فصلنامه علمی مطالعات قدرت نرم

دوره ۱۳، شماره ٤، شماره پیاپی (۳۵)، زمستان ۱٤۰۲، ص ٥٤ ـ ۳۵

مقاله پژوهشی

بررسی چگونگی اعمال حاکمیت بر قلمرو سایبری ملی به مثابه قدرت نرم در پرتو حقوق بین‌الملل

سید حسین علوی[۱]، محمدرضا حسینی[۲]، مهراب رامک[۳]

تاریخ دریافت: ۱۴۰۲/۰۹/۰۷ تاریخ پذیرش: ۱۴۰۲/۱۱/۰۶

چکیده:

هم اکنون به طور گسترده‌ای پذیرفته شده است که اعمال حاکمیت بر فضای سایبر ملی باید از جنبه‌های سخت تا جنبه های نرم این فضا را پوشش دهد. امروزه جنبه های سخت اعمال حاکمیت بر فضای سایبر ملی با استفاده حداکثری از سخت افزارها و نرم افزارها به صورت فزاینده ای پیگیری می شود. مسئله اصلی 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 می‌نماید 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 متون (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 کشورها برخوردار نیست و عموما 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 به منظور اعمال حاکمیت بر فضای سایبر ملی، ناگزیر به کاربست دو راهکار قلمروگذاری و مرزبانی موثر از فضای سایبری کشور در عرصه ملی و همچنین دیپلماسی سایبری، همکاری و هماهنگی با کشورهای همسو با هدف تبیین مواضع تقویت‌کننده حاکمیت سایبری در عرصه بین‌المللی هستیم.

واژگان اصلی: قلمرو سایبری، حاکمیت ملی سایبری، قدرت نرم، اصول و قواعد حقوق بین‌الملل.

۱. دانشجوی دکتری مدیریت راهبردی فضای سایبری دانشگاه عالی دفاع ملی، تهران، ایران (نویسنده مسئول)
h.alavi@aut.ac.ir

۲. دانشیار حقوق بین‌الملل دانشگاه عالی دفاع ملی، تهران، ایران.

۳. دکتری مدیریت راهبردی فضای سایبری دانشگاه عالی دفاع ملی، تهران، ایران.

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 تامین نیازهایش بکارگرفته و مدیریت می شود، 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 تجلی های دیجیتالی آن از بین نمی رود. با این تفاوت که قلمرو و مرز در فضای سایبری از ماهیت مجازی و دیجتالی برخوردار بوده و محدوده آن با شاخص‌های متفاوتی نسبت به فضای واقعی تعیین می گردد.

از این رو بکارگیری فضای سایبر در شئونات مختلف زیست بشری موجب گردیده است اعمال حاکمیت در فضای سایبر کشورها یکی از ابعاد جدید حاکمیت ملی و امری ضروری به شمار آید. لیکن ویژگی‌ها و شرایط خاص فضای سایبری ایجاب می‌نماید برخلاف سایر عرصه‌های فیزیکی(زمینی، هوایی، دریای و فضایی) که اعمال حاکمیت با استفاده از شیوه‌ها و فرآیندهای اعمال قدرت سخت انجام می‌پذیرد، اعمال حاکمیت بر قلمرو ملی در این فضا از طریق کاربست شیوه‌ها و فرآیندهای قدرت نرم نیز پیگیری گردد. در حال حاضر دولت‌ها با فناوری فیلترینگ به عنوان یکی از ابزارهای اعمال قدرت سخت، دسترسی کاربران به محتوای مخرب و ناسالم را محدود و مانع اشاعه ارزش‌ها، فرهنگ و سبک زندگی دیگر کشورها در در قلمرو سایبر ملی خود می‌شوند. در کنار این موضوع دولت‌ها سعی می‌نمایند با اقناع و همراه‌سازی شهروندان نسبت به سانسور محتوای مخرب شبیه هرزه‌نگاری کودکان، تبلیغات‌های تروریستی و موضوعاتی از این دست؛ هنجارسازی و مشروعیت بخشیدن به سانسور محتوای مخرب را به عنوان یکی از ابزارهای قدرت نرم نیز دنبال نمایند. بنابراین خط مشی‌گذاری و تعیین رویه‌های عمل مجاز برای تولیدکنندگان، ارایه‌دهندگان و مصرف‌کنندگان خدمات و محتوا به طور فزاینده‌ای در دست انجام است (Baur-Ahrens, A. 2017). بنابراین پایش و رصد نظام‌مند و مستمر فرصت‌ها و تهدیدهای پیش روی فضای سایبر ملی، تنظیم فعالیت‌های کنشگران این فضا و تضمین یک محیط سایبری مطمئن برای آحاد جامعه یکی از مهمترین وظایف حاکمیت در ارتباط با

فضای سایبر ملی به شمار می‌رود.

