فصلنامه علمی امنیت ملی
سال سیزدهم، شماره چهل و هفتم، بهار ۱۴۰۲
مقاله اول از صفحات ۹-۳۶

مقاله پژوهشی: گونه‌شناسی مفهوم و عناصر اصلی فضای سایبر در اسناد راهبردی امنیت سایبری ملی کشورهای منتخب

۲۰.۱۰۰۱.۱.۳۳۲۹۲۵۳۸.۱۴۰۲.۱۳.۴۷.۱.۵

محمد رضا کریمی قهرودی[۱]، شیما معین آزاد[۲] و ابراهیم کریمی قهرودی[۳]

تاریخ دریافت:۱۴۰۰/۰۴/۲۹ تاریخ پذیرش:۱۴۰۱/۰۱/۲۴

چکیده

مفهوم‌شناسی و تعیین عناصر اصلی فضای سایبر دغدغه بسیاری از اندیشمندان در جهان بوده و سازمان‌ها و مراکز علمی کشورهای مختلف تعاریف گوناگونی برای فضای سایبر و عناصر اصلی آن ارایه داده‌اند، وجود برداشت‌ها و تعاریف متنوع بین‌بازیگران و ذینفعان سبب ایجاد ابهام، پیچیدگی و بروز تعارضات و ناهماهنگی در سیاست‌گذاری‌ها، برنامه‌ریزی‌ها و توسعه و اتلاف منابع در کشورمان شده است.

پژوهش حاضر با هدف گونه‌شناسی مفهوم و عناصر اصلی فضای سایبر انجام شده است. ابتدا ۴۰ سند راهبرد ملی (امنیت) سایبری از ۳۵ کشور جهان که طی افق ده ساله اخیر از سال ۲۰۰۹ تا ۲۰۱۹ منتشر شده‌اند، مورد مطالعه قرار گرفت و در ادامه با رویکرد کیفی و بر اساس روش تحلیل مضمون، مهمترین مضامین پایه، مضامین سازمان دهنده و مضامین فراگیر فضای سایبر و عناصر اصلی آن استخراج شدند، در نتیجه چهار عنصر اصلی و پنج گونه مختلف مفهوم فضای سایبر شناسایی و اشتراکات و افتراقات آنها تعیین شد، سپس کشورهای مختلف بر اساس این گونه‌شناسی گروه‌بندی شدند. بر اساس یافته‌های این پژوهش چهار عنصر اصلی فضای سایبر شامل تجهیزات، داده‌ها، نقش‌ها و عملیات می‌باشند و پنج گونه مفهوم استخراج شده از این ۴۰ سند عبارتند از: ۱- فضای سایبر به عنوان زیرساخت اطلاعاتی و ارتباطی(تجهیزات) ۲- فضای سایبری به عنوان یک زیرساخت اطلاعاتی، ارتباطی و داده‌های موجود در آن ۳- فضای سایبری به عنوان مجموعه‌ای از تجهیزات، داده‌ها و افراد ۴- فضای سایبری به عنوان مجموعه‌ای از تجهیزات، داده‌ها و عملیات ۵- فضای سایبری به عنوان مجموعهٔ جامعی از تجهیزات، داده‌ها، افراد و عملیات.

کلیدواژه‌ها: فضای سایبر، امنیت سایبری ملی، گونه‌شناسی، مفهوم‌شناسی، اسناد راهبردی

[۱]- عضو هیئت علمی دانشگاه صنعتی مالک اشتر (نویسنده مسئول) favad۱۰@gmail.com

[۲] - محقق حوزه سایبر

[۳] - دانشجوی مقطع دکتری دانشگاه عالی دفاع ملی

۱. مقدمه و بیان مسئله

واژه فضای سایبر نخستین بار در سال ۱۹۸۱ توسط ویلیام گیبسون[۱] معرفی شد و از آن زمان تاکنون این مفهوم و عناصر اصلی آن در یک سیر تاریخی توسعه و تکامل یافته‌اند، در ابتدای دهه ۱۹۸۰ این فضا کاملاً مجزا از فضای فیزیکی تلقی می‌شد و در ادامه برخی از اندیشمندان بر این که این فضا کاملاً فیزیکی است تمرکز و توجه کردند. همچنین برخی از اندیشمندان و کشورها بر ابعاد فناوری شامل تجهیزات، ذخیره‌سازی، پردازش و تبادل اطلاعات تمرکز نموده و به ابعاد اجتماعی انسانی این فضا توجهی ندارند، در حالی که برخی دیگر بر کاربران و ابعاد انسانی و اجتماعی این فضا تمرکز نموده‌اند. تا قبل از عصر سایبر هویت انسان به نژاد، قبیله و عرصه جغرافیایی استوار بود و زیست جهان مشهود و نامشهود در مکان و زمان خاص جغرافیایی فرهنگ را تشکیل می‌داد اما با شکل‌گیری و رشد سریع فضای سایبر مفاهیم عرصه زندگی نیز به سمت تغییر ماهوی گام برداشت. (کریمی قهرودی و کیان‌خواه، ۸۲:۱۳۹٤). امروزه این فضا بخش جدایی‌ناپذیر از زندگی مردم را تشکیل می‌دهد و زندگی بشر بیش از پیش با این فضا و مظاهر آن نظیر رسانه‌های اجتماعی، اینترنت و فناوری‌های مرتبط آمیخته شده است و جهان به سرعت و شتاب روزافزون به سمت جامعه سایبری- فیزیکی یا جامعه الحاقی در حرکت است.

سازمان‌ها، مراکز و نهادهای علمی و پژوهشی کشورهای مختلف تاکنون تعاریف و توصیف‌های گوناگونی برای فضای سایبر و عناصر اصلی آن ارایه داده‌اند، وجود برداشت‌ها، توصیف‌ها و تعاریف نسبتاً متنوع در کشورمان سبب ایجاد ابهام، ضعف زبان مشترک، بروز مشکلات، ناهماهنگی و تعارض‌هایی در سیاستگذاری‌ها، تقنین، تقسیم کار ملی، برنامه‌ریزی‌ها و توسعه فضای سایبر و امنیت فضای سایبری و ... در کشور شده است. سازماندهی نامناسب، موازی‌کاری‌ها و پراکنده‌کاری‌ها، ضعف در قاعده‌گذاری‌ها و بروز اختلافات و چالش‌ها در تقسیم کار ملی از جمله شواهد این مساله است. از سوی دیگر از آنجایی که فضای سایبر و فناوری‌های مرتبط با آن توسط کشورهای پیشتاز این حوزه ابداع و توسعه داده شده، بدیهی است که مفاهیم و عناصر اصلی آن برای زیست‌بوم ما نامانوس و دارای ابهام باشد.

بهبود مدیریت و ارتقای حکمرانی و سازماندهی مناسب فضای سایبر در گام اول نیازمند شناخت ظرافت‌ها و پیچیدگی‌ها و تبیین عمیق این فضا و نگاه جامع به عناصر اصلی آن است. وجود خلاء و شکاف اندیشه‌ای در مفهوم‌شناسی این فضا با توجه به کاربرد روزافزون آن در همه عرصه‌های زندگی اعم از دفاعی و ملی؛ محققان این پژوهش را بر این داشت که به هستان‌شناسی و گونه‌شناسی مفهوم و عناصر اصلی فضای سایبر بپردازند.

بررسی پیشینه و سیر تکاملی مفهوم فضای سایبر، شناخت عمیق هستان‌شناسی و پیچیدگی‌های این فضا و شناسایی عناصر اصلی و نگاه جامع به این عناصر، سبب ایجاد زبان مشترک، توجه به توازن و تناسب عناصر و هم‌افزایی بیشتر در برنامه‌ریزی‌ها، سیاست‌گذاری‌ها، تعیین موثرتر اولویت‌ها و تخصیص اثربخش منابع و نیز قاعده‌گذاری‌های موثرتر در این حوزه خواهد شد که پیامد آن جلوگیری از اتلاف و صرفه‌جویی در منابع خواهد بود. علاوه بر این گونه شناسی تعاریف سبب کاهش تکثر و تنوع ٤٠ تعریف در قالب پنج گونه شده و فهم مناسبی

---

۱. William Gibson

از نگاه و رویکرد کشورهای مختلف فراهم نموده و همکاری‌ها و تعاملات فنی- حقوقی و مشارکت و یارگیری در معاهدات جهانی را تسهیل می‌نماید.

بررسی محقق نشان می‌دهد که تاکنون بررسی جامعی از سیر تکاملی مفهوم فضای سایبر و گونه‌شناسی و طبقه‌بندی تعاریف و مفاهیم مختلف و متنوع این فضا و عناصر اصلی آن انجام نشده است. بنابراین سوالات این پژوهش شامل موارد زیر می‌باشد:

سوال اصلی:

- «گونه‌های مختلف مفهوم فضای سایبر و عناصر اصلی آن در اسناد راهبردی کشورهای منتخب کدامند؟»

سوالات فرعی:

- «سیرتکامل تاریخی مفهوم فضای سایبر چگونه است؟»
- «عناصر اصلی فضای سایبر در اسناد راهبردی کشورهای منتخب کدامند؟»
- «چگونه می‌توان مفاهیم مختلف فضای سایبر را دسته‌بندی و گونه‌شناسی نمود؟»
- «هر یک از کشورهای منتخب در کدام گونه جای می‌گیرند؟»

در این مقاله، در ابتدا به مرور پیشینه و سیر تکاملی مفهوم و عناصر اصلی فضای سایبر از سال ۱۹۴۸ به بعد پرداخته می‌شود سپس به عناصر اصلی سازنده فضای سایبر که مبنای دسته‌بندی و گونه‌شناسی این مفهوم در اسناد راهبرد امنیت سایبری کشورها می‌باشند تبیین می‌شود. و در ادامه به روش تحلیل مضمون ۴۰ سند راهبرد امنیت سایبری کشورها مورد تحلیل و پس از استخراج مضامین پایه، محوری و فراگیر، گونه‌های مفاهیم استخراج می‌شوند. و در نهایت کشورهای منتخب بر اساس گونه‌های شناسایی شده طبقه‌بندی شده‌اند.

