

The Role and Position of Territorialization and Border Guarding of Cyberspace in Exercising Sovereignty Over National Cyberspace

Mohammadreza Hoseini

Associate Professor Department of International Law, Higher National Defense University, Tehran, Iran
rezahsn88@gmail.com

Mehrab Ramak

Department of Cyber Space Strategic Management, Higher National Defense University, Tehran, Iran
m.ramak@sndu.ac.ir

Ehsan Kiakhah

Department of Cyber Space Strategic Management, Higher National Defense University, Tehran, Iran
h.kiakhah@sndu.ac.ir

Seyed Hosein Alavi

Department of Cyber Space Strategic Management, Higher National Defense University, Tehran, Iran
(Corresponding Author) h.alavi@aut.ac.ir

Keywords:

Principles and Rules of International Law, National Sovereignty, Territorialization and Border Guarding of Cyberspace

Abstract

With the increasing use of cyber technologies and equipment in people's personal and social lives, we are witnessing countries paying more attention to the phenomenon of national cyber territory with the aim of exercising sovereignty and preventing aliens from dominating the national Cyberspace. This research investigates the role and position of territorialization and border guarding of cyberspace in the exercise of sovereignty over national cyberspace by examining the literature related to sovereignty over territorial territory and how the principles and rules of international law related to national sovereignty are adapted to national cyberspace. According to the purpose, the current research is of developmental-applied type and the research methodology used in this research is descriptive-analytical, which has been used to collect information from library and internet sources, and attempts have been made in extracting the necessary basics to explain the topic from up-to-date Iranian and foreign sources. After analyzing the gathered data, it was concluded that territorialization and border guarding of cyberspace can play a significant role in exercising sovereignty over the national cyberspace, and that exercising due principles and rules of international law, applying legal pursuits and defending national cyberspace are contingent upon existence of definition and declaration of the national cyberspace are regarded as effective elements with this regard. In addition, lack of appropriate definition of the national territory and border in the cyberspace will not lead to the lawful behavior of private and government actors in a legal space and will lead to the weakening of the ruling system and national security. The results of this research will lead to the expansion of knowledge and better understanding of the decision-makers and authorities of the Country.



This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY)

license: <http://creativecommons.org/licenses/by/4.0/>

نقش و جایگاه قلمروگذاری و مرزبانی فضای سایبری در اعمال حاکمیت بر فضای سایبر ملی

محمد رضا حسینی

دانشیار گروه حقوق بین الملل دانشگاه عالی دفاع ملی، تهران، ایران
rezahsn88@gmail.com

مهراب رامک

گروه مدیریت راهبردی فضای سایبری، دانشگاه عالی دفاع ملی، تهران، ایران
m.ramak@sndu.ac.ir

احسان کیان خواه

گروه مدیریت راهبردی فضای سایبری، دانشگاه عالی دفاع ملی، تهران، ایران
h.kiankhah@sndu.ac.ir

سید حسین علوی

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

تاریخ پذیرش: ۲۷ اردیبهشت ۱۴۰۳

تاریخ دریافت: ۱ مهر ۱۴۰۲

چکیده

با گسترش روزافزون بهره‌برداری از فناوری‌ها و تجهیزات سایبری در زندگی فردی و اجتماعی انسان‌ها، شاهد توجه بیش از پیش از پیش کشورها به پدیده قلمرو سایبر ملی با هدف اعمال حاکمیت و ممانعت از تسلط بیگانگان در فضای سایبری ملی هستیم. این پژوهش با بررسی ادبیات مرتبط با حاکمیت بر قلمرو سرزمینی و چگونگی انطباق اصول و قواعد حقوق بین‌الملل مرتبط با حاکمیت ملی بر فضای سایبر ملی به تحقیق پیرامون نقش و جایگاه قلمروگذاری و مرزبانی فضای سایبری در اعمال حاکمیت بر فضای سایبر ملی می‌پردازد. تحقیق حاضر با توجه به هدف، از نوع توسعه‌ای-کاربردی است و روش تحقیق مورد استفاده در این پژوهش توصیفی-تحلیلی است که برای گردآوری اطلاعات، از منابع کتابخانه‌ای و اینترنتی استفاده شده است و سعی شده تا مبانی لازم جهت تبیین موضوع از منابع به روز داخلی و خارجی استخراج گردد. پس از تجزیه و تحلیل اطلاعات نتیجه‌گیری شد قلمروگذاری و مرزبانی فضای سایبری می‌تواند نقش بسزایی در اعمال حاکمیت بر فضای سایبر ملی داشته باشد و برخورداری از اصول و قواعد حقوق بین‌الملل، پیگیری‌های قانونی و دفاع از فضای سایبر ملی مستلزم تعریف و اعلان قلمرو سایبری ملی و مرزبانی موثر این فضا می‌باشد. به علاوه تعریف نشدن قلمرو و مرز ملی در فضای سایبری، رفتار قانون‌مند کنشگران خصوصی و دولتی در یک فضای قانونی را به همراه نخواهد داشت و منجر به تضعیف نظام حاکم و امنیت ملی خواهد شد. نتایج حاصل از این تحقیق گسترش دانش و شناخت بهتر تصمیم‌گیران و متولیان امر در کشور را به همراه خواهد داشت.

واژگان کلیدی: اصول و قواعد حقوق بین‌الملل، حاکمیت ملی، قلمروگذاری و مرزبانی فضای سایبری

مقدمه

تهدیدات متنوع و روزافزون پیش روی فضای سایبری که به واسطه ماهیت به هم پیوسته این فضا امکان‌پذیر گردیده، موجب شده است ساختارهای اینترنت و فضای سایبری از دهه ۱۹۹۰ میلادی با رشد چشم‌گیری به نفع تمرکز و کنترل بیشتر تغییر نمایند. از این رو دولت‌ها طی سال‌های گذشته به طور مداوم نظارت و کنترل خود برای محافظت از فضای سایبری ملی را افزایش داده‌اند. البته هیچ‌گاه رابطه و مرز بین تمرکز و عدم تمرکز ساختارهای به هم پیوسته فضای سایبری ملی به هیچ وجه آشکار نبوده است. عدم تمرکز به دلیل انعطاف‌پذیری و در دسترس بودن ارتباطات و تعاملات در فضای سایبری و تمرکز به واسطه نیازهای کنترل و مراقبت از منابع و منافع ملی سایبری اعمال شده است.

هنگام پیدایش فضای سایبری و اینترنت، بسیاری پیش‌بینی می‌کردند این فضا چالش بزرگی برای حاکمیت ملی (سرزمینی) کشورها ایجاد می‌کند. اما تفسیرهای اخیر حاکی از این است که اگر چه فضای سایبری و به خصوص رسانه‌های اجتماعی، به کنشگران غیردولتی نیز قدرت داده است، ولی دولت‌ها همچنان به دنبال تقویت مواضع و اعمال حاکمیت بر فضای سایبر ملی هستند.

