدیدی از آن توسط دولت‌ها مورد استفاده قرار گرفته است. یکی از این روش‌ها، حملات سایبری می‌باشد .سلاح‌های مورد استفاده در حملات سایبری، نمونه سلاح‌های جدیدی است که توانایی این سلاح‌ها و حملات در آسیب رساندن، کشتن و تخریب فیزیکی در فضای سایبر، مفهوم توسل به زور را متحول ساخته است. در این پژوهش، هدف، بررسی جرایم و فضای سایبری برای روشن نمودن ماهیت حملات سایبری و ارتباط این حملات با توسل به زور می‌باشد.این پژوهش با روش توصیفی تحلیلی به این نتایج رسیده است که توسعه عرصه ارتباطات باعث گسترش حملات جدیدی شده که در فضای سایبر رخ می‌دهد و به دلیل ویژگی‌های منحصر به فردی که این حملات دارند، دولت‌ها تمایل زیادی به استفاده از این حملات دارند. همچنین زمانی که این حملات در مقیاس وسیعی صورت بگیرند و زیرساخت‌های حیاتی کشوری را مورد هدف قرار دهد، درواقع توسل به زور رخ داده است و تفاوتی ندارد که این زیرساخت‌ها دچار آسیب شوند یا خیر. صرف حمله سایبری به این زیرساخت‌ها، توسل به زور است و با اصل ممنوعیت توسل به زور مندرج در بند ۴ ماده ۲ منشور در تعارض است.

کلید واژگان: توسل به زور، جرایم سایبری ، حملات سایبری ، فضای سایبری، مخاصمات مسلحانه

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

مقدمه

دو اصل مهم در حقوق بین‌الملل که مباحث زیادی پیرامون این دو مفهوم مطرح شده است توسل به زور و ممنوعیت آن هستند. توسل به زور در اسناد مختلفی از جمله منشور سازمان ملل متحد بیان شده است و در این اسناد توسل به زور توسط هر کشوری علیه کشور دیگر محکوم شده است. مطابق با این اسناد توسل به زور ممنوع و فقط در صورتی که دولتی مورد تجاوز واقع شده باشد و در مقام دفاع از خود باشد، می‌تواند متوسل به زور شود[1].در گذشته جنگ به صورت سنتی و با سلاح‌های سنتی مانند اسلحه صورت می‌گرفته اما امروزه مفهومی جدید از جنگ و زور در جوامع ایجاد شده است. نویسندگانی همچون فریده شایگان و سید حامد صفوی کوهساره در مقاله‌ای تحت عنوان عملیات سایبری به مثابه توسل به زور بیان نموده‌اند که فضای سایبر و حملات سایبری به عنوان فضای پنجم حقوق بین‌الملل نامگذاری شده است. با ورود جهان به عصر انقلاب تکنولوژیک و همه گیر شدن روند جهانی شدن دیگر مسائل داخلی کشورها تنها معطوف و مربوط به مرزهای داخلی حاکمیت کشورها نیست بلکه جنبه‌های جهانی به خود گرفته است؛ این مسئله هنگامی اهمیت می‌یابد که گروه‌هایی برای رسیدن به اهداف خود دست به جرایم در قالب سازمان یافته می‌زنند که عمدتا روابط بین‌المللی را متاثر می‌کند. رشد فناوری اطلاعات و ارتباطات ماهیت منازعات را تغییر داده و اصطلاح نوینی را تحت عنوان حملات سایبری وضع نموده است. حملات سایبری درواقع اقداماتی هستند که با استفاده از شبکه‌های رایانه‌ای، به منظور تخریب، ایجاد اختلال، مخدوش یا حذف اطلاعات و تاسیسات هدف حمله به کار گرفته می‌شوند. بنابراین در این پژوهش سوالی که مطرح می‌شود این است که حملات سایبری چه جایگاهی در توسل به زور دارند و ماهیت این حملات چگونه باید باشد که بتوان گفت توسل به زور رخ داده است؟ در پاسخ به این سوال باید بیان داشت که ؛ زمانی که حملات سایبری در مقیاس وسیعی صورت بگیرند و زیرساخت‌های حیاتی یک کشور را مورد حمله قرار دهند، توسل به زور رخ داده است و مقیاس این حملات بر اساس سه محور؛ ابزار محور[2] ، هدف محور[3] و اثر محور[4] مورد سنجش قرار می‌گیرد.اگر ابزار مورد استفاده شده در این حملات، از ابزارهای متعارف در فضای سایبر باشد و هدف این حملات، زیر ساخت‌های حیاتی یک کشور باشد و آثاری که این حملات بر جای می‌گذارند مانند اثرات انواع خسارات فیزیکی بمب یا شلیک موشک باشد، توسل به زور است و مرتکبین این حملات، ناقضین اصل ممنوعیت توسل به زور هستند و به علت حملات آنها صلح و امنیت جوامع به خطر خواهد افتاد.این مقاله به صورت توصیفی تحلیلی گردآوری و تنظیم شده است و روش گردآوری این تحقیق به صورت کتابخانه‌ای بوده و روش تجزیه و تحلیل اطلاعات نیز به صورت کیفی می‌باشد . ارتباط بین حملات سایبری و توسل به زور و اینکه حملات سایبری در چه صورتی مصداقی از توسل به زور هستند، هدف اصلی نگارش این مقاله می‌باشد و در همین راستا، بخش اول مقاله به اصل منوعیت توسل به زور در حقوق بین‌الملل می‌پردازد، در بخش دوم مقاله به حملات سایبری و اصل منع توسل به زور پرداخته می‌شود و در بخش سوم ،به حملات سایبری، به عنوان شیوه‌ای نو در توسل به زور پرداخته خواهد شد .