طی سال‌های گذشته یکی از شیوه‌های موثر در اعمال حاکمیت سایبری ملی، اتکا به حقوق بین‌الملل در این زمینه بوده است و تسلط و توانایی در ارایه مستندات و دلایل حقوقی در پیگیری حقوقی و قضایی اقدامات و فعالیت‌های ناقض حاکمیت ملی سایبری در مجامع بین‌المللی، بخشی از قدرت ملی به حساب می‌آید. پایش، نظارت و اعمال قدرت حقوقی(قضایی) بر قلمرو سایبر ملی به چارچوب‌های قانونی مربوط به فعالیت‌ها و تعاملات در حال وقوع در فضای سایبر یک کشور اشاره دارد. این قوانین، مقررات و رویه‌های عمل مجاز می‌تواند جنبه‌های مختلف فعالیت‌های آنلاین، حفاظت از داده‌ها، حقوق مالکیت معنوی، حریم خصوصی، آزادی بیان، جرایم سایبری و ... را در بر گیرد (*Möllers, N. 2021*).

مسلماً از آنجا که فضای سایبری در امتداد فضای واقعی است، دولت‌ها می‌توانند بر مردم و اشیاء موجود در قلمرو خود اعمال قدرت سخت و نرم داشته باشند 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 قانون مند کنشگران ملی و بین‌المللی در یک فضای قانونی را به همراه نخواهد داشت (محمدعلی شعبانی و همکاران، ۱۴۰۲).

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 فضای سایبری کشور و نقض حاکمیت ملی در این عرصه، امکان‌پذیر نخواهد بود. همچنین در صورت مشخص نشدن چگونگی اعمال حاکمیت بر فضای 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 مساله 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 سوال 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

۲. ۱. 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؛ بیم ها 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 بپردازند و بر این نکته تاکید 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 دولت ها بوده است. به باور نگارندنگان 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 انگشت شمار 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 درفصلنامه 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 تاکید 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، مسعود مظاهری و همکاران (۱٤۰۱) در مقاله‌ای با عنوان "بررسی تاثیر جریان آزاد اطلاعات بر حاکمیت دولت‌ها از منظر حقوق بین‌الملل" که در فصنامه علمی مطالعات قدرت نرم

به چاپ رسیده است، به بررسی شیوه ها و فرآیندهای بکارگیری ابزارهای نوین رسانه ای و ایجاد جنگ نرم توسط برخی از کشورهای قدرتمند علیه حاکمیت دولت ها پرداخته اند. این مقاله ضمن تاکید بر اینکه اعمال حاکمیت بر قلمرو سایبر ملی، جنبه های نرم قدرت را نیز شامل می شود؛ نتیجه می گیرند، به دلیل عدم وجود ضمانت های اجرایی حقوقی کافی، طی سال های گذشته کشورهای پیشرو به بهانه آزادی اطلاعات و حق دسترسی به آن؛ اخبار، اطلاعات و یا آموزش های مد نظر خود را به مردم سایر کشورها القا و از این طریق با تاثیر بر افکار و آرمان‌های یک ملت (بدون در نظر گرفتن بافت‌های فرهنگی، عقیدتی و دینی آن جامعه) موجب تهدید علیه امنیت ملی و حاکمیت ملی آن کشور می شوند (مسعود مظاهری و همکاران، ۱٤۰۱)

علی‌رغم انجام پژوهش‌های متعدد در زمینه حقوق بین‌الملل، 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 سرمایه‌های 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 خلاء دانشی موجود در این زمینه، انجام این پژوهش ضروری به نظر می رسد.

۲. ۲. مفهوم شناسی تحقیق

۲. ۲. ۱. قلمرو سایبری

قلمرو عبارت است از فضای جغرافیایی مشخص، اعم از واقعی و مجازی که منعکسکننده عرصه حاکمیت و فرمانروایی یک بازیگر سیاسی به ویژه حکومت یا حوزه کنترل و نفوذ یک کارکرد و فعالیت سیاسی، اجتماعی، فرهنگی و ... آن میباشد. همانطور که در فضای واقعی حیات و فعالیت انسان‌ها، قلمروها و عرصه‌های مختلف برای اعمال حاکمیت وجود دارد، در فضای سایبری نیز عرصه‌های 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 سامانه‌های اطلاعاتی و ارتباطی تحت اختیار آن کشور می باشد. مرزهای حاکمیت فضای سایبری یک کشور از مجموعه تجهیزات شبکه‌ای آن کشور که به طور مستقیم به تجهیزات شبکه‌ای کشورهای دیگر متصل هستند تشکیل می شود. حاکمیت

فضای سایبری به منظور حفاظت از عملیات‌های مختلفی که کاربران سایبر روی داده‌ها انجام می‌دهند اعمال می‌گردد.