۲. مبانی نظری پژوهش

۲-۱. مرور پیشینه و سیر تکاملی مفهوم و عناصر اصلی فضای سایبر

واژۀ «سایبر» نخستین بار توسط نوربرت واینر مطرح شد. او در کتاب خود با عنوان سایبرنتیک یا کنترل و ارتباط در حیوانات و ماشین‌ها که در سال ۱۹۴۸ منتشر شد سایبرنتیک را تعریف کرد. واینر معتقد بود افراد می‌توانند به یک ماشین متصل شوند و نظام حاصل می‌تواند محیط جدیدی برای تعامل فراهم کند. این اندیشه اساس شکل‌گیری مفهوم فضای سایبری را تشکیل داد (وینر،۱۹۴۸)[۱].پس از آن، واژۀ «سایبر» یک پیشوند تلقی شد. به عنوان مثال، دولت فنلاند در راهبرد امنیت سایبری خود سایبر را این گونه تعریف کرد: «واژۀ سایبر تقریباً همیشه پیشوندی برای یک واژه یا توصیف‌کننده‌ای برای یک کلمۀ مرکب می‌باشد، نه یک واژۀ مستقل. این واژه اغلب به پردازش داده‌های/ الکترونیکی، فناوری اطلاعات، ارتباطات الکترونیکی (انتقال داده) یا سامانه‌های اطلاعاتی و رایانه‌ای مربوط می‌شود. واژۀ سایبر از واژۀ یونان باستان «کیبریو[۲]» به معنای «راهبری، هدایت یا کنترل کردن» ریشه می‌گیرد[۳]».

واژۀ «فضای سایبری» نخستین بار در سال ۱۹۸۱ توسط ویلیام گیبسون، نویسندۀ آثار علمی تخیلی، در رمان کروم مشتعل[۴] مطرح شد (ویلیام، ۲۰۱۶)[۵]. سپس گیبسون در رمان خود با نام نئورومانسر[۱] که در سال ۱۹۸۴ منتشر شد

---

[۱] Wiener, ۱۹٤۸: ۹-۲٤

[۲] kybereo

[۳] Finland's Cyber Security Strategy,۲۰۱۳:۹-۱۰

[٤] Burning Chrome

[۵] William,۲۰۱٦:۱۱-۳۰

بارها از واژهٔ «فضای سایبری» استفاده کرد و از آنجا که این رمان سه جایزهٔ مهم در حوزهٔ علمی تخیلی را از آن خود کرد این واژه در کل جهان شناخته شد گیبسون اذعان کرد هنگام ساختن واژهٔ «فضای سایبری» از واژهٔ «سایبرنتیک» واینر الهام گرفته است. او در کتاب خود فضای سایبری را این گونه تعریف کرد: «یک تجسم مشترک که روزانه توسط میلیاردها کاربر مجاز در تمام کشورها و توسط کودکانی که به یادگیری مفاهیم ریاضی می‌پردازند تجربه می شود». این تعریف بر برداشت مردم از یک محیط جدید تمرکز می‌کند و هنگامی که از امکان ایجاد یک فضای سایبری در دنیای واقعی خبر می‌دهد، سبب می‌شود تا مردم ویژگی‌های فضای سایبری را احساس کنند.

مفهومی که در دههٔ ۱۹۸۰ پدید آمد، در ابتدا فضایی کاملاً مجزا از دنیای فیزیکی تلقی می‌شد. حتی برخی از نظریه‌پردازان تصریح کردند فضای سایبری از مرزهای جغرافیایی و ملی فراتر می‌رود و از این رو مفهوم سنتی حاکمیت و امنیت را تغییر می‌دهد. افزون بر این، آبراهام ام. دنمارک، در کتاب خود با نام حوزه‌های مشترک مورد اختلاف: آیندهٔ قدرت آمریکا در یک جهان چندقطبی تصریح کرد: امروزه چهار حوزهٔ مشترک جهانی وجود دارد: دریا، هوا، فضا و فضای سایبری (دنمارک و همکاران، ۲۰۱۰)[۲]. هر یک از این حوزه‌های مشترک با حوزه‌های دیگر کاملاً تفاوت دارد. این حوزه‌ها چهار ویژگی عمدهٔ مشترک دارند: (۱) توسط هیچ فرد، نهاد یا کشور منفردی کنترل نمی‌شوند؛ (۲) هنگامی که یکپارچه هستند در مقایسه با زمانی که به قسمت‌های کوچک‌تر تجزیه می‌شوند به میزان بیشتری سودمند هستند؛ (۳) آن دسته از بازیگران کشوری و غیرکشوری که از قابلیت‌های فناورانهٔ لازم برخوردار هستند می‌توانند به آن‌ها دسترسی پیدا کنند و از آن‌ها برای اهداف اقتصادی، سیاسی، علمی و فرهنگی استفاده نمایند؛ و (٤) آن دسته از بازیگران کشوری و غیرکشوری که از قابلیت‌های فناورانهٔ لازم برخوردار هستند می‌توانند از آن‌ها به عنوان ابزاری برای فعالیت نظامی و عرصه‌ای برای نبرد نظامی استفاده کنند. در حال حاضر فضای سایبری بخش جدایی‌ناپذیری از زندگی نوین را تشکیل می‌دهد؛ مردم نقاط مختلف جهان از طریق مجموعه‌ای از پیوندهای شبکه‌شده که کل دنیا را در بر می‌گیرند به تعامل، همکاری و رقابت با یکدیگر می‌پردازند.

فضای سایبری که از تلفیقی از ارتباطات سادهٔ وب‌محور و شبکه‌هایی از زیرساخت‌های پیچیده‌تر تشکیل می‌شود می‌تواند توانایی نهادهای خصوصی و دولتی در زمینهٔ ارائهٔ خدمات ضروری را بهبود بخشد. این شبکه که توسط وزارت دفاع آمریکا شکل گرفته، بستر هیجان‌انگیزی را ایجاد نموده که قابلیت ارائهٔ خدمات متنوع، سریع و جذاب را دارد. خدمات قابل ارائه روی شبکه اینترنت به علت قابلیت ذاتی و فضای قابل رشد شبکه رو به افزایش است (کیان‌خواه، ۱۳۹۷: ۱۵۸).

با این حال، گرِگ راترِی تصریح کرد فضای سایبری یک محیط کاملاً فیزیکی است که از طریق ارتباط سامانه‌ها و شبکه‌های فیزیکی ایجاد می‌گردد و بر اساس قوانینی که در پروتکل‌های نرم‌افزارها و ارتباطات تعریف شده‌اند مدیریت می‌شود تمام این موارد در مرزهای قلمرو کشورها واقع شده‌اند و اگرچه بخش اعظمی از اطلاعات در فضای سایبری عمومی تلقی می‌شوند ولی عناصر فیزیکی این فضا دسکتاپ‌ها، لپ‌تاپ‌ها، سرورها، یخچال‌های اینترنتی، مسیریاب‌ها، تلفن‌ها، تلفن‌های همراه، کابل‌های شبکه، کابل‌های فیبر نوری صاحبان مشخصی دارند (راتری[۳] و همکاران،۲۰۱٦) وولف هاینتشل فان هاینگ، عضو مؤسسهٔ حقوق اروپا واقع در دانشگاه گوتهٔ فرانکفورت،

---

[۱] Neuromancer

[۲] Denmark A, et.al, ۲۰۱۰.

[۳] Rattray, et.al, ۲۰۱٦:۱۲-۳۱

خاطرنشان ساخت: فضای سایبری مستلزم یک معماری فیزیکی است؛ تجهیزات متصل به یک شبکهٔ انتقال انحصاری معمولاً در درون قلمرو یک کشور واقع شده‌اند؛ این تجهیزات به دولت یا شرکت‌ها تعلق دارند؛ ادغام عناصر فیزیکی سایبر که در قلمرو یک کشور واقع شده‌اند در «حوزهٔ جهانیِ» فضای سایبری نباید نادیده‌گیری حاکمیت آن کشور بر قلمرو خود پنداشته شود (ولف،۲۰۱۳)[۱]. از سال ۱۹۸٤ تاکنون، کارشناسان زیادی تلاش کرده‌اند معنای پایهٔ فضای سایبری را تعریف کنند ولی بیشتر تعریف‌های آن‌ها نحوهٔ استفاده از سایبر را توضیح می‌دهند. در سال ۱۹۹۹، لانس اِستِریت یک طبقه‌بندی سه‌سطحی جهت توصیف فضای سایبری ارائهٔ کرد. او فضای سایبری را به سه سطح تقسیم نمود: «سطح صفر»، که به هستی‌شناسی و فضازمانِ سایبری مربوط می‌شود؛ «سطح اول»، که فضای سایبری فیزیکی، مفهومی و ادراکی را در بر می‌گیرد؛ و «سطح دوم»، که به ترکیب فضای رسانه‌ای شبکه‌ای مربوط می‌شود و معنا و دامنهٔ فضای سایبری را غنی می‌سازد (استرایت، ۱۹۹۹)[۲].

در فرهنگ واژه‌های نظامی وزارت دفاع آمریکا فضای سایبری این گونه تعریف شده است: «محیطی مفهومی که در آن اطلاعات دیجیتال‌سازی‌شده از طریق شبکه‌های رایانه‌ای منتقل می‌شوند»[۳].(راتری و همکاران،۲۰۱٦).در سال ۲۰۰٦، وزارت دفاع و ستاد مشترک ایالات‌متحده در راهبرد نظامی ملی برای عملیات‌های فضای سایبریِ این کشور تعریفی کلی از فضای سایبری ارائه دادند. طبق این تعریف، فضای سایبری عبارت است از «حوزه‌ای که در آن از الکترونیک و طیف الکترومغناطیسی جهت ذخیره‌سازی، پردازش و تبادل داده‌ها از طریق سامانه‌های شبکه‌شده و زیرساخت‌های فیزیکی مرتبط استفاده می‌شود» (ولف،۲۰۱۳)[٤]. یاناکاجورگوس نیز فضای سایبری را «حوزهٔ استفاده از الکترونیک و طیف الکترومغناطیسی جهت ذخیره‌سازی، پردازش و انتقال اطلاعات از طریق سامانه‌های شبکه‌شده و زیرساخت‌های فیزیکی» تعریف کرد (یاناکوجیارگاس،۲۰۰۹)[۵]. سپس، اینگلند، معاون وزیر دفاع آمریکا، فضای سایبری را «یک حوزهٔ جهانی در درون محیط اطلاعاتی که از شبکهٔ به‌هم‌پیوستهٔ زیرساخت‌های فناوری اطلاعات از جمله اینترنت، شبکه‌های مخابرات، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های موجود در آن‌ها تشکیل می‌گردد» تعریف کرد(انگلندگوردن،۲۰۰۸) [٦]. این تعاریف عنصر فناوری را در بر می‌گیرند ولی به عنصر انسان هیچ اشاره‌ای نمی‌کنند. این در حالی است که در تعریف پیشنهادی واینِر و گیبسون انسان یک عنصر مهم می‌باشد.

