

Feasibility Study and the Requirements for Generalizability of the Border Phenomenon to Cyberspace

Seyed Mohammad Mahdi Ghamami

Assistant Professor, Public and International Law, Imam Sadiq University, Tehran, Iran.
mmghamamy@gmail.com

Sajad Khalilinezhad

Corresponding Author, M.Sc. Student of Islamic Education and Public Law, Imam Sadegh University, Researcher in Rushd Center, Imam Sadegh University, Tehran, Iran.
sakhne@gmail.com

Abstract

Governments have recognized cyberspace, after the three domains of their national territories, as the fourth realm of their national sovereignty but some elements of nation-states including borders have not yet emerged in cyberspace. This study aims at examining the feasibility of generalizing the border phenomenon from real space to cyberspace and the necessity of this generalization, and providing a clear definition of cyber border. Then, the requirements for the realization of borders in cyberspace, including the methods of demarcation in this space and the feasibility of technical realization of cyber borders, are examined. In terms of its purpose, this study is an exploratory-descriptive research with qualitative data collected through library method and analyzed qualitatively. Findings show that not only is the existence of borders in cyberspace possible, but also due to the types of hard and soft threats in cyberspace, their necessity is double that of the real space. As a result of the remarkable developments of the cyberspace era, the real meaning and main functions of border have not changed while merely some methods of border demarcation and border guarding in information and communication technology have undergone some considerable changes. Accordingly, the borders of cyberspace like those of the real space have established the boundaries of the sovereignty of nation-states in digital space and, in accordance with certain rules, prevent the hard and soft threats of cyberspace.

Keywords: *Nation-state, border, cyberspace border, cyber sovereignty, national information network*

امکان‌سنجی و الزامات تعمیم‌پذیری پدیده مرز به فضای مجازی^۱

سید محمد مهدی غمامی

استادیار دانشکده معارف اسلامی و حقوق، دانشگاه امام صادق (ع)، دکترای تخصصی حقوق عمومی، تهران،
ایران mmghamamy@gmail.com

سجاد خلیلی نژاد

نویسنده مسئول، دانشجوی کارشناسی ارشد معارف اسلامی و حقوق عمومی، دانشگاه امام صادق (ع)،
پژوهشگر مرکز رشد دانشگاه امام صادق (ع)، تهران، ایران sakhne@gmail.com

چکیده

دولت‌ها، فضای مجازی را پس از عرصه‌های سرزمینی سه‌گانه، به‌عنوان قلمرو چهارم اعمال حاکمیت ملی به رسمیت شناخته‌اند، اما هنوز برخی از عناصر دولت – ملت‌ها در فضای مجازی، از جمله مرزها ظهور و بروز قابل‌توجهی نداشته‌اند. هدف از پژوهش حاضر، امکان‌سنجی تعمیم‌پذیری مرز از فضای واقعی به فضای مجازی، ضرورت آن و ارائه یک تعریف از مرز سایبری است. سپس، الزامات تحقق مرزها در فضای مجازی از جمله شیوه‌های مرزگذاری در فضای مجازی و امکان تحقق فنی مرز سایبری مورد بررسی قرار می‌گیرد. پژوهش حاضر از حیث هدف اکتشافی – توصیفی و داده‌های استفاده‌شده در این پژوهش، کیفی است که به روش کتابخانه‌ای، گردآوری و به شیوه‌ی کیفی تحلیل شده است. یافته‌های این پژوهش، نشان می‌دهد نه تنها وجود مرزها در فضای مجازی امکان‌پذیر است، بلکه با توجه به انواع تهدیدهای سخت و نرم در فضای مجازی، ضرورت آن‌ها نسبت به فضای واقعی دوجندان است. در اثر تحولات عصر فضای مجازی، معنای مرز و کارکردهای اصلی آن دچار تغییر و تحول نشده و صرفاً برخی شیوه‌های مرزگذاری و مرزبانی در فناوری اطلاعات و ارتباطات متحول شده است. بنابراین مرزهای فضای مجازی مشابه فضای واقعی، حدود قلمرو حاکمیت دولت-ملت‌ها را در فضایی دیجیتالی مشخص کرده و مطابق قواعد خاصی در مقابل تهدیدهای سخت و نرم فضای مجازی مانع ایجاد می‌کند.

واژه‌های کلیدی: دولت – ملت، مرز، فضای مجازی، مرز فضای مجازی، حاکمیت

سایبری، شبکه ملی اطلاعات

تاریخ دریافت: ۹۹/۱۱/۳۰ تاریخ بازبینی: ۰۰/۰۲/۲۴ تاریخ پذیرش: ۰۰/۰۳/۰۴

فصلنامه راهبرد اجتماعی – فرهنگی، سال ۱۰، شماره ۳۸، بهار ۱۴۰۰، صص ۶۵-۹۸

مقدمه و بیان مسأله

ظهور و بروز فضای مجازی، فناوری اطلاعات و ارتباطات به‌عنوان یکی از برآیندهای جهانی شدن، به‌صورت گسترده و اثرگذار در روابط اجتماعی، در نیمه‌ی دوم قرن بیستم و قرن بیست و یکم، سبب تغییر و تأثیر اساسی در مفاهیم پایه حقوق عمومی، علوم سیاسی و جغرافیای سیاسی همچون: مفهوم ملت، حکومت، حاکمیت، مرز و بسیاری از مفاهیم دیگر شده است. انقلاب در فناوری اطلاعات و ارتباطات شبیه به انقلاب صنعتی، در حال تغییر شکل دادن جهان و ایجاد الگوی جدید در قلمروهای فرهنگی، اقتصادی و سیاسی است و بسیاری از تعاملات در این حوزه‌ها بر بستر فضای مجازی منتقل شده است (Racicot, Hayes, Szibbo, & Trudel, 1998, p. 96). در عرصه‌ی سیاست که مناسبات قدرت اهمیت پیدا می‌کند، امروزه ظرفیت فضای مجازی و شبکه‌های اجتماعی به‌عنوان قدرتی نوظهور و مهم جلوه پیدا کرده است و روابط سنتی قدرت را بر هم زده است و بازیگران مختلفی مانند شرکت‌های تجاری، مردم و نهادهای مردمی را به قدرت رسانده است. این امر منجر شده است، ادبیات حاکمیت مطلق دولت‌ها تبدیل به ادبیات حکمرانی دولت‌ها شود، چراکه حکمرانی زمانی مطرح می‌شود که دیگر دولت‌ها تنها بازیگر عرصه قدرت نباشند و بازیگران مختلفی، قدرت و اثرگذاری داشته باشند.

با این اوصاف، ورود دولت‌ها در امر تنظیم‌گری و تمشیت روابط در عرصه‌ی فضای مجازی، ضروری به نظر می‌رسد، اما مداخله دولت‌ها در این عرصه الزاماتی با خود به همراه دارد. دولت - ملت‌های مدرن با سه عنصر: سرزمین، جمعیت و قدرت عالی شناخته می‌شوند. مرزها یکی از الزامات و مقدمات دولت - ملت‌های

مدرن محسوب می‌شود که مشخص‌کننده‌ی حدود سرزمینی و حدود صلاحیت اعمال حاکمیت قدرت عالی است. بنابراین، برای تحقق حاکمیت ملی در عرصه سایبری، ابتدا باید مرزهای ملی در این عرصه مشخص شود. از طرفی، با وجود ویژگی‌های خاص عرصه‌ی فضای مجازی این مسئله وجود دارد که آیا اصلاً مرزگذاری در فضای سایبری امکان‌پذیر است یا خیر؟ هم‌چنین ضرورت مرزگذاری در فضای مجازی، محل تردید واقع می‌شود. مسئله مرز فضای مجازی، تنها به ضرورت و امکان تحقق آن خلاصه نمی‌شود، بلکه الزامات مختلفی از جمله روش‌های مرزگذاری مختلف، که هر یک می‌تواند محل پژوهش قرار گیرد.

۱. اهداف و سؤالات پژوهش

در این مقاله، به دنبال پاسخ به این پرسش هستیم که آیا امکان تعمیم پدیده‌ی مرز به فضای مجازی وجود دارد؟ الزامات آن چیست؟ در راستای رسیدن به پاسخ سؤال اصلی پژوهش، سؤالات فرعی پاسخ داده می‌شود از جمله اینکه، آیا مفهوم مرز در فضای مجازی مصداق دارد؟ در این صورت مفهوم آن چه تغییری می‌کند؟ در ادامه بررسی می‌شود ضرورت مرزگذاری در فضای مجازی چیست؟ و آیا اساساً، مداخله دولت‌ها در فضای مجازی ضرورت دارد؟ روش‌های مرزگذاری در فضای مجازی چیست؟ و رویکرد کشورهای مختلف از جمله؛ چین و ایران در قبال مرز سایبری چه بوده است؟

هدف از بررسی مرز سایبری در حقوق عمومی و علوم سیاسی، بررسی مرزهای سایبری با دیدگاه فنی و مهندسی یا روش‌های فنی مرزبانی سایبری و تعیین تجهیزات امنیت سایبری نیست، بلکه هدف، تعیین رویکرد در دغدغه مبهم حاکمیت سایبری و امنیت سایبری در قالب نهادهایی متمرکز، مانند مرز است که از عدم قطعیت‌های ماهوی در این حوزه کاسته شود و قسمتی از رویکرد و نظریه‌ی حکمرانی جمهوری اسلامی ایران در فضای مجازی تکمیل شود. به همین سبب، در قسمت اول این پژوهش به مبانی نظری مرتبط با تعریف فضای مجازی، مفهوم مرز و جایگاه نظری مفهوم مرز در علوم سیاسی و حقوق عمومی پرداخته می‌شود و در ادامه به تعریف و تعمیم پدیده مرز در فضای مجازی و الزامات

تحقق مرز سایبری از نظر حقوقی اشاره خواهد شد و به دو رویکرد عمده در موضوع حاکمیت سایبری اشاره و نهایتاً، با تعیین رویکرد مختار به امکان‌سنجی مرز در فضای مجازی پرداخته می‌شود.