تعریف سازمان ملل متحد از حاکمیت ملی سایبری عبارت است از: «حاکمیت ملی، هنجارها و اصول بین‌المللی که از حاکمیت نشئت می‌گیرند، در مورد فعالیت‌های کشورها در ارتباط با فناوری اطلاعات و ارتباطات و اختیار آنها بر زیرساخت‌های اطلاعاتی و ارتباطی موجود در قلمرو سرزمینی نیز صادق می باشد. بر این اساس اگر چه در تعریف مذکور به طور مستقیم به واژه «فضای سایبری» اشاره نشده است ولی این تعریف نشان می‌دهد حاکمیت ملی در دو سطح اعمال می‌گردد: سطح فنی و سطح اجتماعی. در سطح فنی حاکمیت ملی در مورد زیرساخت‌های 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 می گیرند، 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 می گردد.» (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 می شوند، ناقض حاکمیت سرزمینی کشورها بوده و در حقوق بین‌الملل ممنوع می‌باشند.

۲ ۲. ۳. قدرت نرم در فضای سایبر ملی

قدرت نرم عبارت است از شکل‌دادن به باورها، ارزش‌ها، هنجارها و ترجیحات دیگران از طریق اقناع و جذب به گونه‌ای نامحسوس که برای کسب نتایج مطلوب به واسطه ایجاد جذابیت یا تطمیع بکار گرفته می‌شود. این شیوه اعمال قدرت با بکارگیری ابزارها و شیوه‌های غیرمستقیم بر منافع یا رفتار دیگران اثر خواهد گذاشت. به بیان دیگر برخلاف قدرت سخت که از ماهیت قهرآمیز برخوردار بوده و بصورت مستقیم و آشکار اعمال می‌گردد، در اعمال قدرت نرم، تصرف ذهن‌ها و قلب‌ها مد نظر قرار می‌گیرد و از این طریق افراد یک جامعه تحت تسلط قرار می‌گیرند. شایان ذکر است به رغم اهمیتی که قدرت نرم در ادبیات علوم سیاسی و روابط بین‌الملل دارد، چگونگی ارزیابی و سنجش قدرت نرم دشوار است. چرا که شاخص‌های آن متغیر و با توجه به ذهنی بودن برخی از شاخص‌های آن،

اندازه‌گیری آنها دشوار می‌باشد (احمدپور محسن و همکاران، ۱٤۰۲). قدرت نرم در فضای سایبر ملی شامل استفاده از ابزارهای غیر اجباری برای شکل دادن به رفتار و برداشت سایر کشورها در حوزه دیجیتال است. این امر از طریق سازوکارهای مختلفی از جمله نفوذ فرهنگی، ایدئولوژیک و نهادی و همچنین ترویج رفتار و هنجارهای مناسب در فضای مجازی قابل تحقق است. علاوه بر این، نفوذ روزافزون قدرت نرم دیجیتال در حال شکل دادن به ادغام فناوری‌هایی مانند نسل پنجم تلفن همراه، هوش مصنوعی، محاسبات کوانتومی و... در فضای سایبر جهانی است. از این رو اندازه‌گیری تأثیر قدرت نرم در فضای سایبری همچنان یک کار پیچیده است. بنابراین نقش قدرت نرم در فضای سایبری به طور فزاینده‌ای به عنوان یک جنبه حیاتی امنیت ملی، انسجام اجتماعی و حتی رفاه اقتصادی شناخته می‌شود و قدرت نرم در فضای سایبری ملی یک حوزه چندوجهی در حال تحول است که ملاحظات مختلف دیپلماتیک، تکنولوژیکی و امنیتی را در بر می گیرد (Lilli, E., & Painter, C. 2023).

۲ ۲,٤. اصول و قواعد حقوق بین الملل مرتبط با حاکمیت ملی سایبری

در این زمینه دو اصل اساسی حقوق بین‌الملل مرتبط با جغرافیای سیاسی فضای سایبری به صورت مختصر مورد بررسی قرار می‌گیرد.