همچنان که برخلاف پیش‌بینی برخی صاحب‌نظران مبنی بر کم‌رنگ شدن مرزهای سرزمینی طی سال‌های آتی و مطرح شدن ایده «دنیای بدون مرز»، که منجر به تحولات اساسی در حاکمیت دولت‌ها بر قلمرو سرزمینی ملی می‌گردد؛ موضع‌گیری کشورها در مقابله با انتشار ویروس کرونا و پس از آن سیاست‌های واکسناسیون کووید ۱۹ نشان داد، راهبردهای قلمرو سرزمینی هنوز در سراسر جهان دارای استحکام و در حال استفاده موثر هستند. در بهار سال ۲۰۲۰ میلادی شاهد بودیم، کشورها به سرعت مرزهای خود را بستند و عبور و مرور انسان‌ها را ممنوع یا حداقل به شدت کنترل کردند. حتی در برخی موارد با اجبار، افراد را از قلمرو سرزمینی ملی اخراج نمودند. پس از آن نیز اعمال سیاست‌های واکسناسیون کووید ۱۹ و اولویت شهروندان در زدن واکسن کووید، نشان از تحکیم میانی ملی (سرزمینی) داشت. همچنین وضع قوانین و مقررات مهاجرتی در بسیاری از کشورها که طی سال‌های گذشته اعمال گردیده است، نمونه دیگری از راهبرد ملی مبتنی بر صیانت از قلمرو ملی می‌باشد. این شواهد بیانگر اهمیت و جذابیت قلمرو ملی در نظام سیاسی مدرن می‌باشد و به ما یادآوری می‌کند، یک واقعیت عمیق در مورد جهان سیاسی ما این است که جهان دارای دولت‌های سرزمینی مستقل است و دولت‌ها مدعی حقوقی در برابر شهروندان خود و در مقابل بیگانگان هستند و از حق کنترل مستقل بر قلمرو خود برخوردار می‌باشند (Paasi et al., 2022).

از آنجایی که حاکمیت در هر عرصه‌ای از چهار عنصر قلمرو و مرز، شهروندان، منابع و نظام تشکیل می‌گردد، پیش شرط اعمال حاکمیت در فضای سایبر نیز تعریف و تحقق این چهار عنصر می‌باشد. یعنی اینکه افراد، تجهیزات و داده‌های موجود در قلمرو سایبری هر کشور تابع حکمرانی آن کشور بوده و از سوی دیگر هیچ کشوری نباید در فضای سایبر واقع در قلمرو کشورهای دیگر مداخله کند. همچنین تمام کشورها (و دولت به عنوان نماینده قانونی حاکمیت) مشروعیت دارند از قلمرو خود در برابر تجاوز محافظت نمایند (کریمی قهرودی محمدرضا و زارعی وحید، ۱۳۹۹). 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 به تبع آن قلمروگذاری و مرزبانی این فضا امری ضروری به حساب آید.

هم‌اکنون قلمروگذاری و مرزبانی فضای سایبر ملی به درجات مختلف توسط دولت‌ها اعمال می‌شود و حتی آزادترین کشورهایی که ادعای آزادی عمل و آزادی بیان دارند (مانند ایالات متحده آمریکا) قلمرو سایبری کشور را به گونه‌ای متفاوت تعیین و مرزهای سایبر ملی را پایش، نظارت و کنترل می‌نمایند. در بسیاری دیگر از کشورها مثل چین و روسیه، با اعمال رویکردهای دولت‌محور که به نوعی قلمروگذاری و مرزبانی فضای سایبر ملی محسوب می‌گردد، حاکمیت بر فضای سایبر داخلی را تقویت می‌نمایند. حتی کشورهای دموکراتیک نیز اخیراً از طریق تدوین راهبردهای ملی سایبری با هدف بومی‌سازی داده‌ها، در جهت ارتقاء حاکمیت فضای سایبری ملی (سرزمینی) حرکت کرده‌اند.

به این ترتیب قلمروگذاری و مرزبانی فضای سایبر ملی اولین گام در صیانت از فضای سایبری کشور و همچنین نقش برجسته و مهمی در حاکمیت ملی و پیشگیری از چالش‌های ناشی از فضای سایبری به فضای واقعی کشور دارد.

مفهوم شناسی و ادبیات تحقیق

حاکمیت ملی

قدرت غایبی و انحصاری بر قلمرو سرزمینی یک کشور را حاکمیت ملی می‌گویند. بنابراین دولت به عنوان بالاترین مرجع حقوقی، از امتیاز اعمال حاکمیت بر قلمرو ملی برخوردار است. صلح و ستفالیبا با به رسمیت شناختن انحصار اقتدار سیاسی دولت بر قلمرو سرزمینی، به ظهور مفهوم مدرن دولت منجر شد. نظم پیش از وستفالیبا به گونه‌ای بود که قدرت لزوماً سرزمینی و البته انحصاری نبود و اعمال حاکمیت اغلب با همپوشانی و پیچیدگی همراه بود. چگونگی بروز اقتدار سیاسی نیز از قاعده و اصول خاصی پیروی نمی‌کرد (Douzet, F. 2020).

در ۲۴ اکتبر ۱۶۴۸ با امضای پیمان موسوم به پیمان وستفالیبا، جنگ خانمان سوز سی‌ساله در اروپای مرکزی پایان یافت. وستفالیبا - منطقه‌ای در شمال غربی آلمان - میزبان این رخداد تاریخ‌ساز بود. عهدنامه وستفالیبا را یکی از نقاط عطف در تاریخ روابط بین‌الملل می‌دانند. وستفالیبا نخستین پیمان صلح چند جانبه پس از قرن‌سناس در اروپا است. این پیمان بعدها منجر به معاهدات بزرگ مشابهی بین کشورها شد که در نهایت به تدوین قانون بین‌الملل انجامید. صلح وستفالیبا، الگو و پایه جامعه‌ی ملل و سپس سازمان ملل متحد گردید. این معاهده مرزهای ملی در قاره اروپا را تعیین کرد، استقلال و حاکمیت کشورها را به رسمیت شناخت و نشان داد حاکمیت ملی، قلمرو ملی و استقلال ملی به اصولی تبدیل شده‌اند که باید در روابط بین‌الملل مورد توجه قرار گیرند. در این پیمان حقوق برابر و یکسان کشورها به عنوان واحدهای سیاسی مستقل برای نخستین بار مطرح و مورد پذیرش قرار گرفت. مطابق این پیمان کشورهای مستقل حق تعیین سرنوشت خود را دارند، برابری و حق دخالت در امور هم را ندارند (کامران دستجردی حسن، ۱۴۰۱).

فرهنگ جغرافیای انسانی حاکمیت را «ادعایی برای اقتدار غایبی و نهایی بر یک جامعه سیاسی» تعریف می‌کند. حاکمیت در حقوق اساسی و در پهنه حقوق عمومی نیز به معنای «قدرت برتر و عالی و صلاحیت اتخاذ تصمیم نهایی و قدرت جمع‌کننده انرژی‌های سیاسی درون جامعه» تفسیر شده است که دارنده آن می‌تواند در مسائل قلمرو تحت پوشش امر و نهی کند. حاکمیت ملی (مردمی) یک ابداع قانونی است که این ابداع قانونی دارای قدرت، برای شکل دادن به نهادهاست. استفاده از این برداشت در واقع ناظر بر امور داخلی کشورهاست که حکومت‌ها بر اساس اختیارات و اقتداری که به طرق دموکراتیک یا دیگر روش‌های مرسوم در دوران حاضر کسب کرده‌اند، قدرت و سلطه مشروع خود را بر قلمرو ملی و مردم خویش اعمال می‌کنند (بدیعی مرجان و همکاران، ۱۳۹۹).

با این توضیح حاکمیت از آن رو بعد جغرافیایی می‌یابد که چهره قانونی اعمال اراده حکومت بر سرزمین (قلمرو) و مردمان (ملت) است و مفهوم اجرای قوانین حکومت برای کنترل مردم و سرزمین در محدوده جغرافیایی‌اش را می‌رساند.