۱- اصل منوعیت توسل به زور در حقوق بین‌الملل

توسل به جنگ در قرن پانزدهم که یک دولت اختیار کامل داشته هر زمانی که بخواهد صلح را خاتمه دهد، امری متعارف بوده است و صرفا دولت ها وظیفه داشتند اعلامیه‌ای رسمی در خصوص اعلان شروع جنگ صادر نمایند و این صدور اعلامیه تنها محدودیتی

[1] ماده ۵۱ منشور بیان می کند که در صورت وقوع حمله مسلحانه علیه یک عضو ملل متحد تا زمانی که شورای امنیت اقدام لازم برای حفظ صلح و امنیت بین‌المللی را به عمل آورد هیچ یک از مقررات این منشور به حق ذاتی دفاع از خود خواه فردی یا دسته جمعی لطمه ای وارد نخواهد کرد . اعضا باید اقداماتی را که در اعمال این حق دفاع از خود به عمل می‌آورند فورا به شورای امنیت گزارش دهند . این اقدامات به هیچ وجه در اختیار و مسئولیتی که شورای امنیت بر طبق این منشور دارد و به موجب آن برای حفظ و اعاده صلح و امنیت بین‌المللی و در هر موقع که ضروری تشخیص دهد اقدام لازم را به عمل خواهد آورد تاثیری نخواهد داشت .

[2] Instrument-based approach
[3] Target-based approach
[4] Consequence-based approach

بود که بر این اختیار دولت‌ها وارد می‌شد (رمضان پور،۵۴:۱۳۹۶). نقطه عطف برای آغاز تلاش‌های بین‌المللی در جهت ایجاد و حفظ صلح بین المللی، شروع جنگ جهانی اول بود و در آن زمان طرفین اختلاف متعهد بودند از طریق رکن داوری یا حل و فصل قضایی اختلافات خود را حل و فصل نمایند.(حیدری،۱۲:۱۳۹۶). همچنین دولت‌ها در بند ۳ ماده ۲ منشور متعهد شده‌اند که به روش‌های مسالمت آمیز اختلاف خود را حل و فصل نمایند به نحوی که صلح و امنیت بین‌المللی را به مخاطره نیندازند.علاوه بر این ، مطابق با آنچه در بند ۴ ماده ۲ منشور بیان شده است، دولت‌ها متعهد شده‌اند که در روابط بین خود از اعمال تهدید یا زور علیه تمامیت سرزمینی یا استقلال سیاسی یک دیگر، خودداری نمایند(اله یاری،۱۷:۱۳۹۳). در بند ۴ ماده ۲ منشور ، علاوه بر اینکه جنگ در شکل رسمی آن ممنوع شده است، توسل به زور و حتی تهدید به استفاده از آن نیز ممنوع اعلام شده است و بنابراین می‌توان گفت که این بند دارای ابعاد گسترده‌ای است(کرابی،۱۵:۱۳۹۲). احتمال توسل به زور با بهانه قانونی بودن آن بسیار ضعیف می‌باشد چرا که، حفظ صلح و امنیت بین‌المللی و همچنین توسعه روابط دوستانه میان ملت‌ها از اهداف سازمان مل متحد می‌باشد (سادات میدانی ،۱۹:۱۳۹۱).زمانی که جنگ‌های وحشیانه اصل ابتدایی و قاعده اساسی بوده یعنی در زمان عصر باستان، به کرات جنگ‌های رخ می‌داده و قراردادهای صلح در آن زمان به صورت موقت و محدود و صرفاً برای مدت زمان کمی منعقد می‌شده است(محمدرضائی و همکاران،۲۱:۱۳۹۸).

