فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره دوم | تابستان ۱۴۰۲
ویگاه مجله: https://cyberlaw.maragheh.iau.ir
دانشگاه آزاد اسلامی واحد مراغه
ISSN: 2821-126X

The conflict of Cyber-Attacks With The Principle of Non-Intervention in International Law, Focusing On The Actions of The United States of America

Saeid Eid Koshayesh
Department of International Law, Maragheh Branch, Islamic Azad University, Maragheh, Iran
saeygo@gmail.com
Hossein Sorayaii Azar
Assistant Professor Department of International Law, Maragheh Branch, Islamic Azad University, Maragheh, Iran (Corresponding Author)
hosseinsorayaiiazar@iau-maragheh.ac.ir
Jahangir Bagheri
Assistant Professor Department of International Law, Maragheh Branch, Islamic Azad University, Maragheh, Iran
jahangir.bagheri.123@gmail.com

Keywords:
Cyber Attacks,
Cyber Warfare,
Non-Intervention,
Coercion,
Cyber Destruction

Abstract
However, the phenomenon of cyberspace in the new age has led to many human advances, but it has also hosted many real space disorders. Today, at the international level, many conflicts have been exploited in this field by using or exploiting the capacity of this space, one of the most important of which is cyber attacks and hostilities. Different States have regarded the space as the battlefield and are in the direction of damages to others who call it their enemy. One of the most important and influential countries is the United States, which uses its advanced equipment to take these measures against other States.In this regard, the necessity of paying attention to cyber attacks that can lead to the responsibility of states is inevitable because some of these attacks can violate the principle of non-interference in the internal affairs of the countries-as a *Jus Cogens* of International Law. The present article, with the help of a descriptive analytical approach, has come to the conclusion that some US cyber attacks are due to elements such as informed invasion, violation of the independence of the states, and the element of coercion violate the principle of non -intervention And the efforts to fill the gaps have led to completely different results from the insertion of democratic values to the unintended strengthening of protectionist tendencies, and so far cyberization has not had a tangible impact on the principle of non-intervention and its quality.

فصلنامه علمی
مطالعات حقوقی فضای مجازی
سال سوم | شماره دوم | پاییز ۱۴۰۴
صفحات مقاله ۵۴ الی ۶۷

تعارض حملات سایبری با اصل عدم‌مداخله در حقوق بین الملل با تمرکز بر اقدامات ایالات‌متحده آمریکا

سعید عیدکشایش
گروه حقوق بین‌الملل، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران
saeygo@gmail.com
حسین ثریائی آذر
استادیار گروه حقوق بین‌الملل، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران (نویسنده مسئول)
hosseinsorayaiiazar@iau-maragheh.ac.ir
جهانگیر باقری
استادیار گروه حقوق بین‌الملل، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران
jahangir.bagheri.123@gmail.com

تاریخ دریافت : ۲۳ تیر ۱۴۰۳ تاریخ پذیرش: ۲۳ تیر ۱۴۰۳

چکیده

هرچند پدیداری فضای سایبر در عصر جدید زمینه‌ساز بسیاری از پیشرفت‌های بشری گردیده ولی در همین راستا نیز بسیاری از نابسامانی‌های فضای حقیقی را نیز میزبانی نموده است. امروزه در سطح بین‌المللی بسیاری از تعارض‌ها با استفاده یا به تعبیری سوءاستفاده از ظرفیت‌های این فضا، در این وادی نمود یافته‌اند که یکی از مهم‌ترین آن‌ها حملات و مخاصمات سایبری است. دولت‌های مختلف فضای مذکور را به‌عنوان میدان جنگ تلقی نموده و در راستای ایراد خسارت به دیگرانی هستند که آنان را دشمن خود خطاب می‌نمایند که یکی از مهم‌ترین و تأثیرگذارترین این کشورها ایالات‌متحده آمریکا می‌باشد که با استفاده از تجهیزات فوق پیشرفته خود به این اقدامات علیه دولت‌های دیگر دست می‌یازد. در همین راستا ضرورت توجه به حملات سایبری که می‌تواند منجر به مسئولیت دولت‌ها گردد اجتناب‌ناپذیر است چراکه برخی از این حملات می‌تواند ناقض اصل عدم‌مداخله در امور داخلی کشورها «به‌عنوان قاعده‌ی آمره حقوق بین‌الملل» گردد. مقاله‌ی حاضر با یاری جستن از روش تحلیلی توصیفی به این نتیجه دست‌یافته است که برخی از حملات سایبری ایالات‌متحده با توجه به دارا بودن عناصری همچون تهاجم آگاهانه، نقض استقلال دولت‌ها و عنصر اجبار ناقض اصل عدم‌مداخله می‌باشد و تلاش‌ها برای پر کردن شکاف‌ها به نتایج کاملاً متفاوتی از درج ارزش‌های دموکراتیک تا تقویت ناخواسته گرایش‌های حمایت‌گرا منجر شده و تاکنون سایبری شدن تأثیر ملموسی بر اصل عدم‌مداخله و کیفیت آن نداشته است.

واژگان کلیدی: حملات سایبری، جنگ سایبری، اصل عدم‌مداخله، اجبار، تخریب سایبری

مقدمه

فضای مجازی فضایی است که قوانین خاص خود را دارد. امروزه تهدیدها در قالب شبکه‌های رایانه‌ای و مخابراتی رو به افزایش است. بخش‌های کلیدی اقتصاد تمامی کشورها در حال حاضر، ازجمله امکانات دولتی و خصوصی، بانکداری و امور مالی، حمل‌ونقل، تولید و پزشکی، همگی برای انجام عملیات روزانه وابسته به رایانه هستند. هدف از حمله‌ی سایبری، دست‌یابی به اطلاعات سایر کشورها، ایجاد وقفه در تجارت و یا ایجاد خدشه در زیرساخت‌ها مانند: «آب، برق، حمل‌ونقل و غیره» به‌نحوی‌که هزینه‌های اقتصادی را افزایش دهند.. وجود نداشتن قواعد و مقررات بین‌المللی لازم‌الاجرای خاص این حوزه باعث شده که هر کشوری به خود اجازه دهد تا بر ضد کشور دیگر وارد حملات و جنگ سایبری شود. با ورود به عصر اطلاعات، کیفیت و شرایط جنگ‌ها از پیچیدگی مفهومی و روشی بسیار زیادی برخوردار شده و جنبه‌های نوینی از درگیری در فضای سایبر شکل‌گرفته است. جنگ سایبری مجموعه‌ای از فنون عملیاتی جدید و سبک نوینی از جنگ است که در مناقشه‌هایی در بالاترین سطح شدت به‌منظور هدف قرار دادن مخالفان به کار می‌رود. این جنگ شکل جدیدی از جنگ فرماندهی و کنترل است که کمتر به جغرافیا بستگی دارد بلکه بیشتر به ماهیت فضای شبکه‌های الکترونیک مربوط می‌شود. جنگ سایبر با هدف اختلال، آسیب زدن یا تغییر آنچه جمعیت هدف فکر می‌کنند با تمرکز بر روی افکار عمومی، نخبگان و یا هر دو به انجام می‌رسد.

امروزه هر دولتی می‌تواند باانگیزه‌های مختلفی و بدون در نظر گرفتن «نورم‌های حقوقی» بین‌المللی، به انجام توسل به زور در فضای سایبری اقدام نماید و این خود به وجود آورنده‌ی اقدامات تلافی جویانه‌ای خواهد بود. حال مسئله این است که این استفاده‌ی غیرقانونی از زور یا تهدید به آن نقض مقررات بین‌المللی محسوب می‌شود یا نه؟ به‌منظور ارائه‌ی تعریفی از توسل به زور در فضای سایبر باید جامعه‌ی بین‌المللی به اجماعی برسد، که تاکنون حاصل نگردیده است. در معنای چنین فعالیت‌هایی در سایه‌روشن منشور سازمان ملل متحد به‌طور خاص بند ۴ ماده‌ی ۲، باید دید که گستره‌ی این مقرره در باب منع توسل به زور متوجه توسل به زور در فضای سایبر نیز می‌شود یا باید مقرره‌های دیگری را تدوین نمود. البته باید بیان نمود که توسل به زور علیه تمامیت ارضی یا استقلال سیاسی هر کشوری که به‌طورکلی مغایر ارزش‌ها و اهداف سازمان ملل باشد، ممنوع است. ایالات‌متحده‌ی امریکا با استفاده از قابلیت‌های فضای سایبر کوشیده است ابعاد نوینی از جنگ نرم بر ضد کشورهای مختلف در این فضا شکل دهد. بررسی این موضوع در حملات و جنگ‌های سایبری ایالات‌متحده علیه کشورهای دیگر موردی است که باید مدنظر قرار گیرد، چراکه استفاده فزاینده از این شیوه‌ی تخاصم، ذهن را بدین مسیر رهنمون می‌نماید که آیا این مساله مداخله در کشور دیگر و نقض حاکمیت آن محسوب می‌گردد یا خیر.

باید یادآور شد که تعیین معیار و ضابطه در برشمردن مصادیقی از حملات سایبری به‌عنوان نقض «اصل عدم‌مداخله» در جامعه‌ی بین‌المللی امر تردیدآمیزی به شمار می‌آید؛ اما ولنگاری در خصوص همین موضوع، می‌تواند چالش‌هایی اساسی برای نظم بین-المللی به وجود بیاورد. از سوی دیگر بررسی موردی این حملات و تحلیل نقض اصل مذکور در هر مورد منجر به این خواهد شد که ازاین‌پس جامعه بین‌المللی موضع منفعل و خنثی در خصوص حملات سایبری نداشته باشد (اصلانی،۱۳۹۵:۲۰۱). با در نظر داشتن این موضوع مقاله‌ی حاضر با یاری جستن از روش توصیفی- تحلیلی به بررسی تعارض حملات سایبری با اصل عدم‌مداخله در حقوق بین‌الملل با تمرکز بر اقدامات ایالات‌متحده آمریکا می‌پردازد.