اصل خودداری از تهدید و توسل به زور

بند ٤ 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 ٤ ماده ۲ منشور ملل متحد در بیان صریح خود انحصارا بر اعضای ملل متحد اعمال می‌شود، ولی ممنوعیت توسل به زور از رهگذر حقوق بین‌الملل عرفی به کشورهای غیر عضو نیز تسری می یابد. (Leigh, M. 1985)

دیوان بین‌المللی دادگستری نیز با استناد به ماده ۲ بند ٤ 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، ضرورتا 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، تاثیری در "بکارگیری 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 حقـوق بین‌الملـل قـرار می‌گیـرد. واضـح اسـت 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 صراحتا به آن اشاره نشده اسـت ولـی طـی سـالیان گذشـته از حقـوق عرفـی برخوردار شده است. بر اساس بیانیه مجمع عمومی سال ۱۹۶۵ میلادی در مورد غیرقابـل قبـول بـودن مداخله در امور داخلی دولت‌ها و حفاظت از استقلال و حاکمیت آنهـا ، کـه مجـدداً در بیانیـه مجمـع 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 خـارجی دولت‌هـای دیگـر را نـدارد." در نتیجـه، مداخله مسلحانه و سایر اشکال مداخله و یا حتی تلاش برای تهدید علیه شخصـیت دولـت و عناصـر سیاسی ، اقتصادی و فرهنگی آن محکـوم اسـت. همچنـین دیـوان بین‌المللـی دادگسـتری در پرونـده 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 نقطـه مقابـل آن، یعنی مداخله را توضیح دهیم. بر اساس تعریف اوپنهایم، مداخله عبارت است از "هر گونه مداخلـه یـا اقدام توام با اجبار و زور که دولت را از کنترل بر موضوع مورد نظر محروم می‌کنـد". از تعریـف فـوق معلوم می شود 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.)

۲. ۲,۵. اسناد حقوق بین الملل مرتبط با حاکمیت ملی سایبری

منشور ملل متحد

با استناد به متن منشور ملل متحد، اعلامیه اصول حقوق بین‌الملل درباره روابط دوسـتانه و همکـاری میان دولت‌ها، اعلامیه ارتقاء اثربخشی اصل خودداری از تهدید یا توسل به زور در روابط بین‌الملـل و آراء دیوان بین‌المللی دادگستری؛ حاکمیت بر قلمرو ملی و سرزمینی یکی از اصول اساسی منشـور ملـل متحـد است که از تساوی حاکمیتی کشورها، عدم توسل به زور علیه تمامیت ارضی و ممنوعیت اقداماتی کـه بـا 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 تاکید می‌نماید. مهم‌تر از آن در بند ٤ ماده ۲ مقرر می دارد «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، ۱۹٤٥)

این اصل پذیرفته شده بین‌المللی، مبنای تدوین قواعد حقوقی بین‌الملل در زمینه احترام به حاکمیت سرزمینی کشورها، ممانعت از هرگونه مداخله غیرمجاز در امور داخلی کشورها (که بر مبنای احترام به حاکمیت در اختیار دولت سرزمینی است) و ممنوعیت دولت‌ها در تهدید و بکارگیری زور علیه آنچه تمامیت ارضی و استقلال سیاسی کشور دیگر به شمار می‌رود، بوده است. همچنین در آرای صادره محاکم قضایی بین‌المللی در مناقشات بین‌المللی بین کشورها، مکرر به این اصل رجوع شده است. دیوان بین‌المللی دادگستری به عنوان رکن قضایی سازمان ملل متحد که از صلاحیت عام قضایی در امور بین‌الملل برخوردار است و اساسنامه آن جزء لاینفک منشور ملل متحد به شمار می رود، با استناد به مفاد این اصل و بهره گیری از حقوق بین‌الملل عرفی و معاهداتی سعی نموده است اختلافات بین‌المللی در این زمینه را حل و فصل نماید و تفسیرهای دقیق‌تری از این اصل ارایه نماید. دیوان در پرونده نیکاراگوئه تاکید می‌نماید، اصل احترام به حاکمیت دولت، با اصول ممنوعیت توسل به زور و عدم مداخله پیوند تنگاتنگی دارد و در ادامه می‌افزاید هر دولتی موظف است به شخصیت، یکپارچگی سرزمینی و استقلال سیاسی سایر دولت‌ها احترام بگذارد و با حسن نیت به تعهدات بین‌المللی خویش پایبند باشد. (Leigh, M. 1985)

از آنجا که منشور ملل متحد دولت‌ها را از مداخله غیرمجاز و توسل به زور علیه تمامیت ارضی دولت دیگر منع نموده است و تمامیت ارضی یک دولت، قلمرو سایبری آن دولت را هم شامل می شود، استفاده از ابزارهای سایبری با هدف مداخله، توسل به زور و نهایتا نقض حاکمیت سایر کشورها ممنوع می باشد. اظهار نظر دیوان بین‌المللی دادگستری در قضیه اختلافات ناوبری و حقوق مرتبط (کاستاریکا علیه نکاراگوئه در سال ۲۰۰۹) نیز این رویکرد را تایید می‌نماید که به عبارات مندرج در معاهدات قدیمی می توان معنای امروزی بخشید. و این موضوع امکان تفسیر و اطلاق اقدامات متخلفانه به عملیات‌های سایبری را میسر می‌سازد.