در اواخر قرن نوزدهم، تغییرات مهمی در نوع نگرش توسل به زور و ضمانت اجرای حفظ امنیت کشورها به وجود آمد. در همین زمان بود که کنفرانس‌های صلح لاهه، نقش مهمی در مورد منع توسل به زور و تحریم جنگ ایفا نمود(سعیدی،۶۷:۱۳۹۶).کنفرانس‌های صلح لاهه ۱۸۹۹ و ۱۹۰۷،آغازگر تلاش‌هایی برای محدود نمودن جنگ بود و ماده ۱ کنواسیون اخیر بیان می‌کند که دولت‌ها پذیرفتند که عملیات خصمانه میان آنها باید بعد از یک اخطار روشن و بدون ابهام باشد (بزرگمهری،۳۸:۱۳۹۵) در میثاق جامعه ملل بیان شده است که اعضا جامعه ملل ملزم بودند قبل از توسل به زور به طریق روش‌های قضایی حل و فصل داوری یا توسل به شورای جامعه ملل، اختلافات خود را حل کنند(بیگدلی،۱۷:۱۳۹۵).

۲- حملات سایبری و اصل منع توسل به زور

منشور سازمان ملل متحد در بند ۴ ماده ۲ درمورد توسل به زور بیان می‌کند که تمامی اعضا در روابط بین‌المللی خود از تهدید به زور یا استعمال آن علیه تمامیت ارضی یا استقلال سیاسی هر کشوری باید خودداری کنند(محمدعلی پور،۲۳۶:۱۳۹۶).توسل به زور در منشور سازمان ملل متحد بیان شده است اما در مورد زور و حملات مسلحانه‌ای که در تعریف این مفهوم بیان شده است صحبتی نشده است .بنابراین در ابتدا باید مشخص شود که استفاده از زور در فضای سایبر نقض اصل منع توسل به زور تلقی می شود یا خیر.مطابق با مفهوم بند ۴ ماده ۲ منشور سازمان ملل متحد ، هر حمله ای اعم از شیمیایی،بیولوژی و ... که در مقیاس وسیعی صورت بگیرد و تاثیر وسیعی را نیز برجای بگذارد، توسل به زور است(بیابانی،۱۴:۱۳۹۳). بنابراین می‌توان گفت که علیرغم اینکه ابزارهای به کار رفته در فضای سایبری جدید بوده و این نوع ابزارها در هیچ معاهده ای بیان نشده است،به علت مقیاس و تاثیری که دارند حمله مسلحانه تلقی می‌شوند.(حبیبی و بذار،۱۶۱:۱۳۹۶).

۲-۲ ماهیت حملات سایبری منتسب به توسل زور

با رشد و توسعه جوامع در تمامی زمینه‌ها، توسل به زور و مخاصمات نیز دچار تحول شدند و امروزه جنگ دیگر به روش‌های سنتی قدیم رخ نمی‌دهد و درواقع فضای سایبری گونه‌ای جدید از سلاح‌های مدرن را ایجاد کرده است. این فضا به قدری قوی و پیشرفته است که توانایی وارد نمودن جراحت، کشتن و ایجاد خسارت‌های فیزیکی را دارد (علیخانی،۲۱:۱۳۹۳). تحولات روز افزون و چشمگیر ارتباطات و اطلاعات باعث شده که دولتها به این نتیجه برسند که به جای استفاده از سلاح‌های سنتی، از سلاح های مدرن و جدید که مزایای بیشتری برای آنها فراهم می‌کند، استفاده کنند(شهسواری،۸۶:۱۳۹۸).به صورت کلی حملات سایبری، فعالیت‌های مجرمانه ای هستند که از طریق اینترنت به صورت تهاجمی و به وسیله اشخاص حرفه‌ای مانند نفوذگران یا بدافزارها به منظور صدمه رساندن و ایجاد خسارت در اهداف مشخص انجام می‌شود و می‌تواند شامل حملاتی مانند سرقت مالکیت فکری یک

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

سازمان، ضبط حساب‌های بانکی آنلاین، ایجاد و توزیع ویروس‌ها بر روی رایانه‌ها و سیستم‌های مخابراتی، ارسال اطلاعات کسب و کار مجرمانه بر روی اینترنت و اختلال در زیرساخت‌های ملی و حیاتی کشور باشد(هاشم زاده،۵۱ : ۱۳۹۶). حملات سایبری محدود به موارد خاصی نیستند و می‌توانند شامل حملات مختلف و گسترده‌ای مانند مختل کردن شبکه‌های رادیویی و تلویزیونی، آشفتگی بازارهای سهام و نظام بانکداری با پخش تبلیغات، تخریب جدی اموال و تلفات انسانی، تهدید امنیت ملی و هدف قراردادن زیرساخت های حیاتی باشند.