۱. فضای سایبر و حملات سایبری

بشر در طول گذران تاریخ خود مراحل مختلفی را طی نموده است و از اوان خلقت در این کره خاکی به دنبال ارتباط با هم نوع خود بوده است. عمر این ماجرا را می‌توان از روزی که بشر با شوق فراوان با ایماء و اشاره با همنوع خود ارتباط برقرار ساخت تا اختراع خط و غیره متصور شد. ولی در سده ۲۰ میلادی بشر با فراگیر شدن ارتباطات در بستری جدید، رویکردی نو در مقابل خویشتن مشاهده کرد و برای اولین بار مسئله‌ای به نام فضای مجازی[1] برایش مطرح گردید (پور قهرمانی و صابر نژاد، ۱۳۹۴: ۲۷)؛ که شاید تا آن زمان تصوّر کردن چنین چیزی برای آدمی محال بود. مسئله‌ای که در این فضا ذهن بشری را به خود جلب کرد این بود که آیا قواعد سابق اجتماع، در این عرصه نیز می‌تواند مصداق داشته باشد یا نه؟ و در صورت امکان، «نورم‌های حقوقی» آن به چه نحوی تبیین خواهد شد؟ ولی مقدّم بر جواب بر این مسائل باید کم و کیف این فضا به‌وضوح شناخته می‌شود.

[1]Virtual space

۱-۱. تبیین فضای سایبر و ویژگی‌های خاص آن

اصطلاح فضای سایبر[1] یا فضای هدایت‌شده، نخستین بار در سال ۱۹۲۸ میلادی در یک داستان علمی – تخیّلی به‌کاربرده شد. از آن زمان تاکنون فضای سایبر را به معنای مکانی غیر فیزیکی و مجازی می‌شناسیم که واقعیت‌ها را با عنوان واقعیت مجازی در فضای الکترونیکی بازتاب می‌دهد (مسعودی، ۱۶:۱۳۸۳). «سایبرسپیس» توهم و تصور باطل توافقی است که انسان‌ها خلق کرده‌اند و ناحیه‌ای است که فعالیت‌هایی در این فضا اتفاق می‌افتد؛ ازجمله تبادل و تجمیع اطلاعات. (بای و پورقهرمانی،۲۱:۱۳۸۸). درواقع فضای سایبر محیطی است مجازی و غیرملموس که در فضای شبکه‌های بین‌المللی (که از طریق اینترنت به هم وصل می‌شوند) وجود دارد. در این محیط، تمام اطلاعات مربوط به روابط افراد، ملت‌ها، فرهنگ‌ها، کشورها، به‌صورت ملموس و فیزیکی (به‌صورت نوشته، تصویر، صوت و اسناد) در یک فضای مجازی و به شکل دیجیتالی وجود داشته و قابل‌استفاده و در دسترس استفاده‌کنندگان و کاربران می‌باشد، کاربرانی که از طریق کامپیوتر، اجزای آن و شبکه‌های بین‌المللی به هم مرتبط هستند (باستانی،۵۶:۱۳۸۳)

با مطرح‌شدن فضای سایبر مهم‌ترین تحولی که در سال‌های اخیر در حوزه حملات خصمانه دولت‌ها و جنگ رخ‌داده است، استقرار و به‌کارگیری فناوری اطلاعات و ارتباطات رایانه محور می‌باشد[2]؛ اما در این بحبوحه‌ی مناظره پرشور در مورد «فناوری اطلاعات و ارتباطات»[3] ما نباید این واقعیت را نادیده بگیریم که آنچه در پس برخی دستگاه‌ها و ابزارهای عملیات اطلاعاتی قرار دارد به‌مراتب گسترده‌تر از فناوری رایانه محور اطلاعات و ارتباطات است و چه‌بسا حتی فناوری را در اموری فراتر از اطلاعات پراکنی درگیر سازد. (هالپین،۲۵۲:۱۳۸۹) درواقع توجه به این نکته ضروری است که با مطرح‌شدن حملات خصمانه و جنگ در این عرصه‌ی نوین، جنگ به محیطی برده شد که آن فضا مترادف با دنیا رایانه و شبکه اینترنت بود (قاجار قیونلو،۱۳۲:۱۳۹۱)

۱-۲. حملات سایبری و گستره‌ی آن

«حمله سایبری»[4] در رایانه‌ها و شبکه‌های رایانه‌ای به هرگونه تلاش برای افشای، تغییر، غیرفعال کردن، تخریب، سرقت یا دستیابی و دسترسی غیرمجاز یا استفاده غیرمجاز از یک دارایی گفته می‌شود. حمله سایبری هر نوع مانور تهاجمی است که سامانه‌های اطلاعات رایانه‌ای، زیرساخت‌ها، شبکه‌های رایانه‌ای یا دستگاه‌های رایانه شخصی را هدف قرار می‌دهد. مهاجم یک شخص یا فرایندی است که سعی در دسترسی به داده‌ها، کارکردها یا سایر مناطق محدود سامانه بدون مجوز، به‌طور بالقوه با قصد مخرب دارد. بسته به شرایط، حملات سایبری می‌تواند بخشی از جنگ سایبری یا سایبر تروریسم باشد. حمله سایبری توسط دولت‌های مستقل، افراد، گروه‌ها، جامعه یا سازمان‌ها قابل‌استفاده است و ممکن است از یک منبع ناشناس سرچشمه بگیرد (پور قهرمانی و صابر نژاد،۴۲:۱۳۹۴). درواقع امر، حملات سایبری اختلال در صحت یا درستی داده‌ها است که معمولاً از طریق کدهای مخرب و تغییر در منطق برنامه و کنترل داده‌ها که به خروجی‌های اشتباه منجر می‌شود، صورت می‌گیرد (Rodriguez,2006:10)؛ که شامل ۴ حوزه می‌باشند:

۱. از دست دادن کلیت داده‌ها
۲. از دست رفتن قابلیت استفاده داده‌ها
۳. از دست رفتن محرمانگی داده‌ها
۴. تخریب فیزیکی داده‌ها (Army,2005:1-3)

جنگ سایبری قطعاً جز جنگ‌های نامتقارن محسوب می‌گردد که در آن تعداد جنگجویان و تسلیحات مشخص نیست و هرکسی می‌تواند به‌عنوان یک افسر نظامی حمله کند مشروط به داشتن مهارت‌های سایبری یا کار با کامپیوتر. بدین ترتیب حملات سایبری می‌تواند یک جنگ سایبری قلمداد شود که تجهیزات رایانه‌ای و ارتباطی ابزار مخاصمات هستند (جعفری و توتونچیان،۳۳۲:۱۴۰۰). مطابق استراتژی نظامی ملی ایالات‌متحده امریکا در خصوص عملیات فضای سایبری (۲۰۰۶)، عبارت است از استفاده‌ی منسجم از توانمندی‌های جنگ الکترونیکی، عملیات شبکه‌ای رایانه‌ای، عملیات روانی، حیله‌های نظامی و عملیات هماهنگ باقابلیت‌های پشتیبانی که به‌منظور تأثیرگذاری، متوقف کردن، تخریب

---

[1] Cyber space

[2] در واقع مراد از ارتباطات رایانه محور همان فضای سایبر در معنای اخص می باشد چرا که حقوق سایبر شاخه ای از حقوق مرتبط با کامپیوتر و اینترنت است؛ که راجع به موضوعاتی مانند حقوق مالکیت فکری، آزادی عقیده و دسترسی آزاد به اطلاعات بحث می کند(blacklawdictionary, 2004:74)

[3] Information & communication technology(ICT)
که معادل فارسی آن فناوری اطلاعات وارتباطات می باشد. عبارتی دربرگیرنده تمام فناوری های پیشرفته ی نحوه ی ارتباط و انتقال داده ها در سامانه های مخابراتی است. این سامانه می تواند یک شبکه مخابراتی ، چندین کامپیوتر مرتبط به هم و متصل به شبکه مخابراتی و همچنین برنامه های استفاده شده در آنها باشد..

[4] Cyber attack

یا سرقت اطلاعات طرف مقابل و درعین‌حال پشتیبانی از فرایندهای تصمیم‌گیری نهادهای ملی صورت می‌گیرد؛ هدف همه عملیات‌های سایبری، ایجاد اختلال، ممانعت، تنزل دادن یا تخریب اطلاعات موجود در رایانه‌ها و شبکه‌های رایانه‌ای می‌باشد (Roscini, 2014: 13), مطابق قاعده ۳۰ دستورالعمل تالین ۱ و قاعده ۹۲ دستورالعمل تالین ۲، حمله سایبری عملیاتی تهاجمی یا دفاعی بوده که رهاورد منطقی آن ورود آسیب یا خسارت و یا مرگ اشخاص و نابودی اشیاء است.)Tallinn Manual2.0, 2017: 415)

نکته‌ی قابل توجه در مورد حملات سایبری آن است که این حملات و در مفهوم عام‌تر جنگ سایبری[1] شکل کاملاً جدیدی از رزم است که بازتاب آن را هنوز به‌طور کامل نتوانسته‌ایم درک کنیم(Clark,2009:32) اما درباره‌ی این موضوع، آنچه به ذهن متبادر می‌گردد این است که به نظر می‌رسد این نوع جنگ با اشکال سابق جنگ تفاوت چندانی ندارد و فضای سایبر را نیز به عرصه‌های سنتی‌تر افزوده است ولی با این تعریف آنچه از چشم پنهان می‌ماند پس‌زمینه جاری حمله سایبری به‌عنوان بخشی از برنامه‌ای کل‌نگر و هماهنگ برای دستیابی به اهداف سیاسی، اقتصادی و اجتماعی کشورهاست (Michael,2010:1) که در حملات سایبری ایالات‌متحده به‌وفور مشاهده می‌گردد. باوجوداین باید به این نکته توجه کرد که برخلاف دیپلماسی نیروی نظامی و جنگ اقتصادی در این عرصه موضوع اصلی- مسئله‌ی کشورها و وجود آن‌ها برای تخاصم بین‌المللی - به چالش کشیده می‌شود. درواقع فضای سایبر این امکان را برای سوژه‌های[2] غیردولتی نظام بین‌المللی، سازمان‌های تجاری و حتی افراد فراهم می‌کند که وسایل و انگیزه برای فعالیت جنگ‌طلبانه را کسب کنند (Conrnish,2010:32) و همین مسئله موجب شده است که در سطح بین‌المللی نیز جهان شاهد چندین حمله سایبری باشیم که مهم‌ترین آن‌هایی که ارتکاب آن منتسب به دولت ایالات‌متحده است به قرار ذیل می‌باشد:

۱. دهه‌ی ۸۰ میلادی حمله‌ی آمریکا به کره شمالی
۲. سال ۱۹۹۹ حمله‌ی آمریکا به یوگسلاوی
۳. سال ۱۹۹۹ حمله‌ی آمریکا به شبکه‌های کامپیوتری صرب
۴. سال ۲۰۰۱ حمله‌ی آمریکا به چین
۵. سال ۲۰۰۱ آمریکا و روسیه
۶. سال ۲۰۱۰ حمله‌ی ویروس استاکس نت[3] به تأسیسات نطنز (مرکز پدافند غیرعامل فاوا،۵۵:۱۳۸۸)

شاید بتوان بیان داشت که همین ویژگی‌های خاص این حملات و سهل‌الوصول و البته گریز از مسئولیت در قبال آن بوده است که جنگ سایبری را به یکی از خطرناک‌ترین نوع جنگ و درگیری تبدیل کرده و همین ویژگی‌ها سبب گردیده است که کشورهایی همچون ایالات‌متحده آمریکا، روسیه و چین این نوع جنگ را مهم‌تر از جنگ خطرناکی همچون نبرد هسته‌ای قلمداد کنند. شاید اگر متوجه ادعای مشاور عالی امنیت ضد تروریسم پیشین ایالات‌متحده شده باشیم که عقیده داشت این نوع جنگ می‌تواند در عرض ۱۵ دقیقه برای ایالات‌متحده بسیار مرگبار و مخرب باشد به اهمیت موضوع پی خواهیم برد.(پور قهرمانی و صابر نژاد،۳۹:۱۳۹۲) چراکه این جنگ توانایی بالقوه به وجود آوردن موقعیتی را دارد که به «آنارشیسم»[4] یا هرج‌ومرج بین‌المللی بیانجامد.

۲. اقدامات بین‌المللی درباره‌ی حملات سایبری

استفاده از حملات سایبری و پدیده جنگ‌های سایبری که درنتیجه پیشرفت‌های روزافزون علوم و فناوری، امروزه به شیوه جدید جنگ در عرصه روابط بین‌المللی بدل گشته است، آرام آرام به‌سوی قانونمند شدن به‌پیش می‌رود، کما اینکه با پیشرفت سلاح‌های سایبری، شاهد مطرح‌شدن مباحث حقوقی در زمینه حقوق بین‌الملل بشردوستانه، جهت تحول مفهوم حقوقی جنگ و توسل به‌زور و تلاش برای قاعده‌مند کردن و تسری قواعد حاکم بر مخاصمات مسلحانه بر این‌گونه رودررویی‌ها از سوی دولت‌ها هستیم. در این راستا، علی‌رغم اینکه شاهد معاهده

---

[1] Cyber war
[2] Subject
[3] استاکس‌نت Stuxnet : یک بدافزار رایانه‌ای (طبق نظر شرکت‌های نرم‌افزار امنیت رایانه‌ای: کرم رایانه‌ای یا تروجان) است که اولین‌بار در تاریخ ۱۳ جولای ۲۰۱۰ توسط ضدویروس وی‌بی‌ای۳۲ شناسایی شد. این بدافزار با استفاده از نقص امنیتی موجود در میانبرهای ویندوز، با آلوده کردن رایانه‌های کاربران صنعتی، فایل‌های با قالب اسکادا که مربوط به نرم‌افزارهای WinCC و PCS7 شرکت زیمنس می‌باشد را جمع‌آوری کرده و به یک سرور خاص ارسال می‌کند.براساس نظر کارشناسان شرکت سیمانتک، این بدافزار به دنبال خرابکاری در تأسیسات غنی‌سازی اورانیوم نطنز بوده‌است.در اواخر ماه مه ۲۰۱۲ رسانه های آمریکایی اعلام کردند که استاکس‌نت مستقیما به دستور اوباما رئیس جمهور آمریکا طراحی، ساخته و راه اندازی شده است(صابرنژاد، هاشم-پور،۴:۱۳۹۲).
[4] Anarchism

الزام‌آوری نبوده‌ایم، اما با تدوین دستورالعمل‌های تالین ۱ و ۲ کوشش شد که سایه قواعد عام حقوق بین‌الملل به‌صورت ملموس بر فعالیت‌های سایبری آشکار شود (گیوکی و همکاران،۱۳۹۷:۱۷۳).

توسعه فناوری، اینترنت و ارتباطات و تجارت رایانه‌ای، با درنوردیدن ثغور، عرصه نوینی از فعالیت‌های انسانی را بازکرده و موجب تضعیف مشروعیت قوانین بر اساس مرزهای جغرافیایی شده است. پدیده حاضر، مرز جدیدی میان دنیای سایبری و دنیای حقیقی به وجود آورده که تهدید بزرگی در مقوله فقدان قانون و همچنین عدم امکان اجرای تمام و کمال قانون احساس می‌شود. استفاده دولت‌ها از فضای ناامن سایبری، زمینه را برای بسیاری از هم نوعان خود جهت خرابکاری، اخلال، ترور، جاسوسی و دیگر جرائم مرتبط هموارساخته‌اند. اقدام به قانون‌گذاری در برخی کشورها، بسته به میزان پیشرفت در دنیای فناوری، جامعه بین‌المللی را نیز به فکر واداشته که بتواند در این آشفته‌بازار فضای مجازی، اقدامی هرچند اندک به‌منظور تلطیف این فضا انجام دهد (صلاحی و کشفی،۱۳۹۵:۲۸). در تاریخچه‌ی قانونمندی این حملات حرکاتی چند دراین‌باره برای تدوین مقرراتی بین‌المللی انجام پذیرفته است که تلالوء آن نخستین بار در نشست سال ۲۰۱۱ مونیخ دیده می‌شود. در این اجلاس، «دیوید کامرون» نخست‌وزیر وقت انگلیس، «آنجلا مرکل» صدراعظم سابق آلمان و «هیلاری کلینتون» و «سرگئی لاوروف» وزرای امور خارجه وقت آمریکا و روسیه حضور یافتند. یکی از اهداف اصلی آنان تدوین مقرراتی برای اماکنی چون بیمارستان‌ها و مدارس برای مصون ماندن از حملات سایبری بود که البته به نتیجه مطلوبی نرسید.

در سال‌های اخیر «سازمان پیمان آتلانتیک شمالی»(ناتو)[1] در این باب اقداماتی انجام داده که قابل‌توجه می‌نماید. مدیریت دفاع سایبری در وضع موجود در ناتو شامل سه رکن می‌شود:

«اولین رکن قابلیت واکنش ناتو در مقابل حوادث کامپیوتری-مرکز فنی-[2] که وب‌سایت‌های مرتبط با ناتو را کنترل می‌کند.

رکن دوم مرکز دفاع سایبری[3] ناتو می‌باشد که در سال ۲۰۰۸ و به‌منظور متحد کردن مدیریت و مشارکت در عملیات مرتبط با دفاع سایبری و قابلیت‌های سراسری این اتحادیه ایجاد شد؛ در آینده این مرکز مشتمل بر اتاق جنگی که اعمال تاکتیکی دفاع سایبری را توسط کشورهای عضو انجام می‌دهد، خواهد شد.

رکن سوم مرکز مشارکت دفاع سایبری است که دکترین تالین نیز بر این پایه بنا نهاده شده است.(Dunn Cavetly,2011)»

با همه‌ی این ساختارها باز باید متوجه بود، که حتی رویکرد ناتو نیز در این زمینه ضعیف و قابل انتقاد است، چراکه ذاتاً این موضوع در حال تکوین بوده و به پختگی‌های خاص خود نرسیده است. در حال حاضر، قانون حاکم بر دفاع سایبری در داخل ساختار ناتو ماده ۴ اساسنامه بوده و بدین شکل است که کشورهای عضو می‌توانند با یکدیگر مشورت‌هایی در مورد حملات سایبری انجام دهند اما موظف نیستند که به یکدیگر درراه 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 باقی‌مانده 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 باقی‌مانده است؛ اما این رویکرد همچنان در ناتو دیده می‌شود که بحث حملات سایبری را در مفهوم تجاوز دانسته و با توجه به ماده ۵ اساسنامه‌ی خود دفاع جمعی در مقابل آن را مجاز شمارد. آنچه مهم است بحث شناسایی مهاجم در این فضا است، همان‌طور که گفته‌شده است چون شناسایی منبع هجوم در این فضا کار دشواری است لذا نسبت دادن آن به یک کشور سخت و در مواردی غیرممکن خواهد بود، چراکه مرز در این فضارنگ باخته است.