اغلب نظریه‌های حاکمیت ملی، «قلمرو» را به عنوان عنصر اساسی حکومت تشخیص می‌دهند و حاکمیت معمولاً مرتبط با یک قلمرو تحدید شده است. در واقع، زمانی که حکومت درون یک متن جغرافیایی قرار می‌گیرد، اولین مشخصه مهم، ویژگی قلمرویی آن است و حکومت از حق تعریف آنچه قانونی است و اجرای قانون درون یک فضای دارای مرز مشخص برخوردار است. مفهوم حاکمیت در مقیاس‌های فضایی گوناگون قابل بررسی است که عبارتند از: فراملی (محلی)، ملی و فراملی. در نگاه کلی‌تر حاکمیت ملی از دو سطح داخلی و خارجی برخوردار است: حاکمیت داخلی به اقتدار مطلق و نهایی دولت بر همه قلمرو افراد، گروه‌ها، نهادها و سازمان‌ها در درون مرزها مربوط می‌شود. اما حاکمیت خارجی (فراملی) به رابطه میان دولت مورد نظر با سایر دولت‌ها مربوط می‌شود و مکمل حاکمیت داخلی (ملی) است. به عبارت دیگر حاکمیت خارجی به معنای شناسایی متقابل از سوی دیگر دولت‌ها درون سیستم بین‌دولتی (بین‌المللی) است.

امروزه بر اساس منشور سازمان ملل متحد، تمام کشورها از حق دفاع از خود در عرصه بین‌المللی، حق استقلال و حق برابری بین‌المللی در حوزه حاکمیت ملی برخوردار هستند. این سه حقوق حاکمیت ملی توسط کشورهای جهان حمایت و اجرا می‌شوند و قلمروگذاری و مرزبانی سرزمینی نقش اساسی در اعمال حاکمیت ملی و برخورداری از حقوق مرتبط بین‌المللی دارد.

۲،۱. قلمرو و مرز

واژه قلمرو ترکیبی از اسم "قلم" و فعل امر "رو" می‌باشد که ظرف مکان و به معنی محل روا بودن قلم کسی و به معنای ملک مطیع است (لغت نامه دهخدا، ۱۳۹۲). قلمرو در عرف نشان دهنده محدوده مالکیت و حاکمیت یک موجودیت زنده مانند حیوان یا انسان یا گروه و سازمانی از آنها بر یک محدوده جغرافیایی اعم از سرزمین، منابع و منافع مادی آن محدوده است. جانوران برای زندگی و فعالیت های زیستی شان، محدوده مشخصی برای خود برمی‌گزینند. حیوانات از رهگذر نشانه‌های ساده بصری، آوایی، چشایی و خواص بویایی مرزهایشان را تعیین، نشانه گذاری (اعلان) و در نگاه‌داشت قلمروشان می‌کوشند. میزان وضوح این نشانه‌ها و اعلان‌ها در فضای مربوطه، به نوعی جدیت و اقتدار بر محدوده قلمرو (مرزها) را القا می‌نماید (بدیعی مرجان و همکاران، ۱۳۹۹).

واژه قلمرو در جوامع انسانی نیز ناظر به فضای محدود شده‌ای است که افراد و گروه‌ها از آن به عنوان محدوده اختصاصی، استفاده می‌کنند و در مقابل هر گونه تهاجم و دست‌اندازی بیگانگان از آن محدوده دفاع می‌نمایند. در نتیجه به فراخور وسعت و توان مادی، قلمروهای مختلفی وجود دارد که زمینه بروز کنش‌های متنوعی از همکاری تا جنگ بین ساکنان را در پی دارد. در حوزه رفتار انسان اجتماعی، قلمرو بخشی از سطح زمین می‌باشد که گروهی خاص یا موجودیتی سیاسی مدعی مالکیت و حاکمیت بر آن است. بنابراین، قلمروها نشان دهنده اعمال قدرت بر فضا هستند که در عالی‌ترین سطح در قالب کشور- ملت‌ها سر برآورده اند. امروزه، قلمرو گستره فضایی قدرت یک کشور و منابع مادی تامین کننده آن قدرت است (کاویانی راد مراد، ۱۳۹۲).

با توضیح ارایه شده، قلمرو در هر عرصه‌ای با ترسیم «مرز» در آن عرصه شکل می‌گیرد و مرزها مهم‌ترین ابزار برای کنترل و محافظت از قلمرو به شمار می‌روند. یعنی ابزار تعیین حدود و کنترل دسترسی به یک قلمرو که به برخی اجازه ورود و از دسترسی برخی دیگر ممانعت به عمل می‌آورد، «مرز» است. در نتیجه مرز نقطه‌ای است که تهدیدات خارجی به واقعیت‌های داخلی تبدیل می‌شود. تحدید مرزها توسط فرآیند قلمروسازی باعث ایجاد یک منطقه خاص می‌شود که در آن قدرت اعمال می‌شود و آن را به یک سرزمین یا فضا تبدیل می‌کند (Medeiros, Goldoni, 2020). بنابراین برای شکل‌گیری قلمرو در هر عرصه یا فضایی، ترسیم و تبیین مرزها نقش موثری دارد.

در سطح ملی تعیین محدوده قلمرو به عنوان فضایی که دولت ملی در آن مشروعیت داشته و قدرت دولتی در آن به رسمیت شناخته می‌شود بر عهده «مرزهای ملی» است. به عبارت دیگر، مرزهای ملی خطوطی هستند که قلمرو بیرونی حاکمیت یک دولت ملی را تعیین می‌کنند و عاملی برای کشف و جدایی یک سازمان سیاسی واحد از کشورهای دیگر هستند. یعنی مرزها دو ملت، دو کشور و دو دولت را از هم جدا می‌کنند. مدیریت مرزی سازوکاری است که امنیت ملی و تنظیم قانونی ورود و خروج برای تامین نیازهای مختلف ملت را فراهم می‌نماید. به همین ترتیب برخورداری از اصول و قواعد حقوق بین الملل مرتبط با حاکمیت سرزمینی (ملی) و اثبات موارد نقض حاکمیت توسط سایر کشورها، با تعریف و اعلان دقیق «قلمرو ملی» و در امتداد آن «مرزهای ملی» رابطه مستقیم دارد (Tsaugourias, 2017).

قلمروگذاری و مرزبانی

قلمروگذاری عبارت است از تلاش یک فرد یا یک گروه برای دستیابی، تاثیرگذاری یا کنترل افراد، پدیده‌ها و روابط، از طریق تحدید حدود و اعمال کنترل بر یک منطقه یا فضای خاص. تعیین قلمرو یک فرآیند است، ساخته و بازسازی می‌شود، شکل گرفته و مدام بروز رسانی می‌شود، یعنی قلمروگذاری یک فرآیند فعال و واکنشی است. به بیان دیگر قلمروها و فضاها به طور طبیعی داده نمی‌شوند، بلکه محصول کنش اجتماعی فعال هستند. با رویکرد بین‌المللی، قلمرو ملی فضایی است که به عنوان مبنای حاکمیت یک دولت شناخته می‌شود و دولت ملی در آن مشروعیت و قدرت کنترل بر منافع، جمعیت، سرمایه‌ها و سایر جنبه‌های مادی و معنوی حاکمیت را دارد. همچنین دولت‌ها با تعیین قلمرو، محدودیت‌هایی را برای دسترسی و بهره‌برداری قدرت‌های خارجی از منافع ملی وضع و اجرا می‌کنند (Medeiros, Goldoni, 2020). به عبارت دیگر قلمرو ملی به «محدوده جغرافیایی یا فضای گسسته و جدا از سایر قلمروها و نشان دهنده ظرفی که دولت توان اعمال قدرت بر آن دارد» گفته می‌شود. بنابراین قلمرو زیربنای اقتدار دولت است و مرزها، محدوده تخصیص اختیار دولت را تعیین می‌کنند (Tsaugourias, 2017).

