

اعمال حاکمیت بر قلمرو سایبری ملی با اتکا به حقوق بین الملل

سید حسین علوی^۱، محمدرضا حسینی^۲، مهراب رامک^۳

^۱ دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
h.alavi@aut.ac.ir

^۲ دانشیار گروه مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
rezahsn88@gmail.com

^۳ دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
m.ramak@aut.ac.ir

چکیده

در ابتدای شکل‌گیری فضای سایبر، برخی نظریه‌پردازان بر این باور بودند، توسعه فضای سایبری و برقراری تعاملات اقتصادی، سیاسی و فرهنگی در سطح جهانی، با تعابیری از قبیل مرززدایی، سرزمین‌زدایی، قلمروزدایی و حاکمیت‌زدایی همراه خواهد بود اما هم‌اکنون به‌طور گسترده‌ای پذیرفته شده است که فضای سایبری یک منطقه عاری از قانون نیست که در آن هر کس بتواند با رفتار بدون ضابطه و بدون نظر گرفتن قوانین، مقررات و قواعد پذیرفته شده بین‌المللی، هر گونه فعالیت خصمانه‌ای انجام دهد. مسئله اصلی این پژوهش این است که آیا اصول و قواعد حقوق بین‌الملل حال حاضر، با قاطعیت و شفافیت از اقدامات خصمانه سایبری که حاکمیت کشورها بر قلمرو سایبری را نقض می‌کنند، جلوگیری می‌کند و این اصول و قواعد قابل اتکا در صیانت از حاکمیت کشورها بر قلمرو سایبری ملی هستند؟ این نوشتار با مرور و بررسی اسناد، اصول و قواعد حقوق بین‌الملل مرتبط با حاکمیت سایبری ملی که با استفاده از روش تحلیل محتوای کیفی و ابزار نرم‌افزار مکس کیودا انجام پذیرفته است نتیجه می‌گیرد، اصول و قواعد حقوق بین‌الملل حال حاضر از کارایی و توانایی لازم در صیانت از حاکمیت سایبری ملی کشورها برخوردار نیست و عموماً اقدامات ناقض حاکمیت سایبری ملی با شدت متوسط و کم (اعم از: توسل به زور، مداخله غیرمجاز و ...) فاقد پیگرد قانونی هستند. از این رو این قواعد و اصول در مقابل اقدامات مخرب و ناقض حاکمیت سایبری ملی از بازدارندگی لازم برخوردار نیستند.

کلمات کلیدی: قلمرو سایبری، حاکمیت ملی سایبری، اصول و قواعد حقوق بین‌الملل.

۱ مقدمه

در ابتدای شکل‌گیری فضای سایبر، برخی نظریه‌پردازان بر این باور بودند، توسعه فضای سایبری و برقراری تعاملات اقتصادی، سیاسی و فرهنگی در سطح جهانی، با تعابیری از قبیل مرززدایی، سرزمین‌زدایی، قلمروزدایی، و دولت‌زدایی همراه خواهد بود و توسعه فناوری اطلاعات و ارتباطات که به ارتباط انسان‌ها

در اقصی نقاط کره زمین و در فضای مجازی منجر شده است به منزله نابودی قلمرو، مرز، حکومت و دولت خواهد بود. لیکن پس از آن مشخص شد چون فضای سایبری از هر حیث بر فضای واقعی تکیه دارد و از سوی دیگر از ماهیت ابزاری برخوردار است که به وسیله انسان در فضای واقعی و در راستای تأمین نیازهایش بکارگرفته و مدیریت می‌شود، تصور نابودی و زدایش این مفاهیم ممکن نیست. بر پایه این استدلال مفاهیم حاکمیت، قلمرو و مرز، ابدی و انکارناپذیر بوده و با تحولات فناورانه از قبیل توسعه فضای سایبری و فناوری‌های اطلاعاتی و ارتباطی و تجلی‌های دیجیتالی آن از بین نمی‌رود. با این تفاوت که قلمرو و مرز در فضای سایبری از ماهیت مجازی و دیجیتالی برخوردار بوده و محدوده آن با شاخص‌های متفاوتی نسبت به فضای واقعی تعیین می‌گردد.

از این رو بکارگیری فضای سایبر در شئون مختلف زیست بشری موجب گردیده است اعمال حاکمیت در فضای سایبر کشورها یکی از ابعاد جدید حاکمیت ملی و امری ضروری به شمار آید. یکی از شیوه‌های مؤثر در اعمال حاکمیت سایبری ملی، اتکا به حقوق بین‌الملل در این زمینه است و تسلط و توانایی در ارایه مستندات و دلایل حقوقی در پیگیری حقوقی و قضایی اقدامات و فعالیت‌های ناقض حاکمیت ملی در فضای سایبری در مجامع بین‌المللی، بخشی از قدرت ملی به حساب می‌آید.

به علاوه، از آنجا که فضای سایبری در امتداد فضای واقعی است، دولت‌ها می‌توانند بر مردم و اشیاء موجود در قلمرو خود اعمال قدرت کنند و فعالیت‌های آنها را تنظیم کنند. یعنی اینکه افراد، تجهیزات و داده‌های موجود در قلمرو سایبری هر کشور تابع حکمرانی آن کشور بوده و تمام کشورها حق دارند از قلمرو خود در برابر هر گونه تجاوز محافظت نمایند. از سوی دیگر اعمال نشدن حاکمیت سایبری ملی، منجر به تضعیف نظام حاکم خواهد شد و رفتار قانون‌مند کنشگران ملی و بین‌المللی در یک فضای قانونی را به همراه نخواهد داشت.

امروزه زیرساخت‌های حیاتی کشور به‌عنوان مؤلفه حائز اهمیت حاکمیت ملی، یا بخشی از فضای سایبر کشور محسوب می‌شوند یا حداقل در این فضا پایش، کنترل، مدیریت و مورد بهره‌برداری قرار می‌گیرند. استفاده از سخت‌افزارها، میان‌افزارها، نرم‌افزارها و پروتکل‌های غیربومی در محیط شبکه‌ای زیرساخت‌های حیاتی، در صورتی که چگونگی اعمال حاکمیت بر قلمرو سایبری ملی مشخص نگردد و تضمین‌های لازم در ممانعت از هر گونه نقض حاکمیت ملی در این فضا با استناد به اصول و قواعد حقوق بین‌الملل احصاء نگردد، می‌تواند عواقب گاه جبران‌ناپذیری در مقابل اقدامات ناقض حاکمیت اعم حملات سایبری خارجی و ... برای امنیت ملی کشور به همراه داشته باشد.