مسئله‌ی دوم در تعمیم ماده‌ی ۵ اساسنامه‌ی ناتو در بحث دفاع جمعی در جنگ سایبری، روشن نمودن نوع حمله‌ی سایبری است. بسیاری از کارشناسان در مورد حدودوثغور این حمله اتفاق‌نظر ندارند، برخی معنای مضیقی از حمله‌ی سایبری ارائه داده و آن را تنها در حملاتی که خساراتی همچون حمله مسلحانه بر جای می‌گذارد، مشمول بحث توسل به‌زور می‌دانند ولی برخی دیگر آن را در معنای موسع صادق دیده و هر حمله‌ی سایبری را توسل به زور محسوب می‌نمایند، که البته این نوع تفسیر نامعقول و آشوب‌طلبانه به نظر می‌رسد. اما باید این نکته مدنظر قرار گیرد که ناتو برای حفظ مکانیزم خاص خود در بحث امنیت سایبری تلاش خواهد کرد که حملات سایبری را در حیطه‌ی ماده‌ی ۵ اساسنامه خود و بحث دفاع جمعی بگنجاند. در همین راستا راهنمایی، پیرامون «حقوق بین‌الملل قابل‌اعمال بر جنگ‌افزارهای سایبری»[4] در

[1] North Atlantic Treaty Organization(NATO)
[2] Technical center
[3] Cyber Defenses Management Authority(CDMA)
[4] International Law Applicable to Cyber Warfare

مارس ۲۰۱۳ منتشر شد که به «راهنمای تالین»[1] معروف می‌باشد، این راهنما، محصول مطالعه سفارشی ناتو و به‌ویژه آمریکا، به گروهی از حقوقدانان بین‌المللی است تا استنتاج مندرج در راهبرد ملی فضای سایبری با زبان حقوقی تشریح و تبیین شود. گزارش مذکور اساساً با قاعده‌سازی هدفمند، به دنبال توجیه‌پذیر کردن نبردهای سایبری غرب علیه کشورهایی نظیر چین و ایران است. تأکید دستورالعمل تالین، در معنای دقیق، بر اقدامات سایبری علیه تجهیزات سایبری، به‌عنوان‌مثال به‌کارگیری اقدامات سایبری علیه زیرساخت‌های حیاتی یک دولت یا حمله سایبری باهدف سامانه‌های کنترلی و فرماندهی دشمن، است؛ بنابراین هدف این دستورالعمل حول محور اقدامات سایبری علیه تجهیزات مادی، همچون حمله هوایی و بمباران مرکز کنترل سایبری، نمی‌چرخد. همچنین حملات نظامی الکترونیک سنتی، مانند انداختن پارازیت را نیز دربر نمی‌گیرد. چنین اقداماتی قبلاً تحت حقوق مخاصمات مسلحانه تعریف‌شده‌اند (Tallinn Manual 1.0,2013:16-19) یکی از محوری‌ترین نکات مرتبط با این گزارش، توسعه مفهوم «توسل به زور» و تلاش برای وسعت بخشیدن به ادبیات حقوقی بین‌المللی مرتبط با آن بوده است. درواقع، تکیه‌گاه این مطالعه، توسیع دامنه مفهوم «توسل به زور» در روابط بین‌المللی است که ادبیات حقوقی معاصر را از نبردهای نظامی و متکی به قدرت سخت‌افزاری جنگی تغییر جهت داده و به سمت نبردهای نرم نیز سوق داده است به‌طوری‌که علاوه بر نبردهای نظامی سنتی و جدید، نبرد در فضای نرم‌افزاری ازجمله سایبری نیز که عاری از کاربرد جنگ‌افزارهای نظامی باشند نیز در مرکز ثقل این مفهوم قرارگرفته‌اند. در این رابطه، باید تهدیدهای حقوقی بین‌المللی نهفته در این گزارش را موردتوجه داشت. تفسیر موسع از توسل به زور، درست برخلاف جهتی است که به تدوین منشور ملل متحد انجامیده است. بر اساس اصول اساسی تدوین‌شده در منشور ملل متحد، توسل به زور ناظر بر اقدامات نظامی در روابط بین‌الدولی است و جنگ اساساً در همین قالب مشمول ممنوعیت قرارگرفته است. بر این اساس، ازآنجاکه اصل بر منع این نوع توسل به زور است، مسائل مرتبط با دفاع مشروع و اقدامات قهری شورای امنیت نیز تنها استثناهایی هستند که توسل به زور را مشروعیت می‌بخشند. ازآنجاکه چین و ایران هدف راهبردی نبردهای سایبری غرب به‌ویژه ایالات‌متحده‌ی آمریکا بوده و هستند، توسعه مفهوم توسل به زور به معنای موجه نمودن جنگ سایبری علیه این کشورها در قالب دفاع مشروع است (ضیایی،خلیل-زاده،۱۳۹۲).

در ادامه‌ی این فرآیند دستورالعمل کالین ۲ نیز طرح و تدوین گردیده است. این دستورالعمل که از دستورالعمل اصلی پیروی می‌نماید برای گسترش دامنه کتابچه راهنمای تالین طراحی شده در فوریه ۲۰۱۷ توسط انتشارات دانشگاه کمبریج در قالب یک کتاب منتشر گردیده است. تمرکز کتابچه راهنمای اصلی تالین بر مخرب‌ترین عملیات سایبری است، آن‌هایی که به‌عنوان «حملات مسلحانه» واجد شرایط هستند و بنابراین به دولت‌ها اجازه می‌دهند در دفاع از خودپاسخ دهند. در مقابل راهنمای تالین ۲ به «عملیات»[2] سایبری در مقابل «تعارضات»[3] سایبری که در راهنمای اول مدنظر بوده اشاره دارد که حملات سایبری مادون جنگ را نیز شامل می‌گردد.[4]

به‌طورکلی می‌توان بیان داشت که کشورهای قدرتمند در نظام بین‌الملل تمایلی به اعلام حق عملیات سایبری تهاجمی ندارند. حتی اگر حمله سایبری در پاسخ به یک حمله قبلی انجام شود، این‌یک رویکرد عاقلانه برای کمک به جلوگیری از جنگ‌های آشکار در فضای سایبری است. بااین‌حال چندین کشور هنوز جنگ سایبری را به‌صورت مخفیانه انجام می‌دهند. شواهدی وجود دارد که نشان می‌دهد جنگ سایبری بین برخی کشورها وجود دارد: روسیه و کشورهای مختلف (گرجستان، استونی و احتمالاً ایالات‌متحده و چندین کشور اروپایی). پاکستان و هند؛ چین و هند؛ چین و تایوان؛ اسرائیل و کشورهای مختلف عربی/ ایران؛ قطر و کشورهای عرب؛ کره شمالی و چندین کشور دیگر. بسیاری از این حملات از طریق هکرهایی انجام شده است که ممکن است وابستگی رسمی به دولت‌هایی داشته یا نداشته باشند که عمداً در پیگرد قانونی آن‌ها کوتاهی می‌کنند. (Dorn, 2017:138) در نشست سال ۲۰۰۸ سران کشورهای عضو ناتو، اولین سیاست دفاع سایبری اتخاذ شد. سپس در نشست سال ۲۰۱۴ با سیاست تقویت شده در مورد دفاع سایبری گامی به جلو برداشته شد. در اجلاس ورشو در سال ۲۰۱۶، کشورهای عضو، فضای سایبری را به‌عنوان یک حوزه به رسمیت شناختند، بنابراین آن را با سایر حوزه‌های نظامی متعارف یعنی زمین، دریا و هوا برابر قلمداد کردند. اجلاس ورشو همچنین به امضای پیمان دفاع سایبری باهدف ایجاد یک شبکه مشترک برای بهبود قابلیت‌های دفاعی و انعطاف‌پذیری ملی در برابر حمله سایبری منجر شد. متعاقباً برنامه‌های عملیاتی متعددی به‌منظور اجرای تعهدات انجام‌شده در پیمان دفاع سایبری اتخاذشده است. (Marrone, Sabatino, 2021)

اما سؤال اساسی در خصوص حملات سایبری و اصل عدم‌مداخله این است که آیا دیجیتالی شدن اصل عدم‌مداخله را تغییر می‌دهد؟ آیا نوع جدیدی از حقوق بین‌الملل ایجاد می‌کند؟ دیجیتالی شدن بحث‌هایی را برانگیخته است که پتانسیل تغییر این اصل را دارد. ادغام ارزش‌های دموکراتیک هدف اصلی عدم‌مداخله را به‌عنوان تجسمی از بی‌طرفی رژیم در حقوق بین‌الملل تغییر می‌دهد. در مقایسه با آن، پیشبرد درک

[1] Tallinn Manual
[2] Operations
[3] Conflict
[4] See:Tallinn Manual 2.0 On The International Law Applicable To Cyber Operation, Perpared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Center of Excellence,Cambridg university press (2017)

قوی‌تر از عدم‌مداخله بسیار متعارف‌تر به نظر می‌رسد، حتی اگر منشأ برخی پیشنهادها که حداقل تأثیر غیرمستقیم در آن زمینه‌دارند، شگفت‌انگیز باشد. اصل عدم‌مداخله همواره دارای بار سیاسی بوده و هست. درنتیجه، ابهام نظارتی اصل همچنان ادامه دارد؛ اما بالاتر از همه، دیجیتالی شدن یک ایده قدیمی را احیا کرده است و آن اینکه حوزه خاصی از امور داخلی یک دولت از مداخله خارجی محافظت شود. به نظر می‌رسد بهترین رویکرد در قبال عدم شفافیت اصل عدم‌مداخله – و به‌طورکلی قوانین بین‌المللی در فضای سایبری – فراخوانی برای تصویب یک معاهده سایبری است؛ چراکه مشکلات منحصربه‌فرد این حوزه ناشی از خصوصیت خاص این فضا هست. اعمال حقوق بین‌الملل عمومی مانند اصل عدم‌مداخله تنها اولین گام است که در رأس آن باید «منشور چارچوب فعالیت‌های فضای مجازی» تدوین شود. بااین‌حال، کشورهای غربی با این رویکرد مخالف بوده و ضرورت آن را تایید نمی‌نمایند. با توجه به این بن بست اساسی، برخی از دولت‌ها از توسعه بیشتر عرف موجود و درنتیجه مقاومت در برابر معاهده جدید حمایت می‌کنند و سایر دولت‌ها طرفدار یک معاهده هستند و بنابراین دیدگاه‌های خود را در مورد چگونگی توسعه عرف موجود ارائه نمی‌کنند. شاید تعجب‌آور نباشد که اجماع فعلی در سازمان ملل از تأیید اعمال قوانین بین‌المللی در فضای سایبری فراتر نمی‌رود و اینکه چگونه هنجارها و اصول خاص و به‌ویژه اصل عدم‌مداخله در شرایط خاص اعمال می‌شود، حداقل در حال حاضر، نامشخص است.[1]