۲. پیشینه پژوهش

بدیعی ازندهای و همکاران (۱۳۹۲)، در مقاله ای با عنوان «تبیین مفهوم مرز در فضای سیاسی - مجازی ایران» بیان می‌کند؛ در عصر گسترش تکنولوژی ارتباطات، مرزهای جغرافیایی اهمیت خود را از دست نداده است بلکه، کارکردهای جدیدی نیز برعهده گرفته است. به طوری که حتی کنترل‌های مرزی امروزه در فضای مجازی به صورت فیلترینگ، کدهای مخابراتی، کارت‌های اعتباری و کدهای اینترنتی اعمال می‌شود. حافظ نیا (۱۳۹۰)، در کتاب «جغرافیای سیاسی فضای مجازی» در یک فصل به بررسی فلسفی و سیاسی مفهوم پدیده‌ی مرز و قلمرو می‌پردازد و تجلی مرز در فضای مجازی را در نام‌های دامنه‌ی اینترنتی، فیلترها، دیوارهای دفاعی، کدهای مخابراتی و کارت‌های اعتباری بررسی می‌کند. هرچند این کتاب، مهم‌ترین منبع در زمینه‌ی مرز در فضای مجازی است، اما به علت عدم در نظر گرفتن تحولات اخیر در فضای مجازی و تجلی مرز در موارد دیگر، قابل اصلاح و تکمیل است. موسوی و مستجابی سرهنگی (۱۳۹۲)، در مقاله‌ی «تبیین مفهوم مرز در فضای سایبر»، نتیجه‌گیری می‌کنند که امروزه مرز اهمیت خود را از دست نداده، بلکه کارکردهای آن متفاوت شده است، به طوری که حتی واپایش‌های مرزی امروزه در فضای مجازی به صورت فیلترینگ، کدهای مخابراتی، کارت‌های اعتباری و کدهای اینترنتی اعمال می‌شود. افضل‌ی و همکاران (۱۳۹۲) در مقاله‌ی «تبیین مفهوم مرز در فضای سیاسی مجازی» بیان می‌کنند، هر چند تحولات دوران معاصر و فناوری‌های ارتباطی و اطلاعاتی توانسته‌اند برخی کارکردهای مرز را تغییر دهند، و لی نتوانسته‌اند ماهیت آن را از بین ببرند. چوزنک و گیرس^۱ (۲۰۱۸) در مقاله‌ی «مرزها در فضای مجازی: آیا حاکمیت می‌تواند با چالش‌های امنیت سایبری سازگار شود» معتقد هستند، مرزها در فضای مجازی می‌توانند یک ساختار بالقوه

مفید برای تقویت امنیت سایبری ملی باشد. در عین حال مرزهای سایبری ممکن است آزادی‌های کاربران فضای مجازی را محدود نماید.

با بررسی پیشینه‌ی پژوهش، مشخص است؛ تحقیقاتی که تاکنون صورت گرفته از بُعد علوم سیاسی و جغرافیای سیاسی به موضوع مرز سایبری توجه کرده، اما پژوهش حاضر از بعد حقوق عمومی نیز به موضوع مرز سایبری پرداخته است. هم چنین تعریفی که در این مقاله از فضای مجازی ارائه شده است در سایر پژوهش‌ها مدنظر نبوده و بیشتر، فضای مجازی از بُعد فنی و سخت‌افزاری مورد توجه قرار گرفته، در حالی که بعد نظامات اجتماعی فضای مجازی اهمیت بسیار زیادی دارد. از طرف دیگر، پژوهش‌های صورت‌گرفته در ارتباط با مرز فضای مجازی به علت زمان تألیف، متوجه تغییرات جدید و شیوه‌های نوین مرزگذاری در فضای مجازی نبوده‌اند و به همین دلیل اقدامات اخیر سایر کشورها از جمله چین و اقدامات ایران در ارتباط با شبکه‌ی ملی اطلاعات مورد بررسی قرار نگرفته است.

۳. ملاحظات مفهومی و نظری

۳-۱. تعریف مفاهیم

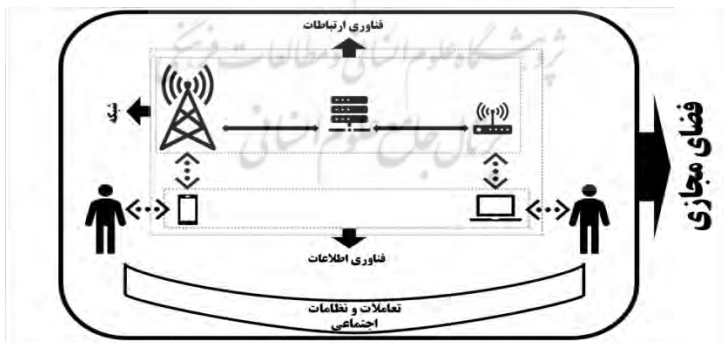
تعاریف متفاوتی از فضای مجازی^(۱) ارائه شده است، با این وجود، تعریف جامعی از این واژه که مورد توافق باشد، وجود ندارد. به‌طور مثال، کرامر^۱، بیست و هشت تعریف متفاوت برای فضای مجازی احصا کرده است (Karmer, 2009, p. 1). در یک نگاه کلی به تعریف‌های مختلف، بسیاری از تعاریف جامع و مانع نیستند، بلکه تنها به ابعاد فنی فضای مجازی توجه کرده‌اند. به‌طور مثال مایر و همکاران^۲ در تعریف فضای مجازی بیان می‌کند: «فضای مجازی یک دامنه پویا و جهانی است که با استفاده ترکیبی از الکترون‌ها و طیف الکترومغناطیسی مشخص می‌شود. هدف از آن ایجاد، ذخیره، اصلاح، تبادل، اشتراک، استخراج، حذف و استفاده از اطلاعات و از هم گسیختن منابع فیزیکی است» (Mayer, 2014, p. 2). لغت‌نامه‌ی

1. F. D. Kramer

2. M. Mayer; L. Martino; P. Mazurier & G. Tzvetkova.

آکسفورد، واژه‌ی فضای مجازی (cyberspace) را این‌گونه تعریف کرده است: «فضایی تئوری که ارتباطات کامپیوتری در آن رخ می‌دهد» (Oxford Online Dictionary, 2020). یا در سندی تحت عنوان واژه‌نامه‌ی مشترک آمریکا و روسیه در موضوع امنیت سایبری^۱، بیان شده است: «یک محیط الکترونیکی و غیر فیزیکی است که از طریق آن اطلاعات ایجاد، ارسال، دریافت، ذخیره، پردازش و حذف می‌شوند» (Godvin III, Kulpin, Rauscher, & Yaschenko, 2014).

بسیاری از تعاریف فضای مجازی، به فناوری اطلاعات و ارتباطات (ICT) تنزیل یافته است. از دیدگاه مانوئل کاستلز^۲ فناوری اطلاعات مرسوم، در دودسته قرار می‌گیرند، فناوری پردازش اطلاعات و فناوری ارتباطات (سلطانی نژاد، اسلامی، & راستگو، ۱۳۹۵، ص. ۸۶). اما باید توجه کرد که اولاً، آنچه فضای مجازی را فضای مجازی می‌کند، اتصال فناوری‌های اطلاعات توسط فناوری‌های ارتباطات نیست، بلکه نظر مثبت کاربران است که این نوع از اتصال را مؤثر دانسته و بر این بستر با یکدیگر ارتباط می‌گیرند. بر این اساس است که فضای مجازی در حکم عالم واقع قرار می‌گیرد. پس تعریف فضای مجازی همان‌طور که در تصویر ۱ مشهود است عبارت است از: «نظام‌های اجتماعی که از تعامل کاربران بر بستر شبکه و فناوری اطلاعات و ارتباطات، شکل می‌گیرد» (آزادی، ۱۳۹۷، ص. ۱۶۶).



تصویر ۱. تعریف فضای مجازی

1. The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations
2. Manuel Castells

کلمه‌ی مرز در معانی مختلفی به کار می‌رود، در تعریف عام لغوی مرز عبارت است از: «هر چیز مشخص‌کننده یا محدودکننده حد و دامنه چیزی»^(۲). موضوع مورد پژوهش در این مقاله رویکرد پژوهش راجع به مرز، سیاسی و حاکمیتی است. از زمانی که دولت‌ها بنابر خواست ملت‌ها به وجود آمدند، مرز مفهوم نوین خود را یافت و منطقه سرحدی جای خود را به خط مرزی داد. امروزه، خطوط مرزی دارای ارزش حقوقی و بین‌المللی می‌باشند، زیرا در سازمان ملل متحد ثبت شده‌اند و توسط کشورها نیز به رسمیت شناخته شده‌اند (رنجکش & کشاورز، ۱۳۹۲، ص. ۷۲).

با مروری بر تعاریف مختلفی که از پدیده مرز ارائه شده است، در عین تنوع تعاریف و تعابیر، ماهیت واحدی از مفهوم مرز قابل برداشت است. «مرز عامل تشخیص و جدایی یک واحد متشکل سیاسی یا کشور، از دیگر واحدهای مجاور و به عبارتی جداساز قلمرو حاکمیتی دو نظام سیاسی است». هسته‌ی اصلی تعریف مرز عبارت است از اینکه؛ مرز تعیین‌کننده‌ی حدود حاکمیت یک کشور است. اما در تعریف‌های مختلف، عناصر دیگری نیز برای تعریف مرز در نظر گرفته شده است که به‌عنوان عناصر فرعی و تبعی در تعریف مرز در نظر گرفته می‌شود که بیشتر ناظر به کارکرد مرزها است نه تعریف چیستی مرز؛ عامل تشخیص و جدایی کشورها، بزرگ‌ترین عامل امنیت و استقلال (رحمتی راد، ۱۳۷۴، ص. ۳)، به وجود آورنده‌ی وحدت سیاسی در کشور (زرقانی، ۱۳۸۶، ص. ۹۹)، مطابق قواعد خاصی در مقابل حرکت انسان، انتقال کالا و افکار مانع ایجاد می‌کند (میرحیدر، ۱۳۸۵، ص. ۱۱۴)، قراردادی است (مجتهدزاده، ۱۳۸۱، ص. ۴۰) و آغاز نقطه تعامل با سایر کشورهاست (کبیری، جان‌پرور، & زرقانی، ۱۳۹۶، ص. ۹۳).

۲-۳. مبانی نظری

دولت مفهومی است که در قلب مفاهیم علوم سیاسی و حقوق عمومی قرار می‌گیرد و اساساً موضوعات و مسائل این علوم، حول مفهوم دولت شکل می‌گیرد. دولت به معنای مدرن و امروزی، پس از شکل‌گیری قرارداد و ستفالی تحت عنوان

دولت - ملت‌ها^۱ یا دولت‌های ملی شکل گرفت. تعاریف متفاوتی از دولت‌های مدرن ارائه شده است، اما اگر بخواهیم قدر مشترکی از تعاریف را به‌عنوان مفهوم دولت بیان کنیم، باید به عناصر اصلی تشکیل دهنده‌ی دولت بپردازیم. دولت «به گروهی از افراد انسانی اطلاق می‌شود که در سرزمینی معین ساکن و تحت تابعیت یک قدرت سیاسی عالی باشند» (غمامی، ۱۳۹۰، ص. ۶۲). بنابراین وجود دولت - ملت‌ها مستلزم وجود سه عنصر جمعیت، سرزمین و قدرت عالی است. برای بررسی جایگاه مرز در علوم سیاسی و حقوق عمومی، باید به بررسی جایگاه مرز در هر یک از این سه عنصر پرداخت.