واضح است در صورت مشخص نشدن چگونگی اعمال حاکمیت بر قلمرو سایبری ملی در پرتو حقوق بین‌الملل و عدم آگاهی و آشنایی متولیان و کنشگران کشور به اصول، قواعد و راهکارهای حقوقی، پیگیری قانونی و حقوقی در صورت تعرض به قلمرو فضای سایبری کشور و نقض حاکمیت ملی در این عرصه، امکان‌پذیر نخواهد بود.

همچنین در صورت مشخص نشدن چگونگی اعمال حاکمیت بر قلمرو سایبری ملی در پرتو حقوق بین‌الملل؛ امکان سیاست‌گذاری، هماهنگی و اجرا بین بخش‌های مختلف کشور، در اعمال حاکمیت سایبری ملی فراهم نخواهد شد.

دغدغه و مسئله این تحقیق، اکتشاف چگونگی اعمال حاکمیت بر قلمرو سایبری ملی با اتکا به حقوق بین‌الملل می‌باشد و گروه محققین، با مرور و بررسی اصول و قواعد حقوق بین‌الملل حال حاضر به دنبال پاسخ به این سؤال هستند که آیا اصول و قواعد حقوق بین‌الملل با قاطعیت و شفافیت از اقدامات خصمانه سایبری که حاکمیت کشورها بر قلمرو سایبری را نقض می‌کنند، جلوگیری می‌کند و این اصول و قواعد قابل اتکا در صیانت از حاکمیت کشورها بر قلمرو سایبری ملی هستند؟

۲ مبانی نظری تحقیق

۱.۲ پیشینه تحقیق

با بررسی‌های انجام شده در منابع مختلف، موارد زیر به عنوان پیشینه تحقیق به دست آمده است: مصطفی فضائلی و موسی کرمی (۱۳۹۹) در مقاله‌ای با عنوان «تحول تاریخی حقوق بین‌الملل توسل به زور تا شکل‌گیری نظام ملل متحد؛ بیم‌ها و امیدها» که در فصلنامه علمی مطالعات دفاع مقدس دانشگاه عالی دفاع ملی به چاپ رسیده است، کوشیده‌اند تا از رهگذر تاریخی به تحلیل چگونگی تنظیم حقوقی توسل به زور تا شکل‌گیری نظام ملل متحد، کاستی‌ها و چالش‌های آن پردازند و بر این نکته تأکید نموده‌اند، طی دهه‌های گذشته جامعه بین‌الملل شاهد گذار از اصل توسل به زور برای حل و فصل اختلافات، به اصل ممنوعیت بکارگیری زور به سان قاعده‌ای بنیادین در روابط میان دولت‌ها بوده است. به باور نگارندگان این پژوهش، این روند تکاملی را باید از نشانه‌های نهادینه شدن تدریجی حقوق بین‌الملل توسل به زور در روابط میان دولت‌ها قلمداد کرد و بر همین پایه می‌توان از کارآمدی نسبی این شاخه حقوقی در کاهش بکارگیری زور در این بستر سخن راند. در نتیجه طی سال‌های گذشته، روابط بین‌الملل از افسارگسیختگی بی‌حد و حصر دولت‌ها در بکارگیری زور تا محدود شدن آن به مواردی انگشت‌شمار و معین را تجربه کرده و شاهد بوده است (مصطفی فضائلی و موسی کرمی، ۱۳۹۹)؛ (Fazaeli, Mustafa & Karami, Musa, 2020).

در پژوهشی دیگر احسان کیانخواه (۱۳۹۸)، طی مقاله‌ای با عنوان «چالش‌های راهبردی حکمرانی با گسترش فضای سایبر» که در فصلنامه علمی امنیت ملی دانشگاه عالی دفاع ملی به چاپ رسیده است، به اکتشاف چالش‌های حکمرانی با گسترش فضای سایبر پرداخته است. این پژوهش نتیجه می‌گیرد، به خدمت گرفتن هر پدیده نیازمند فهم دقیق آن است و توجه به مصالح و مفاسد آن دارد. درجه پیچیدگی فهم پدیده‌ها بر اساس کارایی و وسعت آثار آن متفاوت است. فضای سایبر در کنار تحولات مطلوب و پرشتاب آن، دارای مفاسدی است که موجب چالش‌های کلیدی برای حکمرانی کشور شده است. در پایان نیز چالش‌های راهبردی حکمرانی با گسترش فضای سایبر را احصا نموده است. این پژوهش تأکید می‌نماید عدم توجه به چالش‌های راهبردی حکمرانی با گسترش فضای سایبر، منجر به وابستگی کشور به بیگانگان و سلطه کفار بر نظام اسلامی خواهد شد. (احسان کیانخواه، ۱۳۹۸)؛ (Kiankhah. 2020).

در مقاله‌ای دیگر، امید جعفرنیا و محمدرضا کریمی قهرودی (۱۳۹۹)، در پژوهشی با عنوان «اهمیت و الزامات حاکمیت فضای سایبری» که در چهارمین کنفرانس ملی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک ایران به چاپ رسیده است، به بررسی اهمیت و الزامات حاکمیت فضای سایبری پرداخته‌اند. این

پژوهش تصریح می کند، حاکمیت فضای مجازی به بخش مهمی از حاکمیت فضای واقعی ملی تبدیل خواهد شد. این پژوهش، ضمن بررسی برخی اختلافات به وجود آمده در نبود حاکمیت فضای مجازی، لزوم وجود حاکمیت فضای سایبری و فواید آن در حاکمیت ملی، کنترل و همکاری در امور مربوط به ایجاد عدالت بین المللی در این فضا را اثبات می نماید. بر این اساس حضور قوی در تعاملات بین المللی فضای مجازی جهت تبیین ملاحظات و الزامات کشور در ساختارهای مدیریت و کنترل جهانی این فضا به عنوان خروجی این تحقیق احصاء شده است (امید جعفرنیا و محمد رضا کریمی قهرودی، ۱۳۹۹؛ (Jafarnia, Omid and Karimi Ghahroudy, Mohammad Reza, 2019).

