

فضای سایبر؛ چالش‌های حاکمیت و امنیت پایدار

مصطفی قادری حاجت*^۱، حمیدرضا نصرتی^۲

تاریخ پذیرش: ۱۳۹۲/۶/۸

تاریخ دریافت: ۱۳۹۲/۱/۲۰

چکیده:

علاوه بر فضای جغرافیایی که دربرگیرنده ساختارهای عینی و قابل درک است، فضایی مجازی هم می‌تواند به موازات فضای جغرافیایی مطرح و دارای الزام‌های خاص خود باشد. فضای مجازی، روزهایی نو را برای ملت‌های جهان و نیز ساختارهای حاکمیتی گشوده است. این فضا، همانند فضای جغرافیایی، تهدیدها، چالش‌ها و فرصت‌هایی را فراهم آورده که حاصل ظهور و کنش بازیگران در این حوزه است و خصوصاً می‌تواند بازخوردی گسترده‌تر از ابعاد محلی یا منطقه‌ای داشته باشد.

کسب، انتقال و استفاده از اطلاعات نیاز به در اختیار داشتن فن‌آوری اطلاعات و نیز روزآمد ساختن و تأمین امنیت در آن است. اگر چه این فن‌آوری در میان همه کشورها به‌طور یکسان وجود ندارد اما اگر عناصر قدرتی بخش جغرافیایی را با نمونه‌های مشابه در بخش سایبر بسنجیم، درمی‌یابیم که قدرت‌های بزرگ، راهبردهای سایبری خود را همسو با راهبردهای سرزمینی و جغرافیایی تقویت می‌کنند. این مقاله به روش توصیفی-تحلیلی و با استفاده از منابع کتابخانه‌ای، ضمن بررسی جغرافیای سیاسی فضای مجازی، از دیدگاه جغرافیای سیاسی به چالش‌های حاکمیت در این حوزه پرداخته و ظهور بازیگران جدیدی را که وضعیت آنان منحصراً بر بازیگران سنتی انطباق ندارد بررسی می‌کند. یافته‌های مقاله، حاکی از وجود چالش‌های پنج‌گانه کاربران خانگی و تجارت‌های کوچک، تشکیلات اقتصادی بزرگ، نواحی بحرانی تأسیسات زیربنایی، آسیب‌پذیری در حوزه ملی و تهدیدهای جهانی حاکمیت‌ها در جهان مجازی است که هر کدام بایسته‌های خود را دارند.

کلیدواژه‌ها: فضای مجازی، فناوری اطلاعات، حاکمیت ملی، امنیت، جغرافیای مجازی.

۱ - دانشجوی دکتری جغرافیای سیاسی، دانشگاه تربیت مدرس* (نویسنده مسؤول) Email: m.ghaderihajat@modares.ac.ir

۲ - کارشناس ارشد جغرافیای سیاسی، دانشگاه شهید بهشتی

۱ - مقدمه

ظهور انقلاب تکنولوژیکی، نویدبخش پدید آمدن فن آوری‌های پیچیده‌ای بود که توسعه آن باعث تحت تأثیر قرار گرفتن دیگر علوم شد؛ به گونه‌ای که فضای جدیدی را در دنیای واقعی به خود اختصاص داد که فضای مجازی از آن تعبیر می‌شود. فضای مجازی^۱ در واقع محیط شبیه‌سازی شده جهان واقعی است که در آن شبکه‌های ارتباطاتی و فن آوری‌های اطلاعاتی بر دیجیتالیزه^۲ کردن تعاملات تأکید می‌ورزند. فضای سایبر^۳ به عنوان بخشی از فضای مجازی، با پافشاری بر عامل سایبرنتیک^۴ که در واقع همان فن آوری‌های رایانه‌ای و شبکه‌ای قابل برنامه‌ریزی و راهبری هستند تأکید می‌کند. فضای مجازی که شبکه جهانی اینترنت محصول عملکرد آن است، نماد پیشرفت علم و فن آوری است که کشورهای قدرتمند به ویژه آمریکا در تولید و معماری آن نقش اصلی را به عهده دارند. فضای مجازی عرصه جدیدی برای حیات بشری است که قابلیت پذیرش و انجام بخش عمده‌ای از نیازها، فعالیت‌ها و شؤون زندگی بشر و اجتماع‌های انسانی و حکومت‌ها را دارد و به عنوان سایه فضای واقعی و از طریق تمرکز، پردازش و جابه‌جایی اطلاعات، توانایی شبیه‌سازی فعالیت‌ها و ساختارهای فضای واقعی را داراست و این شبیه‌سازی را با اثربخشی در فضای واقعی انجام می‌دهد (حافظ‌نیا، ۱۳۹۰: ۱). تبیین جغرافیای فضای سایبر به عنوان حوزه‌ای نو در مطالعات جغرافیایی ذهن صاحب‌نظران را به خود مشغول ساخته است. هر چند برخی از نظریات جغرافیدانان درباره این موضوع دریچه‌های جدیدی را در گفتمان مطالعات جغرافیایی گشوده اما هنوز مبحث جغرافیای فضای مجازی و پیرو آن جغرافیای فضای سایبر جایگاه خود را نیافته است. هاروی^۵ با طرح پیچیدگی و درهم‌تنیدگی فضا و زمان به عنصر زمان در مطالعات جغرافیایی پرداخت و مک لوهان مسئله دهکده جهانی را

۱ - Virtual space

۲ - Digitalizing

۳ - Cyberspace

۴ - Cybernetic

۵ - Harvey

با در نظر گرفتن این فن آوری، قابل توجه دانست. شکل‌گیری جامعه شبکه‌ای در گستره شبکه جهانی اینترنت که شاید بتوان ادعا کرد محلی برای شبیه‌سازی همه امور حقیقی است، خود فرصت‌ها، چالش‌ها و تهدیدهایی را می‌آفریند که پرداختن به آن‌ها بر عهده کسانی است که توانایی درک این جغرافیای جدید و نیز همگامی با توسعه و پیشرفت فن آوری را دارند. جغرافیای سیاسی فضای سایبر نیز علاوه بر درک فضایی تعاملات شبکه‌ای به سیاست‌های دولت‌ها در این محیط می‌پردازد. علاوه بر آن ایجاب می‌کند سیاست‌گذاری قدرت‌های بزرگ که در فضای جغرافیای حقیقی در رقابت با یکدیگر شکل می‌گیرد در جغرافیای سایبر تبیین شود.

۲- روش تحقیق

این نوشتار با استفاده از روش تحقیق توصیفی - تحلیلی و با استفاده از منابع کتابخانه‌ای و پایگاه‌های اینترنتی در پی تبیین ابعاد چالش‌های حاکمیتی و امنیتی کشورها در عصر جهانی شدن‌هاست.

۳- مباحث نظری

۳-۱- مفهوم فضای سایبر

سایبر^۱ واژه‌ای است برگرفته از لغت «cybernetics» به معنای سکاندار یا راهنما. نخستین کسی که واژه فضای سایبر را به کار برد، ویلیام گیتسون نویسنده داستان‌های علمی - تخیلی، در کتاب نورومنسر^۲ بود.

فضای سایبر یا فضای مجازی^۳ در تعریف برخی از نویسندگان عبارت است از «مجموعه‌ای از ارتباطات میان انسان‌ها از راه رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی». البته شاید بهتر باشد آن را چنین تعریف کنیم: «محیط الکترونیکی

۱ - cyber

۲ - neuromancer

۳ - Cyber Space

واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص خود، به گونه‌ای زنده و مستقیم در آن روی می‌دهد. «واقعی»، مانع از این است که تصور شود مجازی بودن این فضا به معنای غیر واقعی بودن آن است؛ چرا که در این فضا نیز همان ویژگی‌های تعاملات انسانی در دنیای خارج (همچون مسؤلیت) وجود دارد. ضمن این که فضای سایبر در واقع یک «محیط» است که ارتباطات در آن انجام می‌شود؛ نه صرف مجموعه‌ای از ارتباطات. از سوی دیگر، این ارتباطات گر چه ممکن است در همه حال «بر خط»^۱ نباشد، ولی زنده، واقعی و مستقیم است. از این رو تأثیر و تأثر بالایی در این روابط رخ می‌دهد.

۳-۱-۱- ویژگی‌های فضای سایبر

الف- جهانی و فرامرزی بودن

از ویژگی‌های منحصربه‌فردی که فضای سایبر را از دیگر فضاها بازشناخته می‌سازد، جهانی بودن آن است. هر فردی در هر نقطه از جهان می‌تواند با آن به آسانی، به جدیدترین اطلاعات دست یابد. مرزهای جغرافیایی تا کنون نتوانسته از گسترش روزافزون فضای سایبر جلوگیری کند. از این رو، هر نوع فیلتر و مرزبندی در برابر آن بسیار دشوار می‌نماید.