تعریف رِین اوتیس، عضو مرکز عالی دفاع سایبری تعاملیِ ناتو، یک عنصر انسانی را در برمی‌گیرد: «فضای سایبری یک مجموعهٔ وابسته به زمان از سامانه‌های اطلاعاتی مرتبط و کاربران انسانی آن‌ها می‌باشد». اوتیس تأکید کرد «توجه داشته باشید که این تعریف کاربران انسانی را نیز در بر می‌گیرد. فضای سایبری یک فضای ساخت بشر است و توسط افراد برای استفادهٔ انسان ایجاد می‌گردد»[۷]. در یکی از اسناد اتحادیهٔ بین‌المللی مخابرات فضای سایبری محیط سایبری نامیده شده و «محیطی متشکل از کاربران، شبکه‌ها، ابزارها، نرم‌افزارها، فرآیندها، اطلاعات ذخیره یا در حال انتقال، برنامه‌ها، خدمات و سامانه‌هایی که می‌توان آن‌ها را به‌طور مستقیم یا غیرمستقیم به شبکه‌ها متصل کرد»

---

[۱] Wolff, ۲۰۱۳:۹-۲٤

[۲] Strate, ۱۹۹۹:۳۸۲-٤۱۲

[۳] Rattray, et.al, ۲۰۱٦:۱۲-۳۱

[٤] Wolff, ۲۰۱۳:۹-۲٤

[۵] Yannakogeorgos,۲۰۰۹:۹-۲٤

[٦] Ingland Gordun, www.wired.com ,۲۰۰۸

[۷] Otis Rin, https://ccdcoe.org/multime,۲۰۱٦

تعریف گردیده است (آی تی یو، ۲۰۱٦)[۱]. سازمان بین‌المللی استانداردسازی فضای سایبری را با تأکید بر تعامل انسانی تعریف می‌کند: «فضای سایبری یک محیط پیچیده می‌باشد که به موجب تعامل افراد، نرم‌افزارها و خدمات در اینترنت شکل می‌گیرد و توسط ابزارهای پیشرفته و شبکه‌های متصل به اینترنت پشتیبانی می‌شود»(سازمان جهانی استاندارد،۲۰۱۲)[۲].

با این حال، تعریف درست فضای سایبر، عنصر فناوری، عنصر انسان و عنصر ارتباط و کنترل را در بر می‌گیرد. اگرچه تعاریف گوناگونی تاکنون ارایه شده ولی اغلب آنها یک بُعد مشترک دارند: هستهٔ فضای سایبر از سخت افزارها و نرم‌افزارهای بین‌المللی متصل به هم و داده‌های مربوط به آن‌ها تشکیل می‌شود. نکتهٔ مهم دیگر این که افراد می‌توانند به این فضا متصل و هنگام استفاده از اینترنت افراد و فضای سایبری در هم آمیخته می‌شوند.

۲-۲. تبیین عناصر اصلی فضای سایبر

در مقاله برخی از اصول راهبرد سایبری، فضای سایبری «حوزهٔ سایبری» نیز نامیده شده و این گونه معرفی گردیده است: «حوزهٔ سایبری یا فضای سایبری توسط اندرو کِرپینِویچ تعریف شده است که بر اساس آن، می‌توان فضای‌سایبری را به دو سطحِ «سایبر» و «فضا [یا «حوزه»]» تقسیم کرد. معنای «سایبر» در زیرساخت‌های رایانه‌ای و خطوط ارتباطی متبلور می‌شود. با این حال، مفهوم واقعی آن در نوع اطلاعات موجود در رایانه و نحوهٔ استفاده از این اطلاعات، که معنی «فضا» را تشکیل می‌دهند، نهفته است. «فضا» به معنای منعکس کردن ویژگی‌های انسان و فعالیت‌ها از طریق سایبر می‌باشد. به موجب ماهیت خاص شبکه، بازیگر اصلی در سایبر یا یک فرد است یا نمایندهٔ آن فرد یا حتی رفتارهای ماشین به عنوان مثال، سامانهٔ هوش مصنوعیِ *آلفاگو*[۳]. بر این اساس، «نقش سایبر» می‌تواند جهت معرفی بازیگر اصلی، که یک «کاربر» انسان، نرم‌افزار، شیء، عنوان یا موارد مشابه می‌باشد، به کار برده شود. در نتیجه در تعریف فضای سایبری تأکید ویژه‌ای بر مفهوم «کاربر» و «نقش» وجود دارد و این «کاربران» و «نقش‌ها» به تعامل می‌پردازند(کریپین ویچ، ۲۰۱٤)[٤].

فضای سایبری چهار عنصر را در بر می‌گیرد: تجهیزات (حامل، یعنی زیرساخت)، داده‌ها (اشیاء، بار)، نقش‌ها (سوژه‌ها، یعنی کاربر) و عملیات (فعالیت‌ها/رفتارها)

عنصرِ «تجهیزات» معادل تلفیقی از «گره پایانی»، «لبه‌های متصل‌کننده[۵]» و «گره سوئیچینگ» در تعریف «شبکه» می‌باشد. می‌توان گفت حامل‌های انواع مختلف بار (سیگنال، داده، اطلاعات و غیره) حکم «تجهیزات» را دارند چرا که همهٔ آن‌ها در فضای سایبری ویژگی‌های یکسانی دارند که تمام آن‌ها به «حمل کردن» مربوط می‌شوند. عنصر «داده» به نشان‌های دیجیتالی اطلاق می‌شود که بیانگر اطلاعاتی از قبیل نور، برق، خاصیت مغناطیسی، کوانتوم (و حتی ذره‌های کوچک‌تری که ممکن است در آینده پدید آیند) و غیره در فضای سایبری هستند و حکم «بار» در تعریف «شبکه» را دارد. افزون بر این، داده‌ها نتایج پردازش‌شده و همچنین انعکاس هدف یک فعالیت مشخص می‌باشند (همان).

---

[۱] www.itu.int,۲۰۱٦

[۲] International Organization for Standardization,۲۰۱۲

[۳] AlphaGo

[٤] Krepinevich,۲۰۱٤:٦-۹

[۵] connecting edges

عنصرِ «تجهیزات» و «داده‌ها» به سطح فناوری مربوط می‌شوند، ویژگی‌های «شبکه» را منعکس می‌کنند و معمولاً به‌مثابه نقاط اقدامی هستند که مدیریت می‌گردند.عنصرِ «نقش‌ها» تمام نقش‌ها و کاربران در فضای سایبری را در برمی‌گیرد. در این فضا، انسان‌ها نقش‌ها می‌باشند. افزون بر این، سازمان‌ها، وسایل، نرم‌افزارها، پایگاه‌های اینترنتی، انسان‌های مجازی (ربات‌ها)، وسایل شبکه (مسیریاب) و غیره نیز می‌توانند نقش‌های اصلی‌ای باشند که قادر به تولید اطلاعات هستند. هم «نقش‌ها» و هم «عملیات» به سطوح اجتماعی تعلق دارند و ویژگی‌های «فضا»، که خصوصیت اجتماعی شیء اصلیِ «مدیریت‌شونده» را منعکس می‌کنند. در فضای سایبری، «نقش‌ها» و «عملیات» از اهمیت زیادی برخوردار هستند. (همان)

۲-۳. مفهوم‌شناسی فضای سایبر در اسناد راهبردی امنیت سایبری کشورهای منتخب

۲.۳.۱. *راهبرد امنیت سایبری ملی افغانستان*

در *راهبرد امنیت سایبری ملی افغانستان*، فضای سایبری این گونه تعریف شده است:

«فضای سایبری: محیطی متشکل از سامانه‌های اطلاعاتی که سراسر جهان را در برمی‌گیرند و همچنین شبکه‌هایی که این سامانه‌ها را به یکدیگر متصل می‌کنند[۱]».

۲.۳.۲. *راهبرد حفاظت و امنیت سامانه‌های اطلاعاتی فرانسه*

در *راهبرد حفاظت و امنیت سامانه‌های اطلاعاتیِ فرانسه*، فضای سایبری این گونه تعریف شده است: «فضای ارتباطی حاصل از پیوند متقابل جهانی بین تجهیزات خودکار پردازش داده‌های دیجیتال[۲]».

۲.۳.۳. راهبرد امنیت ملی ژاپن

در *راهبرد امنیت ملیِ ژاپن* ، فضای سایبری این گونه تعریف شده است: «یک حوزهٔ جهانی متشکل از سامانه‌های اطلاعاتی، شبکه‌های مخابرات و غیره که بستری برای انجام فعالیت‌های اجتماعی، اقتصادی، نظامی فراهم می‌کند[۳]».

۲.۳.٤. برنامهٔ توسعهٔ امنیت اطلاعات الکترونیکی (امنیت سایبری) ۲۰۱۱ تا ۲۰۱۹ لیتوانی

در سند *برنامهٔ توسعهٔ امنیت اطلاعات الکترونیکی (امنیت سایبری) برای سال ۲۰۱۱ تا ۲۰۱۹ لیتوانی* ، فضای سایبری این گونه تعریف شده است: «فضای سایبری یک فضای جهانی بدون هر گونه مرز ملی می‌باشد و از این رو تهدیدها به سرعت در آن گسترش می‌یابند[٤]».