علی رغم انجام پژوهش های متعدد در زمینه حقوق بین الملل، حاکمیت ملی و حاکمیت سایبری که در منابع داخلی و خارجی ارایه گردیده است، و با توجه به شرایط خاص کشور ما که همواره دشمنان در پی نقض حاکمیت سایبری ملی و وارد نمودن آسیب به منافع و سرمایه های ملی کشور هستند، بررسی چگونگی اعمال حاکمیت سایبری ملی با اتکا به حقوق بین الملل که مد نظر این پژوهش است، تاکنون انجام نشده است و با توجه به خلأ دانشی موجود در این زمینه، انجام این پژوهش ضروری به نظر می رسد.

۲.۲ مفهوم شناسی تحقیق

۱.۲.۲ قلمروی سایبری

قلمرو عبارت است از فضای جغرافیایی مشخص، اعم از واقعی و مجازی که منعکس کننده عرصه حاکمیت و فرمان رویی یک بازیگر سیاسی به ویژه حکومت یا حوزه کنترل و نفوذ یک کارکرد و فعالیت سیاسی، اجتماعی، فرهنگی و ... آن می باشد. همان طور که در فضای واقعی حیات و فعالیت انسان ها، قلمروها و عرصه های مختلف برای اعمال حاکمیت وجود دارد، در فضای سایبری نیز عرصه های حاکمیتی و قلمروهای فعالیت، با فضا و چارچوب مشخص وجود دارد. با این تفاوت که این قلمروها از ماهیت مجازی و دیجیتالی برخوردارند (حافظ نیا، ۱۳۹۰؛ (Hafeznia Mohammad Reza, 2011).

۲.۲.۲ حاکمیت ملی سایبری

حاکمیت فضای سایبری یک کشور مبتنی بر سامانه های اطلاعاتی و ارتباطی تحت اختیار آن کشور می باشد. مرزهای حاکمیت فضای سایبری یک کشور از مجموعه تجهیزات شبکه ای آن کشور که به طور مستقیم به تجهیزات شبکه ای کشورهای دیگر متصل هستند تشکیل می شود. حاکمیت فضای سایبری به منظور حفاظت از عملیات های مختلفی که کاربران سایبر روی داده ها انجام می دهند اعمال می گردد.

تعریف سازمان ملل متحد از حاکمیت ملی سایبری عبارت است از: «حاکمیت ملی، هنجارها و اصول بین المللی که از حاکمیت نشئت می گیرند، در مورد فعالیت های کشورها در ارتباط با فناوری اطلاعات و ارتباطات و اختیار آنها بر زیرساخت های اطلاعاتی و ارتباطی موجود در قلمرو سرزمینی نیز صادق می باشد. بر این اساس اگرچه در تعریف مذکور به طور مستقیم به واژه «فضای سایبری» اشاره نشده است ولی این تعریف نشان می دهد حاکمیت ملی در دو سطح اعمال می گردد: سطح فنی و سطح اجتماعی. در سطح فنی حاکمیت ملی در مورد زیرساخت های اطلاعاتی و ارتباطی، که در سطح «سایبر» قرار دارند و اینترنت و

انواع مختلف شبکه‌های مخابراتی و سامانه‌های ارتباطی، شبکه‌های رادیویی و تلویزیونی، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های موجود در تجهیزات صنعتی کلیدی را در بر می‌گیرند، اعمال می‌شود. در سطح اجتماعی، حاکمیت ملی در مورد فعالیت‌های مرتبط با فناوری اطلاعات و ارتباطات که در سطح «فضا» قرار دارند و فعالیت‌های مختلف که سکوی نظام فناوری اطلاعات و ارتباطات را در بر می‌گیرند، اعمال می‌گردد.» (کریمی قهرودی، ۱۳۹۹)؛ (Karimi Ghahroudi Mohammad Reza, 2020).

از این رو اقدامات و عملیات‌های سایبری که از اعمال امتیازات حاکمیتی دولت ممانعت به عمل می‌آورند و موجب نقض اقتدار حاکمیتی دولت در فضای سایبری می‌شوند، ناقض حاکمیت سرزمینی کشورها بوده و در حقوق بین‌الملل ممنوع می‌باشند.

۳.۲.۲ اصول و قواعد حقوق بین‌الملل مرتبط با حاکمیت ملی سایبری

اصل خودداری از تهدید و توسل به زور. بند ۴ ماده ۲ منشور ملل متحد مقرر می‌دارد، کلیه اعضای ملل متحد در روابط بین‌الملل خویش از تهدید و بکارگیری زور علیه یکپارچگی سرزمینی یا استقلال سیاسی کشور دیگر به هر شیوه‌ای که با اهداف ملل متحد ناسازگار باشد خودداری خواهند ورزید و امروزه این ممنوعیت قاعده‌ای از حقوق بین‌الملل عرفی به حساب می‌آید. یعنی اگر چه بند ۴ ماده ۲ منشور ملل متحد در بیان صریح خود انحصاراً بر اعضای ملل متحد اعمال می‌شود، ولی ممنوعیت توسل به زور از رهگذر حقوق بین‌الملل عرفی به کشورهای غیر عضو نیز تسری می‌یابد (Leigh, M. 1985).