ب- دستیابی آسان به آخرین اطلاعات

چنانچه به دسترسی به آخرین تحولات در همه زمینه‌های عمومی و تخصصی، در سطح جهان نیاز باشد، ساده‌ترین و سریع‌ترین راه، استفاده از فضای سایبر است. این فضا با قابلیت‌های منحصربه‌فرد خود زمینه این کار را فراهم می‌کند.

پ- جذابیت و تنوع

رسانه‌ها فیلم، عکس، متن و هر هنر دیگری را برای گیرایی خویش به کار می‌گیرند و این ابزارها در فضای سایبر قابل دستیابی است و هیچ نظارت و فیلتری توان محدودسازی

آن را ندارد. از ویژگی‌های یگانه‌ای که در تنوع و جذابیت فضای سایبر تأثیر به‌سزایی دارد، مشتری‌محوری محض است. در متون نوشتاری ارتباطی تنگاتنگ میان نویسندگان و خوانندگان وجود دارد و خواننده به راحتی می‌تواند نظر خود را با نویسنده در میان بگذارد. از سوی دیگر، امکان نظرسنجی و ارزیابی در این فضا بسیار آسان‌تر و روزآمدتر است و این توانایی را به داده‌پردازان، فروشندگان و عرضه‌کنندگان کالاها در اینترنت می‌دهد تا از آخرین خواست‌های مشتریان و مخاطبان خود آگاه شوند.

ت- آزادی اطلاعات و ارتباطات

۲-۳- حاکمیت

حاکمیت، قدرت ناشی از آزادی و استقلال یک دولت مستقل است. دولت‌های مستقل می‌توانند روابط خارجی و امور داخلی خود را با اعمال حق حاکمیت، بر وفق تمایلات خود تنظیم کنند. هم‌چنین، قدرت عالی تصمیم‌گیری و اجرای تصمیمات در اختیار دولت است و هیچ نهاد اجتماعی دیگری از آن برخوردار نیست. حق حاکمیت به مفهوم آزادی مطلق دولت‌ها نیست. رفتار دولت‌ها به وسیله قواعد و احکام حقوق بین‌المللی و مقررات سازمان‌های بین‌المللی که دولت‌ها در آن‌ها عضویت دارند، مشروط می‌شود (روشن، ۱۳۸۵: ۱۳۸۷). بحث «حاکمیت» حکومت در جغرافیای سیاسی محدود به این توضیح است که اداره امور سرزمین و ملت بدون اقتدار و حاکمیت امکان‌پذیر نیست. بنابراین حکومت، اقتدار و حاکمیت تفویض شده از سوی ملت به خود را که در فرآیند دموکراسی انجام پذیرفته، برای اداره کشور از راه به اجرا درآوردن قانون اساسی و قوانین پیرو آن اعمال می‌کند (مجته‌زاده و حافظ‌نیا، ۱۳۸۷: ۴). حاکمیت از لحاظ ژئوپلیتیکی قدرت، تصرف و استقلال فرماندهان، حاکمان و پادشاهان را در دوره‌های مختلف به نمایش می‌گذارد. این مفهوم گرچه با روند تحولات تمدن بشری متحول شده اما همواره لازمه حکمرانی و بقای کشورها و ملت‌ها بوده است.

طبق ضرب‌المثل برزیلی به نقل از روبرتو داماتا «حاکمیت برای دشمنان قانون، برای دوستان همه چیز است» (Cox, ۲۰۰۸: ۱۱۷). بنابراین، در هر نظام سیاسی باید حدودی از

قدرت مطلق برای تصمیم‌گیری نهایی وجود داشته باشد تا شماری از افراد یا نهادهایی که برای تصمیم‌گیری صالح تشخیص داده شده‌اند، آن را در یک قلمرو جغرافیایی مشخص اعمال کنند و قادر به اجرای تصمیمات باشند.

مفهوم حاکمیت یا اقتدار حکومت، در اروپای قرن‌های شانزدهم و هفدهم شکل گرفت و با نابودی نهادهای فئودالی به اوج خود رسید؛ زمانی که دولت‌های سرزمینی یا دولت‌های ملی نوین شکل گرفتند. در این باره، معاهده صلح وستفالی در سال ۱۶۴۸ نقطه عطف در تاریخ است. این معاهده سرآغاز کوششی شد که تا امروز ادامه دارد؛ تلاش برای کشف روش‌هایی که بر اساس آن‌ها دولت‌های مستقل بتوانند حاکمیت خود را بر سرزمین‌شان اعمال کنند و منافع خویش را به گونه‌ای تأمین سازند که نه زیان‌بار به حال خودشان باشد و نه به حال جامعه بین‌المللی که عضوی از آن هستند (احمدی نیاز، ۱۳۸۵: ۲۱).

۴- یافته‌های تحقیق

۴-۱- زمان و فضا در روزگار فن‌آوری

تحلیل فضا و مکان همواره از مباحث اصلی دانش جغرافیا بوده است. این در حالی است که طرح موضوع زمان در شاخه‌های مختلف جغرافیا کاری جدید محسوب می‌شود. انقلاب فن‌آوری پس از نیمه قرن بیستم تأثیر به‌سزایی در شکل‌گیری فضا‌های نوین جغرافیایی یا دگرگونی و توسعه تعاریف کاربردی آن نهاد. در واقع فن‌آوری اطلاعاتی با پست مدرنیسم همراه شد و جامعه اطلاعاتی جدیدی را در آغاز دهه ۱۹۷۰ تشکیل داد. سه ویژگی اصلی این جامعه عبارت‌اند از: ۱- سرگرم دگرگونی از تولید کارآ به جامعه خدماتی ۲- تأکید بر کدگذاری دانش نظری برای ابداع و اختراع در فن‌آوری. ۳- ایجاد فن‌آوری فکری تازه‌ای که همچون کلید تحلیل نظام‌ها و نظریه تصمیم‌گیری به کار می‌آید (رجایی، ۱۳۸۲: ۱۱۶). با این حال یکی از نظریه‌های مربوط به تغییر و تولید فضا، تأکید بر فن‌آوری به‌عنوان عامل تعیین‌کننده است؛ به این صورت که هر گونه تغییر در نیروی فن‌آوری، تغییرات خاصی را در فضای جغرافیایی به‌وجود می‌آورد (شکوئی، ۱۳۸۲: ۱۲۱).

توسعه فن‌آوری سبب شکوفایی و گسترش آن شده و امروزه تمرکز بر مکتب تکنولوژیک در جغرافیا دامنه‌های بسیاری را در زندگی فرا گرفته است. شاید بتوان گفت که انسان محکوم به جبر تکنولوژیک است. به‌رغم کارآیی تکنولوژی در حوزه‌های مختلف جغرافیا، تلاش بر آن است تا قسمتی از ره‌آورد فن‌آوری را که ویژگی‌های خاص جغرافیایی بر آن متصور است با عنوان جغرافیای فضای سایبر تحلیل و معرفی شود. بنابراین پرداختن به مسأله مکان که از نخستین و مهم‌ترین مباحث در جغرافیا است، ضرورت دارد؛ همان‌گونه که گفته می‌شود مکان در مرکز علائق جغرافیا واقع شده است^۱ (Cresswe, ۲۰۰۹: ۱۶۹). برای تبیین جغرافیای مجازی باید تلاش‌ها را معطوف به پدیدار شدن این فضا کرد. از این‌رو نیاز است تا فضای سایبر برای ادراک شدن، دیدنی ساخته شود. یکی از راه‌های نیل به این مقصود دست‌یافتن به تقسیمات سایبر است (Dodge, ۱۹۹۹: ۶). شناخت خصوصیات مکان، شامل ابعاد (که دربرگیرنده طول و عرض جغرافیایی و شکل هندسی مکان است) و ارتباط مکانی که یک محیط با محیط‌های دیگر به‌طور ویژه در ابعاد تاریخی و طبیعت منحصر به یک مفهوم مکانی است (McColl, ۲۰۰۵: ۷۲۸). از جمله الزام‌های درک و تعمیم‌پذیری جغرافیای مجازی هستند. تا کنون از پیشرفت فن‌آوری به‌عنوان عامل اثرگذار یاد می‌شد. هر چند که این مفهومی صحیح است اما توسعه فضای مجازی ناشی از فن‌آوری به حدی رسیده است که می‌توان برای این فضای مجازی به‌ویژه پس از ظهور اینترنت و نفوذ آن در میان ملت‌ها و دولت‌ها، جغرافیای جدیدی با نام سایبر را تعریف کرد. در تفسیر مکان جغرافیایی، ابعاد فیزیکی محیط سنجیده می‌شود و در نهایت «وجود» را نتیجه می‌دهد.