۲.۳.۵. راهبرد امنیت سایبری نیوزیلند

در *راهبرد امنیت سایبری نیوزیلند*، فضای سایبری این گونه تعریف شده است: «یک شبکهٔ جهانی متشکل از زیرساخت‌های فناوری اطلاعات، شبکه‌های مخابرات و سامانه‌های پردازش رایانه‌ای مرتبط که در آن ارتباط برخط صورت می‌گیرد[۵]».

۲.۳.٦. راهبرد پادشاهی عربستان سعودی برای توسعهٔ امنیت اطلاعات ملی

در *راهبرد پادشاهی عربستان سعودی برای توسعهٔ امنیت اطلاعات ملی* (پیش‌نویس۷)، فضای سایبری این گونه تعریف شده است: «یک حوزهٔ جهانی در درون محیط اطلاعاتی که از شبکه‌های به‌هم‌پیوستهٔ زیرساخت‌های سامانه

---

[۱] National Cyber Security Strategy of Afghanista,۲۰۱٤

[۲] Information Systems Defence and Security, France's Strategy, ۲۰۱

[۳] Japan National Security Strategy,۲۰۱۳

[٤] On the Approval of the Programme for the Development of Electronic Information,۲۰۱۱

[۵] New Zealand's Cyber Security Strategy,۲۰۱۱

های اطلاعاتی از جمله اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های موجود در آن‌ها تشکیل می‌شود[۱]».

۲.۳.۷. راهبرد ملی حفاظت از سوئیس در برابر تهدیدهای سایبری

در *راهبرد ملی حفاظت از سوئیس در برابر تهدیدهای سایبری*، فضای سایبری این گونه تعریف شده است: «دولت، بخش خصوصی و جامعه از زیرساخت‌های اطلاعاتی و ارتباطی و فضای سایبری (اینترنت، شبکه‌های سیار و برنامه‌ها، تجارت الکترونیک، دولت الکترونیک و برنامه‌های کنترل رایانه‌محور) استفاده می‌کنند[۲]».

۲.۳.۸. راهبرد امنیت سایبری ملی و طرح اقدام ۲۰۱٤-۲۰۱۳ ترکیه

در *راهبرد امنیت سایبری ملی و طرح اقدام ۲۰۱٤-۲۰۱۳ ترکیه*، فضای سایبری این گونه تعریف شده است: «محیطی متشکل از سامانه‌های اطلاعاتی که سراسر جهان را در بر می‌گیرند و همچنین شبکه‌هایی که این سامانه‌ها را به یکدیگر متصل می‌کنند[۳]».

۲.۳.۹. راهبرد ملی ایمن‌سازی فضای سایبری آمریکا

در *راهبرد ملی ایمن‌سازی فضای سایبریِ آمریکا*، فضای سایبری این گونه تعریف شده است: «فضای سایبری از صدها هزار رایانه، سِرور، مسیریاب ، سوئیچ و کابل فیبر نوری به‌هم‌پیوسته که امکان فعالیت مؤثر زیرساخت‌های حیاتی ما را فراهم می‌کنند تشکیل شده است[٤]».

۲.۳.۱۰. طرح ملی مشاغل و مطالعات امنیت سایبری آمریکا

در واژه‌نامهٔ *طرح ملی مشاغل و مطالعات امنیت سایبریِ آمریکا*، فضای سایبری این گونه تعریف شده است: «شبکهٔ به‌هم‌پیوستهٔ زیرساخت‌های فناوری اطلاعات که اینترنت، شبکهٔ مخابرات، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های موجود در آن‌ها را در بر می‌گیرد[٥]».

۲.۳.۱۱. سیاست فضای سایبری: تضمین قابل اطمینان و تاب‌آور بودن زیرساخت‌های ارتباطی آمریکا

در گزارش *سیاست فضای سایبری: تضمین قابل اطمینان و تاب‌آور بودن زیرساخت‌های ارتباطیِ آمریکا*، فضای سایبری این گونه تعریف شده است: «زیرساخت اطلاعاتی و ارتباطی دیجیتال جهانی به‌هم‌پیوسته‌ای که «فضای سایبری» نامیده می‌شود اساس تقریباً تمام ابعاد جامعهٔ مدرن را تشکیل می‌دهد و از اقتصاد، زیرساخت‌های مدنی، ایمنی عمومی و امنیت ملی آمریکا پشتیبانی حیاتی می‌کند[٦]»

---

[۱] Developing National Information Security Strategy for the Kingdom of Saudi Arabia, DRAFT ۷,۲۰۱٦

[۲] National Strategy for the Protection of Switzerland Against Cyber Risks,۲۰۱۲

[۳] National Cyber Security Strategy and ۲۰۱۳–۲۰۱٤ Action Plan,۲۰۱۳-۲۰۱٤

[٤] National Strategy to Secure Cyberspace,۲۰۱٦

[٥] National Initiative for Cybersecurity Careers and Studies,۲۰۱٦

[٦]Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,۲۰۰۹.

۲.۳.۱۲. راهبرد امنیت سایبری بلژیک

در *راهبرد امنیت سایبری بلژیک*، فضای سایبری این گونه تعریف شده است: «فضای سایبری محیطی جهانی برای ارتباط متقابل سامانه‌های اطلاعاتی و ارتباطی می‌باشد. فضای سایبری از دنیای رایانه وسیع‌تر است و شبکه‌های رایانه‌ای، سامانه‌های کامپیوتری، رسانه‌های دیجیتال و داده‌های دیجیتال فیزیکی یا مجازی را نیز در بر می‌گیرد[۱]»

۲.۳.۱۳. راهبرد امنیت سایبری کانادا، برای کانادایی قوی‌تر و موفق‌تر

در *راهبرد امنیت سایبری کانادا، برای کانادایی قوی‌تر و موفق‌تر*، فضای سایبری این گونه تعریف شده است: «فضای سایبری جهانی الکترونیکی است که از شبکه‌های به‌هم‌پیوستهٔ فناوری اطلاعات و اطلاعات موجود در این شبکه‌ها تشکیل می‌شود. این فضا یک حوزهٔ مشترک جهانی است که در آن بیش از ۱/۷ میلیارد نفر با برقراری ارتباط با یکدیگر به تبادل اندیشه‌ها، خدمات و دوستی با همدیگر می‌پردازند[۲]».

۲.۳.۱٤. راهبرد امنیت سایبری آلمان

در *راهبرد امنیت سایبری آلمان*، فضای سایبری این گونه تعریف شده است:

«فضای سایبری عبارت است از فضای مجازی تمام سامانه‌های فناوری اطلاعاتی که در مقیاس جهانی در سطح داده به یکدیگر متصل هستند. اینترنت به عنوان یک شبکهٔ جهانی و عمومی برای ارتباط و انتقال که می‌توان با استفاده از شبکه‌های دادهٔ اضافی آن را توسعه بخشید اساس فضای سایبری را تشکیل می‌دهد. سامانه‌های فناوری اطلاعاتی که در یک فضای مجازی مجزا قرار دارند جزء فضای سایبری نیستند[۳]».

۲.۳.۱۵. راهبرد امنیت سایبری ملی مجارستان

در *راهبرد امنیت سایبری ملی مجارستان*، فضای سایبری این گونه تعریف شده است: «منظور از فضای سایبری سامانه‌های اطلاعاتی الکترونیکی، جهانی، به‌هم‌پیوسته، غیرمتمرکز و فزاینده و همچنین فرآیندهای اجتماعی و اقتصادی‌ای که در و از طریق این سامانه‌ها در قالب داده و اطلاعات شکل می‌گیرند می‌باشد[٤]».

۲.۳.۱٦. چارچوب راهبردی ملی برای امنیت فضای سایبری ایتالیا

در نسخهٔ ۲۰۱۳ *چارچوب راهبردی ملی برای امنیت فضای سایبری ایتالیا*، فضای سایبری این گونه تعریف شده است: «فضای سایبری یک حوزهٔ ساخت بشر متشکل از گره‌ها و شبکه‌های فناوری اطلاعات و ارتباطات می‌باشد که حجم فزاینده‌ای از داده‌هایی را که برای کشورها، شرکت‌ها، شهروندان و همچنین تمام تصمیم‌گیرندگان سیاسی، اجتماعی و اقتصادی اهمیت راهبردی دارند در بر می‌گیرد و پردازش می‌کند[۵]».

۲.۳.۱۷. راهبرد سایبری دفاع هلند

در *راهبرد سایبری دفاع هلند*، فضای سایبری این گونه تعریف شده است: «فضای سایبری تمام مواردی را که به صورت دیجیتال به یکدیگر متصل هستند یا ممکن است متصل گردند شامل می‌شود. این حوزه هم اتصال‌های دائمی

---

[۱] Belgium Cyber Security Strategy, ۲۰۱۲

[۲] Canada's Cyber Security Strategy, for a Stronger and More Prosperous Canada,۲۰۱۰

[۳] Cyber Security Strategy for Germany,۲۰۱۱

[٤] National Cyber Security Strategy of Hungary,۲۰۱۳

[۵] National Strategic Framework for Cyberspace Security, ۲۰۱۳

را در بر می‌گیرد و هم اتصال‌های موقتی یا محلی را و در تمام موارد به نوعی به داده‌ها (کد منبع، اطلاعات و سایر مواردِ) موجود در حوزه مربوط می‌شود[۱]».

۲.۳.۱۸. فرهنگ واژه‌های نظامی و مرتبط با حوزهٔ نظامی وزارت دفاع آمریکا

در *فرهنگ واژه‌های نظامی و مرتبط با حوزهٔ نظامی وزارت دفاعِ آمریکا*، فضای سایبری این گونه تعریف شده است: «فضای سایبری: یک حوزهٔ جهانی در درون محیط اطلاعاتی که از شبکه‌های به‌هم‌پیوستهٔ زیرساخت‌های فناوری اطلاعات از جمله اینترنت، شبکه‌های مخابرات، سامانه‌های رایانه‌ای، پردازشگرها و کنترل‌کننده‌ها و همچنین داده‌های موجود در آن‌ها تشکیل می‌گردد[۲]».