از آنجا که حفاظت از شهروندان یکی از اهداف اساسی کشور است، امنیت مرزها به وضوح به عنوان یک مسئولیت اصلی دولت تلقی می‌گردد که از آن تحت عنوان «مرزبانی» یاد می‌شود. تلاش‌ها و سازوکارهای سنتی که برای حفظ امنیت مرزها (مرزبانی) توسط دولت‌ها در همه عرصه‌ها انجام شده، آشکار و تا اندازه بسیار زیادی قابل قبول است. این اقدامات مجموعه‌ای از بازدارنده‌های فیزیکی و قابلیت‌های بازرسی در مرزهای کشور برای شناسایی و کنترل آنچه مجاز به عبور از مرزهای کشور می‌باشد را تشکیل می‌دهند که مرزبانی نامیده می‌شود. در مرزبانی ملی حق و وظیفه دولت است که کنترل کند چه کسی و چه چیزی از مرزها عبور نماید تا از کشور و مردم آن در برابر تهدیدات خارجی محافظت کند. این تهدیدها از موارد آشکار مانند تروریست‌ها و متجاوزین که به دنبال انجام یک حمله یا ارتکاب جنایت هستند تا موارد کمتر آشکار مانند محصولات کشاورزی و مواد غذایی آلوده که می‌تواند صنعت کشاورزی کشور را به شدت تحت تاثیر قرار دهد یا جمعیت را بیمار کند متغیر است (Osborn, 2017).

۲. انطباق حاکمیت فضای سایبر ملی بر حاکمیت سرزمینی با استناد به اصول و قواعد حقوق بین الملل

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 تاکید 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).

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 می‌رود، با استناد به مفاد این اصل و بهره‌گیری 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 ارائه 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. همچنین دیوان بین‌المللی دادگستری با استناد به وظیفه عدم مداخله غیرمجاز تصریح می‌نماید، هیچ دولتی حق مداخله منابع و مآخذ ذکله 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 ترسیم و پیاده سازی نماید (اسمعیل‌زاده پرستو و عبدالهی محسن، ۱۳۹۹). از مفاد اصول و قواعد حقوق بین‌الملل و آراء دیوان بین‌المللی دادگستری می‌توان استنباط کرد، این اصول و قواعد قابل انتساب به همه جنبه‌های مادی (فیزیکی) و معنوی حاکمیت ملی می‌باشند. کریمی قهرودی و زارعی در کتاب «حاکمیت فضای سایبری» تاکید می‌نمایند؛ چنانچه یک کشور با سازماندهی انواع جنگ‌های شبکه‌ای، از قبیل حمله به زیرساخت‌های واقع در قلمرو کشور دیگر با استفاده از سلاح‌های سایبری، ضربه الکترونیکی، الکترونیکی-زیستی و موارد مشابه به حاکمیت کشور دیگری تعدی کند، این حمله همزمان به مردم و شبکه غیرنظامی آن کشور نیز آسیب وارد خواهد کرد. از این رو حاکمیت فضای سایبری و حاکمیت ملی (قلمرو) به طور طبیعی یکپارچه هستند (کریمی قهرودی محمدرضا و زارعی وحید، ۱۳۹۹).

۳. چگونگی اعمال حاکمیت بر فضای سایبر ملی در پرتو ویژگی‌های خاص فضای سایبری

در نگاه اول به نظر می‌رسد ویژگی بدون مرز بودن فضای سایبری با مفاهیم سنتی حاکمیت سرزمینی (ملی) و اصول و قواعد حقوق بین‌الملل در این زمینه سازگاری ندارد و عملاً امکان اعمال حاکمیت سرزمینی (ملی) در فضای سایبری وجود ندارد. در این زمینه سوالاتی مطرح می‌شود



که آیا حقوق بین الملل می‌تواند به عنوان یک ابزار تنظیم‌کننده در فضای سایبری عمل کند و اینکه دامنه صلاحیت نظارتی آن چیست؟ به علاوه اینکه آیا دولت‌ها می‌توانند منبع مقررات در فضای سایبری باشند؟

در بازنمایی اولیه فضای سایبری اینگونه به نظر می‌رسید که این فضا غیرقلمروی و بدون مرز است و به همین دلیل نمی‌توان آن را مشمول اصول و قواعد به رسمیت شناخته شده دنیای فیزیکی و پایش، نظارت و اعمال قدرت دولتی دانست. پس این فضا را نیازمند ساختارهای قانونی متفاوت و مختص به خود می‌دانستند. یکی از دیدگاه‌های مطرح در این زمینه دیدگاه جان پری بارلو است که در «اعلامیه استقلال فضای مجازی» به آن اشاره شده است. جان پری بارلو در این اعلامیه که در سال ۱۹۹۶ میلادی منتشر شده است، با رد اعمال حاکمیت دولتی و قوانین مرتبط با فضای واقعی در فضای سایبری (مجازی) آورده است:

- دولت‌های جهان صنعتی، شما غول‌های خسته فولاد، من از فضای مجازی، خانه جدید ذهن آمده‌ام. از طرف آینده از شما گذشته‌ها می‌خواهم که ما را تنها بگذارید. شما در میان ما خوش آمدید. شما در جایی که ما جمع می‌شویم هیچ «حاکمیتی» ندارید.
- ما هیچ دولت منتحبی نداریم و احتمالاً هم نخواهیم داشت... ما فضای اجتماعی جهانی را بنا می‌نهیم. به طور طبیعی مستقل از ظلم‌هایی که می‌خواهید بر ما تحمیل کنید، اعلام می‌کنم، شما حق اخلاقی ندارید که بر ما حکمرانی کنید و هیچ روشی برای اجرا در این زمینه ندارید که باعث نگرانی ما باشد.
- دولت‌ها اختیارات ذاتی خود را از رضایت حکومت شونده‌ها می‌گیرند. شما نه درخواست از ما دارید و نه دریافت کرده‌اید. فضای مجازی در محدوده حاکمیت شما قرار ندارد.
- ما در حال شکل‌دادن به قراردادهای اجتماعی خودمان هستیم. این حکومت بر اساس شرایط دنیای ما به وجود خواهد آمد و دنیای ما متفاوت از دنیای شما است.
- مفاهیم حقوقی مورد استفاده شما از دارایی، بیان، هویت، حرکت و زمینه در مورد فضای مجازی صدق نمی‌کند و همه آن‌ها بر اساس ماده هستند. حال اینکه در فضای مجازی ماده‌ای وجود ندارد.
- ما امیدواریم بتوانیم راه حل‌های خاص خود را برای این فضا بسازیم. اما نمی‌توانیم راه حل‌هایی شما دوست دارید بر ما تحمیل کنید را بپذیریم.
- ما باید دنیای خود را مصون از حاکمیت شما بسازیم، حتی اگر همچنان به حکومت شما بر بدن و دنیای فیزیکی رضایت دهیم. ما خودمان را در سراسر این سیاره پخش خواهیم کرد تا کسی نتواند افکار و اندیشه‌های ما را تسخیر کند.
- ما تمدن ذهن را در فضای مجازی ایجاد خواهیم کرد. باشد که از دنیایی که دولت‌ها ساخته‌اند، انسانی‌تر و عادلانه‌تر باشد.

(BARLOW'S, 1996)

همچنین جانسون و پست در مقاله‌ای با عنوان «قانون و مرزها: ظهور قانون در فضای مجازی» در سال ۱۹۹۶ میلادی، اعمال مفاهیم موجود حاکمیت و قانون در فضای سایبری را به دلیل ویژگی متمایز غیرسرزمینی و بدون مرز بودن آن رد می‌کنند و به همین دلیل، تدوین قوانین اختصاصی برای فضای سایبری را پیشنهاد می‌کنند. جانسون و پست نتیجه می‌گیرند که اگر چه فضای سایبری یک فضای بدون ضابطه نیست و نیاز به تنظیم‌گری و هنجارسازی دارد لیکن قوانین موجود مبتنی بر قلمرو فیزیکی برای اعمال بر فضای سایبری مناسب نیستند. جانسون و پست اعمال اصول و قواعد حقوق بین‌الملل در فضای سایبری را رد نمی‌کنند و علاوه بر این برای اعمال قوانین و مقررات در فضای سایبری، به قلمروگذاری و مرزبانی در این فضا تاکید دارند. هر چند آنها بین قلمرو در فضای سایبری و فیزیکی تفاوت قائل هستند و نوع متفاوتی از مرزها را برای فضای سایبری با توجه به ویژگی‌های خاص آن متصور هستند. به عقیده آنها اگر چه شخصیت بدون مرز فضای سایبری امکان پایش، نظارت و تنظیم قانونی این فضا را تضعیف می‌کند و به چالش می‌کشد؛ قدرت و اقتدار همان طور که پیش‌تر گفته شد، جوهره حاکمیت است و فقدان قلمرو و مرز، قدرت اعمال حاکمیت را از دولت‌ها سلب می‌نماید. بنابراین همچنان قلمرو و مرز نقش سازنده و کارکردی در

قاعده گذاری، اعمال و اجرای قانون در فضای سایبری بازی می کند و مرزها سازمان حاکمیت در فضای سایبری را تعریف می نمایند (Johnson, Post, 1996).