جدول ۱: تطبیق ویژگی‌های مکان جغرافیای واقعی با جغرافیای سایر

ویژگی‌های مکان در جغرافیای واقعی	تیبین ویژگی‌های مکان در جغرافیای سایر
مکان به‌عنوان محل یا جای فیزیکی	مکان به‌عنوان جایی برای دامنه‌ها و سرورها
مکان به‌عنوان محل فرهنگی یا اجتماعی	مکان به‌عنوان محلی برای شبکه‌های سایبری و...
مکان به‌عنوان محلی دارای یک سابقه مشخص	مکان به‌عنوان محلی برای انباشت داده‌ها و بازیابی آنان
مکان به‌عنوان یک سازه اجتماعی در طول زمان	مکان به‌عنوان جوامع متعدد شبکه‌ای
مکان به‌عنوان یک فرآیند اجتماعی	مکان به‌عنوان یک فرآیند اجتماعی

(Stabeli, ۲۰۰۳: ۱۵۹)

جدول شماره ۱ سعی در اثبات مکان‌پایه بودن جغرافیای سایر و تبیین مکانی با امکان دسترسی و تبادل و ذخیره‌سازی اطلاعات را دارد. اما این مکان خصوصیات تغییر شکل یافته‌ای از جغرافیای واقعی را دربرمی‌گیرد که سراسر آن دال بر وجود ماهیتی نو و تعریفی جدید از واژه مکان است. در جغرافیای فضای سایر این اطلاعات و تبادل آن‌هاست که ایفای نقش کلیدی دارد.

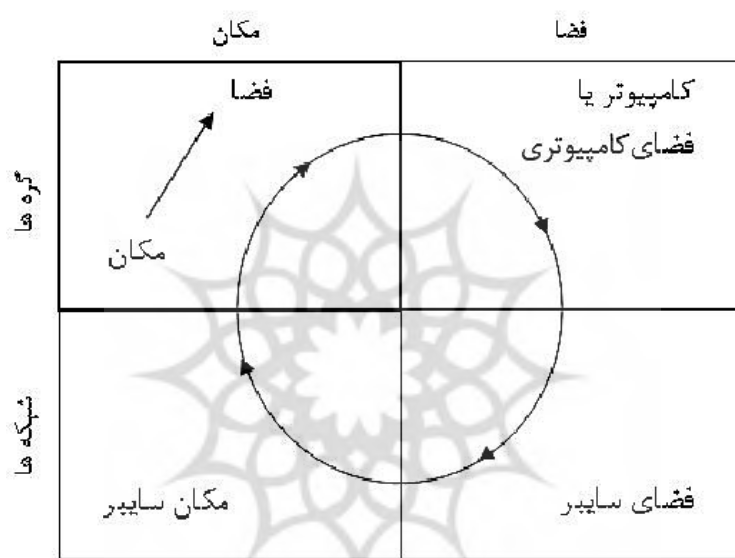
بحث فضای جغرافیایی نیز علاوه بر موضوع مکان می‌تواند زمینه‌ساز گسترش موضوع فضای سایر باشد. وجود تحلیل‌های فضایی با کمک نرم‌افزارهای شبیه‌ساز، کمک‌های شایانی به پیشرفت علم جغرافیا کرده است. سیستم تعیین وضعیت جغرافیایی^۱، سیستم اطلاعات جغرافیایی^۲ و بسیاری دیگر از نرم‌افزارها و سخت‌افزارهای موجود امکان به‌وجود آوردن رویکردی مجازی را در تحلیل فضاهای جغرافیای واقعی به‌وجود می‌آورد. فضا در بسیاری از روش‌ها، کلید موضوعی جغرافیا محسوب می‌شود (Elden, ۲۰۰۹: ۲۶۲). بنابراین تجزیه و تحلیل فضای اشغال‌شده در حوزه مکان مشخص، همواره قابل اهمیت است. با توجه به ابعاد تکنیکی حاکم بر جغرافیای فضای سایر که اهمیت آن بستگی مستقیم به داده‌های پردازش شده و نشده دارد، این حجم از اطلاعات و انتقال آن‌ها چشم‌اندازی نوین را به‌لحاظ کمی و کیفی در توجه به این فضا به‌لحاظ کمی و کیفی ایجاد

۱ - Geographic position system (GPS)

۲ - Geographic information system (GIS)

می‌کند. در واقع می‌توان تشبیه چشم‌انداز جغرافیایی در محیط‌های واقعی را در محیط‌های مجازی و به‌ویژه در فضای سایبر با عنوان Datascape تعریف کرد. این واژه برگرفته از کتاب neuromancer نوشته ویلیام گیbson^۱ است. تصویر آینده در آن کتاب، چشم‌انداز وسیع داده‌های ساخته‌شده از اطلاعات رایانه‌ای است و کاربران به‌وسیله اتصالشان مستقیم و آگاهانه به شبکه جهانی رایانه‌ای دسترسی پیدا می‌کنند (Bell, ۲۰۰۹: ۴۶۸).

شکل ۱: جغرافیای مجازی



(Dodge & Kitchen, ۲۰۰۱: ۲۲)

تبیین فرآیندهای موجود در شکل ۱ می‌تواند جغرافیای سایبر را بهتر متصور سازد. مکان و فضای موجود در فضای سایبر دربردارنده رایانه‌های بسیار و نیز فضای رایانه‌ای شامل نرم‌افزارها و اطلاعات و ماشین‌آلات شخصی است که آن‌ها در محیطی به‌واسطه گره‌ها و شبکه‌ها به یکدیگر پیوند می‌خورند و چشم‌انداز جغرافیای سایبر را به‌وجود می‌آورند. به‌رغم موضوعیت مکان و فضا در جغرافیای فضای سایبر نقش‌آفرینی زمان را نیز نمی‌توان نادیده انگاشت. تبیین زمان در دسترسی به این فضا، پیوند مستقیم با فضای

۱ - William Gibson

فن آورانه دارد. فن آوری به هر اندازه بیش تر رشد کند و کارآمدی آن در خدمت فضای سایبر باشد زمان مصرف شده برای دسترسی به اطلاعات و برقراری ارتباط و نیز تبادل داده سرعت بیشتری به خود می گیرد. از این رو است که فضای سایبر، صحنه‌ای برای به نمایش گذاشتن قدرت بر مبنای زمان کمتر مصرف شده است. در واقع حتی امروز نیز زمان و مکان، محدودیت‌های اساسی برای آزادی عمل و کنش‌ها و واکنش‌ها به وجود می آورد. با وجود این امروزه شاید قالب‌های یک بعدی زمان و مکان با کمک فضای سایبر و فن آوری‌های جدید [توسعه یافته] و امکان بازیگری بیشتر فعالان اجتماعی، در انواع پیمایش‌های انجام شده در زندگی روزمره را فراهم آورد (Davies, ۲۰۰۱: ۱۳۴).

۴-۲- قلمرو در فضای سایبر

تعیین حدود قلمروها در جغرافیا همواره در طول تاریخ باعث بروز اختلاف‌ها، تنش‌ها و جنگ‌های بسیاری شده و این موضوع را به مبحثی مناقشه‌برانگیز تبدیل کرده است. با این حال پس از تبیین جغرافیای فضای سایبر این نکته دارای اهمیت است که آیا در این فضای جدید جغرافیایی نیز می توان قلمروهایی را تعیین کرد؟ تحلیل و تفسیر این مسأله در واقع آغازی است برای ورود جغرافیای سیاسی به فضای سایبر.

قلمرو بیانگر یک فضای جغرافیایی دامنه‌دار است و قلمروخواهی، گویای قصد کنترل آن فضا است (Storey, ۲۰۰۹: ۲۴۵) در واقع موضوع اساسی جغرافیای سیاسی قلمرو و قلمروخواهی است؛ تحلیل‌ها در جغرافیای سیاسی بر این مبنا شکل می گیرد (Blacksell, ۲۰۰۶: ۱۱). از این رو، رقابت‌های موجود در میان حکومت‌های ملت‌پایه و گروه‌های مختلف، همواره محور مطالعاتی جغرافیای سیاسی (در جغرافیای واقعی) است.

نکته قابل توجه این است که برخی از مفاهیم کلیدی در حوزه قلمرو و قلمروخواهی که در جغرافیای واقعی تجلی می‌یافت ممکن است در فضای سایبر متصور نشود و اگر تعمیم یابد نیز با شرایط ویژه‌ای این تطبیق امکان‌پذیر شود؛ چرا که در واقع مهمترین عامل نقش آفرین در فضای سایبر، اطلاعات است. بنابراین قلمروهای اطلاعاتی در تبیین مسأله

قلمروخواهی جایگاه ویژه‌ای را به خود اختصاص خواهند داد. اگر در دانش ژئوپلیتیک، این خاک و سرزمین بود که اهمیت قابل توجهی در مطالعات داشت در جغرافیای فضای سایبر جای خود را به فضای اطلاعاتی (که خود دربرگیرنده دامنه‌ها^۱، بانک‌های اطلاعاتی^۲، شبکه‌ها و سرویس‌دهندگان اینترنتی است)، داده است. از این‌رو دامنه‌های اینترنتی به مثابه خاک در ژئوپلیتیک متصور می‌شود. مبحث سایبر در قرن بیستم شامل فضای سایبر، تنش سایبری، دموکراسی الکترونیکی و... اصولاً متمایل به تحلیل نوینی از اطلاعات اجتماعی است و تقسیمات قلمروهای جدید سایبرنتیک از قبیل شبکه «نظامی - صنعتی - رسانه‌ای - تفریحی»، و کالت سایبری و تجارت الکترونیک شکل یافته است (Armitage & Roberts, ۲۰۰۲: ۱۲).