۲.۳.۱۹. راهبرد امنیت سایبری ژاپن: به سوی یک فضای سایبری سرآمد، تاب‌آور و قوی

در *راهبرد امنیت سایبری ژاپن: به سوی یک فضای سایبری سرآمد، تاب‌آور و قوی*، فضای سایبری این گونه تعریف شده است: «فضاهای مجازی جهانی از قبیل اینترنت که از سامانه‌های اطلاعاتی، شبکه‌های اطلاعاتی و ارتباطی و سامانه‌های مشابه تشکیل می‌شوند و حجم‌های وسیعی از انواع مختلف اطلاعات را انتقال می‌دهند به سرعت توسعه یافته‌اند و در حال فرا گرفتن فضای واقعی هستند[۳]».

۲.۳.۲۰. قطع‌نامهٔ شمارهٔ ۳۶۱۱: بهبود قابلیت‌های فضای سایبری ملی رژیم صهیونیستی

در *قطع‌نامهٔ شمارهٔ ۳۶۱۱: بهبود قابلیت‌های فضای سایبری ملیِ رژیم صهیونیستی*، فضای سایبری این گونه تعریف شده است: «حوزه‌ای فیزیکی و غیرفیزیکی که تمام یا بخشی از این عناصر را در برمی‌گیرد: سامانه‌های مکانیزه یا رایانه‌ای، شبکه‌های رایانه‌ای و ارتباطی، برنامه‌ها، اطلاعات رایانه‌ای، محتوایی که توسط رایانه‌ها منتقل می‌شوند، داده‌های ترافیکی و نظارتی و افرادی که از این داده‌ها استفاده می‌کنند[۴]».

۲.۳.۲۱. راهبرد امنیت سایبری ملی قطر

در *راهبرد امنیت سایبری ملی قطر*، فضای سایبری این گونه تعریف شده: «یک محیط مجازی یا الکترونیکی متشکل از شبکهٔ به‌هم‌پیوستهٔ فناوری‌های اطلاعاتی و ارتباطی (از قبیل اینترنت، شبکه‌های مخابرات، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های موجود در آن) که زمینهٔ دسترسی افراد به خدمات و اطلاعات را فراهم می‌کند[۵]».

۲.۳.۲۲. اعلامیه تدوین سیاست امنیت سایبری ملی آفریقای جنوبی

در *اعلامیه تدوین سیاست امنیت سایبری ملی آفریقای جنوبی*، فضای سایبری این گونه تعریف شده: «فضای سایبری یک محیط فیزیکی و غیرفیزیکی می‌باشد که تمام یا برخی از این عناصر را در برمی‌گیرد: رایانه‌ها، سامانه‌های رایانه‌ای، شبکه‌ها و برنامه‌های رایانه‌ای آن‌ها، داده‌های رایانه‌ای، داده‌های محتوایی، داده‌های ترافیکی و کاربران[۶]».

---

[۱] Defence Cyber Strategy of the Netherland,۲۰۱۲

[۲] Department of Defense Dictionary of Military and Associated Terms,۲۰۱۶

[۳] Japan’s Cybersecurity Strategy: Towards a World-leading, Resilient and Vigorous Cyberspace,۲۰۱۳

[۴] Resolution No. ۳۶۱۱: Advancing N.C

[۵] Qatar National Cyber Security Strategy,۲۰۱۴

[۶] Notice of Intention to Make South African National Cybersecurity Policy,۲۰۱۰.)

۲.۳.۲۳. راهبرد امنیت سایبری ملی اسپانیا

در *راهبرد امنیت سایبری ملیِ اسپانیا*، فضای سایبری این گونه تعریف شده است: «فضای سایبری، که به حوزهٔ جهانی و پویای متشکل از زیرساخت‌های فناوری اطلاعات از جمله شبکه‌های اینترنتی و سامانه‌های اطلاعاتی و ارتباطی اطلاق می‌شود، مرزها را از بین برده است و کاربران خود را در یک جهانی‌سازی بی‌سابقه مشارکت می‌دهد که این امر فرصت‌های جدیدی ایجاد می‌کند ولی در عین حال چالش‌ها، ریسک‌ها و تهدیدهای تازه‌ای را نیز به وجود می‌آورد[۱]».

۲.۳.۲٤. قانون امنیت سایبری و تغییر قوانین مرتبط جمهوری چک

در *قانون امنیت سایبری و تغییر قوانین مرتبطِ جمهوری* چک، فضای سایبری این گونه تعریف شده است: «فضای سایبری یک محیط دیجیتال می‌باشد که امکان ایجاد، پردازش و تبادل اطلاعات را فراهم می‌کند و از سامانه‌ها و خدمات اطلاعاتی و شبکه‌های ارتباطی الکترونیکی تشکیل می‌شود[۲]».

۲،۳،۲۵. راهبرد امنیت سایبری فنلاند

در *راهبرد امنیت سایبری فنلاند*، فضای سایبری این گونه تعریف شده است: «حوزهٔ سایبری (محیط سایبری) یک حوزهٔ پردازش اطلاعات (داده‌های) الکترونیکی می‌باشد که از یک یا چند زیرساخت فناوری اطلاعات تشکیل می‌شود. این حوزه استفاده از الکترونیک و طیف الکترومغناطیسی جهت ذخیره‌سازی، پردازش و انتقال داده و اطلاعات از طریق شبکه‌های مخابرات را در بر می‌گیرد. منظور از پردازش اطلاعات (داده‌ها) گردآوری، ذخیره، سازماندهی، به‌کارگیری، انتقال، نمایش، بایگانی، پردازش، تلفیق، محافظت، حذف و از بین بردن اطلاعات (داده‌ها) و انجام سایر اقدامات مشابه روی آن‌ها می‌باشد[۳]».

۲.۳.۲٦. راهبرد امنیت سایبری دولت کنیا

در *راهبرد امنیت سایبری دولت کنیا*، فضای سایبری این گونه تعریف شده است: «فضای سایبری تنها اینترنت و فناوری‌های اطلاعاتی و ارتباطی را در بر نمی‌گیرد. فضای سایبری حوزه‌ای شبیه حوزه‌های زمین، هوا، دریا و فضا است ولی ویژگی‌ها و چالش‌های خاص خود را دارد. مشخصهٔ حوزهٔ سایبری ذخیره‌سازی، پردازش و تبادل داده از طریق سامانه‌های شبکه‌شده می‌باشد. این حوزه توسط زیرساخت‌های اطلاعاتی حیاتی پشتیبانی می‌شود و دارای ابعاد ملی و بین‌المللی‌ای است که صنعت، تجارت، مالکیت فکری، امنیت، فناوری، فرهنگ، سیاست و دیپلماسی را در بر می‌گیرند. از این رو، فضای سایبری نقش مهمی در اقتصاد جهانی ایفا می‌کند[٤]».

۲.۳.۲۷. راهنمای تالین پیرامون قوانین بین‌المللی قابلِ اعمال در جنگ سایبری

در راهنمای ناتو با عنوان راهنمای تالین پیرامون قوانین بین‌المللی قابلِ اعمال در جنگ سایبری، فضای سایبری این گونه تعریف شده است: «محیطی متشکل از عناصر فیزیکی و غیرفیزیکی که استفاده

---

[۱] National Cyber Security Strategy,۲۰۱۳

[۲] Draft Act on Cyber Security and Change of Related Acts,۲۰۱٤.

[۳] Finland's Cyber Security Strategy,۲۰۱۳

[٤] Government of Kenya Cybersecurity Strategy,۲۰۱٤

از رایانه‌ها و طیف الکترومغناطیسی جهت ذخیره‌سازی، پردازش و تبادل اطلاعات از طریق شبکه‌های رایانه‌ای را در بر می‌گیرد[۱]»

۲.۳.۲۸. راهبرد امنیت سایبری بریتانیا: ایمنی، امنیت و تاب‌آوری در فضای سایبری

در *راهبرد امنیت سایبری بریتانیا: ایمنی، امنیت و تاب‌آوری در فضای سایبری*، فضای سایبری این گونه تعریف شده است: «فضای سایبری انواع مختلف فعالیت‌های دیجیتال شبکه‌ای را در بر می‌گیرد. این فضا محتوا و فعالیت‌هایی که از طریق شبکه‌های دیجیتال انجام می‌شوند را شامل می‌شود[۲]».

۲.۳.۲۹. راهبرد امنیت سایبری بریتانیا: حفاظت و ارتقاء بریتانیا در دنیای دیجیتال

در *راهبرد امنیت سایبری بریتانیا: حفاظت و ارتقاء بریتانیا در دنیای دیجیتال*، فضای سایبری این گونه تعریف شده است: «فضای سایبری یک حوزهٔ تعاملی متشکل از شبکه‌های دیجیتال است که جهت ذخیره‌سازی، پردازش و انتقال اطلاعات به کار برده می‌شود. فضای سایبری از اینترنت و همچنین سایر سامانه‌های اطلاعاتی که به تجارت، زیرساخت‌ها و خدمات کمک می‌کنند تشکیل می‌شود[۳]».

۲.۳.۳۰. راهبرد امنیت سایبری اتریش

در *راهبرد امنیت سایبری اتریش*، فضای سایبری این گونه تعریف شده : «فضای سایبری عبارت است از فضای مجازی تمام سامانه‌های فناوری اطلاعاتی که در مقیاس جهانی در سطح داده به یکدیگر متصل هستند. اینترنت به عنوان یک شبکهٔ جهانی و عمومی برای ارتباط و انتقال که می‌توان با استفاده از شبکه‌های دادهٔ اضافی آن را توسعه بخشید اساس فضای سایبری را تشکیل می‌دهد. فضای سایبری به شبکهٔ جهانی زیرساخت‌های مستقل و مختلف فناوری اطلاعات، شبکه‌های مخابرات و سامانه‌های رایانه‌ای نیز اطلاق می‌شود. در حوزهٔ اجتماعی، استفاده از این شبکهٔ جهانی افراد را به تعامل، تبادل نظر، انتشار اطلاعات، حمایت اجتماعی، فعالیت‌های اقتصادی، کنترل فعالیت‌ها، خلق آثار هنری، بازی، مشارکت در بحث‌های سیاسی و بسیاری موارد قادر می‌سازد[۴]».