اعلامیه "اصول حقوق بین‌الملل در مورد روابط دوستانه و همکاری بین دولت‌ها مطابق منشور ملل متحد" که با تاکید و یادآوری قطعنامه‌های پیشین و منشور ملل متحد؛ با هدف حفظ و ارتقاء صلح

و امنیت بین‌المللی، توسعه روابط دوستانه و همکاری بین دولت‌ها در سال ۱۹۷۰ میلادی به تایید کشورهای عضو ملل متحد رسیده است، دولت‌های را ملزم می‌نماید از تهدید و توسل به زور و همچنین اجبار نظامی، سیاسی، اقتصادی و یا هر گونه اجبار علیه استقلال سیاسی و تمامیت ارضی دیگر کشورها خودداری نمایند. در این اعلامیه که ۷ قاعده کلی حقوق بین‌الملل مورد تایید کشورهای عضو قرار گرفته است، تاکید می‌گردد، اهداف سازمان ملل متحد، تنها در صورتی قابل اجرا است که دولت‌ها از برابری حاکمیتی برخوردار بوده و الزامات این اصل را در روابط خود به طور کامل رعایت نمایند. این اعلامیه با استناد به اصل منع تهدید یا توسل به زور، تمامی دولت‌ها را موظف می نماید، از سازماندهی یا تشویق نیروهای نامنظم و گروه‌های مسلح برای تجاوز به قلمرو دولت دیگر و یا سازماندهی، تحریک، کمک و مشارکت در درگیری‌های مدنی یا اقدامات تروریستی در قلمرو دولت‌های دیگر خودداری کنند. همچنین در ادامه با استناد به وظیفه عدم مداخله غیرمجاز تصریح می نماید، هیچ دولتی حق مداخله مستقیم یا غیرمستقیم و یا هر گونه مداخله که شخصیت دولت دیگر یا عناصر سیاسی، اقتصادی و فرهنگی آن دولت را خدشه دار کند، ندارد و هر کشوری از این اصل مسلم برخوردار است که نظام‌های سیاسی، اقتصادی و فرهنگی خود را بدون دخالت دیگر کشورها پیاده سازی نماید. (Keller, H. 2009. Friendly Relations Declaration (1970))

کتابچه راهنمای تالین

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 می پردازد، در قالب ۱۵٤ 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 می باشند و همه این قواعد به حاکمیت بر قلمرو سایبری کشورها و ممانعت از هرگونه تجاوز و دست اندازی به قلمرو و مرزهای سایبر ملی تاکید دارند، اشاره می‌گردد.

صلاحیت سرزمینی و حاکمیت بر قلمرو از اصول بنیادین حقوق بین‌الملل به شمار می روند. 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 ٤ 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 ٣٤ تا ٣٨ 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 بازتاب دهنده هنجارهای عرفی اصلی حقوق بشر مورد تایید همگان است.

به واسطه پیوند روزافزون جامعه جهانی و وابستگی رو به رشد دولت‌ها به بهره گیری از زیرساخت‌های سایبری، این عرصه فرصت‌هایی را برای مداخله سایر دولت‌ها در امور داخلی کشورها قرار داده است. بر این اساس قواعد ٦٦ و ٦٧ 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.

مفاد قواعد ٦٨ تا ٧٠ راهنمای تالین دو به ممنوعیت تهدید و توسل به زور در فضای سایبر تاکید می‌نماید. بر اساس این قواعد، عملیات‌های سایبری که موجب شکل‌گیری تهدید یا بکارگیری زور علیه یکپارچگی سرزمینی یا استقلال سیاسی یک دولت شود یا به هر طریق دیگری با اهداف منشور ملل متحد ناسازگار باشد غیر قانونی است. (Schmitt, M. N. 2017. Tallinn manual 2.)

گروه کارشناسان دولتی سازمان ملل متحد در زمینه توسعه فناوری اطلاعات و ارتباطات

طی سال‌های اخیر، کارگروه کارشناسان دولتی سازمان ملل متحد در زمینه توسعه فناوری

اطلاعات و ارتباطات از راه دور در چارچوب امنیت بین المللی (GGE[1]) بسیاری از جنبه‌های اساسی مرتبط با حاکمیت دولت‌ها در قلمرو سایبری خود را مشخص نموده‌اند که از مهمترین آنها می توان بـه ممنوعیت استفاده از زور و عدم مداخله در امور داخلی سایر کشورها و همچنین صلاحیت دولت‌ها بر کنترل و مدیریت زیرساخت‌های سایبری واقع در قلمرو آنها اشاره دارد.