دیوان بین‌المللی دادگستری نیز با استناد به ماده ۲ بند ۴ منشور ملل متحد، ممنوعیت هر گونه بکارگیری زور توسط دولت‌ها (فارغ از تسلیحات مورد استفاده) به منظور نقض یا خدشه‌دار نمودن حاکمیت سرزمینی کشور دیگر را اعلام نموده است. لزومی ندارد عملی که «بکارگیری زور» به شمار می‌آید، ضرورتاً توسط نیروهای مسلح یک کشور انجام شده باشد یا صرف اینکه یک رایانه (و نه یک اسلحه یا سامانه تسلیحاتی) در انجام عملیات به کار رود، تأثیری در «به‌کارگیری زور» قلمداد شدن یا نشدن عملیات ندارد. هر گونه توسل به زور که توسط عوامل دولتی انجام شود یا وفق حقوق مسئولیت دولت، قابل انتساب به یک دولت باشد ذیل این اصل حقوق بین‌الملل قرار می‌گیرد. واضح است اقدامات بازیگران غیردولتی از جمله افراد، گروه‌های سازمان‌یافته و سازمان‌های تروریستی قابل تسری به این ممنوعیت نخواهد بود مگر اینکه قابل انتساب به دولت باشند (Falk, R. 1997).

اصل ممنوعیت مداخله غیرمجاز در امور داخلی دیگر کشورها. ممنوعیت مداخله غیرمجاز در امور داخلی دیگر کشورها، یک اصل اساسی حقوق بین‌الملل است که در منشور ملل متحد صراحتاً به آن اشاره نشده است ولی طی سالیان گذشته از حقوق عرفی برخوردار شده است. بر اساس بیانیه مجمع عمومی سال ۱۹۶۵ میلادی در مورد غیرقابل قبول بودن مداخله در امور داخلی دولت‌ها و حفاظت از استقلال و حاکمیت آنها، که مجدداً در بیانیه مجمع عمومی سال ۱۹۷۰ میلادی در مورد روابط دوستانه و همکاری میان دولت‌ها نیز تکرار شد: «هیچ دولتی حق مداخله مستقیم یا غیر مستقیم در امور داخلی و خارجی دولت‌های دیگر را ندارد». در نتیجه، مداخله مسلحانه و سایر اشکال مداخله و یا حتی تلاش برای تهدید علیه شخصیت

دولت و عناصر سیاسی، اقتصادی و فرهنگی آن محکوم است. همچنین دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه، ممنوعیت مداخله را «حق هر دولت مستقل برای انجام امور [خارجی یا داخلی] خود بدون دخالت خارجی» تعریف کرده است (Leigh, M. 1985).

برای تعریف محتوا و معنای اصل عدم مداخله در حقوق بین‌الملل، باید معنای نقطه مقابل آن، یعنی مداخله را توضیح دهیم. بر اساس تعریف اوپنهایم، مداخله عبارت است از «هر گونه مداخله یا اقدام توأم با اجبار و زور که دولت را از کنترل بر موضوع مورد نظر محروم می‌کند». از تعریف فوق معلوم می‌شود که برای انتصاب مداخله، باید دو شرط برآورده گردد: اول باید بر امور و موضوعاتی که در حاکمیت یک دولت قرار دارند تأثیر بگذارد و ثانیاً باید اجباری باشد (Oppenheim, L. 1921).

۴.۲.۲ اسناد حقوق بین‌الملل مرتبط با حاکمیت ملی سایبری

منشور ملل متحد. با استناد به متن منشور ملل متحد، اعلامیه اصول حقوق بین‌الملل درباره روابط دوستانه و همکاری میان دولت‌ها، اعلامیه ارتقاء اثربخشی اصل خودداری از تهدید یا توسل به زور در روابط بین‌الملل و آراء دیوان بین‌المللی دادگستری، حاکمیت بر قلمرو ملی و سرزمینی یکی از اصول اساسی منشور ملل متحد است که از تساوی حاکمیتی کشورها، عدم توسل به زور علیه تمامیت ارضی و ممنوعیت اقداماتی که با مقاصد منشور در تضاد هستند نتیجه می‌شود. منشور ملل متحد در فصل اول، پس از برشمردن مقاصد ملل متحد در ماده یک؛ برای نیل به مقاصد یاد شده، در ماده دوم به اصل تساوی حاکمیت تمامی اعضا تأکید می‌نماید. مهم‌تر از آن در بند ۴ ماده ۲ مقرر می‌دارد «تمامی اعضا در روابط بین‌الملل خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی و استقلال سیاسی کشورهای دیگر، از هر روشی که با مقاصد منشور ملل متحد در تضاد باشد، خودداری خواهند نمود» (منشور ملل متحد، ۱۹۴۵).

کتابچه راهنمای تالین ۲. یکی از مهم‌ترین تلاش‌ها برای تحقیق روی قواعد بین‌المللی حاکم بر اقدامات سایبری، توسط گروه کارشناسان بین‌المللی به دعوت مرکز تعالی دفاع سایبری ناتو تحت عنوان راهنمای تالین یک و دو انجام پذیرفته است. راهنمای تالین یک با عنوان «دستورالعمل حقوق بین‌الملل قابل اعمال در نبرد سایبری» توسط متخصصین و صاحب‌نظران حقوقی و فنی در قالب ۹۵ قاعده اساسی در سال ۲۰۱۳ میلادی توسط انتشارات دانشگاه کمبریج به چاپ رسیده است. نسخه تکمیلی راهنمای تالین یک، تحت عنوان راهنمای تالین دو که به حقوق بین‌الملل قابل اعمال بر عملیات‌های سایبری می‌پردازد، در قالب ۱۵۴ قاعده کلی حقوق بین‌الملل حاکم بر اقدامات سایبری در سال ۲۰۱۷ تدوین و به چاپ رسیده است.

در این زمینه قواعد تالین دو که مرتبط با احترام به حاکمیت سرزمینی کشورها و ممنوعیت نقض حاکمیت ملی در فضای سایبر، احترام به حقوق بشر، منع مداخله در امور داخلی کشورها، ممنوعیت تهدید و توسل به زور می‌باشند و همه این قواعد به حاکمیت بر قلمرو سایبری کشورها و ممانعت از هرگونه تجاوز و دست اندازی به قلمرو و مرزهای سایبر ملی تأکید دارند، اشاره می‌گردد.