موضع جان پری بارلو و برخی دیگر از نظریه پردازان در مورد ماهیت استثنایی فضای سایبری توسط جک گلداسمیت در مقاله ای با عنوان «علیه هرج و مرج سایبری» به چالش کشیده شده است. از نظر او فضای سایبری نیز از افراد و اشیاء تشکیل شده است. بنابراین دولت ها می توانند بر مردم و اشیاء در قلمرو خود اعمال حاکمیت نمایند و فعالیت ها در این فضا را تنظیم کنند. همچنین گلداسمیت، نظر جانسون و پست را به چالش می کشد و استدلال می کند قواعد و هنجارهای پذیرفته شده فضای فیزیکی در برخی حوزه ها می تواند در فضای سایبری نیز دارای اعتبار و قابل اتکا باشد. به گفته گلداسمیت دولت می تواند بر فضای سایبر ملی اعمال قدرت و فعالیت ها در این فضا را تا حد زیادی از طریق تکنیک های موجود تنظیم کند. این دیدگاه هم اکنون به عنوان دیدگاه غالب نسبت به فضای سایبر ملی پذیرفته شده است (Goldsmith, 1998). موارد فوق بیانگر دیدگاه هایی است که طی دهه های گذشته و به خصوص سال های اولیه ظهور فضای سایبری بیان شد. آنچه مشخص است، امروزه قریب به اتفاق صاحب نظران به هنگام رویارویی با فضای سایبری، بر هنجارسازی و تنظیم گری این فضا و همچنین بر نقش قلمرو و مرز در این زمینه به طور صریح یا ضمنی تاکید دارند.

۴. حق، وظیفه و خواست دولت ها مبنی بر قلمروگذاری فضای سایبر ملی

اگر چه دولت ها در روزهای اولیه شکل گیری فضای سایبری مقررات چندانی مرتبط با این حوزه وضع نکرده و کنترل چندانی بر این فضا اعمال نمی کردند، طی سال های اخیر هم به صورت یک جانبه و هم در ترتیبات چند جانبه در اعمال حاکمیت ملی بر فضای سایبری فعال تر شده اند. یعنی دولت ها می خواهند که محدوده سرزمینی مقررات و اجرای قوانین در اینترنت و فضای سایبری منعکس کننده محدودیت های سرزمینی جهان فیزیکی باشد. آنها پی برده اند با قلمروگذاری و مرزبانی فضای سایبر ملی، دامنه نظارت دولت بر قلمرو فیزیکی نیز افزایش می یابد. همچنین اشاره شد عناصر اصلی حاکمیت عبارتند از: جمعیت، قلمرو تعریف شده، دولت (که وظیفه پایش، نظارت و اعمال قدرت بر قلمرو را بر عهده دارد) و منابع و ظرفیت های لازم برای اداره امور داخلی و برقراری روابط با دولت های دیگر. لیکن از آنجایی که حاکمیت دیجیتال نشئت گرفته از اصل کلی حاکمیت می باشد حق ذاتی هر دولت است بر عناصر حاکمیت در عرصه سایبری به خصوص قلمرو سایبر ملی نیز اعمال قدرت نماید. بنابراین دولت ها می توانند بر مردم و اشیاء در قلمرو خود اعمال قدرت کنند و نسبت به تنظیم گری روابط در محدوده قلمرو ملی سیاست گذاری و خط مشی گذاری نمایند. به علاوه تدوین، اعمال و اجرای قوانین و مقررات در فضای سایبر ملی مستلزم قلمروگذاری فضای سایبر ملی و به تبع آن تعریف و تعیین محدوده مرز قلمرو سایبر ملی خواهد بود (Lambach, 2020).

همچنین فضای سایبری جدا از دنیای واقعی (فیزیکی) نیست و این دو در امتداد هم هستند. از این رو باید از اندیشیدن به قلمرو سایبری به عنوان قلمروی جدا از دنیای واقعی اجتناب نمود. این دیدگاه نسبت به فضای سایبری به عنوان یک «قلمرو متمایز» در عصری پدیدار شد که دسترسی به اینترنت نادر بود و نیاز به زیرساخت های ثابت و اختصاصی داشت. بر خلاف دنیای امروز که دسترسی به فضای سایبری در همه جا امکان پذیر است. با پیشرفت فناوری، ما شاهد تلفیق و ترکیب پیوسته ای هستیم که فضای سایبری و فضای واقعی به طور پیچیده در این فرآیند پویا و متقابل با یکدیگر در ارتباط هستند.

با این توضیح قلمروگذاری سایبری یکی از راهکارهای مهم در تولید قدرت ملی و همچنین بازسازی و حفظ هویت ملی محسوب می گردد. در نتیجه حق، وظیفه و خواست دولت است که کنترل کند چه کسی و چه چیزی از مرزهای کشور عبور می کند تا از کشور و مردم آن در برابر تهدیدات خارجی محافظت کند. این موضوع در عرصه سایبری نیز صدق می کند و خواست دولت ها مبنی بر قلمروگذاری و مرزبانی فضای سایبر ملی مشهود است (Möllers, 2021).

گروه کارشناسان دولتی سازمان ملل متحد طی سال های گذشته موفق شدند بسیاری از جنبه های اساسی مربوط به حاکمیت دولت در فضای سایبری را مشخص کنند. از جمله موارد مورد وفاق می توان به صلاحیت دولت ها بر زیرساخت های سایبری واقع در قلمرو آنها اشاره نمود (Broeders, van den Berg, 2020). به علاوه نباید از این نکته غافل شد که قلمروگذاری و مرزبانی فضای سایبری اولین گام در دفاع



سایبری و نقش برجسته و مهمی در کنترل و پیشگیری از چالش‌های ناشی از فضای سایبری به فضای واقعی کشور دارد (Janparvar et al., 2015). همه این موارد بر حق، وظیفه و خواست دولت‌ها مبنی بر قلمروگذاری فضای سایبر ملی تاکید دارند.

۵. عدم شفافیت و ناتوانی حقوق بین الملل در صیانت از حاکمیت ملی در فضای سایبری

به نظر می‌رسد حق دولت برای اعمال صلاحیت خود در مورد فعالیت‌های اشیاء و اشخاصی که به طور فیزیکی یا قانونی در قلمرو آن حضور دارند، بلامنازع است (Heintschel von Heinegg, 2013). اگر چه با شواهد سرزمینی شدن فضای سایبری می‌توان استنباط کرد اصول و قواعد موجود حقوق بین‌الملل تا حد امکان قابل اعمال در فضای سایبری هستند. اما عدم شفافیت و ناتوانی حقوق بین‌الملل در صیانت از حاکمیت ملی در فضای سایبری و استفاده کشورهای صاحب فناوری از خلاء قانونی در فضای سایبری برای منافع ملی خود بیش از پیش به چشم می‌خورد (Dziwisz, 2022).