از آن‌جا که گستره مطالعاتی فضای سایبر محدود به مکان خاصی نمی‌شود بنابراین جامعه اجتماعی تشکیل شده در این فضا می‌تواند درباره مسایل گوناگونی تبادل اطلاعات کند. این موضوع علاوه بر پویایی ذاتی جغرافیای سیاسی آن را بسیار فعال‌تر از گذشته نشان خواهد داد. بیان مشخص از قلمرو یک مدعی در فضای سایبر دشوار به نظر می‌رسد؛ زیرا محدوده مشخصی را نمی‌توان برای این قلمرو تعیین کرد. اما مسأله قلمروخواهی که بر پایه عنصر رقابت تحلیل می‌شود، عملکرد متفاوتی دارد. تلاش برای توسعه فعالیت و اثرگذاری که به مقصود کسب منافع اقتصادی و نفوذ اجتماعی یا سیاسی صورت می‌پذیرد همواره امکان بهره‌گیری از این فضا را برای مدعیان فراهم می‌کند. بنابراین از آن‌رو که فلسفه فضای سایبر ورود به جهانی شبکه‌ای و جوامع جهانی است نمی‌توان قلمروهایی معین برای آن تعریف کرد. هر چند این بحث خود جای تأمل دارد که محدوده‌های امنیتی تعریف شده برای سازمان‌ها، گروه‌ها و افراد در فضای سایبر آیا به آن شکل قلمرو می‌بخشد؟ و یا تنها شکلی محدودکننده از دسترسی به اطلاعات خاص است که دست‌یابی به آن‌ها برای همگان مجاز نیست.

۱ - Domain

۲ - Database

۴-۳- فضای سایبر و بازسازی قلمروخواهی^۱

توسعه فن آوران می تواند همه جهان آنلاین را در یک لپ تاب قابل دسترس کند. این به آن معنی است که محدودیت های زمان و فضا در این عرصه رو به کاهش نهاده است (Frisson, ۱۹۹۷: ۱۱۶). در واقع دسترسی به حجم انبوهی از اطلاعات در فرصت کوتاه و با داشتن حداقل امکانات، از ویژگی های یک جامعه تکنولوژیک محسوب می شود. در این فضا می توان تبادلات الکترونیکی را با سرعت زیادی انجام داد. با این حال ضرورت های رقابت در جغرافیای واقعی تکلیف می کند تا در فضای سایبر نیز رقابت ها گراگرد منافع ملی دولت ها و یا دیگر گروه های غیر دولتی و حتی ذینفعان خصوصی در جریان باشد. تطبیق دو شیوه قلمروخواهی در هر دو محیط بیان کننده تفاوت های عملکردی دو حوزه قلمروخواهی است. در واقع تصمیم سازی در محیط سایبر برای بازسازی قلمروخواهی های واقعی شکل می گیرد و بازسازی قلمروخواهی به تخریب یا بازساخت یک قلمروخواهی ویژه می پردازد (Coleman, ۲۰۰۹: ۲۵۵). آنچه که حائز اهمیت است آن است که بازسازی قلمرو در فضای سایبر قابل توجه و ممکن است اما در آن مبحث امنیت به شدت شکننده و قلمروخواهی نیز بر مبنای آن متزلزل خواهد شد (Herrera, ۲۰۰۷: ۷۵). درک مفهوم قلمروخواهی در تفسیرهای ژئوپلیتیک بیان کننده وجوه کسب قدرت از طریق عوامل جغرافیایی است که علاقه های ژئوپلیتیک را بیان می کند. در اساس، فضای سایبر به دلیل عمومیت جهانی آن به محلی برای ساخت قلمروهای جدید بدل شده است و از آن جا که این قلمروها مرزبندی های رایج در جغرافیای واقعی را رعایت نمی کنند به لحاظ امنیتی همواره با چالش روبه رو هستند. به دلیل درهم تنیدگی ساختارها در فضای سایبر، تحلیل فضایی از قلمروها، دشوار به نظر می رسد. این تحلیل بستگی به عواملی چون ساختارهای فن آوران، فهم فضای سایبر، تقسیمات حاکم بر آن و نیز منافع دولت ها و ملت هاست. این

۱- Deterritorialization

موضوع باعث می‌شود قلمروهای ساخته‌شده در فضای سایبر از پویایی ذاتی برخوردار باشند که همواره تحولات گسترده‌ای از چشم‌اندازهای موازی داده‌ها را به همراه دارد. بنابراین بازسازی قلمروخواهی در جهان واقعی به شیوه‌ای همگون و متناسب با جهان سایبر دوباره معنا می‌شود.

۴-۴- مرزها در جغرافیای فضای سایبر

پدیده جهانی‌شدن بدون در نظر گرفتن ابزارهای ارتباطی که پیوندهای شبکه‌ای را توسعه می‌بخشد بی‌معنا به نظر می‌آید. بنابراین ضرورت گسترش تفکرات جهانی در همه ابعاد اقتصادی، فرهنگی و...، وجود شبکه‌های ارتباطی برخوردار از کارکرد جهانی است. علاوه بر آن، خصوصیت جهانی‌شدن، کمرنگ‌شدن مرزها را اقتضا می‌کند. این در حالی است که فضای سایبر به‌طور اساسی مرزبندی‌های جغرافیای سیاسی جهان را با خود همراه ندارد؛ دلیل آن‌هم پیوستگی شبکه‌ای حکومت‌های ملت‌پایه در سرتاسر جهان در جغرافیایی با عنوان فضای سایبر است. (Mosco, 2004: 88-89). آن‌چه در جهانی‌شدن از آن با عنوان کمرنگ‌شدن مرزها یاد می‌شود، در واقع تجلی جامعه شبکه‌ای و دسترسی به جغرافیایی است که در آن برای ورود به کشور دیگر و ملاقات مجازی حتی با رئیس‌جمهور آن نیاز به گذراندن هیچ‌گونه مراحل دیپلماتیک ندارد. این گسترش دامنه دسترسی‌ها، مرزهای ملی را با توجه به سوابق کمرنگ می‌کند؛ اگر چه هنوز در قالب کدهای ورود و دامنه‌های مختلف همچنان ادامه دارد. نه تنها مرزهای ملی به‌طور فزاینده‌ای در فضای سایبر با چالش مواجه می‌شوند، بلکه آن‌ها با ساختارهای جدید و به‌هم‌پیوسته که مبتنی بر روان‌بودن (سیالیت) جوامع مجازی سایبرنتیک و زیستگاه است، جایگزین می‌شوند (Everett, 2009: 33). شکل جدید مرزها را باید در جغرافیای فضای سایبر از دو سو بررسی شود: مرزهای میان جغرافیای واقعی و جغرافیای مجازی و نیز مرز میان قابلیت‌های نقش‌آفرینی در جغرافیای فضای سایبر.

۱- مرزهای میان جغرافیای واقعی و جغرافیای سایبر. تحلیل روابط میان دو فضا می‌تواند مرزهایی را میان آن‌ها شذنی سازد؛ همان‌گونه که برای جهان فراطبیعی و جهان واقعی مرزهایی وجود دارد. از سوی دیگر نمی‌توان اثرگذاری آن دو جهان را بر یکدیگر منکر شد، زیرا این تجربه‌پذیری و نیز تجربه‌ناپذیری است که تعیین‌کننده مرز میان آن دو است. بنابراین مرزهای میان جغرافیای واقعی و جغرافیای سایبر همواره در حال کم‌رنگ شدن است چرا که با پیشرفت فن‌آوری فضای سایبر در سراسر شئون زندگی ایفای نقش می‌کند. از این رو می‌توان گفت مرزها در کارکردهای مجازی، روندی پس‌گرایانه دارند؛ به عبارتی از مرز به سوی سرحدات و از سوی سرحدات تا محو شدن آن حرکت می‌کنند. فضای سایبر کم‌رنگ‌کننده مرزهای میان واقعیت و مجازی، عمومیت و اختصاصی، مکان و مکان‌زدایی، طبیعی و تکنولوژیکی، ذهنی و جسمی، زندگی و مرگ و سرشت و فرهنگ، در اغلب سطوح است (Dodge & kitchen, ۲۰۰۱: ۲۰۵).