در گزارش ۲۰۱۳ گروه متخصصان دولتی سازمان ملل متحد (GGE) در مورد تحـولات در زمینـه فناوری اطلاعات و ارتباطات، تأیید شد که حقوق و هنجارهای بین‌المللی پذیرفته شده در فضای واقعی و به ویژه منشور سازمان ملل متحد، در مورد فضـای سـایبری نیـز اعمـال گـردد. ایـن کـارگروه همچنـین برحاکمیت فعالیت‌های مرتبط با فناوری اطلاعات و ارتباطات در قلمرو سـرزمینی دولت‌هـا و صـلاحیت دولت‌ها در کنترل و مدیریت زیرساخت‌های فناوری اطلاعات و ارتباطات در قلمرو سرزمینی تاکید دارد.

گزارش سال ۲۰۱۵ گروه کارشناسان دولتی سازمان ملل متحد، با بیان هنجارها و اصول بین‌المللی خاصی که در فضای سایبری اعمال می شود یا باید اعمال شود ، گامی فراتر در ایـن زمینـه محسـوب می‌شود. این گزارش ۱۱ هنجار داوطلبانه، غیر الزام‌آور، قوانین یا اصول رفتار مسـئولانه کشـورها را بـا هدف ارتقا یک محیط فناوری اطلاعات و ارتباطات باز، امن، پایدار، قابل دسترس و مسالمت‌آمیز ذکر کرده است. از جمله اصول حقوق بین‌الملل که در مورد فضای سایبری مورد تایید اعضا کارگروه قـرار گرفت، می توان به اصل حاکمیت دولت و اصل عدم مداخله در امور داخلی سایر کشورها اشاره کرد.

گروه متخصصان دولتی سازمان ملل متحد، در سال ۲۰۱۷ به دلیل عدم توافق دربـاره چگـونگی اعمال هنجارها و اصول خاص در فضای سایبری ، موفق به تهیه گزارشی نشد.

گزارش‌های اجماع گروه متخصصان دولتی سازمان ملل متحد، بـه وضـوح نتیجـه می‌گیـرد کـه دولت‌ها در حفاظت از زیرساخت‌های فناوری اطلاعات و ارتباطات واقع در قلمرو خود تعیـین کننـده هستند و از صلاحیت مدنی و کیفری در مورد فعالیت‌های مجاز و غیرمجاز در زیرساخت‌های سایبری خود برخوردار می‌باشند. (2013, 2015 &2017 UN GGE – Reports)

۳ روش‌شناسی تحقیق

۳. ۱. نوع تحقیق

نظر به اینکه انجام این پژوهش به بررسی چگونگی اعمال حاکمیت بر قلمرو سایبری ملی با اتکا

[1] Group of Governmental Experts

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.

۳. ۲. روش تحقیق

روش تحقیق مورد استفاده، با رویکرد کیفی از نوع تحلیل محتوا و ابزار مورد استفاده نرم‌افزار مکس‌کیودا[1] 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 ارتقاء اثربخشی اصل خودداری از تهدید یا توسل به زور در روابط بین‌الملل، آراء دیوان بین‌المللی دادگستری، گزارش‌های گروه کارشناسان دولتی سازمان ملل متحد در زمینه توسعه فناوری اطلاعات و ارتباطات (GGE) و کتابچه راهنمای تالین دو (به عنوان یکی از مهم‌ترین تلاش‌ها برای تحقیق روی قواعد بین‌المللی حاکم بر اقدامات سایبری که توسط گروه متخصصین بین‌المللی به دعوت مرکز تعالی دفاع سایبری ناتو انجام پذیرفته است)؛ با استفاده از نرم‌افزار مکس‌کیودا 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 تاکید دارد اعم از قواعد احترام به حقوق بشر بین‌المللی، 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 مکس‌کیودا 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 بصورت رفت و برگشتی چند بار مرور شد تا از صحت فرآیند دست‌یابی به زیرطبقات اطمینان حاصل شود.

[1] Maxqda 10

٤ تجزیه و تحلیل یافته‌ها

پس از بررسی واحدهای معنایی و زیرطبقات مرتبط با حاکمیت بر قلمرو سایبری ملی در اسناد حقوق بین‌الملل، 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 بین‌الملل 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 بین‌الملل میسر نیست. از این رو می توان استنباط نمود، اسناد حال‌حاضر حقوق بین‌الملل، حاکمیت سایبری ملی کشورها را تضمین نمی‌نمایند و موارد نقض متعدد غیرقابل پیگیری در حقوق بین‌الملل وجود دارد.