هدف قرار دادن زیر ساخت‌های حیاتی، مهم‌ترین نوع حملات سایبری است که در سه بخش؛ هدف قرار دادن زیرساخت‌های ارتباطی، هدف قرار دادن حمل و نقل و هدف قرار دادن زیر ساخت‌های حیاتی تقسیم‌بندی می‌شوند. در زیرساخت‌های ارتباطی، بستن و یا ایجاد اختلال در سیگنال شبکه‌های تلفن و بستن تمام پهنای باند اینترنت کل کشور و محروم کردن افراد از اینترنت مورد هدف است و در زیرساخت های حمل و نقل، هدف، به طور مثال سقوط هواپیما به دلیل اختلال در هدایت برج‌های کنترل ترافیک هوایی، ایجاد انحراف در مسیر قطارها با دسترسی به سیستم‌های کامپیوتری راه‌آهن می‌باشد و در زیرساخت‌های حیاتی، مواردی مانند تامین آب، سدهای آبی، سیستم‌های توزیع، شبکه برق، نیروگاه‌های برق و انرژی هسته‌ای مورد هدف قرار می‌گیرند (جعفری، ۳۰:۱۳۹۱).

۲-۲رویکردهای توسل به زور در حملات سایبری

در خصوص اینکه این حملات تحت شمول بند ۴ ماده ۲ منشور قرار می گیرد یا خیر، سه رویکرد؛ابزار محور،هدف محور و اثر محور مطرح شده است.رویکرد ابزار محور به ابزارهای استفاده شده در حملات سایبری می پردازد.بر خلاف قدیم که از فشار اقتصادی در زور استفاده می نمودند ، در حملات سایبری از سلاح های مدرن استفاده می‌شود و بنابراین زمانی حمله سایبری توسل به زور محسوب می شود که به این ابزار مدرن در حملات متوسل شوند.به طور مثال اگر سرورهای رایانه ای یا کابل های اینترنتی توسط ابزارهای متعارف سایبری صورت بگیرد و شدت این حملات زیاد باشد،توسل به زور رخ داده است(شایگان و کوهساره،۴۳۲:۱۳۹۷).در رویکرد هدف محور، زمانی یک حمله سایبری به آستانه توسل به زور می رسد که این حمله زیرساخت های حیاتی یک کشور را مورد هدف قرار دهد و تفاوتی ندارد که این زیرساخت ها مورد لطمه واقع شوند یا خیر. مطابق با نظرات بسیاری، اگر حملات سایبری خسارات مادی یا تلفاتی را درخصوص حمله به زیرساخت های حیاتی یک کشور وارد نکند، بازهم ناقض اصل ممنوعیت توسل به زور است و به نظر آنها زمانی که زیرساخت‌های حیاتی کشوری مورد حملات سایبری قرار می‌گیرد، صلح و امنیت جوامع به طرز چشمگیری در معرض خطر قرار می گیرد و این امر مخالف با بند ۴ ماده ۲ منشور سازمان ملل متحد است(Deluca,2013:34). در رویکر اثر محور، شدت تاثیرات یک حمله سایبری مورد توجه و ارزیابی قرار می‌گیرد و آن را به یک حمله مسلحانه تبدیل می‌کند.زمانی که پیامدهای فیزیکی حملات سایبری آثاری مانند خسارات فیزیکی ناشی از جنگ باشد، توسل به زور است(توحیدی و سیجانی،۵۲:۱۳۹۸).برای اینکه عملی به عنوان حمله مسلحانه قرار بگیرد چهار معیار لازم دارد.معیار اول آن است که عملیات صورت گرفته در مفهوم زور قابل گنجاندن باشد. با توجه به مطالب گفته شده درمورد حملات سایبری مشخص شد که این حملات در مفهوم زور قابل گنجاندن هستند. معیار دوم آن است که عمل صورت گرفته اثر تخریب‌کنندگی داشته باشد و در حملات سایبری، مختل‌کنندگی جایگزین تخریب‌کنندگی قرار می‌گیرد. بسیاری از حملات سایبری که رخ می‌دهد اثر مختل کنندگی بالایی دارند و اختلال در شبکه‌های ارتباطی کشوری اثری به مراتب بدتر از تخریب انبار مهمات آن کشور دارد(حسینی،۲۴:۱۳۹۱). در حملات سایبری درست است که به صورت فیزیکی حمله‌ایی رخ نداده است اما همین حملات ممکن است حتی منجر به مرگ افراد نیز شود. به طور مثال در سال ۲۰۰۷ توربین سدی در روسیه مورد حملات سایبری قرار گرفت و آن سد دچار خود انفجاری شد و در اثر این حمله تولید برق مختل شد، در آن منطقه سیل ایجاد شد و تعدادی نیز کشته شدند. بنابراین با وجود این معیار نیز حملات سایبری می‌توانند یک حمله مسلحانه باشند.