در حال حاضر به طور گسترده‌ای پذیرفته شده است که قوانین بین‌المللی موجود در فضای سایبری نیز اعمال شود. گزارش سال ۲۰۱۳ گروه کارشناسان دولتی ملل متحد در زمینه تحولات فناوری اطلاعات و ارتباطات^۱، تصریح می‌کند قوانین بین‌المللی موجود، به ویژه منشور سازمان ملل متحد باید در فضای سایبری اعمال شود و حاکمیت دولت‌ها و اصول و هنجارهای بین‌المللی که از حق حاکمیت ناشی می‌شود در فعالیت‌های مرتبط با حوزه فناوری اطلاعات و ارتباطات نیز بایستی رعایت گردد. از این اصول می‌توان به صلاحیت کنترل و مدیریت زیرساخت‌های سایبری موجود در قلمرو سرزمینی دولت اشاره کرد. گزارش سال ۲۰۱۵ این گروه با بیان هنجارها و اصول بین‌المللی خاص، قدم را فراتر نهاده و ۱۱ هنجار و اصول (داوطلبانه و غیر الزام آور) رفتار مسئولانه دولت‌ها که با هدف ترویج یک محیط باز، امن، پایدار، در دسترس و صلح‌آمیز حوزه فناوری اطلاعات و ارتباطات مطرح شده‌اند را معرفی می‌نماید. در این هنجارها و اصول به صلاحیت دولت‌ها در کنترل و مدیریت فضای سایبری ملی، احترام به حاکمیت سایبری ملی کشورها توسط دیگر دولت‌ها و ممانعت از نقض حاکمیت سایبری ملی تاکید شده است. علاوه بر این فهرستی از اصول حقوق بین‌الملل قابل اجرا در فضای سایبری اعم از حاکمیت دولت، برابر حاکمیتی دولت‌ها، حل و فصل اختلافات از طریق مسالمت‌آمیز، خودداری از تهدید یا استفاده از زور در روابط بین‌الملل، عدم مداخله در فضای داخلی سایر کشورها و احترام به حقوق بشر و آزادی‌های اساسی اشاره شده است.

در سال ۲۰۱۷ گروه کارشناسان بین‌المللی سازمان ملل متحد به دلیل عدم اجماع در مورد چگونگی اعمال هنجارها و اصول خاص فضای سایبری موفق به تهیه گزارش نشد، اما با وجود این، گزارش‌های قبلی این دیدگاه را تایید می‌کنند که اصول و هنجارهای توسعه‌یافته برای جهان فیزیکی تا حد امکان قابل اجرا در فضای سایبری هستند. این مفاهیم را می‌توان سرزمینی (ملی) شدن فضای سایبری توصیف کرد و کاربرد مفاهیم قلمروگذاری و مرزبانی ملی و اعمال حاکمیت ملی در فضای سایبری را نتیجه گرفت (Tsaugourias, 2017).

نکته‌ای که وجود دارد و استناد به اصل حاکمیت برای ارزیابی قانونی بودن یا نبودن اقدامات، عملیات‌ها و حملات سایبری را حائز اهمیت می‌کند این است که تاکنون در عرصه بین‌المللی، اکثر حملات سایبری از شدت کم برخوردار بوده و به ندرت باعث آسیب فیزیکی به زیرساخت‌های کشور دیگر می‌شود. بنابراین حملات سایبری به ندرت به محدوده استاندارد مداخله ممنوعه (مداخله غیر مجاز در امور داخلی یا توسل به زور) قرار می‌گیرند یا به سطح «حمله مسلحانه» می‌رسند که طبق ماده ۵۱ منشور ملل متحد باعث ایجاد حق دفاع از خود شود. یعنی اگر چه 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، اما همین 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 سایبری و 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 (Assaf, Moshnikov, 2020).

¹ GGE

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.

یک پژوهش انجام شده توسط موسسه کاتو به بررسی ۲۷۲ عملیات سایبری مستند بین کشورهای رقیب بین سال‌های ۲۰۰۰ تا ۲۰۱۶ میلادی پرداخته است. در طبقه‌بندی این عملیات‌ها، آنها ۳۲ درصد را به عنوان اختلال، ۵۴ درصد را به عنوان جاسوسی و ۱۲ درصد را به عنوان تخریب یا عملیات‌های مضر تخمین زده‌اند که به منظور از کار انداختن یا آسیب اساسی به اهداف انجام می‌شود. مهم‌تر از همه، نویسندگان این مطالعه به این نتیجه رسیدند که اکثر کشورها (۱/۶۸٪) الگوی انتقام‌جویی را مستند نمی‌کنند. محققان این پژوهش معتقدند سطح بالایی از عملیات‌های سایبری هنجاری است و تا زمانی که اصول و قواعد حقوق بین‌الملل مرتبط با فضای سایبری تصویب و هنجارسازی لازم در این زمینه انجام نپذیرد، شاهد رشد روزافزون اقدامات زیرآستانه و عملیات‌های مخفی در این فضا خواهیم بود. بدین سبب، بدون توافق در مورد حقوق بین‌الملل و اعمال آن در حوزه سایبری، بسیاری از جنبه‌های دیگر از جمله هنجارها، اقدامات اعتمادساز، ظرفیت‌سازی‌ها و ... در هوا باقی می‌ماند. زیرا به اندازه کافی دیدگاه‌ها با یکدیگر متفاوت است و همگرایی را مختل می‌کند (Goel, 2020).

کشورهای چین و ایالات متحده آمریکا طی سال‌های گذشته بحث‌ها و مذاکراتی را پیرامون اعمال قواعد و اصول بین‌المللی اعم از احترام به حاکمیت سرزمینی و عدم مداخله در امور داخلی و به طور کلی رفتار قابل قبول در فضای سایبری آغاز کرده‌اند و این کار را به صورت دوجانبه و همچنین چند جانبه از طریق سازمان ملل متحد و دیگر انجمن‌ها پی گرفته‌اند. دو کشور حتی در دسامبر ۲۰۱۵ بر روی مجموعه محدودی از اصول بازدارنده در مورد جاسوسی صنعتی، سرقت مالکیت معنوی، هدف قرار دادن زیرساخت‌های حیاتی و نیاز به همکاری در زمینه تحقیقات جرایم الکترونیکی توافق کردند. مواضع، سیاست‌ها و اسناد منتشر شده از سوی طیف وسیعی از کشورها نیز مبین تلاش‌ها در همین جهت است (Deibert, Pauly, 2019).

بر این اساس، اصل حاکمیت پیش‌بینی شده در حقوق بین‌الملل برای ارزیابی قانونی بودن اقدامات و عملیات‌ها در فضای سایبری تا اندازه‌ای مهم است و لزوم مواجهه فعالانه به فضای سایبر کشور در جهت صیانت از حاکمیت سایبری ملی، بیش از پیش ضروری به نظر می‌رسد. بنابراین نیازمند شناسایی و اتخاذ راهکارهایی با هدف تقویت و ارتقاء حاکمیت بر فضای سایبری ملی در کنار اتکا به اصول و قواعد حقوق بین‌الملل هستیم.

۶. رقابت‌های دولتی مداوم در فضای سایبری و لزوم قلمروگذاری فضای سایبر ملی

ایجاد سازوکارهای مختلف کنترل مرزی در همه عرصه‌ها که با مقاصد گوناگون از پایش و نظارت بر مرزها، کنترل مهاجرت تا پیشگیری از جرم، جنایت و حملات نظامی انجام می‌پذیرد نشان می‌دهد حاکمیت سرزمینی و قلمرو دولتی حتی در جنبه‌های فیزیکی نیز هنوز معنای خود را از دست نداده‌اند و گاهی با قدرت مضاعف ادامه دارد. بنابراین روند تقویت مرزهای ملی و کنترل‌های دولتی هنوز در دست انجام است. ویژگی‌های خاص فضای سایبری که بخش قابل توجهی از تهدیدات علیه امنیت ملی در فضای سایبری را به همراه داشته است و از سوی دیگر دشواری انتساب حملات در این فضا، موجب گردیده است شاهد رقابت‌های دولتی مداوم در قلمروگذاری فضای سایبری و اعمال سیاست‌های صیانت از قلمرو سایبری باشیم.