عنصر جمعیت در شکل‌گیری دولت - ملت‌ها به‌عنوان خمیرمایه در نظر گرفته می‌شود (قاضی، ۱۳۹۳، ص. ۵۷)، اما مفهوم جمعیت صرفاً به معنای کنار هم قرار گرفتن توده‌ای از افراد نیست، بلکه افراد باید احساس همبستگی کنند. طبق نظریه‌ی ملت که قدرت تبیین‌کنندگی بالاتری برای مفهوم جمعیت دارد، عوامل مختلف مادی و معنوی می‌تواند در احساس همبستگی جمع دخیل باشد (غمامی، ۱۳۹۰، ص. ۶۳-۶۵). یکی از مهم‌ترین عوامل ایجاد همبستگی در میان جمعیت در سیر تاریخی کشورها مرزها بوده است که توانسته، انسان‌ها را از نژادهای مختلف مذهب‌های مختلف و فرهنگ‌های مختلف متحد و همدل کند.

عنصر سرزمین، مکانی است جغرافیایی که اولاً برای سکونت گروه انسانی و ثانیاً برای تعیین قلمرو اعمال حاکمیت حکومت ضروری است و شامل آب، خاک و فضای هوایی محدود به مرزها است که متناسب با نظام حقوق بین‌الملل و یا معاهدات بین دولت‌ها تعیین و مرزبندی می‌شود (قاضی، ۱۳۹۳، ص. ۶۰). نقش مرز در این عنصر واضح و عامل اساسی محسوب می‌شود و اساساً سرزمین هر دولت - ملت، توسط مرزها از یکدیگر متمایز می‌شود.

عنصر قدرت عالی در واقع، عنصر سازمان‌دهنده به سرزمین و جمعیت برای تأمین اهداف جامعه محسوب می‌شود (غمامی، ۱۳۹۰، ص. ۶۹). قدرت عالی از دو بُعد تشکیل می‌شود که بعد سخت آن به حکومت و بُعد نرم آن به حاکمیت

تعبیر می‌شود. کارکرد حکومت‌ها متناسب با نظریه‌ی دولت و ایدئولوژی حاکم در آن کشور، موسع یا مضیق می‌شود، اما یکی از کارکردهای اصلی در تمامی نظریات دولت، برقراری نظم و امنیت، پاسداری از تمامیت سرزمینی و تلاش برای پیشبرد منافع یکایک شهروندان خویش است (شیرزادی، ۱۳۹۷، ص. ۹۶). در این عنصر نیز مرزها نقش اساسی دارند. در بعد خارجی، برای رفع تعارضات حکومت‌های مختلف و هم‌جوار و هم‌چنین در بحث استقلال و تمامیت ارضی و در بعد داخلی، در تعیین قلمرو صلاحیت حاکمیت دولت‌ها، مرزها نقش تعیین‌کننده‌ای دارند.

از طرفی مرزها، تعیین‌کننده‌ی محدوده‌ی اعمال حق تعیین سرنوشت توسط ملت است. حق تعیین سرنوشت در اسناد مهم بین‌المللی جایگاه ویژه‌ای دارد از جمله در بند ۲ ماده ۱ منشور ملل متحد و به‌عنوان یکی از اهداف ملل متحد گنجانده شده است. هم‌چنین ماده ۱ مشترک میثاق بین‌المللی حقوق مدنی و سیاسی و هم‌چنین میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی، مقرر می‌دارد که همه‌ی مردم حق تعیین سرنوشت دارند. اکنون، «تعیین سرنوشت» یک اصل اساسی در حقوق بین‌الملل محسوب می‌شود. در این اصل بیان می‌شود که مردم حق دارند؛ دولت مستقل، حاکم و حکمرانان خویش را خود تعیین کنند و یک حکومت دموکراتیک داشته باشند (Cassese, 1995, p. 37)، درعین‌حال، دولت‌های دیگر متعهد می‌شوند از مداخله در امور داخلی دیگر دولت‌ها و اشغال سرزمین خارجی و در نتیجه محروم کردن مردم آن از حق تعیین سرنوشت خود، خودداری کنند.

یکی از ویژگی‌های بنیادین هر قانون اساسی، وجود اصلی است درباره حدود و ثغور و نحوه‌ی تغییر و دفاع از مرز یا قلمرو سرزمینی دولت - ملت که به نحوی مؤکد، ویژگی‌های عمومی آن تعیین می‌شود. قانون اساسی جمهوری اسلامی ایران هم متکی بر نگاه به درون بوده و هم اتکایی بر نگاه به بیرون داشته است، هم پایبند به مرز جغرافیایی بوده و هم به فراتر رفتن از مرزهای سیاسی به وسیله‌ی مقولات ایدئولوژیک اشاره داشته است (خلیلی، ۱۳۹۰، ص. ۷). با بررسی

مشروح مذاکرات خبرگان قانون اساسی می‌توان به این نتیجه دست یافت که خبرگان قانون اساسی، بیش از آنچه به علایق امت‌نگرانه و فرا وطن‌گرایانه (بی‌مرزی عقیدتی) روی آورده باشند، هوادار گرایش‌های مرتبط با کشورداری و مرز جغرافیایی بوده‌اند. از نظر آنان تا زمان دستیابی به دولت فراگیر و جهان‌گیر اسلامی، رابطه (مرزبانی) از مرزهای دولت تازه تأسیس جمهوری اسلامی، امری حقیقی، عینی و واجب به شمار رفته است (خلیلی، ۱۳۹۰، ص. ۴۱).

رویکرد قانون اساسی در موضوع مرز، بیانگر اهمیت و ضرورت پدیده‌ی مرز در حاکمیت است. حال، نکته اساسی این است که با گسترش گستره‌ی حاکمیت حکومت‌ها، از عرصه خاکی، آبی و هوایی سرزمین‌ها به عرصه فضای مجازی به‌عنوان چهارمین قلمرو اعمال حاکمیت حکومت‌ها، آیا ملزومات حاکمیت دولت - ملت‌ها، از جمله مرزها، نباید در عرصه فضای مجازی نیز محقق شود؟

۴. روش تحقیق

پژوهش حاضر به لحاظ ماهیت، بنیادین و از نظر روش در دسته‌ی تحقیقات توصیفی - تحلیلی قرار می‌گیرد و برای گردآوری اطلاعات مورد نیاز، از روش کتابخانه‌ای استفاده شده است. در پژوهش حاضر و با مطالعه‌ی منابع، اسناد و نظریات مختلف در ارتباط با مفهوم مرز در علوم سیاسی، حقوق عمومی و مفهوم مرز در فضای مجازی و حاکمیت سایبری، نظرات مختلف دسته‌بندی و تحلیل شده است و نظر مختار بیان شده است. در ادامه، تفاوت‌های مرزهای فیزیکی و مجازی تحلیل شده است و شیوه‌های مرزگذاری و الزامات حقوقی آن‌ها مورد بررسی قرار گرفته است.

۵. یافته‌های تحقیق

۵-۱. تعریف مرز در فضای مجازی

در این قسمت به این پرسش پاسخ داده می‌شود که مفهوم مرز در فضای مجازی چیست و چه تفاوت‌ها و شباهت‌هایی با مفهوم مرز در فضای حقیقی دارد؟ مرزها در فضای مجازی همانند فضای واقعی وجود دارند اما، ماهیت و تجلی آن‌ها

تفاوت می‌کند. کارکرد اصلی آن‌ها نیز همانند فضای واقعی، کنترل تعاملات، جریان و فرآیندهای فضای مجازی در قلمرو حاکمیت کشورها در فضای جغرافیایی هر کشور و انسان‌های مقیم در آن است (حافظ‌نیا، ۱۳۹۰، ص. ۱۱۰). در تعریف پدیده‌ی مرز در فضای مجازی، برخی دچار اشتباه شده و همان‌گونه که، فضای مجازی را به فناوری اطلاعات و ارتباطات تقلیل دادند، مرز در فضای مجازی را نیز در سطح فنی فناوری اطلاعات و ارتباطات تقلیل می‌دهند. به‌طور مثال فنگ بیان می‌کند: «مرزها از مجموعه‌ای از دستگاه‌های داخلی پورت شبکه‌ای دولت که مستقیماً به دستگاه‌های شبکه سایر کشورها متصل شده باشد، تشکیل می‌شوند» (Fang, 2018, p. 85). برای تعریف مفهوم مرز در فضای مجازی، می‌توان همان تعریف مرز در فضای فیزیکی را تعمیم داد، یعنی؛ مرز در فضای سایبری نیز «عامل تشخیص و جدایی یک واحد متشکل سیاسی یا کشور، از دیگر واحدها است»، اما در کارکردها، روش مرزگذاری، آثار و الزامات آن می‌تواند، بسیار متفاوت باشد.

مرز در فضای مجازی، ویژگی‌های خاصی دارد که با مرزها در فضای واقعی، تفاوت‌ها و شباهت‌هایی دارد:

- مرزهای واقعی ماهیت فیزیکی دارد، اما مرزهای مجازی ماهیت غیر فیزیکی و دیجیتال دارد،
- مرزها در فضای مجازی هویت، قلمرو و مرزهای حاکمیت کشورها در فضای واقعی را منعکس می‌کند،
- در مرزهای واقعی، همواره دو طرف مجاور وجود دارد اما در مرزهای سایبری یک‌طرف با تمام دولت‌ها، نهادهای غیردولتی و حتی اشخاص هم‌مرز می‌شود،
- شروش‌های مرزگذاری در مرزهای سایبری با مرزهای واقعی متفاوت است،
- روش مرزبانی در دو نوع مرز متفاوت خواهد بود،
- نهادهای مرزبان در دو نوع مرز می‌تواند متفاوت باشد، البته در هر دو مرز ضرورت دارد که هم نهادهای نظامی و انتظامی و هم، نهادهای فنی و تخصصی به مرزبانی کمک کنند،

- مرزهای فیزیکی متکثر و با یکدیگر متفاوت هستند و هر مرزی از اهمیت متفاوتی برخوردار است، اما مرزهای سایبری یکسان‌تر و یکپارچه‌تر از مرزهای فیزیکی به نظر می‌رسد و

- امروزه اهمیت مرزهای سایبری، بسیار بیشتر از مرزهای فیزیکی است. چراکه حجم تهدیدات در مرزهای سایبری بسیار بیشتر از تهدیدات در مرزهای فیزیکی است. به‌طور مثال اگر تهدیدی مثل گروه‌های تروریستی در مرزهای فیزیکی وجود داشته باشد، تنها مرزنشینان مورد تهدید واقع می‌شوند، اما در مورد فضای مجازی اگر تهدیدی از مرزهای سایبری ملی عبور کند، هم‌زمان کل کشور تهدید می‌شود.

یکی از مهم‌ترین عواملی که اعتبار مرزهای در فضای مجازی را ضروری می‌نماید، بحث هویت‌یابی و هویت‌سازی ملت‌هاست. با توجه به این‌که، یکی از نیازهای اساسی بشری هویت است، انسان‌ها در هر قالبی از قوم، اقلیت، ملت، گروه‌های دینی، مذهبی و ... از ابعاد هویتی خود در برابر فرآیندهای همگون‌سازی جهانی شدن دفاع خواهند کرد و بیش از گذشته به واپایش مرزهای محلی، ناحیه‌ای و ملی خواهند پرداخت (عبادی نژاد، نصرتی، & مستجابی، ۱۳۹۲، ص. ۵۹). بنابراین، یکی از عوامل ضرورت و ایجاد مرزها در فضای مجازی، مانند مرزها در فضای واقعی، کارکرد هویت‌یابی و هویت‌سازی است که به نظر می‌رسد این نیاز بشر در فضای مجازی نیز نمود پیدا خواهد کرد و شاهد مرزبندی‌های بیشتری در فضای مجازی خواهیم بود.