صلاحیت سرزمینی و حاکمیت بر قلمرو از اصول بنیادین حقوق بین‌الملل به شمار می‌روند. قواعد ۱ تا ۱۳ راهنمای تالین دو، تصدیق می‌نمایند صلاحیت سرزمینی و فراسرزمینی و نیز حاکمیت دولت‌ها بر قلمرو،

می‌بایست در فضای سایبری نیز اعمال گردد. اگر چه اصل صلاحیت سرزمینی در دل اصل حاکمیت نهفته است، گروه کارشناسان بین‌المللی تالین این اصول را در قالب قواعد تفکیک شده تدوین نموده‌اند. از میان قواعد مبتنی بر صلاحیت سرزمینی و حاکمیت دولت‌ها در فضای سایبری، قاعده شماره ۴ که به ممنوعیت نقض حاکمیت دولتی کشورها در این فضا اشاره دارد، از اهمیت بیشتری برخوردار است. قواعد تالین دو مقرر می‌نمایند، یک دولت، با لحاظ محدودیت‌های مقرر در حقوق بین‌الملل، از صلاحیت سرزمینی و فراسرزمینی بر فعالیت‌های سایبری مرتبط با خود برخوردار است.

قواعد ۳۴ تا ۳۸ راهنمای تالین دو، از نظام بین‌الملل حقوق بشر در فعالیت‌های سایبری، تعهد دولت‌ها به احترام و حمایت از حقوق بشر و موارد استثناء قابل قبول در تخطی از حقوق بشر، سخن می‌گوید. کارشناسان تدوین تالین دو بر این باورند، اعلامیه جهانی حقوق بشر، به عنوان بازتاب‌دهنده هنجارهای عرفی اصلی حقوق بشر مورد تأیید همگان است.

به واسطه پیوند روزافزون جامعه جهانی و وابستگی رو به رشد دولت‌ها به بهره‌گیری از زیرساخت‌های سایبری، این عرصه فرصت‌هایی را برای مداخله سایر دولت‌ها در امور داخلی کشورها قرار داده است. بر این اساس قواعد ۶۶ و ۶۷ راهنمای تالین دو، به مبانی حقوق بین‌الملل منع مداخله جبرآمیز دولت‌ها و ملل متحد (به استثناء آنچه ذیل فصل هفتم منشور ملل متحد قرار می‌گیرد) در امور داخلی کشورها در فضای سایبری و با استفاده از ابزارهای سایبری اختصاص یافته است. اصل برابری حاکمیتی و احترام به حاکمیت دولت‌ها ایجاب می‌نماید، دولت‌ها از اقدامات و اموری که در حیطه حاکمیت دولت دیگر هستند و مداخله در آنها، حاکمیت دولت سرزمینی را خدشه‌دار می‌نماید از طریق ابزارهای سایبری اجتناب نمایند (Schmitt, M. N., 2017. Tallinn manual 2).

۳ روش‌شناسی تحقیق

۱.۳ نوع تحقیق

نظر به اینکه انجام این پژوهش به بررسی چگونگی اعمال حاکمیت بر قلمرو سایبری ملی با اتکا به حقوق بین‌الملل منجر می‌شود و نتایج حاصل از این پژوهش شناخت بهتر و افزایش توان اتخاذ مناسب‌ترین تصمیمات توسط متولیان امر در کشور را به همراه خواهد داشت، جنبه کاربردی دارد. همچنین با توجه به اینکه توسعه پژوهش‌های گذشته و گسترش دانش در این حوزه را به دنبال دارد، توسعه‌ای به حساب می‌آید. بنابراین تحقیق حاضر با توجه به هدف، از نوع توسعه‌ای-کاربردی می‌باشد.

۲.۳ روش تحقیق

روش تحقیق مورد استفاده، با رویکرد کیفی از نوع تحلیل محتوا و ابزار مورد استفاده نرم‌افزار مکس کیودا^۱ می‌باشد. در این پژوهش اسناد حقوق بین‌الملل مرتبط با حاکمیت سایبری ملی و سرزمینی اعم از منشور ملل متحد، منشور حقوق بشر، اعلامیه حقوق بین‌الملل درباره روابط دوستانه و همکاری میان دولت‌ها، اعلامیه

^۱MAXQDA 10

ارتقاء اثربخشی اصل خودداری از تهدید یا توسل به زور در روابط بین الملل، آراء دیوان بین المللی دادگستری، گزارش‌های گروه کارشناسان دولتی سازمان ملل متحد در زمینه توسعه فناوری اطلاعات و ارتباطات (GGE) و کتابچه راهنمای تالین دو (به‌عنوان یکی از مهم‌ترین تلاش‌ها برای تحقیق روی قواعد بین المللی حاکم بر اقدامات سایبری که توسط گروه متخصصین بین المللی به دعوت مرکز تعالی دفاع سایبری ناتو انجام پذیرفته است)؛ با استفاده از نرم‌افزار مکس کیودا در قالب روش تحلیل محتوای استنباطی از نوع قراردادی یا عرفی مورد بررسی قرار گرفت.

در این زمینه قواعدی که به موضوع حاکمیت سایبری ملی کشورها تأکید دارد اعم از قواعد احترام به حقوق بشر بین المللی، احترام به حاکمیت سرزمینی کشورها، ممنوعیت نقض حاکمیت ملی، ممنوعیت تهدید یا توسل به زور و منع مداخله غیرمجاز در امور داخلی کشورها؛ با استفاده از نرم‌افزار مکس کیودا تحلیل محتوا و کدگذاری گردید که منجر به احصاء ۸۱ کد یا واحد معنایی در زمینه حاکمیت بر قلمرو سایبری ملی و سرزمینی گردید. در ادامه پس از چند بار مرور کدها، کدها یا واحدهای معنایی نزدیک به هم با یکدیگر ترکیب گردید تا واحدهای معنایی منسجم و ساختاریافته‌تری ایجاد گردد. در مرحله بعد پس از مرور چندباره واحدهای معنایی، واحدهای معنایی که با یکدیگر مرتبط و یک مقوله خاصی را تداعی می‌نمایند، دسته‌بندی گردید تا زیرطبقات مورد بحث تولید گردند. در این مرحله نیز واحدهای معنایی و زیرطبقات به صورت رفت و برگشتی چند بار مرور شد تا از صحت فرآیند دستیابی به زیرطبقات اطمینان حاصل شود.