معیار سوم در تشخیص حملات سایبری به عنوان یک حمله مسلحانه، میزان و تاثیر خسارات ایجاد شده در زیرساخت‌های حیاتی کشوری در اثر آن حمله می‌باشد. مطابق با تعریفی که مجمع عمومی از زیرساخت‌های حیاتی ارائه نموده است «زیرساخت‌های

حیاتی شامل آنهایی است که برای تولید، حمل و نقل و توزیع انرژی، حمل و نقل هوایی و دریایی ، خدمات بانکی و مالی تجارت الکترونیک، تهیه آب، توزیع غذا و بهداشت عمومی و زیر ساخت‌های اطلاعاتی مهم که به طور فزاینده فعالیت‌های آنها را متاثر و به هم مرتبط کرده است، می‌باشد، اگر حمله‌ای به این زیرساخت‌ها آسیب و خسارتی وارد کند، می‌تواند یک حمله مسلحانه باشد. معیار آخر در تعیین حملات سایبری، آزمایش شش مرحله‌ای پروفسور میشائیل اشمیت است[5] . مطابق با این آزمایش اگر حمله‌ای اوصاف شدت، فوریت یا بی‌واسطگی، صراحت ، مداخله‌آمیز بودن، قابل اندازه‌گیری بودن و مشروعیت احتمالی را داشته باشد، حمله‌ای است که می‌تواند مسلحانه باشد(رکن آبادی و نورعلی وند،۱۳۹۱:۱۳)

۳-حملات سایبری، شیوه ای نو در توسل به زور

توسل به زور به عنوان ایجاد کننده نقض حقوق بین‌الملل است که نباید هرگز به عنوان وسیله حل و فصل مسائل بین‌المللی لحاظ شود.امروزه روش‌های جدیدی از توسل به زور در روابط بین‌المللی مطرح شده است(جاوید،۱۳۹۳:۱۶). پدیده‌ای که در جوامع امروزه و در عصر حاضر به کرات در جوامع مختلف در حال رخ دادن است، استفاده از حملات سایبری به کشور دیگر است. فعالیت‌های مزبور می تواند در برخی شرایط موجد مفهوم توسل به زور در منشور ملل متحد و عرف بین‌المللی باشد. اینگونه فعالیت‌ها اگر به مرگ، صدمه یا خسارت جدی منجر شوند، می‌توانند به عنوان توسل به زور قلمداد شوند (صفائی ،۱۳۹۷:۱۶).در این خصوص باید عواملی مانند هدف، محل،قصد، اثرات ، زمینه حادثه‌ای که به خسارات منجر می‌شود، عاملی که مرتکب این اقدام می‌شود و موارد دیگر مورد توجه قرار بگیرد. فعالیت‌هایی مانند ایجاد بحران در تاسیاست هسته‌ای ، باز شدن سد بر روی جمعیت انسانی و آسیب جانی به آنها (زوار جلالی و موسوی فر،۱۳۹۷:۶۷)، ایجاد اخلال در ترافیک هوایی و ایجاد تصادمات هوایی، فعالیت‌های سایبری هستند که توسل به زور را به همره دارند(کرابی،۱۳۹۲:۲۳). در منشور ملل متحد، توسل به زور مانند جنگ، تهدید به جنگ، اقدامات مقابله به مثل مسلحانه، محاصره دریایی، در روابط بین‌المللی ، علیه هر دولتی ممنوع اعلام شده است(آقازاده ،۱۳۹۵:۱۵).