همانطور که در بالا اشاره شد، فعالیت‌های زیرسطح آستانه توسط به زور در فضای سایبری که با نادیده گرفتن قلمرو ملی کشورها و قواعد بین‌المللی انجام می‌پذیرد، به طور فزاینده‌ای در حال افزایش است. فقدان قلمروگذاری ملی و مرزهای تعریف شده در فضای سایبری به نفع کشورهای بسیار توسعه یافته با قابلیت‌های تهاجمی سایبری است. از آنجایی که فضای سایبری دستیابی به اهداف سیاسی را آسان‌تر، کارمدرتر و بدون خطر قرار گرفتن در معرض انتقاد بین‌المللی، ممکن می‌سازد؛ فقدان قلمروگذاری ملی و به تبع آن پایش و اعمال قدرت دولتی در قلمرو ملی، اقدامات خصمانه زیر سطح آستانه توسط به زور در فضای سایبری علیه فضای سایبر ملی را تشدید می‌نماید (Dziwisz, 2022).



۷. شواهد قلمروگذاری در فضای سایبری ملی در دیگر کشورها

امروزه اقدامات و فعالیت‌های پایش، نظارت و اعمال قدرت کشورها بر قلمرو سایبر ملی که به درجات مختلف در کشورها اعمال می‌شود به نوعی بیانگر قلمروگذاری و مرزبانی این فضا حتی در کشورهایی است که در ظاهر مدعی فضای سایبری بدون مرز هستند. یعنی برخی از کشورها در قلمروگذاری و مرزبانی فضای سایبر ملی شفاف‌تر عمل می‌کنند ولی حتی در کشورهایی که به ظاهر مدعی فضای سایبر به هم پیوسته جهانی و گردش آزاد اطلاعات در این فضا هستند نیز کنترل و اعمال قدرت بر قلمرو سایبری کشور خود را به گونه‌ای متفاوت اعمال می‌نمایند. هم‌اکنون طیف اقدامات بومی‌سازی و ملی‌گرایی داده‌ها در کشورهای دموکراتیک تا کشورهای اقتدارگرا آغاز شده و الزامات وضع شده توسط دولت‌ها مبتنی بر مکان تولید داده‌ها در حال افزایش است.

با یک گونه‌شناسی و تجزیه و تحلیل از اشکال مختلف اعمال کنترل ملی بر داده‌ها می‌توان پی برد این اقدامات با اهدافی نظیر حفاظت از داده‌ها و حریم خصوصی شهروندان، نظارت و پایش اطلاعات در گردش در قلمرو سایبری ملی و در برخی موارد نیز به منظور کنترل نوع اطلاعاتی که از مرزهای فضای سایبری کشور جریان می‌یابند اعمال می‌شوند.

دولت چین از مدت‌ها پیش با ترویج نسخه قوی از ملی‌گرایی داده‌ها که به آن «حاکمیت سایبری» نیز گفته می‌شود، اقدامات مرتبط با این حوزه را دنبال می‌کند. روسیه از طریق فعالیت‌های خود در فضای سایبری نوعی «خط مقدم دیجیتال» را ایجاد می‌کند که به نوعی تداعی کننده خط مقدم نظامی در سایر عرصه‌ها است. در کنار پیاده‌سازی الزامات ذخیره‌سازی داده‌ها در قلمرو سرزمینی یا به اصطلاح "بومی‌سازی داده‌ها" در کشورهایی مثل روسیه، هند و چین؛ اتحادیه اروپا نیز مجموعه‌ای از محدودیت‌های انتقال داده از قلمرو سرزمینی این اتحادیه را اعمال نموده است که برای محافظت از حریم خصوصی شهروندان و ساکنان اتحادیه اروپا طراحی شده است (Stadnik, 2021).

در ایالات متحده آمریکا، علاوه بر الزام شرکت‌های تحت مالکیت روسیه و چین به ذخیره‌سازی داده‌های مربوط به شهروندان آمریکایی در قلمرو سرزمینی ایالات متحده آمریکا؛ طی سال‌های گذشته کنگره آمریکا تغییراتی را در کمیته سرمایه‌گذاری خارجی به تصویب رسانیده است تا شرکت‌ها و برنامه‌های کاربردی خارجی را که داده‌های شخصی و حساس را جمع‌آوری و نگهداری می‌کنند، با هدف محافظت در برابر استفاده‌های ناپسند خارجی در معرض بررسی‌های امنیت ملی قرار می‌دهد (Stewart, 2018).

فرانسه بر حق حاکمیت بر قلمرو سایبری ملی تأکید دارد و هر گونه عملیاتی که منجر به نقض محرمانگی، یکپارچگی و دسترس بودن سامانه‌های سایبری شود نقض حاکمیت به حساب می‌آورد. این نقض نه تنها زمانی رخ می‌دهد که اثرات آن در قلمرو فرانسه نمایان شود بلکه حتی زمانی که به فضای سایبر ملی فرانسه نفوذ می‌شود هم صادق است (Broeders, van den Berg, 2020).

هم‌اکنون ابزارهای متنوعی برای دولت‌هایی وجود دارد که به دنبال بازسازی قلمرو ملی خود در فضای سایبری هستند. دیوارهای آتش ملی یکی از شناخته شده‌ترین روش‌ها برای دولت‌ها است تا هم ادعای سرزمینی خود را اعلام کنند و هم قدرت خود را در فضای محدود نشان دهند. این فایروال‌ها طیف وسیعی از مکانیسم‌های فیلترینگ مانند مسدود کردن IP و جستجوی کلمات کلیدی را برای سانسور بحث در مورد موضوعات حساس و عدم دسترسی به وب سایت‌هایی که خرابکارانه تلقی می‌شوند، ترکیب می‌کنند. «دیوار آتش بزرگ چین» مشهورترین مثال در این زمینه است، اما سایر کشورها نیز سامانه‌های مشابه را توسعه داده یا در حال توسعه هستند. کره شمالی احتمالاً افراطی‌ترین نمونه‌ای است که تا همین اواخر، کاربران فقط می‌توانستند به شبکه داخلی^۱ در سراسر کشور دسترسی داشته باشند. امروزه دسترسی به برخی از سایت‌های اینترنتی تحت محدودیت‌های شدید و نظارت دقیق دولت امکان‌پذیر است.

روش‌شناسی تحقیق

این پژوهش از منظر هدف توسعه‌ای-کاربردی می‌باشد. روش تحقیق مورداستفاده در این پژوهش توصیفی-تحلیلی است که با استفاده از روش جمع‌آوری اطلاعات کتابخانه‌ای و اینترنتی، مجموعه اسناد و مقالات مرتبط با موضوع تحقیق مورد بررسی جامع قرار گرفت. در ادامه با تجزیه و تحلیل اسناد در این حوزه، نقش و جایگاه قلمروگذاری و مرزبانی فضای سایبری در اعمال حاکمیت بر فضای سایبر ملی را مورد

¹ Kwangmyong

پژوهش قرار گرفت. نتایج حاصل از این پژوهش می‌تواند ارتقاء دانش مدیران و متولیان کشور را در زمینه اعمال حاکمیت بر فضای سایبر ملی به همراه داشته باشد.