۵-۲. مبانی ضرورت مرزگذاری در فضای مجازی

این بخش در پاسخ به این سؤال ارائه شده است که ضرورت مرزگذاری در فضای مجازی چیست؟ و آیا اساساً، مداخله دولت‌ها در فضای مجازی ضرورت دارد؟ رویکردهای مختلفی پیرامون امکان‌سنجی پدیده‌ی مرز در فضای مجازی مطرح شده است، اما ریشه امکان‌سنجی مرز سایبری به مسئله کلان‌تری برمی‌گردد که همان به رسمیت شناختن حاکمیت ملی در عرصه فضای مجازی است. در یک دسته‌بندی کلی، اندیشمندان در رابطه با حاکمیت سایبری در دو دسته

قرار می‌گیرند:

الف- معتقدین به جهانی‌سازی^۱ یا لیبرال‌ها که اعتقاد به عدم‌مداخله دولت‌ها در عرصه فضای مجازی دارند.

ب- رئالیست‌ها که مخالف جهانی‌سازی و معتقد به ضرورت حاکمیت ملی سایبری هستند.

برای بررسی مهم‌ترین دلایل هر گروه از روش تحلیل نگاشت احتجاجات طرفین استفاده می‌شود:

مفهوم جهانی‌شدن در میان محققان برداشت یکسانی ندارد. این ابهام نیز به دلیل چندوجهی بودن پدیده یا فرایند جهانی‌شدن است (گل محمدی، ۱۳۸۳، ص. ۱۸). معتقدین به جهانی‌سازی بر این باورند که با توسعه و تحولات فناوری اطلاعات و ارتباطات، مرزها به‌عنوان نماد قدرت حکومت‌ها، با چالشی جدی مواجه شده‌اند (Kearney, 2004, p. 35). برخی معتقدند مرزهای جغرافیایی تا حدود زیادی بی‌معنا شده‌اند (Stanbury & Vertinsky, 1994, p. 87). برخی گفته‌اند؛ انقلاب ارتباطات و اطلاع‌رسانی به زوال و مرگ فاصله منجر می‌شود و پیامد آن جهان بدون مرز است (Cairncross, 1997, p. 23). تا جایی که مارشال مک لوهان^۲ از دهکده جهانی سخن به میان آورد و بارلو^۳ اعلامیه‌ی «استقلال فضای مجازی» را تنظیم کرد تا مانع از مداخله‌ی دولت‌ها در فضای مجازی شود. بارلو فضای مجازی را فضایی خودتنظیم، معرفی نمود که نیازی به تنظیم‌گری حکومت‌ها ندارد (Ziolkowski, 2013, p. 193). در عصر جهانی‌شدن، نقش دولت‌ها از حالت دستورده و ناظر خارج می‌شود. فضای مجازی، هیچ سرزمینی ندارد و هیچ اقتدار واحدی بر آن حاکم نیست (صدوقی، ۱۳۸۶، ص. ۴۷). امروز تفکر جدیدی نسبت به مرزهای مجازی به وجود آمده است که فضای مجازی را فضایی بین‌المللی، مانند دریای آزاد، قطب جنوب و فضای ماورای جو تلقی می‌کند (جان‌پرور، ۱۳۸۷، ص. ۹۸). همان‌گونه که در این سه فضا هیچ حاکمیتی

1. Globalization

2. Marshall McLuhan

3. John Perry Barlow

وجود ندارد و صلاحیت حکومت‌ها در آن‌ها بر اساس ملاحظه‌های دیگری مانند تابعیت تعیین می‌شود، در فضای مجازی نیز صلاحیت حکومت‌ها بر مبنای سرزمین تعیین نمی‌شود.

برخلاف رویکرد اول متناسب به جهان‌گرایان، اگرچه فرایندها در این فضا غیردولتی و فرا سرزمینی است، ولی رویکردها و پاسخ‌ها اکثراً دولتی، سرزمینی و مبتنی بر مرزهاست که در تقابل با جریان‌های مورد نظر ایجاد می‌شود و مؤلفه‌ی امنیت نیز موجب تلاش برای مرزسازی‌های مجدد می‌گردد (حیدری فر، ۱۳۸۹، ص. ۸۹). با توسعه‌ی اینترنت، شبکه به دنیای واقعی متصل و واقعیت حقوقی، داخل فضای مجازی شده است و پدیده‌هایی مانند «جرائم مجازی» و «تروریسم مجازی» به وجود آمد. جنبه‌های مختلفی از مسائل تجاری و مالی مانند قوانین مالیاتی، حقوق مالکیت معنوی، تجارت الکترونیک و ...، حکومت‌ها را واداشته تا نسبت به تنظیم حقوق در عرصه فضای مجازی چاره‌اندیشی کنند (Thornton, 1997, p. 8). از طرفی پیشرفت تکنولوژی منجر به تقویت مرزها نیز شده است، مانند ماهواره‌ها و تکنولوژی‌های احراز هویت بیومتریک و ... که برای کنترل و مدیریت مرزها مورد استفاده قرار گرفته، به شکلی که امروزه مرزهای هوشمند مطرح شده‌اند.

فضای مجازی از هر حیث بر فضای واقعی تکیه دارد، بنابراین با توجه به اصالت فضای واقعی و به‌ویژه، نقش فعال انسان نسبت به فضای مجازی و اینکه مؤلفه‌های قلمرو و مرز از خصلت‌های ذاتی زندگی جمعی انسان‌ها است که در رفتار سیاسی آن‌ها تبلور می‌یابد، تصور نابودی و زدایش مفاهیم و مؤلفه‌های قلمرو، مرز و حکومت از فضای مجازی، ممکن نیست. بر پایه‌ی این استدلال، مؤلفه‌ها و مفاهیم قلمرو، مرز و حکومت، ابدی و انکارناپذیر بوده و با تحولات فناوری از قبیل فضای مجازی و فناوری‌های اطلاعاتی و ارتباطی و تجلی‌های دیجیتالی آن از بین نمی‌رود. ولی موقعیت، کارکرد، تعامل و ماهیت آن‌ها دچار تحول می‌شود (حافظ‌نیا، ۱۳۹۰، ص. ۹۹).

از طرفی حق تعیین سرنوشت، که ایجاب می‌کند مردم هر کشور بر سرنوشت

سیاسی خود حاکم باشند، در عرصه سایبری نیز حاکم است. به همین جهت، اعمال حاکمیت بر اساس اراده ملت‌ها در عرصه سایبری مستلزم وجود حکومت و مرزهای سیاسی است تا محدوده این صلاحیت را مشخص نماید.

بر اساس قاعده‌ی اول از دستورالعمل تالین^۱ در مورد حقوق بین‌الملل قابل اعمال در جنگ سایبری «یک دولت می‌تواند بر زیرساخت‌ها و فعالیت‌های سایبری در سرزمین تحت حاکمیتش اعمال کنترل کند» (Schmitt, 2013, p. 25). این قاعده، حاکی از آن است که هرچند هیچ دولتی نمی‌تواند ادعای حاکمیت بر تمام فضای مجازی را نماید، با وجود این، می‌تواند بر هرگونه زیرساخت سایبری و فعالیت‌های سایبری در سرزمین خود، اعمال حاکمیت کند. در واقع، برخورداری از حاکمیت دلالت بر آن دارد که یک دولت می‌تواند دسترسی به سرزمینش و استفاده از آن را، از جمله دسترسی به زیرساخت‌های سایبری و استفاده از آن را از حیث حقوقی و عملی - به لحاظ برخورداری از قدرت انحصاری تصمیم‌گیری در خصوص اقدامات تقنینی، اجرایی و قضایی - کنترل کند، چراکه دولت به‌طور کلی، در حدود معین‌شده به موجب معاهدات و حقوق بین‌الملل عرفی از حق انحصاری اعمال صلاحیت و قدرت در سرزمینش برخوردار است (Tuukkanen, 2018, p. 38). در نتیجه، دولت‌ها دو قلمرو حاکمیتی دارند؛ فضای جغرافیایی واقعی و فضای جغرافیایی مجازی که هر دو مرتبط و وابسته به یکدیگرند و فضای مجازی در واقع انعکاس مجازی فضای واقعی است. بنابراین، اصل حاکمیت حکومت ملی بر هر دو فضا از پایداری برخوردار است، هرچند ممکن است کیفیت و سطح آن بین دولت‌ها متفاوت باشد (حافظ‌نیا، ۱۳۹۰، ص. ۱۵۶).

در نهایت، دولت‌ها به این نتیجه رسیدند که تنها دو راه پیش رو دارند، یا حاکمیت سایبری را در قلمرو مرزهای فضای مجازی خودشان به رسمیت بشناسند و از ایده‌های جهان بدون مرز و جامعه باز، صرف‌نظر کنند و یا اینکه در برابر جهانی‌شدن موضعی انفعالی بپذیرند و سرنوشت کشور خود در عرصه‌های مختلف را به دست کشورهای هژمون بسپارند. همین امر، سبب ایجاد ایده‌هایی

1. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

مانند اینترنت چینی و اینترنت اروپایی و تقویت شبکه ملی اطلاعات در کشورهای مختلف شده است. همان ضرورت‌هایی که ایجاب می‌کند دولت در فضای حقیقی وجود داشته باشد و اعمال حاکمیت کند، همان ضرورت‌ها هم ایجاب می‌کند دولت و حاکمیت در فضای مجازی وجود داشته باشد. با پذیرش ضرورت حاکمیت سایبری ملی در عرصه‌ی فضای مجازی، طبیعتاً ضرورت وجود مرزهای سایبری هم اثبات می‌شود.

۵-۳. شیوه‌های مرزگذاری در فضای مجازی

در این قسمت، پاسخ روش‌های مرزگذاری در فضای مجازی چیست، تبیین می‌شود. با توجه به نوین بودن عرصه‌ی فضای مجازی دولت - ملت‌ها هنوز به شیوه‌های منسجم و ثابتی از مرزگذاری در فضای مجازی نرسیده‌اند، اما با ملاحظه‌ی تجربه‌ی انباشته کنونی، می‌توان روش‌های مرزگذاری در فضای مجازی را به دودسته کلی تقسیم نمود. یک دسته از روش‌ها مرزگذاری در فناوری ارتباطات و یک دسته از روش‌ها، مرزگذاری در فناوری اطلاعات است. هرکدام از شیوه‌ها ممکن است هم در فناوری اطلاعات و هم در فناوری ارتباطات استفاده شود، اما بنا بر غلبه در هر دسته، جزء آن دسته محسوب می‌شود. همچنین مرزگذاری فنی از مرزگذاری اقتصادی و فرهنگی جدا نیست و هر شیوه مرزگذاری می‌تواند، اثرات اقتصادی و فرهنگی نیز به همراه داشته باشد، پس در تجویز شیوه‌های مرزگذاری در فضای مجازی باید به پیوست فرهنگی و اقتصادی هر روش توجه نمود.