۳ـ۱ حملات سایبری و توسل به زور در جنگ روسیه و اوکراین

کشور اوکراین از زمان بعد از جنگ جهانی دوم، برای روسیه، کشوری با ارزش تلقی می شده چرا که پس از فروپاشی اتحاد جماهیر شوروی، روسیه به کشوری ضعیف تبدیل شد و سعی داشت تا با کنترل اوکراین به قدرت سابق خود باز گردد. اهمیت اوکراین از این جهت بود که این کشور در زمان شوروی مقر بسیاری از سلاح‌های هسته‌ای شوروی بوده و یکی از قدرتمند ترین کشورهای اتحادیه به شمار می‌رفته است و بخش بزرگی از اتباع این کشور را روسی‌ها تشکیل می‌دادند. در سال ۲۰۰۴ آمریکا و اروپا در این کشور نفوذ پیدا کردند و همین امر باعث از بین رفتن نفوذ روسیه در این کشور شد. در سال ۲۰۱۴ نیز در اوکراین انقلابی دیگر صورت گرفت و روسیه دوباره شکست خورد و نهایتا در اقدامی غیرقابل پیش‌بینی شبه جزیره کریمه در اوکراین را به خاک خود اضافه نمود.حمله سایبری روسیه به اوکراین بخشی از رویارویی این دو کشور بعد از فروپاشی اتحاد جماهیر شوروی است.در سال ۲۰۱۵، روسیه با هک کردن شبکه برق اوکراین این حملات را آغاز نمود و در سال ۲۰۱۶ خزانه‌داری دولتی اوکراین مورد حمله هکرها قرار گرفت و در ۲۰۱۷ هکرهای قوی به زنجیره غذایی دولت اوکراین حمله نمودند(Gertz,2021:16). اوکراین در سال ۲۰۲۲ نیز مورد حمله نظامی روسیه قرار گرفت. مرکز اطلاعات امنیتی اوکراین بیان نمود که وزارت دفاع این کشور و دو بانک اوکراین مورد حمله سایبری روسیه قرار گرفت. این حملات باعث از دسترس خارج شدن سایت وزارت دفاع اوکراین شد و تراکنش‌های مالی اوشابانک و پریوات بانک با تاخیر و اخلال مواجه شد(Milanovice,2022:16). سرتاسر خاک اوکراین در این حملات مورد حملات موشکی و هوایی روسیه قرار گرفت و نیروهای زمینی روسیه نیز از جهت‌های مختلف به خاک این کشور

[5]Michael Schmid

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

حمله کردند. با این حملات مشخص است که روسیه بند ۴ ماده ۲ منشور را که توسل به زور را ممنوع می‌داند نقض نموده و در مقیاس وسیعی مبادرت به توسل به زور نموده است.

نتیجه

توسل به زور از زمان‌های گذشته تاکنون به عنوان یکی از مباحث مهم و اساسی در جامعه بین‌المللی بوده است. در قرن‌های گذشته دولت‌ها در توسل به زور آزاد عمل می‌کردند و این عمل را برای خود مجاز می‌دانستند و در دورانی که قدرت در اختیار کلیسا بود، از توسل به زور به عنوان جنگ عادلانه‌ای که در اختیار پادشاهان است، یاد می‌کردند و توسل به زور را به عنوان یک حق مورد مقبولیت قرار داده بودند. در قرون بعد ،تلاش‌هایی برای محدود کردن جنگ و توسل به زور صورت گرفت، اما هیچ یک از آنها موفقیتی را در این زمینه ایجاد ننمودند. پس از جنگ جهانی اول و دوم به علت اینکه نقض‌های شدیدی ایجاد شد و بسیاری از مردم کشته شدند، جامعه بین‌المللی و دولت‌ها به این فکر افتادند که ممنوعیتی را برای توسل به زور ایجاد کنند. زمانی که سازمان ملل متحد تشکیل شد، این سازمان، هدف اولیه خود از ایجاد را حفظ صلح و امنیت بین‌المللی اعلام نمود و بیان نمود که تمامی اعضا باید برای حفظ صلح و امنیت در جامعه بین‌المللی با یکدیگر همکاری کنند. منشور سازمان ملل متحد، صراحتاً در بند ۴ ماده ۲، توسل به زور را ممنوع اعلام نمود. یکی از دستاوردهای مهم سازمان ملل متحد تثبیت قاعده ممنوعیت توسل به زور و حل فصل مسالمت‌آمیز اختلافات میان ملت‌ها بوده است. منشور سازمان ملل متحد به عنوان یکی از مهم‌ترین اسناد در خصوص ممنوعیت توسل به زور است. بند ۴ ماده ۲ منشور به عنوان سنگ بنای منشور است که در این بند توسل به زور ممنوع اعلام شده است و این قاعده به عنوان یک قاعده آمره برای همه کشورهای عضو لازم‌الاجرا می‌باشد و بر همین مبنا هیچ کشوری حق تعرض به حاکمیت و تمامیت ارضی سایر کشورها را ندارد. با رشد و توسعه کشورها و همچنین رشد و پیشرفت فناوری ها، مفاهیمی جدیدی از توسل به زور نیز مطرح شده ست.یکی از مفاهیم فضای سایبر و حملات سایبری است. فضای سایبر امروزه بخش انکارناپذیر زندگی بشر را تشکیل می دهد و در عین حال که می تواند فضائی رقابتی باشد، می تواند فضائی خصمانه نیز باشد.باتوجه به عناصری که برای یک حمله مسلحانه لازم است، می توان ابزارهای به کار رفته در حملات سایبری را به عنوان ابزار حملات مسلحانه شناسایی نمود و این نوع حملات را تحت عنوان زور قلمداد نمود. حملات سایبری به علت ویژگی هایی مانند کم هزینه بودن، سرعت، فراملی بودن، اتوماتیک بودن و .... که دارد، در دو دهه اخیر به صورت چشمگیری افزایش پیدا کرده‌اند و توسط کشورهای مختلفی مورد اسفاده قرار گرفته‌اند. باتوجه به مطالب بیان شده، باید بیان داشت که حملات سایبری به عنوان مفهوم جدید توسل به زور مورد استفاده کشورهای مختلف قرار می گیرد و نقض بند ۴ ماده ۲ مشور سازمان مل متحد می باشد و به علت ماهیتی که این حملات دارند(مخفیانه ماندن مهاجم) انتساب عمل با دشواری هایی رو به رو است.با توضیحاتی که درمورد حملات سایبری داده شد، مشخص می‌شود که این حملات در زمره توسل به زور هستند و حاکمیت کشورها را دچار اخلال می کنند و بنابراین برای جلوگیری حداقلی از حملات سایبری و پیامدهای آن، پیشنهاد می شود که:۱) زیرساخت های بومی شده فضای سایبر اعم از تجهیزات سخت افزار و نرم افزار و در اختیار قرار گرفتن سرورهای ملی و کنترل آنها جهت پیشگیری از حملات سایبری طراحی شود، ۲) باتوجه به اینکه اولین سنگر دفاعی در فضای سایبر استفاده از آنتی ویروس می باشد و به اعتقاد برخی آنتی ویروس ها با کمک یک فایرال مناسب و انعطاف پذیر امنیت رایانه ها را تضمین می‌کنند، کشورها از این موارد استفاده کنند و در آخر از طریق کنوانسیون‌های بین‌المللی یک سیستم جامع نظارتی و کنترلی با عنوان ممنوعیت توسل به حملات سایبری مانند ممنوعیت استفاده از سلاح‌های شیمیایی و ممنوعت توسل به زور، ایجاد شود تا از طریق این کنوانسیون‌ها بتوانند این حملات را محدود و ممنوع کنند.