تجزیه و تحلیل

با تجزیه و تحلیل موارد یاد شده می‌توان استنباط کرد که در وحله نخست باید از تشبیه ساده قلمرو در فضای سایبری با سایر قلمروهای سنتی اجتناب کرد. زیرا ساختار به هم پیوسته و جهانی فضای سایبری ایجاب می‌نماید قلمرو در این فضا متخلخل باشد و با توجه به وجود بازیگران مختلف که در فضای سایبر جهانی کنش و اعمال قدرت می‌نمایند با همپوشانی قلمرو کنشگران روبرو هستیم. این موضوع سبب شده است. دولت‌ها در صورت اراده، با استفاده از راهکارها و فناوری‌های نوین به قلمرو ملی دیگر کشورها تعرض نمایند.

در وحله بعد اگر چه احترام به حاکمیت ملی کشورها یک اصل اساسی در حقوق بین‌الملل به شمار می‌رود و از آن قواعد و هنجارهای بازدارنده‌ای از حقوق بین‌الملل مانند 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 ناشی می‌شود که مورد پذیرش همگان است؛ 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 دیگر کشورها را از طریق فضای سایبری انجام می‌دهند و پیگرد قانونی آنها از طریق حقوق بین‌الملل مقدور نیست.

افزون بر این 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.

از این رو قلمروگذاری و مرزبانی فضای سایبر ملی، به عنوان راهکاری برای محافظت بیشتر از داده‌ها و شهروندان در برابر تهدیدات خارجی و مهم‌تر از آن اعمال حاکمیت ملی سایبری، می‌تواند مورد توجه ویژه قرار گیرد. از این رو دولت‌ها که وظیفه اساسی محافظت از منابع و منافع ملی، مدیریت و تنظیم‌گری در تمامی عرصه‌ها و به تبع آنها اعمال حاکمیت ملی را بر عهده دارند قادرند با اعمال سیاست‌های قلمروگذاری و مرزبانی فضای سایبر ملی، اعمال حاکمیت در این فضا را ارتقاء دهند.



نتیجه گیری

حاکمیت در هر عرصه‌ای از چهار عنصر قلمرو، شهروندان، منابع و سیاست تشکیل می‌گردد و پیش شرط اعمال حاکمیت در فضای سایبر نیز تعریف و تحقق این چهار عنصر می‌باشد. یعنی اینکه افراد، تجهیزات و داده‌های موجود در فضای سایبری هر کشور، تابع حکمرانی آن کشور بوده و هیچ کشوری نباید در فضای سایبر واقع در قلمرو کشورهای دیگر مداخله کند. از سوی دیگر تمام کشورها حق دارند از قلمرو خود در برابر تجاوز محافظت نمایند. به علاوه قلمروگذاری و مرزبانی در تمامی عرصه‌ها یکی از راهکارهای مهم در تولید قدرت ملی و بازسازی و حفظ هویت ملی محسوب می‌گردد. در نتیجه حق، وظیفه و خواست دولت است که کنترل کند چه کسی و چه چیزی از مرزهای کشور عبور می‌کند تا از کشور و مردم آن در برابر تهدیدات خارجی محافظت نماید. این موضوع در عرصه سایبری نیز صدق می‌کند. در نتیجه قلمروگذاری و مرزبانی فضای سایبری کشور می‌تواند نقش بسزایی در اعمال حاکمیت بر فضای سایبری ملی داشته باشد.

از سوی دیگر 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. ولی به هر حال برخورداری از اصول و قواعد حقوق بین‌الملل، پیگیری‌های قانونی و دفاع از فضای سایبر ملی مستلزم تعریف و اعلان قلمرو سایبری ملی و مرزبانی موثر این فضا می‌باشد. در نتیجه تعریف نشدن قلمرو و مرز ملی در فضای سایبری، رفتار قانون‌مند کنشگران خصوصی و دولتی در یک فضای قانونی را به همراه نخواهد داشت و این مسئله منجر به تضعیف نظام حاکم و امنیت ملی خواهد شد.



پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

۱. بدیعی ازندهای، مرجان و میراحمدی، فاطمه سادات و غلامی، بهادر. (۱۳۹۹). مقایسه مفهوم «حاکمیت ملی» در قوانین اساسی مشروطه و جمهوری اسلامی ایران
۲. کریمی قهرودی، محمدرضا و زارعی وحید. (۱۳۹۹). حاکمیت فضای سایبری، انتشارات موسسه آموزشی و تحقیقاتی صنایع دفاعی.
۳. کامران دستجردی، حسن. (۱۴۰۱). کاربرد حاکمیت درمقیاس های فضایی. نشریه تحقیقات کاربردی علوم جغرافیایی، سال بیست و دوم، شماره ۶۵.
۴. کاویانی راد، مراد. (۱۳۹۲). پردازش مفهوم «قلمرو» از دیدگاه جغرافیای سیاسی. برنامه ریزی و آمایش فضا (مدرس علوم انسانی)، ۱۷(۴)، ۴۳-۶۱.
۵. اسمعیل زاده ملاباشی، پرستو، عبدالمهی. (۱۳۹۹). حملات سایبری و نقض اصل عدم مداخله. فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ۵۰(۲)، ۷۱۱-۷۳۶.
6. Paasi, A., Ferdoush, M. A., Jones, R., Murphy, A. B., Agnew, J., Ochoa Espejo, P., & Fall, J. J. (2022). Locating the territoriality of territory in border studies. *Political Geography*, 95, 102584.
7. Douzet, F. (2020). Cyberspace: the new frontier of state power. *Handbook on the Changing Geographies of the State*.
8. Medeiros, B. P., & Goldoni, L. R. F. (2020). The Fundamental Conceptual Trinity of Cyberspace. *Contexto Internacional*, 42, 31-54.
9. Tsagourias, N. (2017). Law, Borders and the Territorialisation of Cyberspace. *Indonesian J. Int'l L.*, 15, 523.
10. Osborn, P. (2017). Cyber Border Security—Defining and Defending a National Cyber Border. *Homeland Security Affairs*, 13.
11. BARLOWS, J. P. (1996). Declaration of independence for cyberspace.
12. Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *stanford law review*, 1367-1402.
13. Goldsmith, J. L. (1998). Against cyberanarchy. *The University of Chicago Law Review*, 65(4), 1199-1250.
14. Lambach, D. (2020). The territorialization of cyberspace. *International Studies Review*, 22(3), 482-506.
15. Möllers, N. (2021). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. *Science, Technology, & Human Values*, 46(1), 112-138.
16. Broeders, D., & van den Berg, B. (Eds.). (2020). *Governing Cyberspace: Behavior, Power and Diplomacy*. Rowman & Littlefield Publishers.
17. Janparvar, M., Ghasri, M., & Hosseinpour Motlagh, M. (2015). Border Management of Cyberspace, First Step of Cyber Defense. *Research on Humanities and Social Sciences*, 5.
18. Heintschel von Heinegg, W. (2013). Territorial sovereignty and neutrality in cyberspace. *International Law Studies*, 89(1), 17.
19. Dziwisz, D. (2022). Non-War Activities in Cyberspace as a Factor Driving the Process of De-Bordering. *Politics and Governance*, 10(2).
20. Assaf, A., & Moshnikov, D. (2020). Contesting sovereignty in cyberspace. *International Cybersecurity Law Review*, 1(1), 115-124.
21. Goel, S. (2020). National cyber security strategy and the emergence of strong digital borders. *Connections*, 19(1), 73-86.
22. Deibert, R. J., & Pauly, L. W. (2019). Mutual entanglement and complex sovereignty in cyberspace. In *Data Politics* (pp. 81-99). Routledge.
23. Stadnik, I. (2021). Russia: An independent and sovereign Internet?. *Power and Authority in Internet Governance*, 147-167.
24. Stewart, D. P. (2018). Recent Developments in US Cyberlaw. *Agenda Internacional*, 25(36), 113-131