۳. حملات سایبری ایالات‌متحده آمریکا و تعارض آن با اصل عدم‌مداخله

اصل عدم‌مداخله از اصول مندرج در منشور ملل متحد است که سازمان ملل متحد را از دخالت در اموری که اساساً در صلاحیت داخلی کشورهاست، منع کرده است. این اصل بر پایه اسناد بین‌المللی در روابط بین دولت‌ها نیز حاکم بوده و از حاکمیت برابر آن‌ها نشئت می‌گیرد (قاسمی،۱۳۹۵:۱۴۳). در عصر اطلاعات، حملات سایبری، نمایانگر نوع جدیدی از توسل به زور هستند و می‌توانند باعث ایجاد آثاری از قبیل صدمات عظیم و وسیع به زیرساخت‌های حیاتی یک دولت، تخریب اموال و کشته شدن انسان‌ها شوند و به‌این‌ترتیب با نقض بند ۴ ماده ۲ منشور سازمان ملل متحد به‌عنوان توسل غیرقانونی به زور در نظر گرفته شوند، اما مسأله آن است که امروزه مشروعیت حملات سایبری از رویکرد عدم توسل به زور، ارزیابی می‌گردد و محققین این حوزه ادعا می‌کنند که حملات سایبری صورت گرفته، زمانی به‌منزله مداخله غیرقانونی در امور داخلی دولت‌ها محسوب می‌شوند که منجر به ایجاد صدمات فیزیکی شده باشند، اما این دیدگاه با این چالش مواجه است که بسیاری از حملات سایبری صورت گرفته در سال‌های اخیر، منجر به ایجاد صدمات فیزیکی نشده‌اند و درنتیجه در چارچوب ممنوعیت مقرر در بند ۴ ماده ۲ منشور قرار نمی‌گیرند (برادران و دیگران، ۱۳۹۶:۲۴۱)؛ لذا در همین خصوص تشتت آراء و دیدگاه بنیادینی وجود دارد.

اگرچه آمریکا به‌عنوان توسعه‌دهنده‌ی اصلی فضای سایبری، کشوری پیشرو در این عرصه تلقی می‌شود. توسعه همه‌جانبه اینترنت و وابستگی بیش‌ازحد زیرساخت‌های حساس امریکا به فناوری اطلاعات آن را در معرض انواع تهدیدات سایبری قرار داده است. شبکه بانکی و مالی تا خدمات عمومی، شبکه‌های مدنی و نظامی همگی به شبکه وابسته بوده در صورت اختلال سایبری همگی آن‌ها از کار می‌افتند (صانعیان،۱۳۹۸:۱۹۱). لذا تشکیل تأسیساتی در مقابله با این خطرات بهانه‌ی خوبی بوده است که این کشور ارتش سایبری مقتدری فراهم آورد که اکثر حملات سایبری علیه کشورهایی را که هم‌مسلک سیاسی آن نیستند را راهبری نماید؛ لذا مرکز «فرماندهی سایبری ایالات‌متحده یا واحد فرماندهی امنیت سایبری ایالات‌متحده»[2] یکی از یازده واحد فرماندهی وزارت دفاع ایالات‌متحده است. فرماندهی سایبری در اواسط سال ۲۰۰۹ در دفتر مرکزی آژانس امنیت ملی در فورت جورج جی. مید، مریلند تشکیل شد. این واحد با شبکه آژانس امنیت ملی همکاری می‌کند و از زمان تشکیل این نیرو به‌طور هم‌زمان ریاست آن با مدیر آژانس امنیت ملی بوده است. اگرچه در ابتدا یک واحد با مأموریت دفاعی در ذهن ایجاد می‌شود، اما به‌طور فزاینده‌ای به‌عنوان یک نیروی تهاجمی موردتوجه قرارگرفته است[3] و حتی در مرحله‌ی عمل در ۱۸ آگوست ۲۰۱۷ اعلام شده است که به یک فرماندهی جنگی متحد کامل و مستقل ارتقا می‌یابد و این موضوع در ۴ می ۲۰۱۸ انجام یافته است. در همین راستا فرماندهی سایبری ایالات‌متحده ۱۳۳ تیم سایبری جدید را به خود اضافه کرد که تفکیک آن‌ها شامل موارد زیر می‌باشد: (Nakashima,2016)

۱. سیزده تیم مأموریت برای دفاع در برابر حملات سایبری گسترده
۲. شصت‌وهشت تیم حفاظت سایبری برای دفاع از شبکه‌ها و سیستم‌های وزارت دفاع در برابر تهدیدات اولویت‌دار
۳. بیست‌وهفت تیم با مأموریت مبارزه و باهدف ارائه حملات یکپارچه در فضای مجازی برای حمایت از برنامه‌های عملیاتی و عملیات احتمالی

[1] See: Rep. of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, para. 2 (May 28, 2021) https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf
[2] United States Cyber Command
[3] See: https://www.washingtonpost.com/world/national-security/obama-to-be-urged-to-split-cyberwar-command-from-the-nsa/2016/09/12/0ad09a22-788f-11e6-ac8e-cf8e0dd91dc7_story.html

۴. بیست‌وپنج تیم برای پشتیبانی سایبری و ارائه پشتیبانی تحلیلی و برنامه‌ریزی مأموریت‌های ملی و تیم‌های مأموریت رزمی.

اقداماتی که این تیم‌های سایبری علیه کشورهای مختلف انجام می‌دهند می‌تواند زمینه‌ساز تخطی به اصل عدم‌مداخله در حقوق بین‌الملل باشد که تحلیل آن در ادامه‌ی مباحث آمده است.

۳-۱. اصل عدم‌مداخله در حملات سایبری ایالات‌متحده

پیشرفت فناوری موجب مواجهه روزافزون دولت‌ها با حملات سایبری شده است. بیشترین حملات سایبری که دولت‌ها با آن مواجه‌اند، از نوع حملات سایبری «نفی یا محروم‌سازی از سرویس توزیع‌شده اینترنتی»[1] است. این‌گونه حملات آثار مخرب مستقیم و آنی ندارند، به همین دلیل ارزیابی آن‌ها در قالب ممنوعیت توسل به زور و حملات مسلحانه قرار نمی‌گیرد و معمولاً دولت‌ها نیز با توجه به‌شدت کمتر آن‌ها در برخی موارد حتی از پیگیری و شناسایی عاملان حملات صرف‌نظر می‌کنند. بااینکه قواعد مستقیم و صریحی در مورد حملات سایبری و نظم بخشیدن به آن‌ها وجود ندارد، نظر به تبعات چنین حملاتی حتی با شدت کم و اقتضای ارزیابی حقوقی این حملات، با بررسی مقررات فعلی حقوق بین‌الملل به این نتیجه می‌رسیم که بعضی ازاین‌گونه حملات غیر مخرب را می‌توان با اصل ممنوعیت مداخله به نظم درآورد و در صورت احراز عاملان و انتساب آن حملات به دولت، مسئولیت بین‌المللی دولت‌ها را در مراجع بین‌المللی مطرح کرد (اسمعیل زاده ملاباشی و عبدالهی،۱۳۹۹:۷۱۱)؛ که حملات سایبری ایالات متحده‌ی آمریکا نیز از این مقوله مستثنی نمی‌باشد. حتی اگر تردیدی در زمینه‌ی تطابق حملات سایبری با توسل به زور مطرح گردد و حمله سایبری مصداقی از توسل به زور تلقی نشود، می‌تواند اصل منع مداخله در امور داخلی دولت‌ها را نقض نماید. حمله سایبری مصداقی از اعلامیه عدم‌مداخله مجمع عمومی مورخ ۱۹۸۱ است؛ آنجا که در بند ۳ پاراگراف اول بیان می‌دارد «حق دولت و مردم در دسترسی آزاد به اطلاعات حق توسعه سیستم‌های اطلاعاتی و رسانه جمعی و استفاده از رسانه‌های اطلاعاتی بدون مداخله و با این هدف که منافع سیاسی، اقتصادی و فرهنگی خود را توسعه دهند». دیوان بین‌المللی دادگستری در قضیه «فعالیت‌های نظامی و شبه‌نظامی در نیکاراگوئه و علیه نیکاراگوئه»[2] مورخ سال ۱۹۸۶ مداخله را در صورت وجود چند شرط غیرقانونی دانست: «اولاً آن‌که مداخله در اموری باشد که هر کشور درنتیجه اصل حاکمیت مجاز به انجام آن‌هاست، ثانیاً روش مورداستفاده کشور مداخله‌گر زورمندانه و قهرآمیز باشد و ثالثاً در مداخله‌ای که به‌طور قهرآمیز و با استفاده از زور صورت گرفته است لازم است عنصر زور و اجبار امری بارز و آشکار باشد (Nicaragua judgment,1986: 227 - 238). همچنین اعلامیه اصول حقوق بین‌الملل راجع به روابط دوستانه و همکاری میان کشورها، هر نوع مداخله مستقیم یا غیرمستقیم در امور داخلی یا خارجی کشور دیگر را به‌منزله نقض تعهدات بین‌المللی می‌داند. ماده ۳۲ قطعنامه منشور حقوق و تکالیف اقتصادی دولت‌ها نیز تأکید کرده است که هیچ کشوری حق استفاده ابزاری از امکانات سیاسی و اقتصادی و غیره به‌منظور دستیابی به اعمال حق حاکمیت خود را ندارد. از مجموع این تعهدات برمی‌آید که حمله سایبری می‌تواند در خوش‌بینانه‌ترین حالت نقض اصل منع مداخله در امور داخلی تلقی شود (ضیایی، خلیل زاده،۱۳۹۲:۹۴). حملات سایبری ایالات‌متحده در چین ۲۰۰۱ و ایران ۲۰۱۰ مصداق بارزی از این نوع مداخلات می‌باشد؛ چراکه در هر یک از این حملات زیرساخت‌های کلیدی مورد خدشه قرارگرفته و نهایتاً آسیب‌پذیری داده‌ها و اثرات فیزیکی را در برداشته است که مصداق بارز نقض «اصل عدم‌مداخله در امور داخلی» می‌باشد.