پس از بررسی واحدهای معنایی و زیرطبقات مرتبط با حاکمیت بر قلمرو سایبری ملی در اسناد حقوق بین الملل، مشخص گردید، علی‌رغم وجود اصول و قواعدی که احترام به حاکمیت کشورها بر قلمرو سرزمینی، پایبندی به حقوق بشر (مردمان) ساکن در قلمرو سرزمینی سایر دولت‌ها، احترام به صلاحیت دولت‌ها در کنترل و مدیریت منابع و زیرساخت‌ها در قلمرو سرزمینی، ممنوعیت تهدید و توسل به زور علیه دولت دیگر و ممنوعیت مداخله در امور داخلی دیگر کشورها را از اصول اساسی در حقوق بین الملل به شمار می‌آورند؛ در اسناد مزبور، واحدهای معنایی و زیرطبقاتی وجود دارند که نه تنها صیانت از حاکمیت ملی و سرزمینی را تضمین نمی‌نمایند بلکه امکان نقض حاکمیت سایبری ملی و سرزمینی را فراهم می‌نمایند و پیگرد حقوقی اقدامات و عملیات‌های سایبری با استناد به اصول و قواعد حقوق بین الملل میسر نیست. از این رو می‌توان نتیجه گرفت، اسناد حال حاضر حقوق بین الملل، حاکمیت سایبری ملی کشورها را تضمین نمی‌نمایند و موارد نقض متعدد غیرقابل پیگیری در حقوق بین الملل وجود دارد.

جدول ۱، واحدهای معنایی و زیرطبقات موارد نقض حاکمیت سایبری ملی در حقوق بین الملل، که با استفاده از نرم‌افزار مکس کیودا احصاء شده است و این واحدهای معنایی و زیرطبقات، نمایان گر طبقه اصلی حاصل از تحلیل محتوای کیفی که «ناتوانی حقوق بین الملل در صیانت از حاکمیت سایبری ملی کشورها» می‌باشد را نشان می‌دهد.

جدول ۱: کدهای هدایت کننده، زیرطبقات و طبقه اصلی

طبقه اصلی	زیرطبقات	کدهای هدایت کننده
ناتوانی حقوق بین الملل در حمایت از حاکمیت سایبری ملی کشورها	<ul style="list-style-type: none"> ابهام و عدم قطعیت اسناد حقوق بین الملل در تعیین اقدامات و عملیات های سایبری غیرمجاز که حاکمیت سایبری ملی دیگر کشورها را نقض می نمایند. 	<ul style="list-style-type: none"> علی رغم وجود نظام حقوق بین الملل عرفی و معاهداتی، فهرست قطعی و نهایی از حقوق بین الملل لازم الاجرا برای دولت ها وجود ندارد. تعریف دقیقی از اقدامات ناقض حاکمیت ملی (اعم از: توسل به زور، مداخله غیرمجاز و ...) در اسناد حقوق بین الملل وجود ندارد. تهدید و توسل به زور، صرفاً به اقدامات مسلحانه یک دولت علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولت دیگر اطلاق می گردد. تفسیر کشورها از اقدامات ناقض حاکمیت ملی در اسناد حقوق بین الملل متفاوت است. تعیین سطح آستانه اقدامات و عملیات های سایبری ناقض حاکمیت سرزمینی به سادگی امکان پذیر نیست. تفسیر کشورها از همترازی اقدامات و عملیات های فضای سایبری با اقدامات و عملیات های فضای واقعی متفاوت است.
	<ul style="list-style-type: none"> اقدامات و عملیات های سایبری مخرب و ناقض حاکمیت سرزمینی، صرفاً در مواردی که قابل انتساب به یک دولت دیگر باشند از پیگرد حقوقی برخوردار است. 	<ul style="list-style-type: none"> هر دولت صرفاً مسئول اقدامات اشخاص و نهادهایی است که به نوعی نماینده دولت محسوب می گردند. صرفاً اقدامات و عملیات هایی که قابل انتساب به یک دولت باشند، امکان پیگیری حقوقی دارد. یعنی اقدامات توسط عوامل دولتی یا عوامل غیردولتی که تحت حمایت، کنترل و مدیریت یک دولت هستند انجام گرفته باشد و یا یک دولت عملیات مزبور را به عنوان عملیات خود تصدیق نموده و بپذیرد. انتساب اقدامات و عملیات های سایبری به دولت متخاصم با پیچیدگی و عدم قطعیت های فنی و حقوقی همراه است. تنبیه دولت متخاصم حتی در صورت قطعیت اقدامات متخلفانه سایبری (اعم از توسل به زور، مداخله غیرمجاز و ...) که حاکمیت سرزمینی کشور دیگر را نقض نموده است، با توجه به عدم امکان انتساب به دولت، عملاً امکان پذیر نیست. عملیات ها و اقداماتی که به سطح توسل به زور و اجبار از سوی یک دولت نرسند، ممنوعیت حقوق بین الملل را نقض نمی نمایند. اقدامات و عملیات های سایبری که توسط کنشگران غیردولتی اعم از افراد، گروه های سازمان یافته، سازمان های تروریستی و ... انجام می پذیرد و قابل انتساب به دولت نباشد، قواعد حقوق بین الملل را شامل نمی شود.
	<ul style="list-style-type: none"> اقدامات و عملیات های سایبری مخرب و ناقض حاکمیت سرزمینی، صرفاً در مواردی که علیه یک دولت انجام شده باشند از پیگرد حقوقی برخوردار هستند. 	<ul style="list-style-type: none"> اقدامات دولت متخاصم که نهادها، شرکت ها، اقوام و ... را هدف قرار می دهند، اگر چه تا اندازه ای حاکمیت دولت سرزمینی را نقض می نمایند، قابل پیگیری از طریق مجاری حقوق بین الملل نیستند. عملیات ها و اقداماتی که به سطح توسل به زور و اجبار علیه دولت دیگر نرسند، ممنوعیت حقوق بین الملل را نقض نمی نمایند. حقوق بین الملل عرفی و معاهداتی، موارد استثناء قابل قبول در تخطی دولت ها از تعهدات بین المللی در برابر سایر دولت ها قائل شده است.
	<ul style="list-style-type: none"> عدم تمایل کشورهای پیشرفته و صاحب فناوری به تدوین نظامات حقوقی روشن و متقن برای فضای سایبری در جهت ممانعت و مقابله با فعالیت های مخرب و ناقض حاکمیت ملی و سرزمینی کشورها 	<ul style="list-style-type: none"> عدم اهتمام کشورهای پیشرفته در تصویب قوانین و هنجارهای بین المللی دقیق در منع استفاده خصمانه از فضای سایبری. استفاده از شرایط بدون مرزی، ابهام و پیچیدگی فضای سایبری توسط کشورهای پیشرفته در جهت استفاده از این فضا برای دست یابی مقاصد و منافع خصمانه. بهره گیری از فضای سایبری به عنوان عرصه ای کم هزینه و آسان در جهت استعمار نوین. به نظر نمی رسد در آینده نزدیک اجماع و توافق بین المللی در تدوین اصول، قواعد و هنجارهای اختصاصی فضای سایبری که تضمین کننده حاکمیت سایبری ملی کشورها باشد، انجام پذیرد.
	<ul style="list-style-type: none"> ناتوانی جامعه بین الملل در تدوین نظامات حقوقی شفاف فضای سایبری 	<ul style="list-style-type: none"> عدم توافق کشورها در تدوین اصول و هنجارهای اختصاصی فضای سایبری. نگرش متفاوت کشورها نسبت به مدل حکمرانی فضای سایبری، دست یابی به نظام واحد حقوقی در این زمینه را دور از ذهن نموده است. با توجه به اینکه مقیاس و آثار اقدامات و عملیات های ناقض حاکمیت سایبری ملی ممکن است در کوتاه مدت امکان پذیر نباشد، تدوین نظام حقوقی متناسب برای آنها نیز میسر نیست.