منابع

کتب

- آقازاده، جواد(۱۳۹۵). شورای امنیت سازمان ملل متحد و حمایت از کودکان در مخاصمات مسلحانه. چاپ اول، تهران: انتشارات خرسندی
-بزرگمهری، مجید(۱۳۹۵). تاریخ روابط بین‌الملل. چاپ ششم، تهران: انتشارات سمت.
-حیدری، حمید(۱۳۹۶). توسل به زور در روابط بین‌الملل از دیدگاه حقوق بین‌الملل عمومی و فقه شیعه. چاپ دوادهم، تهران: انتشارات اطلاعات.
-رمضان پور، رقیه(۱۳۹۶).توسل به زور در حقوق بین الملل.چاپ سوم.تهران:انتشارات خرسندی.
-سعیدی،مریم(۱۳۹۶).اصول توسل به زور در حقوق بین الملل.چاپ اول.تهران: انتشارات خرسندی
-زوار جلالی، امیر ، موسوی فر، سید حسین(۱۳۹۷). خشونت و توسل به زور. چاپ اول، تهران: انتشارات خرسندی.
-ضیائی بیگدلی، محمدرضا(۱۳۹۵). حقوق جنگ. چاپ بیست و سوم، تهران: انتشارات دانشگاه علامه‌ی طباطبایی.