۲- مرز میان توانایی کارکرد بازیگران در صحنه جغرافیای سایبر در واقع اهمیت قدرت فن‌آورانه را مطرح می‌سازد؛ این‌که چگونه به کارگیری فن‌آوری موجب تمایزها می‌شود؛ همان‌گونه که عوامل قدرت‌بخش در جغرافیای واقعی، مرزهایی را میان بازیگران مشخص می‌سازند.

۴-۵- دولت - ملت در جغرافیای سایبر آینده

تصوری از شکل آینده دولت - ملت‌ها، بستگی به فاکتورهایی بسیار (با توجه به وضعیت جغرافیایی آن‌ها) خواهد داشت و فعالیت یا رکود آن‌ها تقریباً با ابهام مواجه است. تبیین وضعیت تقریبی پنج‌هزار ملت در سرتاسر جهان تحت استعاره «جهان چهارم» با اثرگذاری جغرافیای سایبر ناممکن به نظر می‌رسد. جهان چهارم از قبل بوده و مقاومت خود را ادامه داده است؛ چنان‌که در طول تاریخ ملل، کشورهای مدرن را در پهنه جهانی به وجود آورده است (عزتی، ۱۳۸۶: ۹۵). اما امروزه دستیابی به فن‌آوری و وابستگی شدید به آن، علاقه به خاک را کاهش داده و گرایش انسان‌ها را به ریشه‌های تاریخی - ملی خود ضعیف کرده است. سند

این گفته، مهاجرت گسترده (به‌ویژه نخبگان) از جوامع در حال توسعه یا بازمانده و نیز میل به بین‌المللی شدن به جای تکیه بر سازه‌های محلی یا منطقه‌ای است. فراملیتی شدن در حال تقویت است و از این رو تداخل نژادها و فرهنگ‌ها در سطح جهان رو به فزونی است. این تغییر و تحولات بیانگر ادغام در جامعه شبکه‌ای بزرگ سایبر است.

هر چند تلاش‌هایی نیز برای حفظ هویت‌ها و فرهنگ‌های محلی در حال انجام است که باید گفت همواره به رقابت با فرهنگ حاکم برخاسته است و برای جلب گروه‌های همفکر در این عرصه جغرافیایی می‌کوشد. فضای سایبر، از گذشته، محلی برای هزاران نفر از گروه‌های مردمی بوده که همدیگر را ملاقات و اطلاعاتشان را به اشتراک می‌گذارند. برخی از این گروه‌ها بزرگ و هم توسعه‌یافته هستند و تنها انتقادی که بر آن‌ها وارد می‌کنند این است که جامعه واقعی نیستند (Bell, 2001: 97). شکل‌گیری چنین جوامعی با این کیفیت، دگرگون‌کننده روابط فرهنگی در جوامع سنتی است. این روابط فرهنگی یکی از مهمترین شکل‌دهنده‌های پیدایش ملت‌ها محسوب می‌شود که در فرهنگ سایبر^۱ متحول می‌شوند. بخش دوم مسأله تحرکات دولت-ملت‌های فعلی برای گریختن از پی‌آمدهای این ادغام است که در دو حالت تلاش و تدافع بروز می‌کند. به‌نظر می‌رسد رشد جوامع شبکه‌ای، تلاش‌ها را برای نیل به دولت-ملت‌های سرزمینی کاهش دهد و از سوی دیگر جوامع پرشمار مجازی را در محیط سایبر سازماندهی کند که در واقع به نحو دیگری به دنبال اهداف خود هستند. بنابراین اگر چه رشد فن‌آوری به‌ویژه در حوزه سایبر ابزارها و امکانات بسیاری را برای توسعه فعالیت‌های دولت-ملت‌ها خلق کرده است و آنان نیز به فراخور اهداف خود از آن بهره می‌گیرند اما رقابت‌های موجود در این فضا باعث ظهور خرده فرهنگ‌های سایبری و در صورت تداوم تشکیل جوامع فرهنگی سایبری خواهد شد که به خودی خود دغدغه‌ای بیش از سرزمین خواهند داشت.

۴-۶- فضای سایبر و حاکمیت

زمانی که فضایی دارای مرزهای معین نباشد به خودی خود کنترل آن نیز مشکل خواهد بود. فضای سایبر نیز از این شیوه مستثنی نیست چرا که با توجه به پیوستگی جهانی و شبکه‌ای شدن روابط، اعمال کنترل را به‌ویژه از سوی دولت‌ها در این فضا با چالش مواجه ساخته است. از سوی دیگر اصولاً فضای سایبر مفهوم حاکمیت را نیز دچار چالش می‌کند زیرا رابطه مستقیمی میان محدودیت - چه در ابعاد فیزیکی یا ابعاد مجازی - با حاکمیت وجود دارد و می‌توان در جغرافیای واقعی اثرات این محدودیت و مرزبندی‌های ناشی از آن را دید؛ اما در جغرافیای فضای مجازی که بر پایه تبادل آزاد اطلاعات شکل گرفته، محدودیت‌ها از طریق مناسبات حقوقی دنبال می‌شوند. با این حال کنترل فضا و مکان امری بدیهی در وظایف حاکمیتی دولت‌ها است. واژگانی چون: مردم‌سالاری، آزادی، حقوق بشر، تروریسم، حمایت از محیط زیست، حقوق زنان، حمایت از کودکان و... همواره در جغرافیای سیاسی نقش به‌سزایی را ایفا می‌کنند. اما در عین حال تعریف هر یک از آن واژگان چه برای دولت‌ها و چه برای گروه‌ها و جوامع اجتماعی متفاوت است. این تفاوت ریشه در کارکردها و مقاصد گوناگون آنان در صحنه روابط اجتماعی است. مردم‌سالاری نمونه مناسبی از این چالش‌هاست. هر چند هیچ تعریف جامع و جهان‌شمولی از مردم‌سالاری وجود ندارد اما نقش‌آفرینی آن در جوامع توسعه‌یافته منجر به ثبات کشور، اما در کشورهای ضعیف‌تر فعالیت در راستای مردم‌سالاری منجر به تزلزل ثبات کشور می‌شود؛ بنابراین چنین دولت‌هایی به‌شدت بر دسترسی به اینترنت نظارت می‌کنند. (Everard, ۲۰۰۰: ۴۴). دولت‌ها نمی‌توانند بر فضای سایبر اعمال حاکمیت تام داشته باشند زیرا فراگیری گسترده فضای سایبر و نقش‌آفرینی بازیگران غیر دولتی این امکان را از دولت‌ها گرفته است. دولت‌ها تنها توانایی اعمال نفوذ بر دامنه‌های اینترنتی ملی خود را دارند؛ آن‌هم به شرطی که بسترهای فنی آن را خودشان ارایه دهند. از دیگر نگاه، دولت‌ها تنها می‌توانند بر اینترنت نظارت داشته باشند و دسترسی به آن را از طرق مختلف محدود کنند اما جهت‌گیری‌های مخالف و منتقد را نمی‌توانند به کنترل خویش درآورند. آنان تنها می‌توانند در قلمرو

سرزمینی خود جریان‌ها را نظارت و راهبری کنند؛ هر چند که آن نیز به‌طور مطلق امکان‌پذیر نیست. تحولات حاکمیت در فضای سایبر به‌شکلی یکسان در جریان نیست؛ یعنی با توجه به الگوهای نهادینه‌شده حاکمیتی تلاش برای نظارت و کنترل جریان‌ها و حتی دولت-ملت‌ها با تنوع مواجه خواهد بود (کاستلز، ۱۳۸۵: ۴۰۹). این الگو به‌خودی‌خود در سرتاسر جهان یکسان نیست. چه بسا حاکمیت و ملت در نزاع و کشمکش درونی به سر برند و در نتیجه عرصه فضای سایبر به جدل‌ها و تنش‌های میان آنان بدل خواهد شد. بنابراین با توجه به روابط میان حاکمیت و فضای سایبر در آینده توسعه و نفوذ این فضا ابعاد حاکمیتی را کمی کمرنگ‌تر خواهد کرد. البته از سوی دیگر رقابت‌ها در فضای سایبر از جانب بازیگران دولتی و غیر دولتی تشدید خواهد شد. فضای مجازی و شبکه جهانی اینترنت به‌دلیل ماهیت عملکردی فراکشوری و نیز قابلیت برقراری ارتباط و جابه‌جایی اطلاعات و داده در مقیاس جهانی و اتصال کاربران و مردمان از سراسر جهان، صرف نظر از ملیت، قومیت، مذهب، نژاد، زبان و... عملاً در تعارض با منافع حکومت‌ها و کشورها و دولت‌های ملی قرار می‌گیرد. به‌عبارتی فضای مجازی و شبکه اینترنت، قدرت حکومت‌ها و دولت‌های ملی و نیز حاکمیت آن‌ها را بر فضای ملی به چالش می‌کشد. این خاصیت فضای مجازی می‌تواند به زایش و رشد نیروهای ضد حکومتی، کاهش مقبولیت حکومت‌ها نزد شهروندان، افزایش قدرت مانور نیروهای ضد حکومتی چه در مقیاس شهروندی و فضای ملی و چه در مقیاس فراکشوری و جهانی و به‌طور کلی امکان تهدید، تضعیف، سقوط و جابه‌جایی دولت‌ها و حکومت‌های ملی و ارزش‌های مورد نظر آن‌ها و جایگزینی نیروهای رقیب و نیز کاهش اقتدار حاکمیتی آنان بیانجامد.