از سوی دیگر باید دانست که «اصل عدم‌مداخله» در امور داخلی کشورها یکی از اصول بنیادین حقوق بین‌الملل است که به‌موجب این اصل عام کشورها از دخالت در امور یکدیگر منع شده‌اند. رعایت اصل مذکور موجب حفظ حاکمیت و استقلال کشورها و نتیجتاً صلح و امنیت بین‌المللی خواهد بود. واضعان منشور ملل متحد سعی نمودند که با تکیه‌بر اصل «عدم توسل به زور» دولت‌ها را از مداخله در امور یکدیگر بازدارند. واگذاری مسئولیت حفظ صلح و امنیت بین‌المللی به اعضای دائم شورای امنیت موجباتی را برای مداخله این سازمان در امور داخلی کشورها در مواردی خاص فراهم آورد. جامعه بین‌المللی در خلال جنگ سرد تلاش نمود که اصل «منع مداخله» را تا حدودی رعایت نماید. بعد از فروپاشی شوروی، شورای امنیت با تفسیر گسترده از مفهوم صلح و امنیت بین‌المللی، «صلح داخلی» را با «صلح بین‌المللی» مرتبط دانست و بدین ترتیب نسبت به رخدادهایی چون نقض حقوق بشر و فجایع انسانی در قلمرو دولت‌ها احساس تکلیف و مسئولیت نموده و اقدام به مداخله نظامی در کشور ناقض حقوق انسانی نمود. به‌این‌ترتیب اصل «عدم‌مداخله» تا حدودی تضعیف گردید. بعد از وقایع ۱۱ سپتامبر ۲۰۰۱ شورای امنیت خود را در قبال مسائلی چون مبارزه با «تروریسم بین‌المللی» و ممانعت از تکثیر سلاح‌های کشتارجمعی مسئول دانست و در مقام مرجع اصلی حفظ صلح جهانی و با تصویب دستورالعمل‌های عام برای کشورها وارد قلمرو و داخلی آن‌ها گردید. همچنین ایالات‌متحده آمریکا با اتخاذ دکترین «دفاع مشروع پیشگیرانه» اعلام نمود که خود را ملتزم به رعایت ضوابط ناظر بر عدم کاربرد زور در منشور ندانسته و در صورت به خطر افتادن منافع آمریکا خود رأساً اقدام می‌نماید (صادقی حقیقی،۱۳۹۰:۹۲). نتیجه رویکرد جدید آمریکا، مداخله نظامی در کشورهایی مثل

[1] حمله محروم‌سازی از سرویس distributed denial-of-service (DDoS) در علم رایانه حمله منع سرویس یا حمله منع سرویس توزیع شده، تلاش برای خارج کردن ماشین و منابع شبکه از دسترس کاربران مجازی است؛ در واقع هر حمله‌ای علیه دسترس پذیری به عنوان حمله منع سرویس تلقی می‌شود.

[2] ICJ Rep. Military and Paramilitary Activities in and against Nicaragua,1986

عراق و افغانستان از اعتبار تنها مرجع حفظ صلح و امنیت بین‌المللی کاست و اصل عدم‌مداخله» را نیز خدشه‌دار نمود. در حال حاضر با معرفی اصول بنیادین حقوق بشر به‌عنوان قاعده آمره، ازنظر حقوقی نه‌تنها حکومت‌ها بایستی آن را رعایت نمایند بلکه در خاتمه دادن به نقض آن نیز مکلف شده‌اند. مسئولیت اولیه حمایت از مردم به عهده دولت است. چنانچه دولتی نتواند و یا نخواهد از اتباع خود و یا جمعیت قربانی در قلمرو خود حمایت نماید. نظریه «مسئولیت بین‌المللی حمایت» جایگزین اصل «عدم‌مداخله» می‌گردد؛ بر اساس این نظریه همه دولت‌ها مسئولیت حمایت از افراد تحت ستم را در چارچوب مقررات منشور بر عهده خواهند گرفت (صادقی حقیقی،۱۳۹۰:۹۳).

۳-۲. ویژگی حملات سایبری ناقض اصل عدم‌مداخله

وجود برخی از ویژگی‌ها در حملات سایبری می‌تواند آن را تبدیل به ناقض اصل عدم‌مداخله نماید. اصولا اقدام مداخله‌آمیز غیرمجاز سایبری شامل دو عنصر می‌باشد:

۱. *عنصر تداخل با امور داخلی یا خارجی دولت هدف*

۲. *قهری بودن عملیات سایبری حادث* (گیوکی، حکاک‌زاده،۱۴۰۱).

در رأی مربوط به قضیه نیکاراگوئه، دیوان بین‌المللی دادگستری، زمانی که ابراز داشت مداخله ممنوعه بایدمداخله‌ای باشد که مقولاتی که وفق اصل حاکمیت، هر دولتی در اتخاذ تصمیم راجع به آن‌ها آزاد است را تحت‌الشعاع قرار می‌دهد، تأکید کرد که مداخله، بر حوزه اختصاصی یک دولت تأثیر می‌گذارد؛ به‌طور خاص، چنین مقولاتی، شامل انتخاب نظام سیاسی، اقتصادی، اجتماعی و فرهنگی و صورت‌بندی سیاست خارجی، می‌گردند. مطابق اعلامیه مربوط به روابط دوستانه، سازمان‌دهی، تحریک، مساعدت، تأمین مالی یا مشارکت در آشوب داخلی یا تروریسم در دولت دیگر یا پذیرش بی‌قیدوشرط فعالیت‌های سازمان‌یافته در قلمرو خود که برای ارتکاب چنین اقداماتی ترتیب داده‌شده‌اند، در شمار مصادیق مداخله هستند. در این راستا، نیازی نیست که مداخله چه به‌صورت طبیعی یا سایبری در حوزه داخلی یک دولت، علیه زیرساخت دولتی هدایت‌شده باشد یا فعالیت‌های دولتی را شامل شود، بلکه، کلید تحقق عنصر ابتداییِ مداخله، این است که عمل موردنظر می‌بایست به‌منظور تضعیف اقتدار دولت بر حوزه اختصاصی خود طراحی‌شده باشد (گیوکی، حکاک‌زاده،۱۴۰۱).

اشاره دیوان بین‌المللی دادگستری به «تصمیم‌گیری آزادانه» در رأی قضیه نیکاراگوئه، ما را به این مطلب هدایت می‌کند که عملیات‌های سایبریِ معینِ استفاده شده جهت وادار ساختن دولتی دیگر برای پایبندی به تعهدات حقوقیِ بین‌المللی خویش، از دامنه اِعمال این قاعده حذف می‌شوند. این امر به این خاطر است که متعهد بودن یک دولت در قبال دولت دیگر، دست‌کم در قبال دولت دوم، موضوع را از دایره حوزه اختصاصی، خارج می‌سازد. درواقع، حقوق بین‌الملل اقدامات متفاوتی، نظیر مقابله‌به‌مثل، یا اقدامات متقابل را که برای قادر ساختن یک دولت به مجبور کردن دولت دیگر جهت محترم شمردن تعهدات حقوقیِ بین‌المللی خویش طراحی‌شده‌اند، مجاز می‌شمارد (Tallinn Manual 2.0, 2017: 317).

همان‌گونه که در رأی قضیه نیکاراگوئه توسط دیوان بین‌المللی دادگستری تأیید شد، عنصر سازنده مداخله ممنوعه، اجبار است، دیوان اشعار داشت مداخله زمانی که از شیوه‌های قهری استفاده کند متخلفانه است؛ عنصر اجبار، مبنای اصلیِ مداخله غیرمجاز را مشخص می‌کند. اقدامات قاهرانه، موجب شکل‌گیری مداخله در چارچوب اهداف این قاعده نمی‌شوند؛ اجبار، به‌گونه‌ای که در این قاعده به‌کاررفته است، به زور فیزیکی محدود نیست، بلکه به عمل ایجابیِ طراحی شده برای محروم ساختن دولتی دیگر از آزادی انتخاب خویش، یعنی وادار ساختن آن دولت به عمل به شیوه‌ای غیرارادی یا خودداریِ غیرداوطلبانه از عمل به شیوه‌ای معین، دلالت دارد (Declaration on Friendly Relations, 1970: 3)؛ که حملات سایبری ایالات‌متحده‌ی آمریکا در این باب تحلیل می‌گردد. اجبار صرف، برای شکل‌گیری نقض ممنوعیت مداخله کفایت نمی‌کند؛ بلکه اقدام جبرآمیز باید به‌منظور تأثیرگذاری بر برآیندها یا رفتار مرتبط با مقوله‌ای که به دولت هدف اختصاص دارد طراحی شده باشد، برای مثال، پویش سایبریِ خرابکارانه هدایت شده علیه زیرساخت سایبریِ متعلق به یک گروه قومی خاص در دولت همسایه ممکن است حاکمیت دولت دوم را نقض کند ولی مداخله ممنوعه به شمار نمی‌آید، زیرا به‌منظور تأثیرگذاری بر هیچ یک از برآیندها یا تصمیم‌های دولت هدف طراحی نشده است. باوجوداین، اگر پویش سایبریِ ذی‌ربط در راستای وادار ساختن دولت مربوطه برای اتخاذ موضعی خاص در یک مناقشه قومیِ داخلیِ جاری تدارک دیده‌شده باشد، واجد این وصف خواهد بود (گیوکی، حکاک‌زاده،۱۴۰۱).