۲.۳.۳۱. راهبرد امنیت فضای سایبری ملی چین

راهبرد امنیت فضای سایبری ملی چین در ۲۷ دسامبر ۲۰۱۶ به طور رسمی منتشر شد ولی فضای سایبری را به روشنی تعریف نمی‌کند. در این راهبرد، فضای سایبری این گونه توصیف شده است: «در پی توسعهٔ گستردهٔ انقلاب اطلاعاتی، یک فضای سایبری متشکل از اینترنت، شبکه‌های مخابرات، سامانه‌های رایانه‌ای، سامانه‌های کنترل خودکار، تجهیزات دیجیتال و کاربردها، خدمات و داده‌های آن‌ها، در حال ایجاد تغییرات اساسی در روش‌های تولید و زندگی مردم و اثرگذاری عمیق بر فرآیند رشد اجتماعی تاریخی بشر است». این توصیف دربرگیرندهٔ تجهیزات (اینترنت، شبکه‌های مخابرات، سامانه‌های رایانه‌ای، سامانه‌های کنترل خودکار، وسایل دیجیتال)، داده (داده‌های

---

[۱] Tallinn Manual on the International Law Applicable to Cyber Warfare,۲۰۱۳

[۲] Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space,۲۰۰۹

[۳] The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World,۲۰۱۱

[۴] Austrian Cyber Security Strategy,۲۰۱۳

آن‌ها)، کاربران (بشر) و عملیات (کاربردها و خدمات آن‌ها) می‌باشد. از این رو، توصیف چین از فضای سایبری تمام چهار عنصر آن را در بر می‌گیرد[۱].

۲.۳.۳۲. رهنمودهای سیاستی کلمبیا پیرامون امنیت سایبری و دفاع سایبری

در *رهنمودهای سیاستی کلمبیا پیرامون امنیت سایبری و دفاع سایبری*، فضای سایبری این گونه تعریف شده است: «محیطی فیزیکی و مجازی متشکل از رایانه‌ها، سامانه‌های رایانه‌ای، برنامه‌ها (نرم‌افزارهای) رایانه‌ای، شبکه‌های مخابرات، داده‌ها و شبکه‌های اطلاعاتی که در آن کاربران به تعامل با یکدیگر می‌پردازند[۲]».

۲.۳.۳۳. سیاست امنیت سایبری ملی هند

در *سیاست امنیت سایبری ملیِ هند*، فضای سایبری این گونه تعریف شده است: «فضای سایبری محیطی پیچیده متشکل از تعامل‌های بین افراد و خدمات می‌باشد که توسط ابزارها و شبکه‌های فناوری‌های اطلاعاتی و ارتباطی در سطح جهان پشتیبانی می‌شود»(NCSP,۲۰۱۳).

۲.۳.۳٤. راهبرد امنیت سایبری لتونی برای سال ۲۰۱٤ تا ۲۰۱۸

در *راهبرد امنیت سایبری لتونی برای سال ۲۰۱٤ تا ۲۰۱۸*، فضای سایبری این گونه تعریف شده است: «فضای سایبری یک محیط تعاملی می‌باشد که از کاربران، شبکه‌ها، فناوری‌های رایانشی، نرم‌افزارها، فرآیندها، اطلاعات ذخیره‌شده یا در حال انتقال، برنامه‌ها، خدمات و سامانه‌هایی که می‌توان آن‌ها را به طور مستقیم یا غیرمستقیم به اینترنت، شبکه‌های مخابرات و شبکه‌های رایانه‌ای متصل کرد تشکیل می‌شود[۳]».

۲.۳.۳۵. راهبرد امنیت سایبری ملی مونته‌نگرو برای سال ۲۰۱۳ تا ۲۰۱۷

در *راهبرد امنیت سایبری ملی مونته‌نگرو برای سال ۲۰۱۳ تا ۲۰۱۷*، «سایبر» این گونه تعریف شده است: «هر چیز مرتبط با یا دربرگیرندهٔ رایانه‌ها یا شبکه‌های رایانه‌ای از قبیل اینترنت. فضای سایبری فراتر از اینترنت است. فضای سایبری نه تنها سخت‌افزارها، نرم‌افزارها و سامانه‌های اطلاعاتی بلکه افراد و تعامل‌های اجتماعی در این شبکه‌ها را نیز در برمی‌گیرد[٤]».

۲.۳.۳٦ سیاست حفاظت از فضای سایبری جمهوری لهستان

در *سیاست حفاظت از فضای سایبری لهستان*، فضای سایبری این گونه تعریف شده: «فضایی برای پردازش و تبادل اطلاعات که از سامانه‌های اطلاعاتی و ارتباطی، پیوندهای بین آن‌ها و روابط با کاربران تشکیل می‌شود[۵]».

۲.۳.۳۷. راهبرد امنیت سایبری رومانی و طرح اقدام در زمینهٔ توسعهٔ نظام امنیت اطلاعات ملی

در *راهبرد امنیت سایبری رومانی و طرح اقدام در زمینهٔ توسعهٔ نظام امنیت اطلاعات ملی*، فضای سایبری این گونه تعریف شده است: «فضایی مجازی که توسط زیرساخت‌های سایبری ایجاد می‌گردد و پردازش، ذخیره‌سازی یا انتقال اطلاعات و عملیات‌های کاربران در این فضا را در برمی‌گیرد[۱]».

---

[۱] National Cyberspace Security Strategy,۲۰۱٦

[۲] Columbia's Policy Guidelines for Cybersecurity and Cyberdefense,۲۰۱۱

[۳] Cyber Security Strategy of Latvia, ۲۰۱٤-۲۰۱۸

[٤] National Cyber Security Strategy for Montenegro, ۲۰۱۳-۲۰۱۷

[۵] Cyberspace Protection Policy of the Republic of Poland, ۲۰۱۳

۲.۳.۳۸. دیدگاه‌های ادراکی در مورد فعالیت‌های نیروهای مسلح فدراسیون روسیه در فضای اطلاعاتی

فدراسیون روسیه معمولاً مخالف استفاده از واژۀ «فضای سایبری» است و فقط از «فناوری‌های اطلاعاتی و ارتباطی» یا در صورت نیاز «فضای اطلاعاتی» استفاده می‌کند. در سند *دیدگاه‌های ادراکی در مورد فعالیت‌های نیروهای مسلح فدراسیون روسیه در فضای اطلاعاتی*، فضای سایبری این گونه تعریف شده است: «فضای اطلاعاتی: یک حوزۀ فعالیت که به تشکیل، ایجاد، تغییر، انتقال، به‌کارگیری و ذخیره‌سازی اطلاعات مربوط می‌شود و بر موارد متعددی از جمله آگاهی فردی و جمعی، زیرساخت‌های اطلاعاتی و خود اطلاعات تأثیر می‌گذارد[۲]».

۲.۳.۳۹. راهبرد ادراکی برای امنیت سایبری فدراسیون روسیه

در *راهبرد ادراکی برای امنیت سایبری فدراسیون روسیه*، فضای سایبری این گونه تعریف شده است: «فضای سایبری: یک حوزۀ فعالیت در فضای اطلاعاتی که توسط مجاری ارتباطیِ اینترنت و سایر شبکه‌های مخابرات و زیرساخت‌های فناوری که عملکرد مؤثر آن را تضمین می‌کنند و هر گونه دادۀ مربوط به فعالیت‌هایی که افراد، نهادها و کشورها در آن انجام می‌دهند ایجاد می‌گردد[۳]».

۲.۳.۴۰. پروژه بررسی مفاهیم پایه و بنیادی حوزه‌های سایبری و کارگروه سایبری ن.م

به شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه شده، کنترل‌کننده‌های صنایع، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات گفته می‌شود که ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد (مفاهیم پایه و بنیادی حوزه‌های سایبری،۱۲:۱۴۰۰)

۳. روش‌شناسی تحقیق

۳-۱. رویکرد و روش تحقیق

پژوهش حاضر با رویکرد کیفی و در زمره تحقیقات تحلیلی- توصیفی می‌باشد. براساس ماهیت داده‌ها از نوع کیفی و از حیث هدف کاربردی می‌باشد. در این پژوهش از روش گونه‌شناسی و تحلیل مضمون استفاده شده است. گونه‌شناسی به عنوان روشی که پیش از این در نظریه‌پردازی‌ها و تحقیق‌های برخی از اندیشمندان مطرح علوم اجتماعی به کار رفته است، در کنار دیگر انواع روش‌های طبقه‌بندی، خود می‌تواند به مثابه روشی برای تبیین و تولید مفاهیم در تحقیقات نظری و حتی کاربردی استفاده شود. این روش در بررسی و مطالعه انواع مکاتب، سازماندهی، تبیین و تولید مفاهیم، ساختارها و موضوعات علمی جایگاه ویژه‌ای دارد. به نحوی که پژوهش‌های نظری در حوزه مدیریت، عمدتاً از این روش استفاده کرده‌اند گونه‌شناسی‌ها قالبی نظام‌مند و رسمی در طبقه‌بندی داده‌های کیفی تلقی می‌شوند(لطیفی،۲۶:۱۳۹۷). مضمون یا تم، مبین اطلاعات مهمی درباره داده‌ها و سؤالات تحقیق است و تا حدی

---

[۱] Cyber Security Strategy of Romania and Action Plan on Nationwide Deployment of National Information Security System,۲۰۱۳

[۲] Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space,۲۰۱۶

[۳] Conceptual Strategy for Cyber Security of the Russian Federation,۲۰۱۶

مفهوم الگوی موجود در مجموعه‌ای از داده‌ها را نشان می‌دهد و حداقل به توصیف و سازماندهی مشاهدات و حداکثر به تفسیر جنبه‌هایی از پدیده می‌پردازد. (بویاتزیس[۱]، ۱۹۹۸:٤).