از این‌رو حکومت‌ها و دولت‌های ملی به تکاپو افتاده‌اند تا از پس این چالش برآیند و تهدیدها را بر علیه خود کاهش دهند یا آن‌ها را از میان بردارند. آنان گاهی تهدیدها را علیه خود به تهدید علیه امنیت ملی تعبیر، تفسیر و معنی می‌کنند و از آن علیه نیروهای رقیب و ضد خودشان استفاده می‌کنند. بنابراین حکومت‌ها و دولت‌ها و نیروهای ضد آن‌ها (چه با مبدأ و مقیاس ملی و چه با مبدأ و مقیاس فراکشوری و جهانی) در فضای مجازی و بر سر فرصت‌ها و قابلیت‌های آن با یکدیگر به رقابت و نبرد می‌پردازند و همدیگر را به چالش می‌کشند.

نیروهای ضد حکومتی، حکومت‌ها را به دیکتاتوری، سانسور اخبار و اطلاعات، ستم به شهروندان و نقض حقوق شهروندی و یا جلوگیری از حق دسترسی آزاد به اطلاعات متهم می‌کنند و از همه ظرفیت‌های فضای مجازی نظیر سایت‌ها، پیام‌های کوتاه تلفن همراه، وبلاگ‌ها، ای‌میل‌ها، شبکه‌های اجتماعی و... برای تبلیغات و رساندن پیام‌ها و نظرات خود به گوش هموطنانشان و نیز جهانیان و کسب هواداری بهره می‌برند.

حکومت‌ها و دولت‌ها نیز در نقطه مقابل معمولاً نیروهای ضد حکومتی و کارهای آن‌ها را برهم‌زننده امنیت ملی، عامل بیگانگی، تخریب ارزش‌های ملی و اخلاقی و آسیب‌رسان به سلامت اجتماعی و عمومی و فرهنگی دانسته و به اشکال مختلف سعی بر محدود کردن یا بی‌اثر ساختن کارها و کوشش‌های آنان و نیز تبلیغ علیه آن‌ها را دارند. آنان برای رسیدن به اهداف خود از روش‌های مختلف استفاده می‌کنند. یکی از روش‌های مورد استفاده حکومت‌ها فیلترینگ اطلاعات است؛ یعنی به کاربردن تکنیک‌هایی که دسترسی به اطلاعات مورد نظر در اینترنت را ناممکن می‌سازد. فیلترینگ به دو شکل انجام می‌شود؛ مسدود کردن نشانی‌ها و مسیرهای دست‌یابی در نقاط کنترل شبکه و نیز تحلیل محتوا و کنترل دسترسی به اطلاعات از طریق شمول واژگان کلیدی خاص در وب‌سایت‌ها. نیروهای ضد حکومتی نیز از روش‌ها و تکنیک‌های ضد فیلترینگ استفاده می‌کنند. آن‌ها همچنین از طریق هکرها و ویروس‌ها در فضای مجازی علیه همدیگر دست به اقدامات تهاجمی همچون حمله، نفوذ، تخریب و... می‌زنند. روش دیگری که حکومت‌ها برای پاسداری از حاکمیت خود در فضای ملی استفاده می‌کنند تدوین و تصویب قوانین برای فضای مجازی و شبکه اینترنت است که به قوانین جرم‌های اینترنتی نیز شناخته می‌شود. در این روش تنها به جلوگیری و سانسور اطلاعات بسنده نمی‌کنند، بلکه با کاربران خطا کار (به‌زعم حکومت‌ها)، چه آن‌که مجرم، تروریست، مهاجم یا... تلقی شوند برخورد می‌شود و نسبت به مجازات آن‌ها با استفاده از ابزارهای قانونی و حقوقی خود اقدام می‌کنند. بر اساس مطالعات انجام‌یافته، رفتار حکومت‌ها نسبت به فیلترینگ و سانسور اطلاعات در فضای مجازی از دیدگاه محتوا یکسان نیست. برخی از کشورها (مانند سنگاپور) بر فیلترینگ گنجانده‌های اجتماعی تأکید دارند، برخی

(همچون اردن) بر فیلترینگ درون‌مایه سیاسی و برخی (چون: هند و کره جنوبی) بر فیلترینگ محتواهای امنیتی تأکید دارند و برخی نیز دو یا سه نوع از محتواهای نام‌برده را مورد هدف فیلترینگ قرار می‌دهند (حافظ‌نیا، ۱۳۹۰: ۱۱-۱۳).

۵- تجزیه و تحلیل

۵-۱- تهدیدها و چالش‌ها در فضای سایبر

فضای سایبر دربرگیرنده مجموعه‌ای وسیع از داده‌ها و اطلاعات است که امروزه فضای فعالیت را برای دسته‌های مختلف بازیگران در این عرصه فراهم ساخته است. همان‌گونه که در جغرافیای واقعی تهدیدها، فرصت‌ها و چالش‌هایی برای گروه‌های مختلف انسانی وجود دارد در جغرافیای سایبر نیز عرصه این دسته از فعالیت‌ها منابع سخت‌افزاری و نرم‌افزاری را در سایه خود قرار می‌دهد. با توجه به این که کسب اطلاعات در روزگار نانو منجر به افزایش قدرت و از اهمیت خاصی برخوردار شده است، بنابراین حفاظت از اطلاعات و منابع اطلاعاتی از اهمیت بسیار برخوردار می‌شود. با این حال بررسی تهدیدها و چالش‌ها در جغرافیای سایبر علاوه بر ابعاد فن‌آورانه و اطلاعاتی برای دولت‌ها، سازمان‌ها و گروه‌ها و نیز افراد، در حوزه اجتماعی نیز مسائلی را بازگو می‌کند. تهدیدها و آسیب‌پذیری‌ها به لحاظ حمله‌های سایبری در پنج سطح تقسیم‌بندی می‌شوند:

- ۱- کاربران خانگی و تجارت‌های کوچک.
- ۲- سازمان‌های اقتصادی بزرگ.
- ۳- نواحی بحرانی تأسیسات زیربنایی.
- ۴- آسیب‌پذیری در حوزه ملی.
- ۵- تهدیدهای جهانی.

۱- **کاربران خانگی / تجارت‌های کوچک.** بیش‌تر رایانه‌های خانگی و شبکه‌های تجارت کوچک که در قالب تجارت محلی سازماندهی می‌شوند جزو بی‌دفاع‌ترین و آسیب‌پذیرترین سطوح فعالان سایبر به حساب می‌آیند. در واقع مشترکان با اتصال به

خط اشتراک دیجیتال^۱ یا اتصالات کابلی می‌توانند از مزایای آن بهره‌گیرند و حمله‌کنندگان کسانی هستند که بدون آگاهی کاربران اصلی از اطلاعات آنان استفاده می‌کنند. نفوذگران با ورود به شبکه‌های کاربران شخصی یا حوزه تجارت‌های کوچک از داده‌ها و بانک اطلاعاتی آنان برای منافع شخصی خود بهره‌می‌برند.

۲- **سازمان‌های اقتصادی بزرگ.** بیش‌تر تشکیلات اقتصادی بزرگ (مانند: شرکت‌ها، نمایندگی‌های دولتی و دانشگاه‌ها) اهداف متداولی برای حمله‌های سایبری محسوب می‌شوند. بسیاری از سازمان‌های اقتصادی بخش مهمی از زیرساخت‌های مهم کشور هستند. از این‌رو لازم است این تشکیلات سیاست‌ها و برنامه‌های امنیت اطلاعاتی خود را برای رسیدن به امنیت لازم در حوزه سایبر برنامه‌ریزی کنند (۷: ۲۰۰۳، The white house). حمله‌کنندگان به چنین مراکزی یا دارای اهداف اقتصادی برای جمع‌آوری اطلاعات مالی هستند یا دارای اهداف سیاسی به انگیزه ضربه‌زدن به زیرساخت‌های اقتصادی.