افزون بر این، اجبار، می‌بایست از متقاعدسازی، انتقاد، دیپلماسی عمومی، تبلیغات، تلافی، کینه‌جوئی صرف و از این دست متمایز شود؛ به این معنا که برخلاف اجبار، این قبیل فعالیت‌ها صرفاً شامل تأثیرگذاری بر اقدامات ارادی دولت هدف یا درصدد عدم اقدام دولت هدف در کل هستند. نکته کلیدی این است که عمل قهری باید تواناییِ بالقوه، جهت وادار ساختن دولت هدف به انجام عملی که در حالت دیگر به آن مبادرت نمی‌ورزد، یا خودداری از انجام اقدامی که در حالت دیگر به آن دست می‌زند را داشته باشد (Tallinn Manual 2.0, 2017: 319). البته تمایز میان عملیات‌های سایبری قهری و غیرقهری همیشه مشخص نیست؛ بااین‌حال، توسل‌به زور سایبری مطابق قاعده ۶۸

دستورالعمل تالین ۲، توسط یک دولت علیه دولت دیگر همواره قهری بوده و بنابراین موجب شکل‌گیری مداخله می‌گردد که در مورد حملات سایبری ایالات‌متحده صدق می‌گردد (گیوکی، حکاک‌زاده،۱۴۰۱).

از طرفی دیگر باید بیان داشت که آگاهی و قصد دولت هدف نسبت به عملیات سایبریِ موجد مداخله ادعایی، پیش‌شرط نقض قاعده منع مداخله، نیست؛ یک عملیات سایبریِ خرابکارانه مخفی در سطح توسل به زور، حتی اگر بدافزار درگیر چنین القا کند که یک نقص فنی موجب خسارت شده است، مداخله به شمار می‌رود. قصد، از دیگر عناصر تشکیل‌دهنده‌ی نقض ممنوعیت مداخله است. وضعیت‌هایی که در آن‌ها فعالیت‌های سایبری واجد اثر جبرآمیز عملی هستند را باید از وضعیت‌هایی که در آن‌ها دولت قصد اجبار رسمی دارد تفکیک کرد، برای مثال، ممکن است یک دولت به فعالیت‌هایی دست بزند که بدون داشتن قصد چنین کاری، کمک عملی به شورشیان حاضر در کشوری دیگر باشد، مثلاً، امکان دارد دولت، امنیت شرکت‌های ملی رسانه‌های اجتماعی خود را ارتقاء ببخشد و از این طریق موجب تقویت رسانه‌های اجتماعی مورداستفاده توسط نیروهای شورشی خارجی برای برقراری ارتباط گردد و دسترسی دولتی که شورشیان علیه آن دست به عملیات می‌زنند به آن ارتباطات را دشوار سازد. اقدامات دولت، موجب شکل‌گیری مداخله نمی‌شود، زیرا قصد مداخله در امور داخلی دولت هدف را نداشته است. یا مذاکرات جاری میان دو دولت همسایه راجع به ایمنی سایبری ضعیف در یکی از آن‌ها را تصور کنید؛ به علت قصور آن دولت در نگاهداری مناسب سامانه‌های خود، فعالیت‌های دولت دیگر به طرز چشمگیری مختل می‌شوند، مذاکرات از هم می‌پاشد و دولت دوم، به‌منظور حفاظت از سامانه‌های خویش، ارتباطات برآمده از دولت نخست را مسدود می‌سازد. ازآنجایی‌که فعالیت‌های سایبری دولت نخست عمدتاً به زیرساخت سایبریِ مستقر در دولت دوم متکی است، به‌گونه‌ای مؤثر مجبور می‌شود که اقدامات درخواستی در خلال مذاکرات را اتخاذ نماید. هدف مبنایِ مسدودسازیِ ارتباطات صرفاً برای حفاظت و نه وادار ساختن بود؛ بنابراین، دولت دوم این قاعده را نقض نکرده است. همچنین، هنگامی‌که اجبار توسط یک دولت از طریق دیگر طرف‌ها اجرا می‌شود، لزومی ندارد که دولت مربوطه، هدفی مشترک با طرف‌های مزبور داشته باشد؛ تنها شرط این است که آن دولت، قصد ایراد اجبار در مقوله‌ای را داشته باشد که به دولت هدف اختصاص دارد.

در مقابل باید بیان کرد که اگر دولت، به عملی رضایت دهد که در صورت عدم رضایت او مداخله ممنوعه به شمار می‌آمد، این قاعده نقض نمی‌شود، زیرا رضایت، وصف متخلفانه بین‌المللیِ یک عمل را رفع می‌کند. به‌این‌ترتیب، اگر یک دولت در سطح استفاده از زور و با درخواست دولت دوم به عملیات‌های سایبری علیه شورشیان در دولت دیگر مبادرت جوید، مداخله غیرقانونی وجود نخواهد داشت (Tallinn Manual 2.0, 2017:321).

از سوی دیگر، مطابق قاعده ۶۷ دستورالعمل تالین ۲، ملل متحد نباید به‌وسیله ابزارهای سایبری در مقولاتی که اساساً تحت صلاحیت یک دولت قرار دارند، مداخله نماید؛ که این اصل به اقدامات اجرایی اتخاذشده توسط شورای امنیت در قالب فصل هفتم منشور ملل متحد، خدشه‌ای وارد نمی‌سازد. قاعده مذکور بر مبنای بند ۷ ماده۲ منشور ملل متحد استوار است که بر اساس آن ملل متحد اجازه ندارد در مقولاتی که اساساً تحت صلاحیت داخلی هر دولت هستند مداخله نماید. زمانی که شورا امنیت به این کار مبادرت ورزد، کلیه دولت‌ها باید تصمیمات آن را بپذیرند و اجرا نمایند، برای نمونه، این شورا می‌تواند قطعنامه الزام‌آوری را به تصویب برساند که از دولت‌ها بخواهد دسترسی به ارتباطات سایبریِ دولتی خاص را قطع کنند یا به دولت‌ها مجوز بدهد تا علیه یک دولت به عملیات‌های سایبری دست بزنند. پایبندی به چنین قطعنامه-ای این قاعده را نقض نخواهد کرد (Tallinn Manual 2.0, 2017: 327).

نتیجه‌گیری

با توجه به آنچه تحلیل شد می‌توان بیان داشت که حملات سایبری افسارگسیخته در جامعه‌ی بین‌المللی به‌عنوان چالشی اساسی برای حقوق بین‌الملل جلوه‌گری می‌نماید. از سوی دیگر مسئله توسل به زور در فضای سایبر چندان‌که باید موردتوجه قرار نگرفته است، چراکه حتی تعریفی اجماعی نیز از این موضوع در حقوق بین‌الملل دیده نمی‌شود. معدود حرکاتی که درباره‌ی توجه به این مسئله به چشم می‌آید به‌طورکلی از طرف ناتو و سردمداران کشورهای عضو آن سازمان می‌باشد؛ این رویکردهای ناتو در سال ۲۰۱۳ منجر به صدور اعلامیه‌ای گردیده است که به راهنمای تالین پیرامون «حقوق بین‌الملل قابل‌اعمال بر جنگ‌افزارهای سایبری» معروف هست. در همین راستا در سال ۲۰۱۷ نیز راهنمای دوم تالین تدوین و توسط انتشارات دانشگاه کمبریج منتشر شده است که به عملیات سایبری به‌صورت تحلیلی‌تری می‌پردازد و قواعدی را ارائه می‌دهد؛ اما نکته شایان توجه عدم اجرایی شدن این قواعد در جامعه‌ی بین‌المللی است چراکه این اسناد صرفاً راهنما بوده و هیچ قدرت اجرایی ندارند و دولت‌های صاحب تکنولوژی و بالطبع آن دارای ارتش مقتدر سایبری همچون ایالات‌متحده‌ی آمریکا به خاطر منافع خویش و قاعده‌ی قدرت حاکم بر حقوق بین‌الملل، به‌هیچ‌وجه بر چنین قواعدی وقعی نمی‌نهند و لذا در عرصه‌ی بین‌المللی حملات سایبری با قواعد و قوانین الزام‌آوری مواجه نیستند و به نظر می‌رسد که باید برای جلوگیری از حملات سایبری یا حداقل تنظیم مقررات آن چاره‌ای در سطح بین‌المللی اندیشیده شود و مقررات آمره‌ای شکل بگیرد تا جلوی جنگ سایبری گرفته شود.