۳-۲. روش جمع‌آوری اطلاعات

روش جمع‌آوری داده‌ها واطلاعات در این پژوهش بصورت کتابخانه‌ای- اسنادی و بررسی متون، شناخت و استخراج مضامین از اسناد می‌باشد. گردآوری اطلاعات بصورت کتابخانه‌ای شامل استفاده از مخزن اسناد راهبردی امنیت سایبری ملی اتحادیه بین‌المللی مخابرات و پایگاه اطلاعات آنلاین آکادمیک می‌باشد.

شناخت مضمون روش‌های متنوعی دارد که در این مقاله برای شناخت مضمون از روش توجه به کلمات موجود در متن و موشکافی و دقت در متن اسناد راهبرد (امنیت) سایبری ملی کشورها و فیش برداری از آن‌ها استفاده شده است و پژوهشگران تلاش نمودند تا با کاوش مفاهیم و عناصر اصلی فضای سایبر و توجه به کلمات مکنون، تکراری و واژه‌های کلیدی در این اسناد به شناخت شباهت‌ها، تفاوت‌ها و طبقه‌بندی و گونه‌شناسی مفاهیم و شناخت عناصر اصلی این فضا دست یابند.

۳-۳. روش تجزیه و تحلیل اطلاعات

تحلیل مضمون ابزار تحقیقاتی منعطف و مفیدی است که برای تحلیل حجم زیادی از داده های پیچیده و مفصل، می‌توان از آن استفاده کرد. به طور کلی، مضمون، ویژگی تکراری و متمایزی در متن است که به نظر پژوهشگر، نشان دهنده درک و تجربه خاصی در رابطه با سؤالات تحقیق است(کینگ و هوراکس[۲]،۲۰۱۰:۱۵۰).

با توجه به پژوهش ما برای گونه‌شناسی مفهوم فضای سایبر از روش *قالب مضامین* که روش مناسبی در تحلیل مضمون است و آترایدـ استیرلینگ (۲۰۰۱) آن را توسعه داده است بهره گرفتیم. مضامین یا الگوی داده‌ها را می‌توان به روش استقرایی (مبتنی بر داده) و روش قیاسی (مبتنی بر نظریه) شناخت. در روش استقرایی، مضامین شناخته به شدت با خود داده‌ها مرتبط هستند(پاتون[۳]،۱۹۹۰:۸۵). در این پژوهش گونه‌شناسی، و تبیین مفهوم فضای سایبر از روش تحلیل مضمون با رویکرد استقرایی استفاده شده است. پس از منبع‌شناسی و تهیه اسناد راهبردی امنیت سایبری ملی این فرایند شامل سه مرحله کلان تجزیه و توصیف اسناد، تشریح و تفسیر متون و نهایتاً ترکیب و ادغام متون است. در این روش به صورت سلسله مراتبی فهرستی از مضامین را استخراج نمودیم، مضامین پایه(کدها و نکات کلیدی متن)، مضامین سازمان دهنده (مضامین به دست آمده از ترکیب و تلخیص مضامین پایه) و مضامین فراگیر (مضامین عالی دربرگیرنده اصول حاکم بر متن به مثابه کل) هستند ابتدا با استخراج مفهوم فضای سایبر از اسناد راهبرد (امنیت) سایبری کشورهای منتخب به مضمون پایه رسیدیم، سپس عناصر اصلی فضای سایبر و در انتها مضمون فراگیر که گونه‌های مختلف فضای سایبر می‌باشد تعیین شدند.

۳-٤. جامعه آماری پژوهش

جامعه آماری این پژوهش شامل آخرین ویرایش ٤۰ سند راهبرد ملی (امنیت) سایبری از ۳۵ کشور منتخب در جهان می‌باشد. این اسناد از آرشیو و مخزن اسناد راهبرد امنیت سایبری ملی اتحادیه بین‌المللی مخابرات و پایگاه‌های آنلاین آن تهیه شده‌اند.

---

[۱] Boyatzis

[۲] King & Horrocks

[۳] Patton

٤. تجزیه و تحلیل یافته‌ها

همانگونه که در بخش روش‌شناسی ذکر شد، تجزیه و تحلیل داده‌ها بر اساس روش قالب مضامین که آترایدـ استیرلینگ آن را توسعه داده و با رویکرد استقرایی انجام شده است. در این پژوهش پس از منبع‌شناسی و تهیه اسناد راهبردی امنیت سایبری ملی کشورها به استخراج مضامین پایه پرداخته شد و در مرحله بعدی تحلیل با تمرکز بر کلیدواژه‌ها و کدهای تعیین شده مضامین محوری و عناصر اصلی فضای سایبر استخراج شدند و در پایان مضامین فراگیر و گونه‌های شناسایی شده فضای سایبری معرفی شدند؛ به دلیل حجم زیاد صفحات مقاله از تفصیل این مباحث در قالب جداول جداگانه پرهیز نموده و نتایج کلیه مراحل فقط در یک جدول ارائه آورده شده‌اند.

٤-۱. استخراج مضامین پایه (تعاریف و توصیف‌های فضای سایبر)

پس از تهیه اسناد راهبردی امنیت سایبری کشورها شامل ویرایش آخر ۳۹ سند از ۳٤ کشور منتخب و کدگذاری و بررسی اولیه آن‌ها ابتدا تعاریف و توصیف‌های فضای سایبر را از هر سند استخراج، که نتایج این کار در جدول شماره ۱ آمده است، ستون سوم جدول تعاریف، توصیف‌ها و مضمون پایه استخراج شده از این اسناد را نشان می‌دهد.

٤-۲. استخراج مضامین محوری(عناصر اصلی فضای سایبر)

در این مرحله از تحلیل با تمرکز بر کلید واژه‌ها و کدهای تعیین شده در بخش قبلی شامل زیرساخت ارتباطی، زیرساخت پردازشی، تجهیزات، شبکه، زیرساخت‌های فناوری اطلاعات، سامانه‌های اطلاعاتی و پردازشی و ..... جستجو و انطباق آن با تعاریف، مضمون محوری هر یک از تعاریف استخراج شدند. نتایج یافته‌های این مرحله در ستون چهارم جدول ۱ آمده است.

٤-۳. استخراج مضامین فراگیر و جمع‌بندی گونه‌های شناسایی شده

در مرحله سوم به تعیین مضامین فراگیر بر اساس عناصر اصلی استخراج شده و مضامین محوری شناسایی شده پرداختیم که نتایج حاصل در ستون ۵ جدول شماره ۱ نشان داده شده است. همچنین در این مرحله براساس این مضامین فراگیر گونه‌های مختلف مفاهیم فضای سایبر مبتنی بر اسناد کشورهای منتخب شامل پنج گونه دسته‌بندی و جمع‌بندی شدند. این پنج گونه عبارتند از: (۱)تعریف فضای سایبری به عنوان یک زیرساخت اطلاعاتی و ارتباطی، یعنی فضایی که تنها به فناوری مربوط می‌شود؛ (۲) تعریف فضای سایبری به عنوان یک زیرساخت اطلاعاتی و ارتباطی و داده‌های موجود در آن، یعنی فضایی که تنها به فناوری مربوط می‌شود؛ (۳) تعریف فضای سایبری به عنوان مجموعه‌ای از تجهیزات، داده‌ها و افراد، یعنی فضایی که هم به فناوری و هم به افراد مربوط می‌شود؛ (٤) تعریف فضای سایبری به عنوان مجموعه‌ای از تجهیزات، داده‌ها و عملیات‌ها، یعنی فضایی که هم به فناوری و هم به فعالیت‌ها مربوط می‌شود؛ و (۵) تعریف فضای سایبری به عنوان مجموعهٔ جامعی از تجهیزات، داده‌ها، افراد و عملیات‌ها، یعنی فضایی که هم به فناوری و هم به جامعه مربوط می‌شود.

سرانجام پس از مرتب کردن و چیدمان گونه‌های مشابه(جابجایی سطرهای جدول) در کنارهم؛ طبقه‌بندی نهایی گونه‌های شناسایی شده از مفهوم فضای سایبر در جدول یک ارایه شده است.

جدول۱. شناسایی مضامین محوری، عناصر فضای سایبر و تعیین مضامین فراگیر و گونه‌های شناسایی شده[۱](منبع،جمع‌بندی مولفان)