- شیوه‌های مرزگذاری در فناوری ارتباطات: کنترل سیستم مسیریابی^۱ و نام دامنه^۲، کنترل دروازه‌های مرزی^۳ اینترنت و پروتکل‌های مرزی^۴، کنترل ترافیک داده‌های خارجی و داخلی، کنترل پهنای باند، فیلترینگ، ایجاد دیواره آتش^۵ ملی،

1. Routing
2. Domain Name System
3. Gateway
4. BGP or Border Gateway Protocol
5. Firewall

استفاده از شیوه‌های کاوش فعال^۱، ذخیره‌سازی داده‌ها در سرورهای ملی، ایجاد شبکه‌ی ملی اطلاعات و کنترل کاربران از طریق نقطه اتصال به شبکه، توسط ارائه‌دهندگان خدمات اینترنت^۲.

- شیوه‌های مرزگذاری در فناوری اطلاعات: فیلترینگ محتوا، احراز هویت^۳

کاربران، مرزگذاری در پلتفرم‌ها، ایجاد قواعد مرزگذاری محتوایی، ابزارهای امنیت اطلاعات، مرزگذاری با قواعد حریم خصوصی و حفاظت از داده‌ها.

هر یک از شیوه‌های مذکور، توضیحات مبسوط و ملاحظات حقوقی، اقتصادی و فرهنگی خاص خود را داشته و هر شیوه، مزایا و معایب خاص خود را دارد که هر دولتی متناسب با سیاست‌های کلان خود می‌تواند از روش‌های مطلوب استفاده کند تا آسیب‌های موجود در این عرصه را به حداقل برساند.

ساده‌ترین روش برای مشخص کردن مرز سایبری، تعمیم روش مرزگذاری سرزمینی در فضای حقیقی به فضای مجازی است. مکانی که کابل‌های انتقال داده از مرزهای ملی فیزیکی عبور می‌کنند، می‌تواند به‌عنوان یک گذرگاه مرزی سایبری شناخته شود. البته، این قیاس دچار نقص است زیرا همه‌ی داده‌ها از طریق کابل‌های مرزی اینترنت منتقل نمی‌شود و داده‌ها می‌توانند از طریق روش‌های دیگری به‌عنوان مثال از طریق ماهواره تبادل شوند که برای روش‌های دیگر انتقال داده، باید مرزهای دیگری تعبیه کرد. بنابراین، مرز سایبری می‌تواند به‌عنوان نظیر FEB^(۳) در فضای واقعی که در آن داده‌ها در اولین نقطه‌ی ممکن از لحاظ عملی، تحت بازرسی قرار می‌گیرند تعریف شوند، مانند یک روتر شبکه، سرور رایانه، رایانه شخصی یا سایر دستگاه‌های شبکه (Osborn, 2017, p. 6).

یکی از مفاهیمی که در فضای مجازی با مفهوم قلمرو در فضای واقعی انطباق می‌یابد، مفهوم نام دامنه (Domain) است. نام دامنه، نامی است که از سوی سازمان پشتیبانی نام‌های دامنه که وابسته به آی‌کان^(۴) است، به سایت‌ها اختصاص داده می‌شود. نام دامنه از ارقام و حروفی تشکیل شده که سه مؤلفه‌ی اصلی آن عبارت است از زیر

1. Active Probing
2. Internet service providers (ISP)
3. Authentication

دامنه، نام دامنه و کارساز (که در دودسته «نام‌های سطح اول عام» که فاقد ماهیت جغرافیایی هستند مانند .net، .org، .com و ... و «نام‌های سطح اول کشوری» که از هویت جغرافیایی برخوردار است مانند .uk، .ir و ... است. نظام نام‌گذاری برای بازیگران، میزبانان و کاربران در فضای مجازی بیانگر فرایند قلمروسازی و حریم دیجیتال برای فعالیت‌ها و نقش‌های ایفا شده در فضای مجازی است که در مورد نام‌های جغرافیایی در واقع، مبتنی بر قلمروهای سرزمینی حکومت‌ها و سازمان‌های منطقه‌ای در فضای واقعی است (حافظ‌نیا، ۱۳۹۰، ص. ۱۰۱).

احراز هویت کاربران فضای مجازی نیز می‌تواند به‌عنوان یکی از مهم‌ترین قواعد مرزگذاری در این فضا عمل کند. کارکرد احراز هویت در فضای مجازی، متناظر با کارکرد گذرنامه و اجازه ورود در فضای واقعی است. به‌طور مثال؛ در پی مقررات گذاری اخیر مجلس ترکیه، پیام‌رسان‌های اجتماعی باید در ترکیه دفتر نمایندگی تأسیس کنند و هم‌چنین موظف‌اند برای ایجاد حساب کاربری برای اشخاص، آن‌ها را از طریق کد ملی احراز هویت کنند^(۵).

برخی کشورها، قوانینی را وضع کرده‌اند که داده‌های شهروندان باید درون مرزهای ملی آن کشورها باقی بماند که به آن محلی‌سازی داده‌ها یا ملی‌گرایی داده، گفته می‌شود (حسنی، ۱۳۹۸، ص. ۹). بر اساس قانون محلی‌سازی داده در روسیه که به‌طور رسمی قانون فدرال شماره 242-FZ نام دارد، همه شرکت‌های داخلی و خارجی ملزم شدند تا اطلاعات شخصی شهروندان روسیه را روی سرورهایی ذخیره‌سازی و پردازش کنند که به‌طور فیزیکی درون مرزهای روسیه قرار گرفته‌اند (حسنی، ۱۳۹۸، ص. ۱۴). قانون امنیت سایبری مصوب ۲۰۱۷ در چین نیز محدودیت‌های مهمی برای ذخیره‌سازی اطلاعات مرتبط با کاربران چینی در سرورهای محلی وضع نموده است^(۶).

پدیده‌ی مرز در فضای مجازی الزامات گسترده‌ای، در ابعاد مختلف دارد که باید مورد توجه دولت‌ها قرار بگیرد. به‌طور کلی می‌توان این الزامات را در ابعاد مختلف به‌صورت زیر دسته‌بندی کرد:

- در بعد اقتصادی: الزامات تجارت الکترونیک داخلی و بین‌المللی، گمرک

سایبری، مالیات و عوارض ورود و خروج داده‌ها.

- در بعد فرهنگی - اجتماعی: الزامات مهاجرت سایبری، مبادلات فرهنگی در فضای مجازی، تهاجم فرهنگی، تبلیغات در فضای مجازی.

- در بعد سیاسی - حکمرانی: الزامات شیوه‌ی جدید حکمرانی اینترنت با توجه به رسمیت شناختن حاکمیت‌های ملی در این عرصه، بازتوزیع قدرت میان حاکمیت و بازیگران.

- در بعد امنیتی - نظامی: الزامات دفاع سایبری، مرزبانی سایبری، پدافند سایبری، حملات سایبری^(۷)، تروریسم سایبری، جنگ سایبری^(۸).

- در بعد حقوقی: الزامات تابعیت مجازی، حقوق بشر و شهروندی در فضای مجازی، جرائم مختلف سایبری مرتبط با مرزها مثل قاچاق، جاسوسی، ورود یا خروج غیرقانونی، معاهدات مرزی سایبری.

ایجاد مرزهای سایبری، الزامات حقوقی متفاوتی خواهد داشت. در مرحله‌ی اول، توجه به نهادهای وابسته به مرز و بازتعریف آنها، مطابق با مقتضیات جدید و ایجاد صلاحیت قانونی برای آنها توسط اصلاح قوانین موجود است مانند گمرک، مرزبانی نظامی، مناطق مرزی، گذرنامه و روادید، احراز هویت، مالیات و عوارض، صادرات و واردات و نهادهای مرتبط دیگر. در مرحله بعد تصویب قانونی جامع، با توجه به سیاست‌های کلان کشور در حوزه حاکمیت سایبری، برای تثبیت نهاد مرز و تعیین سازوکارها و نهادهای مرزبانی. در سال ۱۳۹۷ و هم‌چنین سال ۱۴۰۰، پیش‌نویس طرح‌هایی در خصوص ساماندهی فضای مجازی در مجلس مطرح شده است که در هر یک، ماده‌ای به مرزبانی سایبری اختصاص یافته است و بصورت خیلی کلی و مبهم، مرزبانی دیجیتال را بر عهده‌ی ستاد کل نیروهای مسلح قرار داده است^(۹). فارغ از تحلیل این ماده از پیش‌نویس، به نظر می‌رسد تعیین تکلیف برای موضوعی مهم در سطح ملی با جزئیات مختلف، در یک ماده، در شأن این موضوع نیست.

مرزگذاری در فضای مجازی در بُعد حقوق بین‌الملل هم الزاماتی به همراه دارد. یک راه‌حل برای مسئله‌ی تهدیدهای سایبری خارجی، تکامل مفهوم مرز

سایبری است. پس از تعریف مفهوم مرز سایبر، دولت می‌تواند از قوانین و مقامات سنتی برای محافظت بهتر ملت در برابر تهدیدهای سایبر خارجی و فعلی استفاده کند (Osborn, 2017, p. 3). اصل حاکمیت ارضی در فضای مجازی نیز اعمال می‌شود و از زیرساخت‌های سایبر واقع در قلمرو یک کشور محافظت می‌کند. کشورها از دخالت در ساخت‌وسازهای سایبری واقع در خاک یک کشور دیگر ممنوع هستند (Czosseck, 2018, p. 3).

۵-۴. امکان‌سنجی فنی تحقق مرز در فضای مجازی

در این بخش، پاسخ سؤال رویکرد کشورهای مختلف از جمله چین و ایران در قبال مرز سایبری چه بوده است، مورد بررسی قرار می‌گیرد. در فرض صحت رویکرد جهان‌گرایان، بحث از امکان‌سنجی مرز در فضای مجازی بی‌معناست، چراکه حاکمیتی در فضای مجازی وجود ندارد که مرزها را محقق کند. اما، نظر به رویکرد قائلین به حاکمیت سایبری، دو رویکرد مخالف و موافق امکان تحقق مرز سایبری وجود دارد. مخالفین امکان تحقق مرز سایبری، دلایل و توجیحات متفاوتی بیان می‌کنند. از جمله این‌که هرچند بپذیریم مرز سایبری ضرورت دارد، اما به‌طور فنی اصلاً امکان مرزگذاری فیزیکی در فضای مجازی، مانند مرزهای کشورها قابل تصور نیست. فناوری‌ها تمرکزگریز، کنترل‌گریز یا فیلترگریز هستند و فناوری‌های جدید مانند بلاک‌چین این امر را مشهود کرده است، از طرفی امکان نفوذ و گذر از مرزهای سایبری به‌راحتی ممکن است و شبکه‌های مخفی یا خصوصی مجازی (VPN) یا پروکسی‌ها (Proxy) این امر را تسهیل کرده‌اند. ایجاد مرزهای سایبری بسیار هزینه‌بر و کم بازده است. مرزگذاری در اینترنت، خلاف اصل جریان آزاد اطلاعات حقوق بشر و شهروندی و آزادی‌های اساسی است.