۳- **بخش‌های بحرانی تأسیسات زیربنایی.** اگر سازمان‌ها در بخش‌های اقتصادی، دولتی یا واحدهای دانشگاهی دارای مشکلات امنیتی سایبر باشند توجه حمله‌کنندگان را به خود جلب می‌کنند. ضربه‌زدن به ساختار اقتصادی، سرقت اطلاعات و بانک‌های اطلاعاتی و تخریب فعالیت‌های جاری این دسته از بخش‌ها و تأسیسات از اهداف حمله‌کنندگان است. هزینه تأمین امنیت سایبری در چنین بخش‌هایی بسیار گزاف است و باید سیستم امنیتی آن‌ها همواره به‌روز باشد تا در مقابل حمله‌های نفوذگران آسیب‌پذیری کمتری داشته باشند.

۴- **موضوع‌های ملی و قابلیت آسیب‌پذیری.** برخی از مشکلات امنیتی سایبر دلالت بر ملی بودن آن دارد که نمی‌تواند به‌وسیله شرکت‌های خصوصی با بخش‌های زیربنایی به‌تنهایی مرتفع شود. همه بخش‌ها به‌طور مشترک در اینترنت حضور دارند و از آن بهره‌می‌گیرند بنابراین همه آن‌ها در ریسک مکانیسمی آن (مانند: پروتکل‌ها^۲ و

۱ - Digital subscriber line (DSL)

۲ - Protocols

روترها^۱ ایمن نیستند. ضعف در بسیاری از موارد از به کارگیری نرم‌افزار و سخت‌افزار تولیدشده می‌تواند مشکلاتی را در سطح ملی ایجاد کند که نیازمند به فعالیت‌های هماهنگ برای تحقیق و توسعه بهبود تکنولوژی‌ها است. علاوه بر آن فقدان آموزش و تأیید حرفه ای امنیتی سایبر در سطح ملی دارای مزیت و اهمیت است.

۵ - تهدیدهای جهانی. استانداردهای مشترک جهانی همکاری میان سیستم‌های رایانه‌ای جهانی را شدنی می‌سازد. به هم پیوستگی و درهم‌تنیدگی شبکه‌های رایانه‌ای در جهان این فرصت را به وجود آورده است که حمله‌کنندگان علیه چارچوب‌های ساختارمند جهانی اقدام کنند و باعث وارد آمدن ضربات شدیدی به نظام شبکه‌ای شوند. می‌توان از حمله‌های سایبری گروه‌های تروریستی در این باره یاد کرد.

برای تبیین شکل‌های فیزیکی تهدیدات و چالش‌های فضای سایبر که همواره توسط نفوذگران در حال تهدید است، جدول ۲ مشروحي از منابع تهدیدها، انگیزه‌ها و اقدام‌های تهدیدآمیز را گزارش می‌دهد. سطوح دربرگیرنده تهدیدهای سایبری، توانایی نفوذ در عرصه جغرافیای سایبر را مطرح می‌کند که پی‌آمدهای خسارت‌بار آن می‌تواند چالش‌های جدی برای افراد، سازمان‌ها و دولت‌ها به بار آورد. این دسته از حمله‌ها (چنانچه بستر فضای شبکه‌ای در جوامع فراهم باشد) می‌توانند در صورت نبود تدبیر به موقع و ارتقای امنیت شبکه، آسیب‌های به‌مراتب سنگین‌تر از یک جنگ در جغرافیای حقیقی را در پی داشته باشند.

جدول ۲: تهدیدهای انسانی، منابع تهدیدها، انگیزش و اقدامهای تهدیدآمیز

منابع تهدید	انگیزه	اقدامهای تهدیدآمیز
هکر ^۱ - کراکر ^۲	چالش‌های سرکش نفسانی	هک کردن، مهندسی اجتماعی نفوذ سیستمی، ورود با اجبار دسترسی غیر مجاز سیستمی
جنایتکار رایانه‌ای ^۳	خرابی اطلاعات، افشای غیر قانونی اطلاعات منافع مالی، تغییر غیر مجاز داده‌ها	جنایت (بزهکاری) رایانه‌ای (مانند کمین سایبری) فعالیت کلاهبرداری (مانند برگرداندن و جعل هویت، رهگیری) ارتشای اطلاعاتی، حقه‌بازی، تجاوز سیستمی
تروریست	نامه‌های الکترونیکی سیاه ^۴ ، تخریب بهره‌برداری، انتقام	بمباران [اطلاعاتی] / تروریسم جنگ اطلاعاتی، حمله‌های سیستمی (مانند: DDos) نفوذ سیستمی، مداخله سیستمی
جاسوسی صنعتی (کمپانی‌ها، مؤسسه‌های دولتی و دیگر منافع دولتی)	مزایای رقابتی، جاسوسی اقتصادی	بهره‌برداری اقتصادی سرقت اطلاعاتی، تجاوز به حریم خصوصی مهندسی اجتماعی، نفوذ سیستمی دسترسی غیر مجاز سیستمی (دسترسی به مطالب طبقه‌بندی شده اختصاصی یا تکنولوژی - روابط اطلاعاتی)
کارمندان داخلی (نارضایتی، آموزش ضعیف، ناخشنودی، بداندیشی، بی‌دقتی، پایان‌کنار یک کارمند)	کنجکاوی، زیرکی، منافع مالی کینه‌جویی، اشتباه‌های غیر عمدی و از قلم افتادگی (مانند: اشتباه در ورود اطلاعات، اشتباه در برنامه‌نویسی)	حمله یک کارمند، نامه الکترونیکی سیاه باز کردن اطلاعات خصوصی، سوء استفاده رایانه‌ای فریب و سرقت، ارتشای اطلاعاتی وارد کردن داده دست‌کاری شده، داده خراب جاسوسی، کدهای خرابکاری (مانند: ویروس‌ها، بمب‌های هوشمند، اسب تروجان)، فروش اطلاعات شخصی اشکالات سیستمی، تجاوز سیستمی خرابکاری سیستمی، دسترسی غیر مجاز به اطلاعات

(US Army Training and Doctrine Command & other, ۲۰۰۵: II-۷&۸)

از سوی دیگر، تهدیدها به‌ویژه برای حاکمیت، همانا تشکیل و تأثیرهای جوامع اجتماعی شبکه‌ای و کارکردهای ناشی از آن در جغرافیای سایبر است. فضای سایبر آشکارگر آزادی

۱ - Hacker

۲ - Cracker

۳ - Computer criminal

۴ - Black email

۵ - یک حمله سایبری که در آن، کراکر یک هدف رایانه‌ای را با هزاران سیگنال جعلی اطلاعاتی (که موجب خروج رایانه از صحنه می‌شود) بمباران می‌کند (۱۰۲: ۲۰۰۶: Schell & Mortni).

مطلق بیان است؛ از این رو افراد و گروه‌های موافق و مخالف سیاست‌های دولت می‌توانند از آن برای دستیابی به اهداف خود استفاده کنند. به وجود آمدن جوامع اجتماعی شبکه‌ای همانند Twitter، facebook و... و عضویت بسیاری از مردم در آن‌ها و نیز شکل گرفتن گروه‌های مختلف اجتماعی که اهداف سیاسی یا فرهنگی را دنبال می‌کنند، می‌تواند سیاست‌های دولت‌ها را به‌ویژه در کشورهای بازمانده یا در حال توسعه دچار چالش سازد. این مسایل به‌ویژه در کشورهایی که دارای قوم‌های بسیارند یا به‌لحاظ دموکراسی دچار ضعف هستند، تشدید می‌شوند. شبکه‌های اجتماعی این امکان را فراهم می‌آورند تا دوستان، همفکران، هم‌حزب‌ها و کسانی که دارای عقاید و دیدگاه‌های مشترک هستند به سرعت همدیگر را بیابند و تبادل نظر و برنامه‌کنندگی کاری که شاید در جغرافیای واقعی با محدودیت‌ها و موانعی روبه‌روست. در واقع حاکمیت در صورتی که در یابد فعالیت‌هایی از این دست مشروعیت او را دچار چالش می‌سازد اقدام به محدودیت دسترسی یا بستن چنین دامنه‌هایی می‌کند؛ که آن نیز با توجه به پیشرفت یا حمایت‌های خارجی اثر زیادی نخواهد داشت. باری؛ حاکمیت برای کاهش ابعاد تهدیدهای اجتماعی باید به رقابت در چنین محیطی اقدام کند؛ چرا که به کاربردن ابزارهای محدودکننده و بازدارنده تنها بازخورد منفی دربر خواهد داشت. نمونه این گونه از اقدام‌ها را می‌توان در چین و ایران ملاحظه کرد.