جدول شماره یک، واحدهای معنایی و زیرطبقات موارد نقض حاکمیت سایبری ملی در حقوق بین‌الملل، که با استفاده از نرم‌افزار مکس‌کیودا احصاء شده است و این واحدهای معنایی و زیرطبقات، نمایان‌گر طبقه اصلی حاصل از تحلیل محتوای کیفی که " ناتوانی حقوق‌بین‌الملل 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 صیانت از حاکمیت سایبری ملی کشورها	**ابهام و عدم قطعیت اسناد حقوق بین‌الملل در تعیین اقدامات و عملیات‌های سایبری غیرمجاز که حاکمیت سایبری ملی دیگر کشورها را نقض می نمایند.**	▪ علی‌رغم وجود نظام حقوق بین‌الملل عرفی و معاهداتی، فهرست قطعی و نهایی از حقوق بین‌الملل لازم الاجرا برای دولت‌ها وجود ندارد. ▪ تعریف دقیقی از اقدامات ناقض حاکمیت ملی (اعم از: توسل به زور، مداخله غیرمجاز و ...) در اسناد حقوق بین‌الملل وجود ندارد. ▪ تهدید و توسل به زور، صرفاً به اقدامات مسلحانه یک دولت علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولت دیگر اطلاق می‌گردد. ▪ تفسیر کشورها از اقدامات ناقض حاکمیت ملی در اسناد حقوق بین‌الملل متفاوت است. ▪ تعیین سطح آستانه اقدامات و عملیات‌های سایبری ناقض حاکمیت سرزمینی به سادگی امکان‌پذیر نیست. ▪ تفسیر کشورها از همترازی اقدامات و عملیات‌های فضای سایبری با اقدامات و عملیات‌های فضای واقعی متفاوت است.
	اقدامات و عملیات‌های سایبری مخرب و ناقض حاکمیت سرزمینی، صرفاً در مواردی که قابل انتساب به یک دولت دیگر باشند از پیگرد حقوقی برخوردار است.	▪ هر دولت صرفاً مسئول اقدامات اشخاص و نهادهایی است که به نوعی نماینده دولت محسوب می‌گردند. ▪ صرفا اقدامات و عملیات‌هایی 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 عملیات‌های سایبری به دولت متخاصم با پیچیدگی و عدم قطعیت‌های 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 امکان‌پذیر نیست. ▪ عملیات‌ها و اقداماتی که به سطح توسل به زور و اجبار از سوی یک دولت نرسند، ممنوعیت حقوق بین‌الملل را نقض نمی‌نمایند.اقدامات و عملیات‌های سایبری که توسط کنشگران غیردولتی اعم از افراد، گروه‌های سازمان‌یافته، سازمان‌های تروریستی و ... انجام می‌پذیرد و قابل انتساب به دولت نباشد، قواعد حقوق بین‌الملل را شامل نمی شود.

	اقدامات و عملیات‌های سایبری مخرب و ناقض حاکمیت سرزمینی، صرفاً در مواردی که علیه یک دولت انجام شده باشند از پیگرد حقوقی برخوردار هستند.	▪ اقدامات دولت متخاصم که نهادها، شرکت ها، اقوام و ... را هدف قرار می دهند، اگر چه تا اندازه‌ای حاکمیت دولت سرزمینی را نقض می‌نمایند، قابل پیگیری از طریق مجاری حقوق بین‌الملل نیستند. ▪ عملیات‌ها و اقداماتی که به سطح توسل به زور و اجبار علیه دولت دیگر نرسند، ممنوعیت حقوق بین‌الملل را نقض نمی‌نمایند. ▪ حقوق بین‌الملل عرفی و معاهداتی، موارد استثناء قابل قبول در تخطی دولت‌ها از تعهدات بین‌المللی در برابر سایر دولت‌ها قائل شده است.
	عدم تمایل کشورهای پیشرفته و صاحب فناوری به تدوین نظامات حقوقی روشن و متقن برای فضای سایبری در جهت ممانعت و مقابله با فعالیت‌های مخرب و ناقض حاکمیت ملی و سرزمینی کشورها	▪ 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.
	ناتوانی جامعه بین‌الملل در تدوین نظامات حقوقی شفاف فضای سایبری	▪ 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 عملیات‌های ناقض حاکمیت سایبری ملی ممکن است در کوتاه‌مدت امکان‌پذیر نباشد، تدوین نظام حقوقی متناسب برای آنها نیز میسر نیست.

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 پی برد، قوانین و هنجارهای فعلی بین‌المللی، اقدامات زیر سطح آستانه این قواعد را نهی 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 پیگیرد بین‌المللی در این زمینه شده است.