۴ تجزیه و تحلیل یافته‌ها

از تحلیل محتوای کیفی اسناد حقوق بشر یافت می‌شود، احترام به حاکمیت کشورها بر قلمرو سرزمینی یک اصل اساسی در حقوق بین‌الملل به شمار می‌رود و از آن قواعد و هنجارهای بازدارنده‌ای از حقوق بین‌الملل ناشی می‌شود که مورد پذیرش همگان است. مهم‌ترین این قواعد، پایبندی به حقوق بشر (مردمان) ساکن در قلمرو سرزمینی سایر دولت‌ها، احترام به صلاحیت دولت‌ها در کنترل و مدیریت منابع و زیرساخت‌ها در قلمرو سرزمینی، ممنوعیت تهدید و توسل به زور علیه دولت دیگر و ممنوعیت مداخله در امور داخلی دیگر کشورها می‌باشد.

اما همچنین از تحلیل محتوای اسناد حقوق بین‌الملل مرتبط با حاکمیت سایبری ملی و سرزمینی کشورها می‌توان به این نتیجه رسید، قوانین و هنجارهای فعلی بین‌المللی، اقدامات زیر سطح آستانه این قواعد را نمی‌کند و دولت‌ها را ملزم نمی‌کند از هرگونه فعالیتی که حاکمیت دولت سرزمینی را خدشه‌دار می‌کند خودداری نمایند. به خصوص اینکه تعیین سطح آستانه اقدامات ناقض حاکمیت سرزمینی کشورها در فضای مجازی و هم‌تراز شمردن اقدامات و عملیات‌های سایبری با اقدامات و عملیات‌های ناقض حاکمیت سرزمینی در فضای واقعی، به دلیل عدم شفافیت و قطعیت اسناد حقوق بین‌الملل در این زمینه، دوچندان مشکل است. به علاوه، با توجه به خصوصیات و ویژگی‌های فضای سایبری، انتساب اقدامات ناقض حاکمیت سرزمینی به دولت متخاصم، در قریب به اتفاق موارد امکان‌پذیر نیست. شواهد این امر را می‌توان در این واقعیت مشاهده کرد که دولت‌ها عملیات‌های نفوذ، جاسوسی و جمع‌آوری اطلاعات حیاتی و حتی تخریب منابع، زیرساخت‌ها و سامانه‌های موجود در قلمرو سرزمینی دیگر کشورها را از طریق فضای سایبری آن کشورها انجام می‌دهند و پیگرد قانونی از طریق حقوق بین‌الملل متصور نیست.

در کنار این موضوعات، بی‌علاقگی یا ناتوانی کشورها در تدوین نظامات حقوقی شفاف و متقن برای فضای سایبری در جهت ممانعت و مقابله با فعالیت‌های مخرب و ناقض حاکمیت ملی و سرزمینی کشورها در فضای سایبری (با توجه به ویژگی‌های منحصر به فرد این فضا)، منجر به پیدایش ابهامات و روزنه‌هایی برای نقض حاکمیت کشورها و عدم امکان تعیین زمان دقیق نقض حاکمیت و به تبع آن عدم پیگیری بین‌المللی در این زمینه شده است.

با عنایت به مراتب یاد شده می‌توان استنباط کرد، رویکردی که در اسناد حال حاضر بین‌المللی فضای سایبر مورد تاکید قرار گرفته است، بر تاثیرات فیزیکی اقدامات سایبری بر علیه قلمرو سرزمینی کشورها تاکید دارد و جنبه مهم دیگر، یعنی احترام به صلاحیت دولت‌ها در کنترل دسترسی، مدیریت و بهره‌برداری از زیرساخت‌ها و سامانه‌های سایبری مستقر در قلمرو ملی کشورها را به هنگام نقض اصول امنیت سایبری ملی مورد توجه قرار نمی‌دهد. از این رو اقداماتی که منجر به آسیب فیزیکی یا از دست رفتن عملکردهای اساسی نشوند که نیازمند تعمیر یا جایگزینی زیرساخت‌ها و سامانه‌ها باشد، نقض حاکمیت ملی سایبری تلقی نمی‌گردند. همچنین اگر نقض تمامیت سرزمینی یک کشور در حوزه سایبری، صرفاً به تجلی آثار فیزیکی حملات یا از دست دادن عملکرد قابل توجه سامانه‌ها بستگی داشته باشد، دولت‌های هدف در برابر عملیات سایبری که در مراحل مقدماتی خود قرار دارند و یا در حال انجام هستند ولی تاکنون منجر به آسیب و خسارت