۶- نتیجه‌گیری

جغرافیای سایبر دربرگیرنده مجموعه فضاهایی است که ارتباطات و روابط در آن از پیچیدگی بسیاری برخوردار است. این فضا علاوه بر دارا بودن محیطی جغرافیایی که در قالب جغرافیای مجازی بررسی می‌شود، برخوردار از حاکمیت عنصر زمان و نیز شبکه‌های ارتباطی رایانه‌ای نیز هست؛ که در واقع ارتباط‌دهنده میلیاردها نفر در سرتاسر جهان بدون محدودیت‌های جغرافیای واقعی است. میل انسان به برخوردار بودن از آن چیزهایی که در واقعیت گردآوری آن‌ها با موانع پرشماری مواجه است باعث تبدیل یک رویا به واقعیت شد. بنابراین جغرافیای فضای مجازی افق مکاتب جغرافیایی را در آینده دچار دگرگونی خواهد کرد و این مبحث با توجه به پویایی ذاتی جغرافیای سیاسی، ورود این گرایش را به

این حوزه امری بدیهی می‌سازد. به‌ویژه با توجه به این که قلمروخواهی در این جغرافیا نیز مفهوم پیدا کرده است و بازیگران با بهره‌گیری از ابزارهای تکنولوژیک از حوزه‌های واقعی در محیط سایبر نقش آفرینی می‌کنند. حاکمیت بر فضای سایبر امر مطلق نیست که دولت یا گروه‌هایی بتوانند مدعی آن شوند. بنابراین در این محیط شبکه‌ای، فاکتورهای زیادی می‌توانند ایفای نقش کنند و رقابت‌های حاصله می‌تواند در جذب شهروندان این جغرافیای جدید مؤثر باشد؛ زیرا مصداق دهکده جهانی درهم آمیختگی فن‌آوری و دیدگاه‌های انسانی فارغ از مرزهای طبیعی است.

همان‌گونه که در جغرافیای واقعی تهدیدها و چالش‌هایی متوجه حاکمیت است باید اذعان داشت که در جغرافیای سایبر تهدیدها و چالش‌های به‌مراتب پیچیده‌تری وجود دارد که می‌تواند هزینه‌های بسیاری را به دولت‌ها و ملت‌ها تحمیل کند. بی‌گمان کشورهایی که ریشه‌های عمیقی در فضای سایبر و شبکه‌ای ساختن کارهای خود دارند از یک سو توانمندی‌های ویژه‌ای نیز در این باره دارند و از سوی دیگر با مشکلات خاصی به‌ویژه در رویارویی با تروریست‌های سایبری، نفوذگرها و حمله‌کنندگان و... دست و پنجه نرم می‌کنند. از دیگر سو، کشورهایی که کمتر در پیوستن به فضای سایبر موفق بوده‌اند یا تلاش کرده‌اند، از بسیاری از مزایای این فضا محروم هستند و البته تهدیدهای امنیتی آنان نیز در حمله به بانک‌های اطلاعاتی کاهش می‌یابد. تهدیدهای حاکمیت و فضای سایبر در جدول ۳ به نمایش درآمده است.

جدول ۳: تهدیدهای حاکمیت و فضای سایبر

تهدیدهای سایبری	عملکرد حاکمیت‌ها
گشایش پنجره‌های نوین ارتباطی میان ملت‌ها	شکل‌گیری چالش‌های نوین حاکمیتی
تغییر الگوی روابط، افزایش خودآگاهی‌ها و ظهور بازیگران جدید	تدوین راهبرد سایبری متناسب با راهبردی ژئوپلیتیکی
اقدام‌های مقاومتی از استفاده روزافزون از فیلتر شکن‌ها و...	اقدام‌های کنترلی در چهارچوب فیلترینگ و جنگ‌های سایبری
چالش‌های پنج‌گانه: کاربران خانگی و تجارت‌های کوچک سازمان‌های اقتصادی بزرگ	فیلترینگ محتوایی، فیلترینگ امنیتی، فیلترینگ سیاسی

منابع

- ۱- احمدی نیاز، حسین (۱۳۸۵)؛ نقش سازمان‌های بین‌المللی بر حاکمیت دولتها، تهران: محل نشر پرتو بیان.
- ۲- حافظ‌نیا، محمدرضا (۱۳۹۰)؛ مفهوم‌سازی ژئوپلیتیک اینترنت و فضای مجازی، فصلنامه ژئوپلیتیک، سال هفتم، شماره اول، صص ۱۳-۱.
- ۳- رجایی، فرهنگ؛ پدیده جهانی شدن - وضعیت بشری و تمدن اطلاعاتی، ترجمه عبدالحسین آذرنگ (۱۳۸۲)؛ چاپ دوم، تهران: محل نشر آگاه.
- ۴- شکوئی، حسین (۱۳۸۲)؛ اندیشه‌های نو فلسفه جغرافیا، جلد ۱، چاپ ششم، تهران: محل نشر گیتاشناسی.
- ۵- عزت‌الله (۱۳۸۶)؛ نظریه‌های جدید جغرافیای سیاسی، تهران: محل نشر قومس.
- ۶- کاستلز، امانوئل؛ اقتصاد، جامعه و فرهنگ عصر اطلاعات - پایان هزاره، ترجمه: احد قلیقلیان و افشین خاکباز (۱۳۸۵)؛ جلد سوم، چاپ پنجم، تهران: محل نشر طرح نو.
- ۷- روشن، علی‌اصغر و نورالله فرهادیان (۱۳۸۵)؛ فرهنگ اصطلاحات جغرافیای سیاسی - نظامی، تهران: محل نشر مؤسسه چاپ و محل نشر دانشگاه امام حسین (ع).
- ۸- مجتهدزاده، پیروز و حافظ‌نیا محمدرضا (۱۳۸۷)؛ برابرسازی معنایی واژگان جغرافیای سیاسی، فصلنامه ژئوپلیتیک، سال چهارم، شماره اول، صص ۸-۱.
- ۹- Armitage, John & Joanne Roberts (۲۰۰۲) living with Cyberspace: Technology & Society in the ۲۱st Century, Continuum publishing.
- ۱۰- Bell, D. (۲۰۰۹) International Encyclopedia of human geography, article: cyberspace/cyber culture, ed: authors, vol ۲, Elsevier publication.
- ۱۱- Bell, David (۲۰۰۱) An Introduction to cyber culture, Rutledge publication.
- ۱۲- Blacksell, Mark (۲۰۰۶) Political geography, Blackwell publishing
- ۱۳- Coleman, M. (۲۰۰۹) International encyclopedia of human geography, ed: authors, article: Sovereignty, vol ۱۰, Elsevier publication
- ۱۴- Cox, Kevin & others (۲۰۰۸). The SAGE Handbook of Political Geography. SAGE Publication, London, UK.

- ۱۵-Cresswe,T(۲۰۰۹) International Encyclopedia of Human geography, edit by author's, Article: Place, vol ۸, Elsevier publication.
- ۱۶-Davies, Karen (۲۰۰۱)Timespace -geographies of temporality ,ed: Jon May and Nigel Thrift ,article : Responsibility and daily life: reflections over timespace, Rutledge publishing.
- ۱۷-Dodge, Martin (۱۹۹۹) the geography of cyberspace, Centre for Advanced Spatial Analysis, <http://www.casa.ucl.ac.uk/cyberspace.pdf>.
- ۱۸-Dodge, Martin & Rob kitchen (۲۰۰۱) Mapping Cyberspace, Rutledge publication.
- ۱۹-Elden, S (۲۰۰۹) International Encyclopedia of human geography, article: Space, ed: authors, vol ۱۰, Elsevier publication.
- ۲۰-Everard, Jerry (۲۰۰۰) Virtual StatesThe Internet and the boundaries of the nation-state, Rutledge publication.
- ۲۱-Everett, Anna (۲۰۰۹) Digital diaspora a Race for Cyberspace, State University of New York Press publication, Albany.
- ۲۲-Frissen ,paul (۱۹۹۷)The governance of cyberspace ,ed: Brine D, Loader , article: The virtual state Postmodernisation, information and public administration ,Rutledge published.
- ۲۳-Herrea, Geoffrey L.(۲۰۰۷)Power and security in the information age ,ed: author's ,article: Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space, ashgate publication.
- ۲۴-MacColl, R.W(۲۰۰۵) Encyclopedia of World geography, Facts On File publication.
- ۲۵-Mosco,Vincent(۲۰۰۴)The Digital Sublime Myth, Power, and Cyberspace, Massachusetts Institute of Technology publication.
- ۲۶-Schell, Bernadette& Clemens Martin(۲۰۰۶)Webster's New World Hacker Dictionary, Wiley Publishing
- ۲۷-Staebeli,laynn A(۲۰۰۳) A companion to political geography ,ed: john agnew - katharyne Mitchell -Gerard toal, article: place ,Blackwell publishing.
- ۲۸-Storey,D(۲۰۰۹)International Encyclopedia of Human geography ,edit by authores, Article: Political geography, vol ۸, Elsevier publication.
- ۲۹-The white house(۲۰۰۳)The national Strategy to secure cyberspace, Washington
- ۳۰-US Army Training and Doctrine Command& other (۲۰۰۵) a military Guide to terrorism in Twenty – First Century: www.hsdec.org.