اما قائلین به امکان تحقق مرز سایبری از روش مثال نقض ادعای مخالفین را رد می‌کنند. سیر تاریخی دو دهه‌ی اخیر کشورهایایی مثل چین، کره جنوبی، روسیه و حتی کشورهای اروپایی در بحث شبکه‌ی ملی اطلاعات و فیلترینگ بیانگر این است که برای این کشورها، مسئله‌ی مهم در مواجهه با فضای مجازی، حفظ حاکمیت، اقتدار دولت در فضای مجازی، استقلال این فضا از اعمال نفوذ سایر

کشورها و همچنین ایجاد نهادهای بین‌المللی ذیل سازمان ملل برای حکمرانی جهانی فضای مجازی در سطح بین‌المللی بوده است و رویکرد امنیتی در مدیریت کلان فضای مجازی در این کشورها اهمیت ویژه‌ای دارد.

در چهارمین اجلاس بین‌المللی مخاصمات سایبری در سال ۲۰۱۲، کایر گیلز^۱ از مرکز تحقیقات مطالعات مخاصمات، در مقاله «موضع عمومی روسیه در مورد فضای مجازی» تحلیل زیر را ارائه داد: «روسیه به همراه تعدادی از ملل متفکر (به‌عنوان مثال اعضای CIS، CSTO و SCO)، از ایده‌ی کنترل ملی کلیه منابع اینترنتی که در مرزهای فیزیکی یک کشور قرار دارد، حمایت می‌کند و ... هر کشور عضو حق دارد هنجارهای حاکمیتی را تنظیم کند و فضای اطلاعات خود را مطابق قوانین ملی خود مدیریت کند» (Giles, 2012, p. 65).

۵-۵. تجربه چینی

برای چین، بسیار مطلوب است که مرزهای خود را در فضای مجازی تحکیم کند و در این زمینه اراده‌ی جدی وجود دارد. علاوه بر این، چین در این موضع تنها نیست. الگوی چینی کنترل اطلاعات اجتماعی و ترجیحات گسترده‌تر تجارت، شیوه نئوکپی‌تالیستی^۲ آن‌ها طنین قدرتمندی در بقیه دولت‌های غیر غربی دارد (Demchak, 2018, p. 56).

اداره‌ی فضای مجازی چین (CAC) با مأموریت روشن ساختن حدّ و مرز ساختارهای کنترل اینترنت در چین در سال ۲۰۱۳ تأسیس شد. این اداره کل، بازوی اجرایی شورای عالی امنیت اینترنت و توسعه‌ی جامعه اطلاعاتی چین است. در جامعه بین‌المللی، CAC همواره یکی از حامیان مفهوم حاکمیت سایبر است. با توجه به این مفهوم، هر کشوری حق دارد که پیش‌نویس قوانین اینترنتی خود را تهیه و اجرا نماید (رضاپور، ۱۳۹۸، ص. ۴).

کشور چین در فاصله‌ی سال‌های ۱۹۹۸ تا ۲۰۰۸، پروژه‌ای تحت عنوان «سپر طلایی» اجرا نموده است. بازه‌ی زمانی اجرای پروژه، حدود یک دهه است که

1. Keir Giles

2. Neo-Capitalistic

فاصله‌ی زمانی قابل توجهی محسوب شده و نشانگر اهمیت ملی پروژه است. تخمین زده می‌شود افراد فعال در این پروژه بین ۳۰ تا ۵۰ هزار نفر بوده‌اند. یکی از خروجی‌های این پروژه، فایروال بزرگ چین بوده که معادل سایبری دیوار بزرگ چین دانسته می‌شود. اجرای این پروژه را می‌توان برابر راه‌اندازی شبکه ملی اطلاعات در کشورمان دانست که البته بسیار زودتر آغاز شده و بالطبع زودتر نیز خاتمه یافته و به بهره‌برداری رسیده است. از دیگر اقدامات کنترلی صورت گرفته توسط چین، می‌توان به کنترل اطلاعات از مبدأ اشاره نمود. بر این اساس، حکومت چین صاحبان سکویهای خارجی را مجبور به اطاعت از خواسته‌های خود کرده که در غیر این صورت، آن سکوی فیلتر خواهد شد. برای مثال، در یک مقطع زمانی، دولت چین، شرکت گوگل را مجبور به نمایش روایتی منحصر به فرد برای کاربران چینی در موضوعی خاص کرده بود. با توجه به توانمندی سپر طلایی چین در بحث فیلترینگ، کمتر سکویی به مخالفت با خواسته‌های حکومت چین تمایل داشته است (رضاپور، ۱۳۹۸، ص. ۹). این قواعد و اقدامات تماماً از جنس قواعد مرزی است.

از طرفی، ایجاد مرز در فضای مجازی هرچند هزینه‌بر است، اما ضروری و مفید است. همان‌طور که ایجاد موانع و استحکامات مرزی و مرزبانی از مرزها در فضای واقعی ممکن است هزینه‌گزافی بر عهده دولت‌ها قرار دهد، اما هیچ دولتی از ضرورت آن غافل نیست. در شبهه‌ی امکان نفوذ در مرزهای سایبری و فیلترگریزی فناوری، مانند فناوری بلاک چین، باید دقت نمود که ادعای کارآمدی صد درصد مرزهای سایبری اشتباه است، همان‌طور که در مرزهای فیزیکی نیز نفوذ صورت می‌گیرد، ممکن است در مرزهای سایبری نیز نفوذ صورت پذیرد. از طرفی در کنار پیشرفت فناوری‌های فیلترگریز، شاهد پیشرفت فناوری‌های اعمال کنترل و فیلتر هستیم و هر دو نوع فناوری، پایه‌ی یکدیگر در حال رشد و توسعه هستند. بنابراین، دیدگاه صحیح این است که هرچند فناوری‌های فیلترگریز در حال توسعه هستند اما فناوری‌های فیلتر یا کنترل‌کننده نیز در حال توسعه است.

۵-۶. رویکرد ایرانی

دغدغه‌ی ایجاد شبکه ملی اطلاعات در دولت نهم، از سال ۱۳۸۴ ایجاد شد^(۱۰) و

تاکنون مهم‌ترین اولویت در طرح‌های راهبردی فضای مجازی کشور را به خود اختصاص داده است. اصطلاح شبکه‌ی ملی اطلاعات، متضمن سه کلیدواژه است که به معنای تمامی شبکه‌های عمومی در سطح ملی و سرزمینی است که خصیصه اطلاعاتی داشته باشند^(۱۱). به عبارت دیگر شبکه‌ی ملی اطلاعات، شبکه‌ی تمام شبکه‌های ملی اطلاعاتی کشور است.

از زمان شکل‌گیری دغدغه‌ی شبکه ملی اطلاعات تاکنون، ابهامات گوناگونی در رابطه با چیستی و چگونگی تحقق آن وجود داشته که به مرور زمان برخی از این ابهامات برطرف شده است. در همین راستا، شورای عالی فضای مجازی در سه مصوبه به‌طور خاص به شبکه‌ی ملی اطلاعات پرداخته است: مصوبه‌ی جلسه‌ی پانزدهم با موضوع «تعریف و الزامات حاکم بر تحقق شبکه ملی اطلاعات» مورخ ۱۳۹۲/۱۰/۳۰، مصوبه جلسه سی و پنجم با موضوع «تبیین الزامات شبکه ملی اطلاعات» مورخ ۱۳۹۵/۹/۲۰ و مصوبه جلسه شصت و ششم با موضوع «طرح کلان و معماری شبکه ملی اطلاعات» مورخ ۱۳۹۹/۶/۲۵^(۱۲). این مصوبات به ترتیب تاریخی، شبکه‌ی ملی اطلاعات را به‌صورت جزئی‌تر و دقیق‌تری تبیین می‌کنند.

در سند تبیین الزامات شبکه‌ی ملی اطلاعات، سند پیشین و ابتدایی شبکه‌ی ملی اطلاعات تشریح شده است. در سند تبیین الزامات به صراحت به مرز سایبری اشاره و بیان شده است، یکی از اصول تحقق شبکه‌ی ملی اطلاعات این است که خدمت ارتباط داخل با شبکه‌های خارجی صرفاً از طریق گذرگاه‌های ایمن مرزی شبکه‌ی ملی اطلاعات که دارای درگاه‌های مشخص اتصال به خارج و اتصال با داخل هستند تأمین می‌شود. در این سند، در تعریف مرزهای شبکه ملی اطلاعات بیان شده است: «مرزهای شبکه ملی شامل مرزهای جغرافیایی بوده ولی عناصر خارج از مرزهای جغرافیایی که توانایی اعمال سیاست‌های حاکمیتی مثلاً از طریق مالکیت بر آن وجود دارد را نیز شامل می‌شود»^(۱۳).

مصوبه «طرح کلان و معماری شبکه ملی اطلاعات»^(۱۴) به جزئیات بیشتری پرداخته و وظایف و صلاحیت‌های نهادهای گوناگون را مشخص کرده است. در

این مصوبه، موضوعات مختلفی اعم از خدمات، ترافیک، محتوا، منابع زیرساختی، سیستم‌عامل‌ها، تلفن‌های همراه، تجهیزات شبکه و سامانه‌های امنیتی به دو بخش داخلی و خارجی تقسیم شده‌اند و برای هرکدام تکلیفی در نظر گرفته شده است. این دوگانه، بیانگر برجسته‌بودن مرز سایبری در شبکه‌ی ملی اطلاعات است.

در اهداف عملیاتی شبکه‌ی ملی اطلاعات، ذیل ماده ۲ به «تحقق کامل گذرگاه‌های ایمن مرزی» به‌طور مستقیم اشاره شده است. هم‌چنین، در بخش معماری فنی شبکه‌ی ملی اطلاعات در ماده ۳، بین اینترنت بین‌الملل و شبکه‌ی ملی اطلاعات، «گذرگاه‌های ایمن مرزی بین‌المللی» و «دروازه‌های مرزی بین‌المللی» تعبیه شده است که بیانگر امکان تحقق عملیاتی مرزی سایبری است. در ماده ۵ تحت عنوان اقدامات کلان و نگاهت نهادی که وظایف نهادهای مختلف در تحقق شبکه ملی اطلاعات را مشخص کرده است، در بند ۱۴، وزارت ارتباطات و فناوری اطلاعات را مکلف به ایجاد و توسعه دروازه‌های مرزی کرده است. از طرفی در بند ۴۱، تکلیف ارتقاء عملکرد گذرگاه‌های ایمن مرزی را بر عهده وزارت ارتباطات و فناوری اطلاعات، وزارت اطلاعات دانسته است، البته وظایف دیگری هم به‌طور غیرمستقیم به مرزهای سایبری اشاره می‌کند، به‌طور مثال بند ۴۴ اجرای طرح ساماندهی VPNها و فناوری‌های حاکمیت‌گریز را بر عهده وزارت ارتباطات و فناوری اطلاعات، وزارت اطلاعات و قوه قضائیه نهاده است.