از سویی دیگر حقوق بین‌الملل به دلیل تنوع و تکثر فضای مجازی نتوانسته است تا به یک چارچوب اساسی و قاعده‌مند برای این حوزه دست یابد؛ که دارای سازوکارهای متنوع باشد، آنچه به‌صراحت مورد غفلت واقع‌شده است و به درک مشترکی نینجامیده است این مطلب است که در زمان رویدادهای تهاجمی مانند حملات یا جنگ سایبری کدام نهاد بین‌المللی مسئول احراز آن است. این موضوعی است که بسیار چالش‌برانگیز شده است، چراکه دولت‌ها به‌تنهایی نمی‌توانند به پاسخ چنین سؤالی برسند. با وضعیت فعلی حاکم بر جامعه‌ی جهانی، بی‌تردید برخی از حملات سایبری ایالات‌متحده علیه کشورهای دیگر مصداق بارز نقض اصل عدم‌مداخله است و در قاعده‌ی ۶۶ راهنمای دوم تالین موضوع عدم‌مداخله مدنظر قرارگرفته و ویژگی‌ها و عناصر یک مداخله و انواع مداخله با استفاده از ابزار سایبری را برشمرده شده است. بر این اساس، استفاده یک دولت از ابزارها و عملیات‌های سایبری به‌منظور تغییر آراء الکترونیکی از راه دور و دست بردن در انتخابات از طریق آن، مداخله محسوب می‌شود. چرایی مداخله بودن اقدامات ایالات‌متحده در این است که اولاً موضوع مداخلات مرتبط با عناصر داخلی کشورهاست و از سوی دیگر ماهیت قهری نیز دارد که طبق قاعده‌ی راهنمای مذکور، دو عنصر اصلی مداخله‌ی غیرمجاز سایبری می‌باشد. از سوی دیگر این حملات اکثراً علاوه بر اجبار عناصری شبیه آموزش، تسلیح و تجهیز برخی نیروهای معاند داخلی را دارد که در این خصوص در فضای حقیقی در قضیه‌ی نیکاراگوئه در خصوص مداخله‌ی غیرمجاز مورد تأیید دیوان بین‌المللی دادگستری بوده است. علاوه بر این مسائل در بسیاری از این اقدامات عنصر قصد و تعمد دولت ایالات‌متحده آمریکا در اعمال و یا وانمود نمودن تهدید دیده می‌شود که طبق قواعد عام حقوق بین‌الملل و منشور سازمان ملل، متحد زمینه‌ساز و یا حتی تشکیل‌دهنده‌ی مداخله‌ی غیرمجاز در حاکمیت دولت‌های دیگر می‌باشد.

بی‌تردید در جمع‌بندی بحث می‌توان خلاء حقوقی ناشی از تشتت آراء و نظریات حقوقدانان در خصوص اصل عدم‌مداخله و خصوصیات آن را در مداخلات سایبری نیز به‌وضوح دید؛ که البته علاوه بر این وضعیت نابسامان، فقدان مقررات مشخص بین‌المللی در حملات سایبری مزید بر علت در به وجود آمدن آنارشیسم در این زمینه است؛ لذا در این خصوص پیشنهاد کاربردی که می‌تواند طرح گردد مشتمل بر دو باب خواهد بود؛ اول اینکه حقوقدانان و جامعه‌ی دانشگاهی یا به تعبیری بهتر دکترین حقوق بین‌الملل بر این موضوع مداقه بیشتری نموده و دکترینی را طرح نماید که قابلیت اجرایی داشته باشد و در بعد دیگر و شاید اساسی‌تر، باید جامعه‌ی بین‌المللی و نهادهای سیاسی و مدنی حاکم بر آن در راستای تدوین مقرراتی کامل و لازم‌الاجرا در این زمینه قدم بردارند.

منابع

۱. بای، حسین‌علی و پور قهرمانی، بابک. (۱۳۸۸). بررسی فقهی و حقوقی جرایم رایانه‌ای، قم، پژوهش گاه علوم و فرهنگ اسلامی
۲. مرکز پدافند غیرعامل فاوا. (۱۳۸۸). «جنگ سایبری»، مجله پردازشگر، سال هفتم، ش ۶۴
۳. صانعیان، علی. (۱۳۹۸). «امنیت سایبری در آمریکا، ساختارها و روندها»، فصلنامه سیاست خارجی، دوره ۳۳، شماره ۱، شماره پیاپی ۱۲۹، بهار، ۱۹۱-۲۲۸
۴. ضیایی، سید یاسر، خلیل زاده، مونا. (۱۳۹۲). «مسؤولیت بین‌المللی دولت‌ها ناشی از حملات سایبری»، فصلنامه‌ی پژوهش‌های حقوقی شهر دانش، دوره ۱۲، شماره ۲۳، بهار، ۸۷-۱۲۲
۵. صادقی حقیقی، دیدخت. (۱۳۹۰)، تحول در مفهوم اصل عدم‌مداخله در حقوق بین‌الملل، فصلنامه مطالعات روابط بین‌الملل، دوره ۴، شماره ۱۶ - شماره پیاپی ۱۶، پاییز، ۹۳-۱۲۸
۶. اسمعیل زاده ملاباشی، پرستو، عبدالهی، محسن. (۱۳۹۹). «حملات سایبری و نقض اصل عدم‌مداخله»، فصلنامه مطالعات حقوق عمومی، تابستان، دوره ۵۰، شماره ۲،۷۱۱-۷۳۶
۷. گیوکی، آذر، کفایی‌فر، محمدعلی، رضایی، محمدتقی. (۱۳۹۷). «قابلیت اعمال قواعد حقوق بشردوستانه بین‌المللی در حملات سایبری با نگاهی به دستورالعمل تالین ۲»، مجله علمی پژوهشی حقوق پزشکی، شماره ۱۲، ۱۷۳-۱۸۶
۸. گیوکی، آذر، حکاک‌زاده، محمدرضا. (۱۴۰۱). «مداخله خارجی در امور داخلی دولت‌ها از طریق عملیات سایبری با توجه به دستورالعمل تالین»، فصلنامه علمی مطالعات حقوقی فضای مجازی، بهار، دوره ۱، شماره ۱
۹. صابر نژاد، علی و هاشم‌پور حمیدی، هادی. (۱۳۹۲). «جنگ سایبری و تحول مفهوم توسل به زور در حقوق بین‌الملل»، پنجمین همایش مجازی بین‌المللی تحولات جدید ایران و جهان، قزوین
۱۰. صلاحی، سهراب، کشفی، سید مهدی. (۱۳۹۵). «جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تالین»، فصلنامه مطالعات قدرت نرم، بهار و تابستان، شماره ۱۴، ۲۸-۴۷
۱۱. قاسمی، غلامعلی. (۱۳۹۵). «چالش‌های اصل عدم‌مداخله و جایگاه آن در حقوق بین‌الملل»، فصلنامه آفاق امنیت، دوره ۹، شماره ۳۳.
۱۲. باستانی، برومند. (۱۳۸۳). جرایم کامپیوتری و اینترنتی، جلوه‌ای نوین از بزهکاری، تهران، بهنامی
۱۳. اصلانی، جبار. (۱۳۹۵). «حملات سایبری در چهارچوب نظام مسئولیت بین‌المللی»، رساله دکتری، دانشگاه تهران
۱۴. هالپین، ادوارد. (۱۳۸۹). جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی، ترجمه آرانی روح‌الله، تهران، مرکز پژوهش‌های مجلس
۱۵. قاجار قیونلو، سیامک. (۱۳۹۱). مقدمه حقوق سایبر، چاپ اول، تهران، نشر میزان
۱۶. پور قهرمانی، بابک، صابر نژاد، علی. (۱۳۹۴). حریم خصوصی در فضای سایبر از منظر حقوق بین‌الملل، انتشارات مجد
۱۷. برادران، نازنین، همایون، حبیبی، زمانی، قاسم، هنجنی، سید علی. (۱۳۹۶). «کاربرد اصل عدم‌مداخله در امور داخلی دولت‌ها در حملات سایبری»، فصلنامه پژوهش‌های سیاسی و بین‌المللی، دوره ۸، شماره ۳۳
۱۸. پور قهرمانی، بابک و صابر نژاد، علی. (۱۳۹۲). «ضرورت تدوین قواعد بین‌الملل برای مبارزه با جنگ سایبری»، چهارمین همایش مجازی بین‌الملل ایران و جهان
۱۹. جعفری، افشین و توتونچیان، مهری. (۱۴۰۰). «بررسی راه‌کارهای تهدید حملات سایبری از منظر حقوق بین‌الملل بشردوستانه»، ماهنامه حقوق شهروندی، شماره ۱۸، فروردین، ۳۵۱-۳۳۱
۲۰. مسعودی، امیر. (۱۳۸۳). «امنیت اطلاعات در فضای سایبر»، تهران، نشریه کتاب ماه
21. black-law-dictionary(2004). approaches to cyber space,london,ashgate publishing
22. Clark,Richard (2009). War from Cyberspace، the National Interest
23. Roscini, Marco. (2014). Cyber operation and use of force in international law, oxford press
24. Schmitt, Michael N. (2013). Tallin Manual on the International Law Applicable to Cyber Warfare, New York, Cambridge University Press
25. Tallinn Manual 2.0 On The International Law Applicable To Cyber Operation (2017). Perpared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Center of Excellence,Cambridg university press

26. Cornish, Paul،David Livingstone (2010)."On Cyber Warfare، a Chatham House Report"، The Royal Institute of International Affairs.
27. Dorn, W. (2017). Cyberpeacekeeping: A new role for the United Nations". Geo. J. Int'l Aff.No.18
28. Dunn Cavetly, Myriam, (2011). "Cyber-Allies",IP Global Edition,Vol. 1, 12
29. Michael Alex (2010). "Cyber Probing،the Politicization of Virtual Attack",Research & Assessment Branch (R&AB), Swindon, United Kingdom.
30. Marrone, A. & Sabatino, E. (2021). "Cyber Defence in NATO Countries: Comparing Models". Istituto Affari Internazionali (IAI).
31. Army, U. (2005),Cyber Operations and Cyber Terrorism In U. Army, U.S. Army Trainin.
32. Declaration on Friendly Relations,1970
33. ICj Reports, Nicaragua judgment,1986
34. Nakashima, Ellen (13 September 2016). "Obama to be urged to split cyberwar command from NSA". The Washington Post. Archived from the original on 14 September 2016
35. Rep. of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, para. 2 (May 28, 2021) https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf
36. Rodriguez, Carlos A. (2006),Cyber terrorism Inter-American Defense College as a prerequisite for the Diploma approved
37. https://www.washingtonpost.com/world/national-security/obama-to-be-urged-to-split-cyberwar-command-from-the-nsa/2016/09/12/0ad09a22-788f-11e6-ac8e-cf8e0dd91dc7_story.html