بنابراین رویکردی که در اسناد حال‌حاضر بین‌المللی فضای سایبر مورد تاکید قرار گرفته است، بر تاثیرات فیزیکی اقدامات سایبری بر علیه قلمرو سرزمینی کشورها در قالب شاخص‌های قدرت سخت تاکید دارد و جنبه مهم دیگر، یعنی هنجارهای مرتبط با احترام به صلاحیت دولت‌ها در کنترل دسترسی و مدیریت 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، صرفا به تجلی اثار فیزیکی حملات یا از دست دادن عملکرد قابل توجه سامانه‌ها بستگی داشته باشد، دولت‌های هدف در برابر مولفه‌های قدرت نرم، هیچ گونه راه‌حل قانونی در دفاع از خود

نخواهند داشت. 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.

نتیجه‌گیری

با بررسی و تحلیل محتوای کیفی اسناد حقوق بین‌الملل که با استفاده از نرم‌افزار مکس‌کیودا انجام شد و با استناد به واحدهای معنایی، زیرطبقه‌ها و طبقه اصلی احصا شده، نتیجه می‌شود، اصول و قواعد فعلی حقوق بین‌الملل از کارایی و توانایی لازم در صیانت از حاکمیت سایبری ملی کشورها برخوردار نیست و بکارگیری مولفه‌های قدرت نرم ناقض حاکمیت سایبری ملی 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 به خصوص در قالب سازوکارهای قدرت نرم، بدون اتکا به اصول و قواعد حقوق بین‌الملل هستیم.

منابع

احمدپور، محسن؛ خداوردی، حسن و کشیشیان سیرکی، گارینه(۱٤۰۲). بررسی و تحلیل روش‌ها و شاخص‌های سنجش قدرت نرم، مطالعات قدرت نرم، ۱۳(۳٤)، ۱٤۱-۱٦٤.

جعفرنیا، امید و کریمی قهرودی، محمدرضا(۱۳۹۹). اهمیت و الزامات حاکمیت فضای سایبری، چهارمین کنفرانس ملی دانش و فناوری مهندسی برق کامپیوتر و مکانیک.

حافظ نیا محمدرضا(۱۳۹۰). جغرافیای سیاسی فضای مجازی. انتشارات سمت.

شعبانی، محمدعلی؛ بخشایش‌اردستانی، احمد؛ توحیدفام، محمد و مطلبی، مسعود(۱٤۰۲). مؤلفه‌های قدرت نرم ایالات‌متحده آمریکا در قبال جمهوری اسلامی ایران (دولت یازدهم و دوازدهم)، مطالعات قدرت نرم، ۱۳(۳٤)، ۱۸۵-۲۱۱.

فضائلی، مصطفی و کرمی، موسی(۱۳۹۹). تحول تاریخی حقوق بین‌الملل توسل به زور تا شکل‌گیری نظام ملل متحد؛ بیم‌ها و امیدها، مطالعات دفاع مقدس، ٦(۲۱)، ۳۱-٦۰.

کریمی قهرودی، محمدرضا و زارعی، وحید(۱۳۹۹). حاکمیت فضای سایبری. تهران: انتشارات موسسه آموزشی تحقیقاتی صنایع دفاعی.

کیان خواه، احسان(۱۳۹۸). چالش‌های راهبردی حکمرانی با گسترش فضای سایبر، امنیت ملی، ۹(۳٤)، ۱۵۳-۱۷٤.

مظاهری، مسعود؛ صلاحی، سهراب و مرادی، مریم(۱٤۰۱). بکارگیری قدرت نرم علیه حاکمیت دولتها از طریق جریان آزاد اطلاعات، مطالعات قدرت نرم، ۱۲(۳۰)، ۱۸۵-۲۰٤.

2013, 2015 & 2017 UN GGE – Reports of the group of governmental experts on developments in the field of information and telecommunications

Baur-Ahrens, A. (2017). The power of cyberspace centralisation: analysing the example of data territorialisation. Security/mobility: Politics of movement, 37-56.

Falk, R. (1997). Nuclear Weapons Advisory Opinion and the New Jurisprudence of Global Civil Society. Transnat'l L. & Contemp. Probs, 7, 333.

Iman Mohammad Taghi and Noshadi Mahmoud Reza, 2011, Qualitative content analysis, research, third year, second issue (In Persian)

Keller, H. (2009). Friendly Relations Declaration (1970). Max Planck Encyclopedia of Public International Law.

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.

Lilli, E., & Painter, C. (2023). Soft power and cyber security: The evolution of US cyber diplomacy. In Soft power and the future of US foreign policy (pp. 161-179). Manchester University Press.

Möllers, N. (2021). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. Science, Technology, & Human Values, 46(1), 112-138.

Oppenheim, L. (1921). The future of international law (Vol. 43). Clarendon Press.

Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

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.