بنابراین مرز سایبری در اسناد شبکه‌ی ملی اطلاعات، جایگاه خود را پیدا کرده است و باید در عمل نیز محقق شود. اما، توجه به این نکته ضروری است که تعیین و مشخص کردن مرزها در فضای مجازی یکی از الزامات تحقق استقلال در فضای مجازی است، اما مرزهای سایبری، تنها یک مؤلفه در تحقق استقلال است و مؤلفه‌های دیگر مانند تأمین تمام نیازهای اصلی در سه لایه زیرساخت، خدمات و محتوا در بعد داخلی نیز باید مورد توجه ویژه قرار گیرد. چراکه هرچند مرزهای سایبری پیشرفته‌ای ایجاد گردد، اما اگر درون مرزها، نیازهای کاربران و جامعه، تأمین نشود، به ناچار و برای تأمین نیازها، مرزها به رسمیت شناخته نخواهد شد.

جمع‌بندی و نتیجه‌گیری

مؤلفه‌ی اصلی پژوهش حاضر، بررسی مفهوم و امکان‌سنجی پدیده‌ی مرز در فضای مجازی و بررسی الزامات تعمیم پدیده‌ی مرز به فضای مجازی از جمله، بررسی شیوه‌های مرزگذاری و ضرورت این مرزگذاری است.

مرز، عامل جداساز قلمرو حاکمیتی دو نظام سیاسی و تعیین‌کننده قلمرو سرزمینی اعمال حاکمیت دولت - ملت‌ها و یکی از عوامل هویت‌بخش به ملت‌ها است. همچنین مرزها تعیین‌کننده‌ی محدوده‌ی اعمال حق تعیین سرنوشت، توسط ملت‌ها هستند. مرز سایبری تعریف مشابه با تعریف مرز در فضای فیزیکی دارد و به‌عنوان عامل تشخیص و جدایی یک واحد متشکل سیاسی یا کشور، از دیگر واحدها در فضای مجازی شناخته می‌شود. اما، روش‌های مرزگذاری آثار و الزامات آن بسیار متفاوت است و برخی کارکردهای متفاوت از مرزهای فیزیکی در پی دارد.

باوجود تهدیدهای بسیار در فضای مجازی در ابعاد مختلف حقوقی، سیاسی، اقتصادی، امنیتی و فرهنگی، لزوم مداخله‌ی دولت‌ها برای برقراری نظم عمومی و تضمین حقوق کاربران، امری ضروری به نظر می‌رسد. در عمل نیز دولت‌های مختلف، اثبات کردند که به مرور، اعمال حاکمیت خود را در فضای مجازی، تقویت و گسترش داده‌اند.

رصد سیر تاریخی دو دهه‌ی اخیر کشورهای مختلف ازجمله چین، کره جنوبی، روسیه و کشورهای اروپایی در مواجهه ملی با فضای مجازی، بیانگر اهمیت حفظ حاکمیت و اقتدار دولتی در فضای مجازی و استقلال این فضا از اعمال نفوذ سایر کشورها و همچنین ایجاد ساز و کار بین‌المللی حکمرانی اینترنت است. کشور چین با ایجاد ساختارهای مختلف و کارآمد و اجرا کردن پروژه‌ی «سپر طلایی» تا حد بسیار زیادی حاکمیت ملی خود را در فضای مجازی، تقویت کرده و از این طریق به مرزبانی در فضای مجازی می‌پردازد.

جمهوری اسلامی ایران نزدیک به ۱۵ سال است که تحقق شبکه‌ی ملی اطلاعات را مهم‌ترین اولویت خود در عرصه‌ی فضای مجازی قرار داده است. فارغ از ارزیابی عملکرد دولت در تحقق شبکه‌ی ملی اطلاعات، سه سند عمده در

طول این سال‌ها به تصویب شورای عالی فضای مجازی رسیده که هرکدام به نسبت قبل، شبکه‌ی ملی اطلاعات را شفاف‌تر و جزئی‌تر مشخص کرده‌اند. مرز سایبری به‌عنوان یکی از ارکان شبکه‌ی ملی اطلاعات پذیرفته شده و مرزبانی سایبری نیز به‌عنوان یکی از اصول شبکه‌ی ملی اطلاعات مطرح شده است. تاکنون مرز سایبری تنها در سطح سیاست‌گذاری و در شورای عالی فضای مجازی تبیین شده است، اما تحقق و عملیاتی شدن مرز سایبری، نیازمند تقنین و خط‌مشی‌گذاری سیاست‌های این حوزه است که تاکنون اقدامی در این سطح صورت نگرفته است. بنابراین پیشنهاد می‌شود در راستای سیاست‌های مصوب شورای عالی فضای مجازی، مجلس شورای اسلامی به تقنین در موضوع مرز سایبری پردازد و صلاحیت‌ها و تکالیف نهادهای ذی‌ربط را مشخص نماید. سپس نهادهای متولی دولتی به‌خصوص وزارت ارتباطات و فناوری اطلاعات در راستای تحقق سیاست‌ها و اجرای قوانین خط‌مشی‌های خود را تنظیم نمایند.



پی‌نوشت‌ها

۱. فضای مجازی در زبان فارسی معادل cyberspace بکار می‌رود.
۲. فرهنگ فارسی عمید، مدخل مرز
۳. جایی که هواپیما فرود می‌آید آنجا معادل عملکردی مرز یا FEB گفته می‌شود. واضح‌ترین مثال FEB می‌تواند به مناطق ورودی خارجی فرودگاه‌های بین‌المللی باشد که مهاجران و بازرسی‌های گمرکی از هواپیماها، مسافران و محموله‌ها به‌دوراز مرز فیزیکی واقعی با معادل کاربردی آن انجام می‌شوند. (Osborn, ۲۰۱۷: ۶)
۴. ICANN: شرکت اینترنتی برای نام‌ها و اعداد واگذار شده، نوعی گروه حاکمیتی چندذینفعی و سازمانی ناسودبر در آمریکا است. مسئولیت شرکت آیکان ایجاد هماهنگی‌هایی در نگهداری و عملکرد پایگاه‌های داده مرتبط با فضای نام و فضای عددی در اینترنت است.
5. <https://www.arabnews.com/node/1706136/middle-east>
6. <https://www.irna.ir/news/83768519>
۷. حملات سایبری، کنش‌های تعمدی برای جایگزینی، درهم‌گسیختن، فریفتن، منحنط کردن یا تخریب سیستم‌ها یا شبکه‌های کامپیوتری و یا اطلاعات و برنامه‌های این سیستم‌ها هستند (Lin, ۲۰۱۱, p. ۶۳)
۸. جنگ سایبری در لغت به معنای تهاجم بر عناصر سایبری است و اصطلاحاً به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستم‌های اطلاعاتی با هدف به مخاطره انداختن عناصر اطلاعاتی دشمن (اطلاعات، پروسه‌های مبتنی بر اطلاعات، سیستم‌های اطلاعاتی و شبکه‌های رایانه‌ای) در یک فضای سایبری است (زابلی زاده & وهاب پور، ۱۳۹۷، ص. ۶۱).
9. https://rc.majlis.ir/fa/legal_draft/show/1084959
10. <http://www.majazi.ir/index.php?module=cdk&func=loadmodule&sy>
11. <https://farsi.khamenei.ir/others-dialog?id=46436>
12. http://www.majazi.ir/web_directory/52731
13. <http://www.majazi.ir/circularinformation/80810>
14. <http://www.majazi.ir/circularinformation/80810>

منابع و ماخذ

- آزادی، جواد (۱۳۹۷)، امنیت سایبری یا امنیت فضای مجازی، تأملات رشد، (۱)، ۱۶۴ - ۱۶۸.
- بدیعی ازندهای، مرجان؛ احمدی فیروزجائی، میثم؛ انصاری زاده، سلمان (۱۳۹۲)، تبیین مفهوم مرز در فضای سیاسی - مجازی ایران، فصلنامه جغرافیا، ۳۶، ۲۹۱ - ۳۱۳.
- جان پرور، محسن (۱۳۸۷). بررسی تحول مفهوم مرز در دوران معاصر، پایان نامه کارشناسی ارشد. تهران: دانشگاه تربیت مدرس.
- حافظ‌نیا، محمدرضا (۱۳۹۰)، جغرافیای سیاسی فضای مجازی. تهران: سمت.
- حسینی، حسین (۱۳۹۸)، محلی سازی داده‌ها، تهران: پژوهشگاه مرکز ملی فضای مجازی.
- حیدری فر، محمدرئوف (۱۳۸۹)، بررسی انتقادی گفتمان جهان بدون مرز، فصلنامه ژئوپلیتیک، ۶(۲)، ۱۲۵ - ۱۵۲.
- خلیلی، محسن (۱۳۹۰)، مفهوم قلمرو در قانون اساسی جمهوری اسلامی ایران: مرز جغرافیایی، بی‌مرزی عقیدتی. راهبرد، ۵۸، ۷ - ۴۵.
- رحمتی راد، محمد حسین (۱۳۷۴)، مرزبانی، گذرنامه و اتباع بیگانه، تهران: معاونت آموزشی ناجا.
- رضاپور، محمدمهدی (۱۳۹۸)، حکمرانی فضای مجازی در کشور چین، تهران: پژوهشگاه مرکز ملی فضای مجازی.
- رنجکش، محمدجواد؛ کشاورز، حمیدرضا (۱۳۹۲)، ساختار - کارگزار: چارچوبی تئوریک برای فهم و ارزیابی پدیده مرز. فصلنامه نگرش‌های نو در جغرافیای انسانی، ۵(۴)، ۶۹ - ۸۷.
- زرقانی، سیدهادی (۱۳۸۶)، مقدمه‌ای بر شناخت مرزهای بین‌المللی، تهران: نیروی انتظامی جمهوری اسلامی ایران.
- سلطانی نژاد، احمد؛ اسلامی، محسن؛ و راستگو، محمدزمان (۱۳۹۵)، فناوری اطلاعات و ارتباطات پیشرفته و تحول مفهوم حاکمیت در روابط بین‌الملل، جستارهای سیاسی معاصر، ۱۷(۱)، ۸۵ - ۱۱۴.
- شیرزادی، رضا (۱۳۹۷)، سرزمین و مرز از دیدگاه ژئوپلیتیک، سیاست و حقوق بین‌الملل، علوم و فنون مرزی، ۹(۳)، ۹۱ - ۱۱۹.