مقالات

-اله یاری، طلعت، مجیدی پرست، سجّاد ، (۱۳۹۳). «گونه شناسی باندهای جرم و فساد در فضای مجازی»، پژوهش های حقوقی، شماره۳.
- بیابانی ، غلامحسین، افسانه مظفری،(۱۳۹۲). «جرایم سازمان یافته ملی و فراملی»، فصلنامه کارآگاه، سال ششم، دوره دوم، شماره۲۴.
-توحیدی،احمدرضا،سیجانی،محسن(۱۳۹۸).«ارزیابی ماهیت حقوقی حملات سایبری با نگاهی به منشور سازمان ملل متحد»،نشریه علمی پدافند غیرعامل،سال دهم،شماره ۴، ۴۷-۵۵
-جاوید،محمد جواد(۱۳۹۳). «بررسی تطبیقی حقوق بشردوستانه با کنوانسیون های چهارگانه ژنو»،مطالعات حقوق عمومی،دوره پنجاه و یکم،شماره(۲)،۴۴۱-۴۵۹
-حبیبی،همایون، بذار،وحید(۱۳۹۶) .«حملات سایبری و ممنوعیت توسل به زور»، فصلنامه تعالی حقوق، دوره جدید، شماره ۱۹
-حاتمی،محمدمهدی(۱۴۰۰).«ماجرای جنگ روسیه و اکراین»،۵ اسفند ۱۴۰۰، سایت خبری تجارت نیوز
-حسینی،محمدرضا(۱۳۹۱).«حملات سایبری از منظر قواعد و مقررات حقوق بین الملل و حقوق بشردوستانه» ،فصلنامه دفاع ملی
-خلیلی پور رکن آبادی،علی،نورعلی وند،یاسر(۱۳۹۱).«تهدیدات سایبری و تاثیرات آن بر امنیت ملی»، فصلنامه مطالعات راهبردی، سال پانزدهم(۲)
-سادات میدانی،سید حسین(۱۳۹۱). «مشروعیت توسل به زور علیه عراق:بررسی نظریه پیش دستی در دفاع از خود»،فصلنامه سیاست خارجی، سال هفدهم، شماره(۱)، ۱۱۴-۱۱۶
-شایگان، فریده،کوهساره،سیدحامد صفوی(۱۳۹۷).«عملیات سایبری به مثابه توسل به زور»،فصلنامه مطالعات حقوق عمومی،دوره ۴۸(۲)، ۴۴-۴۱۹
-صفائی، حسین(۱۳۹۷).« مداخله در امور کشورهای دیگر از دیدگاه حقوق بین‌الملل»، مجله حقوقی دفتر خدمات حقوقی و بین‌المللی جمهوری اسلامی ایران، (۹)، ۶۹-۸۳
-علیخانی،مهدی(۱۳۹۳). «قاعده منع توسل به زور و دفاع مشروع در شرایط قابل پیش بینی»،فصلنامه مطالعات بین المللی،سال یازدهم، شماره(۴)، ۲۱-۵۵
- محمدرضایی، حسن؛ میرعباسی، سید باقر و کمالی، علی(۱۳۹۸).«مبانی توسل به زور و ممنوعیت آن در حقوق بین المللی با تأکید بر منشور سازمان ملل متحد». فصلنامه تحقیقات حقوق تطبیقی ایران و بین الملل، سال دوازدهم(۴۵)،۱۴۱-۱۱۹
-محمد علی پور،فریده(۱۳۹۶).«حملات سایبری و چالش های جدید اصل منع استفاده از زور در روابط بین الملل»، فصلنامه سیاست جهانی ،دوره ششم(۳)،۲۳۳-۲۵۵

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال اول | شماره دوم | تابستان ۱۴۰۱

پایان نامه

– دوران. بهزاد .۱۳۸۱. تأثیر فضای سایبر بر هویت اجتماعی. پایان‌نامه دکتری. دانشگاه تربیت مدرس. دانشکده علوم انسانی. پائیز۱۳۸۱.

–جعفری،کامران۱۳۹۱.جنگ سایبری در حقوق بین الملل.پایان‌نامه کارشناسی ارشد،دانشکده حقوق دانشگاه پیام نور تهران

–شهساری،علی.۱۳۹۸.تحولات اصل منع توسل به زور با تاکید بر حملات سایبری، پایان نامه کارشناسی ارشد ،دانشکده حقوق و علوم سیاسی، دانشگاه مازندران

–کرابی، ع.۱۳۹۲.رابطه اصل منع توسل به زور و دکترین مسئولیت حمایت در حقوق بین الملل با تاکید بر بحران سوریه.پایان نامه کارشناسی ارشد، دانشکده علوم انسانی و مدیریت دانشگاه سمنان.

–هاشم زاده،رضا.۱۳۹۶.مسئولیت ناشی از حملات سایبری مخربانه در حقوق بین الملل و راهکارهای مقابله با آن، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد صفادشت

منابع انگلیسی

-DeLuca, Christopher D. 2013. The Need for International Laws of War to Include Cyber Attacks Involving State and Non_State Actors, Pace International Law Review.Vol.3. No.9

-ICJ.Reports .(1998).Peremptory Norms in International Law

-Getz, Bill (2020).Inside the Ring: Cybercoms Michael Rogers confirm Russia conducted cyber attack against Ukraine. The Washington Times.

-Milanovic, Marko(2022). What is Russia Legal Justification for Using Force against Ukraine? Ejil Talk, Blog of the European Journal of International Law