سطح بالا نشده اند، هیچ گونه راه حل قانونی در دفاع از خود نخواهند داشت. امروزه عملیات‌های سایبری پیچیده و گسترده علیه زیرساخت‌های یک کشور، به چندین مرحله مقدماتی اعم از شناسایی هدف، انتخاب بردار حمله مناسب، دور زدن امنیت زیرساخت‌ها و سامانه‌های سایبری کشور هدف و در نهایت انجام فعالیت مورد نظر نیاز دارد (در برخی مدل‌های تحلیلی، مراحل مقدماتی انجام عملیات سایبری تا ۷ مرحله عنوان شده است). رویکرد فعلی نقض حاکمیت ملی سایبری در صورت عدم ظهور آثار فیزیکی، تمامی این مراحل را که منجر به نقض اصول امنیت سایبری ملی کشور هدف می‌شوند، نقض حاکمیت بر قلمرو سایبری کشور هدف نمی‌داند و اقدام متقابل و الزام به توقف تحت قواعد و هنجارهای بین‌المللی را به همراه ندارد. در این شرایط و در مورد عملیات‌های سایبری متوسط و کم‌شدت که منجر به خسارت فیزیکی عمده نشوند، مصداق توسل به زور به حساب نیایند یا مداخله آشکار در امور داخلی کشور هدف نباشند عدم قطعیت قانونی وجود دارد.

۵ نتیجه‌گیری

با بررسی و تحلیل محتوای کیفی اسناد حقوق بین‌الملل که با استفاده از نرم‌افزار مکس کیودا انجام شد و با استناد به واحدهای معنایی، زیرطبقه‌ها و طبقه اصلی احصا شده، نتیجه می‌شود، اصول و قواعد حقوق بین‌الملل از کارایی و توانایی لازم در صیانت از حاکمیت سایبری ملی کشورها برخوردار نیست و عموماً اقدامات ناقض حاکمیت سایبری ملی با شدت متوسط و کم (اعم از: توسل به زور، مداخله غیرمجاز و ...) فاقد پیگرد قانونی هستند. از این رو این قواعد و اصول در مقابل اقدامات مخرب و ناقض حاکمیت سایبری ملی از بازدارندگی لازم برخوردار نیستند.

همچنین با توجه به اینکه هنوز هیچ گونه قواعد و هنجار اختصاصی برای اقدامات زیرآستانه استفاده از زور و مداخله آشکار در فضای سایبر سایر کشورها توسعه نیافته است، تعیین دقیق مرز بین اقدامات مجاز و غیر مجاز سایبری با استناد به قوانین، مقررات و هنجارهای بین‌المللی امکان‌پذیر نیست و در بسیاری از موارد دولت‌ها آزاد هستند در این زمینه مطابق تفسیر و میل خود عمل کنند.

از این رو با توجه به یافته این پژوهش لزوم مواجهه فعالانه با موضوع فضای سایبر کشور در جهت صیانت از حاکمیت سایبری ملی، بیش از پیش ضروری به نظر می‌رسد و نیازمند شناسایی و اتخاذ راهکارهایی با هدف تقویت و ارتقاء حاکمیت بر قلمرو سایبری ملی بدون اتکا به اصول و قواعد حقوق بین‌الملل هستیم. از نظر نگارندگان این نوشتار دو راهکار قلمروگذاری و مرزبانی مؤثر و کارآمد از فضای سایبری کشور در عرصه ملی و دیپلماسی، همکاری و هماهنگی با کشورهای همسایه و حضور مؤثر در مجامع بین‌المللی با هدف تبیین مواضع تقویت کننده حاکمیت سایبری در عرصه بین‌المللی می‌تواند راهگشا باشد.

مراجع

- [1] Fazaeli, Mustafa & Karami, Musa. (2020). The historical evolution of the international law of the use of force until the formation of the United Nations system; Insurance and hopes. Scientific Quarterly of Sacred Defense Studies, 6 (1), 31-60. (In Persian).

- [2] Kiankhah. (2020). Research Article: Strategic Governance Challenges with the Expansion of Cyberspace DOR: 20.1001. 1.33292538. 1398.9. 34.5. 5. National Quarterly Journal of National Security, 9 (34), 153-174 (In Persian).
- [3] Jafarnia, Omid and Karimi Ghahroudy, Mohammad Reza, 2019, The importance and requirements of cyberspace governance, 4th National Conference on Computer Science and Technology of Electrical Engineering, Iran, Tehran (In Persian).
- [4] Hafeznia Mohammad Reza, 2011, Political Geography of Cyberspace, Samat Publications (In Persian).
- [5] Karimi Ghahroudi Mohammad Reza, 2020, The Rule of Cyberspace, Publications of the Defense Industries Educational and Research Institute (In Persian).
- [6] Leigh, M. (1985). Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America). 1984 ICJ Reports 392. American Journal of International Law, 442-446.
- [7] Falk, R. (1997). Nuclear Weapons Advisory Opinion and the New Jurisprudence of Global Civil Society. Transnat'l L. & Contemp. Probs, 7, 333.
- [8] Oppenheim, L. (1921). The future of international law (Vol. 43). Clarendon Press.
- [9] United States. President (1945-1953: Truman). (1945). The Charter of the United Nations with the Statute of the International Court of Justice Annexed Thereto: Address by the President of the United States Delivered Before the Senate on July 2, 1945 Presenting the Charter of the United Nations, with the Statute of the International Court of Justice Annexed Thereto: and a Message from the President of the United States Transmitting a Certified Copy of the Charter of the United Nations, with the Statute of the International Court of Justice Annexed Thereto ... US Government Printing Office.
- [10] Keller, H. (2009). Friendly Relations Declaration (1970). Max Planck Encyclopedia of Public International Law.
- [11] Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.
- [12] 2013, 2015 & 2017 UN GGE – Reports of the group of governmental experts on developments in the field of information and telecommunications.
- [13] Iman Mohammad Taghi and Noshadi Mahmoud Reza, 2011, Qualitative content analysis, research, third year, second issue (In Persian).