- صدوقی، مرادعلی (۱۳۸۶)، *تکنولوژی اطلاعات و حاکمیت ملی*، تهران: دفتر مطالعات سیاسی و بین‌المللی وزارت امور خارجه.
- عبادی نژاد، سیدعلی؛ نصرتی، حمیدرضا؛ و مستجابی، حمید (۱۳۹۲)، تأثیر جهانی شدن بر مرز در فضای سایبر، *علوم و فنون مرزی*، ۵۳ - ۷۲.
- غمامی، سید محمدمهدی (۱۳۹۰)، *حقوق اساسی جمهوری اسلامی ایران*، تهران: مرکز اسناد انقلاب اسلامی.
- قاضی، سید ابوالفضل (۱۳۹۳)، *بایسته‌های حقوق اساسی*، تهران: سمت.
- کبیری، ملیحه؛ جان‌پرور، محسن؛ زرقانی، سید هادی (۱۳۹۶)، تبیین و سطح بندی عوامل مؤثر بر اهمیت مرزها؛ با تاکید بر مرزهای خشکی، *پژوهش نامه ایرانی سیاست بین‌الملل*، ۵(۲)، ۹۳ - ۱۱۷.
- گل محمدی، احمد (۱۳۸۳)، *جهانی شدن و فرهنگ و هویت*، تهران: نشر نی.
- مجتهدزاده، پیروز (۱۳۸۱)، *جغرافیای سیاسی و سیاست جغرافیایی*، تهران: سمت.
- میرحیدر، دره (۱۳۸۵)، *مبانی جغرافیای سیاسی*، تهران: سمت.
- Cairncross, Francis (1997). *The death of distance: How the communications revolution will change our lives?* Harvard: Harvard school press.
- Cassese, Antonio (1995). *Self-determination of peoples: a legal reappraisal*. Cambridge: Cambridge University Press.
- Czosseck, Christian; Geers, Kenneth (2018). *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?* In F. Hare, *The Virtual Battlefield: Perspectives on Cyber Warfare* (pp. 49 - 74). Amsterdam: IOS press BV.
- Demchak, Chris. C. (2018). *Uncivil and Post-western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age*. *The Cyber Defense Review*, 49 - 74.
- Fang, Bixing (2018). *Cyberspace Sovereignty; Reflections on Building a Community of Common Future in Cyberspace*. Beijing: Springer Singapore.
- Giles, Keir (2012). *Russia's public stance on cyberspace issues*, 4th international conference on cyber conflict. Tallinn: NATO CCD COE publication.
- Godvin III, James; Kulpin, Andrey; Rauscher, Karl. Fredrick; Yaschenko, Valery (2014). *The Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2*. New York: EastWest Institute and the Information Security Institute of Moscow State University.
- Karmer, Franklin (2009). *Cyberpower and national security*. Washington

- D.C.: Center for Technology and National Security Policy.
- Kearney, Michael (2004). The classifying and valuefiltering missions of borders. *Anthropological Theory*, 4(2).
- Lin, Herbert (2011). Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion. *Journal of International Affairs*, 127 - 135.
- Mayer, Marco (2014). How would you define Cyberspace? *First Draft Pisa*.
- Osborn, Phillipe (2017). Cyber Border Security – Defining and Defending a National Cyber Border. *Homeland Security Affairs*.
- Oxford Online Dictionary (2020, 11 4). Retrieved from lexico: <https://www.lexico.com/definition/cyberspace>
- Racicot, Michael; Hayes, Mark S; Szibbo, Alec R; Trudel, Pierre (1998). The cyberspace is not a ‘no law land’ a study of the issues of liability for content circulating on the internet. *Computer Law & Security Review*, 14(2), 96-106.
- Schmitt, Michael N (2013). Tallinn manual on the international law applicable to cyber warfare .Cambridge: Cambridge University Press.
- Stanbury, William Thomas; Vertinsky, Ilan. B. (1994). Information technologies and transnational interest groups: The challenge for diplomacy. *Canadian Foreign Policy Journal*, 2(3), 87 - 99.
- Thornton, Sean M (1997). State Criminal Laws in Cyberspace: Reconciling Freedom for Users with Effective Law Enforcement. *Richmond Journal of Law & Technology*, 4(2), 5.
- Tuukkanen, Topi (2018). Sovereignty in the cyber domain. *The Fog of Cyber Defence*, 37 - 45.
- Ziolkowski, Katharina (2013). *Peacetime regime for state activities in cyberspace*. Tallinn: NATO CCD COE Publications

References

- Azadi, Javad (2018). Cyber security or cybersecurity. *Growth reflections*, 1 (1), 164– 168. (in Persian)
- Badiee Azandahi, Marjan; Ahmadi Firoozjaei, Meysam; Ansarizadeh, Salman (2013). Explaining the concept of border in Iran's political-virtual space. *Geography Quarterly*, 36, 291 - 313. (in Persian)
- Cairncross, Fransis (1997). *The death of distance: How the communications revolution will change our lives?* Harvard: Harvard school press.
- Cassese, Antonio (1995). *Self-determination of peoples: a legal reappraisal*. Cambridge: Cambridge University Press.
- Czosseck, Christian; Geers, Kenneth (2018). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? In F. Hare, *The Virtual Battlefield: Perspectives on Cyber Warfare* (pp. 49 - 74). Amesterdam: IOS press BV.
- Demchak, Chris. C. (2018). Uncivil and Post-western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age. *The Cyber Defense Review*, 49 - 74.
- Ebadi Nejad, Seyed Ali; Nosrati, Hamidreza; Mustajabi, Hamid (2013). The Impact of Globalization on the Border in Cyberspace. *Border Science and Technology*, 53 - 72. (in Persian)
- Fang, Bixing (2018). *Cyberspace Sovereignty; Reflections on Building a Community of Common Future in Cyberspace*. Beijing: Springer Singapore.
- Ghamami, Seyed Mohammadmahdi (2011). *Constitutional rights of the Islamic Republic of Iran*. Tehran: Islamic Revolution Documentation Center. (in Persian)
- Ghazi, Seyed Abolfazl (2014). *Constitutional rights requirements*. Tehran: Samat. (in Persian)
- Giles, Keir (2012). *Russia's public stance on cyberspace issues*, 4th international conference on cyber conflict. Tallinn: NATO CCD COE publication.
- Godvin III, James; Kulpin, Andrey; Rauscher, Karl. Fredrick; Yaschenko, Valery (2014). *The Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations 2*. New York: EastWest Institute and the

- Information Security Institute of Moscow State University.
- Ghol Mohammadi, Ahmad (2004). Globalization and culture and identity. Tehran: Ney Publishing. (in Persian)
- Hafznya, Mohammadreza (2011). The political geography of cyberspace. Tehran: Samat. (in Persian)
- Hassani, Hossein (2019). Data localization. Tehran: National Cyberspace Center Research Institute. (in Persian)
- Heydarifar, Mohammadrauf (2010). Critical study of the discourse of a world without borders. *Geopolitical Quarterly*, 6 (2), 125 - 152. (in Persian)
- Janparvar, Mohsen (2008). A Study of the Evolution of the Concept of Border in Contemporary Times, Master Thesis. Tehran: Tarbiat Modares University. (in Persian)
- Kabiri, MAlihe; Janparvar, Mohsen; Zarghani, Seyedhadi (2016). Explain and level the factors affecting the importance of borders; With emphasis on land borders. *Iranian Journal of International Politics*, 5 (2), 93-117. (in Persian)
- Karmer, Franklin (2009). Cyberpower and national security. Washington D.C.: Center for Technology and National Security Policy.
- Kearney, Michael (2004). The classifying and valuefiltering missions of borders. *Anthropological Theory*, 4(2).
- Khalili, Mohsen (2013). The concept of territory in the Constitution of the Islamic Republic of Iran: Geographical border, *ideological boundless*. *Strategy*, 58, 7 - 45. (in Persian)
- Lin, Herbert (2011). Responding to sub-threshold cyber intrusions: a fertile topic for research and discussion. *Journal of International Affairs*, 127 - 135.
- Mayer, Marco (2014). How would you define Cyberspace? First Draft Pisa.
- Mujtahidzade, Piruz (2002). Political Geography and Geographical Politics. Tehran: Samat. (in Persian)
- Mir Haider, Dorre (2006). Fundamentals of Political Geography. Tehran: Samat. (in Persian)
- Osborn, Phillipe (2017). Cyber Border Security – Defining and Defending a National Cyber Border. Homeland Security Affairs.
- Oxford Online Dictionary (2020, 11 4). Retrieved from lexico: <https://www.lexico.com/definition/cyberspace>
- Racicot, Michael; Hayes, Mark S; Szibbo, Alec R; Trudel, Pierre (1998). The

- cyberspace is not a 'no law land' a study of the issues of liability for content circulating on the internet. *Computer Law & Security Review*, 14(2), 96-106.
- Ranjekesh, Mohammadreza; Keshavarz, Hamidreza (2013). Structure - Agent: A theoretical framework for understanding and evaluating the boundary phenomenon. *Quarterly Journal of New Attitudes in Human Geography*, 5 (4), 69-87. (in Persian)
- Rahmati Rad, Mohammadhossein (1997). Border guards, passports and foreign nationals. Tehran: NAJA Deputy Minister of Education. (in Persian)
- Rezapour, Mohammadmahdi (2019). Cyber governance in China. Tehran: National Cyberspace Center Research Institute. (in Persian)
- Sadughi, Moradali (2007). Information technology and national sovereignty. Tehran: Office of Political and International Studies, Ministry of Foreign Affairs. (in Persian)
- Schmitt, Michael N. (2013). Tallinn manual on the international law applicable to cyber warfare. Cambridge: Cambridge University Press.
- Shirzadi, Reza (2018). Territory and borders from the perspective of geopolitics, politics and international law. *Border Science and Technology*, 9 (3), 91 - 119. (in Persian)
- Soltaninejad, Ahmad; Islami, Mohsen; Rastgoo, Mohammadzaman (2016). , Advanced information and communication technology and the evolution of the concept of sovereignty in international relations. *Contemporary Political Essays*, 7 (1), 85-114. (in Persian)
- Stanbury, William Thomas; Vertinsky, Ilan. B. (1994). Information technologies and transnational interest groups: The challenge for diplomacy. *Canadian Foreign Policy Journal*, 2(3), 87 - 99.
- Thornton, Sean M. (1997). State Criminal Laws in Cyberspace: Reconciling Freedom for Users with Effective Law Enforcement. *Richmond Journal of Law & Technology*, 4(2), 5.
- Tuukkanen, Topi (2018). Sovereignty in the cyber domain. *The Fog of Cyber Defence*, 37 - 45.
- Zarghan, Seyedhadi (2007). An Introduction to Recognizing International Borders. Tehran: The police force of the Islamic Republic of Iran. (in Persian)
- Ziolkowski, Katharina (2013). Peacetime regime for state activities in cyberspace. Tallinn: NATO CCD COE Publications.