ردیف	عنوان سند راهبرد ملی امنیت سایبری	مضمون پایه	عناصر اصلی سازنده فضای سایبر	مضمون فراگیر
۱	راهبرد امنیت سایبری ملی افغانستان	«فضای سایبری: محیطی متشکل از سامانه‌های اطلاعاتی که سراسر جهان را در بر می‌گیرند و همچنین شبکه‌هایی که این سامانه‌ها را به یکدیگر متصل می‌کنند».	تجهیزات (حامل، زیرساخت)	فضای سایبری به عنوان یک زیرساخت اطلاعاتی و ارتباطی
۲	راهبرد حفاظت و امنیت سامانه‌های اطلاعاتی فرانسه	«فضای ارتباطی حاصل از پیوند متقابل جهانی بین تجهیزات خودکار پردازش داده‌های دیجیتال».		
۳	راهبرد امنیت ملی ژاپن	«یک حوزهٔ جهانی متشکل از سامانه‌های اطلاعاتی، شبکه‌های مخابرات و غیره که بستری برای انجام فعالیت‌های اجتماعی، اقتصادی، نظامی و غیره فراهم می‌کند».		
٤	سند در باب تأیید برنامهٔ توسعهٔ امنیت اطلاعات الکترونیکی (امنیت سایبری) برای سال ۲۰۱۱ تا ۲۰۱۹ لیتوانی	«فضای سایبری یک فضای جهانی بدون هر گونه مرز ملی می‌باشد و از این رو تهدیدها به سرعت در آن گسترش می‌یابند».		
٥	راهبرد امنیت سایبری نیوزیلند	«یک شبکهٔ جهانی متشکل از زیرساخت‌های فناوری اطلاعات، شبکه های مخابرات و سامانه‌های پردازش رایانه‌ای مرتبط که در آن ارتباط برخط صورت می‌گیرد».		
٦	راهبرد پادشاهی عربستان سعودی برای توسعهٔ امنیت اطلاعات ملی	«یک حوزهٔ جهانی در درون محیط اطلاعاتی که از شبکه‌های به‌هم پیوستهٔ زیرساخت‌های سامانه‌های اطلاعاتی از جمله اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های موجود در آن‌ها تشکیل می‌شود».		
۷	راهبرد ملی حفاظت از سوئیس در برابر تهدیدهای سایبری	«دولت، بخش خصوصی و جامعه از زیرساخت‌های اطلاعاتی و ارتباطی و فضای سایبری (اینترنت، شبکه‌ها و برنامه‌های همراه، تجارت الکترونیک، دولت الکترونیک و برنامه‌های کنترل رایانه‌محور) استفاده می‌کنند».		
۸	راهبرد امنیت سایبری ملی و طرح اقدام ۲۰۱٤-۲۰۱۳ ترکیه	«محیطی متشکل از سامانه‌های اطلاعاتی که سراسر جهان را در بر می‌گیرند و همچنین شبکه‌هایی که این سامانه‌ها را به یکدیگر متصل می‌کنند».		
۹	راهبرد ملی ایمن‌سازی فضای سایبری آمریکا	«فضای سایبری از صدها هزار رایانه، سرور، مسیریاب ، سوده و کابل فیبر نوری به‌هم‌پیوسته که امکان فعالیتَ مؤثر زیرساخت‌های حیاتی ما را فراهم می‌کنند تشکیل شده است».		
۱۰	طرح ملی مشاغل و مطالعات امنیت سایبری آمریکا	«شبکهٔ به‌هم‌پیوستهٔ زیرساخت‌های فناوری اطلاعات که اینترنت، شبکهٔ مخابرات، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های موجود در آن‌ها را در بر می‌گیرد».		
۱۱	گزارش سیاست فضای سایبری: تضمین قابل	«زیرساخت اطلاعاتی و ارتباطی دیجیتال جهانی به‌هم‌پیوسته‌ای که «فضای سایبری» نامیده می‌شود اساس تقریباً تمام ابعاد جامعهٔ مدرن را		

[۱] . با توجه به تاکید دبیرخانه نشریه و بدلیل پرهیز از افزایش حجم مقاله جداول تفکیکی فرایند تحلیل مضمون از متن مقاله حذف شدند و صرفاً جمع‌بندی نهایی در جدول حاضر ارائه شده است.

	اطمینان و تاب‌آور بودن زیرساخت‌های ارتباطی آمریکا	تشکیل می‌دهد و از اقتصاد، زیرساخت‌های مدنی، ایمنی عمومی و امنیت ملی آمریکا پشتیبانی حیاتی می‌کند».		
۱۲	راهبرد امنیت سایبری بلژیک	«فضای سایبری محیطی جهانی برای ارتباط متقابل سامانه‌های اطلاعاتی و ارتباطی می‌باشد. فضای سایبری از دنیای رایانه وسیع‌تر است و شبکه‌های رایانه‌ای، سامانه‌های کامپیوتری، رسانه‌های دیجیتال و داده‌های دیجیتال فیزیکی یا مجازی را نیز در بر می‌گیرد».	تجهیزات + داده‌ها (اشیا، بار)	فضای سایبری به عنوان یک زیرساخت اطلاعاتی و ارتباطی و داده‌های موجود در آن
۱۳	راهبرد امنیت سایبری کانادا، برای کانادایی قوی‌تر و موفق‌تر	«فضای سایبری جهانی الکترونیکی است که از شبکه‌های به‌هم‌پیوستهٔ فناوری اطلاعات و اطلاعات موجود در این شبکه‌ها تشکیل می‌شود. این فضا یک حوزهٔ مشترک جهانی است که در آن بیش از ۱/۷ میلیارد نفر با برقراری ارتباط با یکدیگر به تبادل اندیشه‌ها، خدمات و دوستی با همدیگر می‌پردازند».		
۱۴	راهبرد امنیت سایبری آلمان	«فضای سایبری عبارت است از فضای مجازی تمام سامانه‌های فناوری اطلاعاتی که در مقیاس جهانی در سطح داده به یکدیگر متصل هستند. اینترنت به عنوان یک شبکهٔ جهانی و عمومی برای ارتباط و انتقال که می‌توان با استفاده از شبکه‌های دادهٔ اضافی آن را توسعه بخشید اساس فضای سایبری را تشکیل می‌دهد. سامانه‌های فناوری اطلاعاتی که در یک فضای مجازی مجزا قرار دارند جزء فضای سایبری نیستند».		
۱۵	راهبرد امنیت سایبری ملی مجارستان	«منظور از فضای سایبری سامانه‌های اطلاعاتی الکترونیکی، جهانی، به‌هم‌پیوسته، غیرمتمرکز و فزاینده و همچنین فرآیندهای اجتماعی و اقتصادی‌ای که در و از طریق این سامانه‌ها در قالب داده و اطلاعات شکل می‌گیرند می‌باشد».		
۱۶	فرهنگ واژه‌های نظامی و مرتبط با حوزهٔ نظامی وزارت دفاع آمریکا	«فضای سایبری: یک حوزهٔ جهانی در درون محیط اطلاعاتی که از شبکه‌های به‌هم‌پیوستهٔ زیرساخت‌های فناوری اطلاعات از جمله اینترنت، شبکه‌های مخابرات، سامانه‌های رایانه‌ای، پردازشگرها و کنترل‌کننده‌ها و همچنین داده‌های موجود در آن‌ها تشکیل می‌گردد».		
۱۷	راهبرد سایبری دفاع هلند	«فضای سایبری تمام مواردی را که به صورت دیجیتال به یکدیگر متصل هستند یا ممکن است متصل گردند شامل می‌شود. این حوزه هم اتصال‌های دائمی را در بر می‌گیرد و هم اتصال‌های موقتی یا محلی را و در تمام موارد به نوعی به داده‌ها (کد منبع، اطلاعات و سایر مواردِ) موجود در حوزه مربوط می‌شود».		
۱۸	چارچوب راهبردی ملی برای امنیت فضای سایبری ایتالیا	«فضای سایبری یک حوزهٔ ساخت بشر متشکل از گره‌ها و شبکه‌های فناوری اطلاعات و ارتباطات می‌باشد که حجم فزاینده‌ای از داده‌هایی را که برای کشورها، شرکت‌ها، شهروندان و همچنین تمام تصمیم‌گیرندگان سیاسی، اجتماعی و اقتصادی اهمیت راهبردی دارند در بر می‌گیرد و پردازش می‌کند».		
۱۹	راهبرد امنیت سایبری ژاپن: به سوی یک فضای سایبری سرآمد، تاب‌آور و قوی	«فضاهای مجازی جهانی از قبیل اینترنت که از سامانه‌های اطلاعاتی، شبکه‌های اطلاعاتی و ارتباطی و سامانه‌های مشابه تشکیل می‌شوند و حجم‌های وسیعی از انواع مختلف اطلاعات را انتقال می‌دهند به سرعت توسعه یافته‌اند و در حال فرا گرفتن فضای واقعی هستند».	تجهیزات + داده‌ها + سوژه‌ها (نقش‌ها یعنی کاربران)	فضای سایبری به عنوان مجموعه‌ای از تجهیزات، داده‌ها و افراد
۲۰	قطع‌نامهٔ شمارهٔ ۳۶۱۱: بهبود قابلیت‌های فضای سایبری ملی رژیم صهیونیستی	«حوزه‌ای فیزیکی و غیرفیزیکی که تمام یا بخشی از این عناصر را در برمی‌گیرد: سامانه‌های مکانیزه یا رایانه‌ای، شبکه‌های رایانه‌ای و ارتباطی، برنامه‌ها، اطلاعات رایانه‌ای، محتوایی که توسط رایانه‌ها منتقل می‌شوند، داده‌های ترافیکی و نظارتی و افرادی که از این داده‌ها استفاده می‌کنند».		
۲۱	اعلامیه تدوین سیاست امنیت سایبری ملی آفریقای جنوبی	«فضای سایبری یک محیط فیزیکی و غیرفیزیکی می‌باشد که تمام یا برخی از این عناصر را در برمی‌گیرد: رایانه‌ها، سامانه‌های رایانه‌ای، شبکه‌ها و برنامه‌های رایانه‌ای آن‌ها، داده‌های رایانه‌ای، داده‌های		

		محتوایی، داده‌های ترافیکی و کاربران».		
۲۲	راهبرد امنیت سایبری ملی قطر	«یک محیط مجازی یا الکترونیکی متشکل از شبکهٔ به‌هم‌پیوستهٔ فناوری‌های اطلاعاتی و ارتباطی (از قبیل اینترنت، شبکه‌های مخابرات، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های موجود در آن‌ها) که زمینهٔ دسترسی افراد به خدمات و اطلاعات را فراهم می‌کند».		
۲۳	راهبرد امنیت سایبری ملی اسپانیا	«فضای سایبری، که به حوزهٔ جهانی و پویای متشکل از زیرساخت‌های فناوری اطلاعات از جمله شبکه‌های اینترنتی و سامانه‌های اطلاعاتی و ارتباطی اطلاق می‌شود، مرزها را از بین برده است و کاربران خود را در یک جهانی‌سازی بی‌سابقه مشارکت می‌دهد که این امر فرصت‌های جدیدی ایجاد می‌کند ولی در عین حال چالش‌ها، ریسک‌ها و تهدیدهای تازه‌ای را نیز به وجود می‌آورد».		
۲٤	پیش‌نویس قانون امنیت سایبری و تغییر قوانین مرتبط جمهوری چک	«فضای سایبری یک محیط دیجیتال می‌باشد که امکان ایجاد، پردازش و تبادل اطلاعات را فراهم می‌کند و از سامانه‌ها و خدمات اطلاعاتی و شبکه‌های ارتباطی الکترونیکی تشکیل می‌شود».	تجهیزات + داده‌ها + عملیات‌ها (فعالیت‌ها/رفتارها)	فضای سایبری به عنوان مجموعه‌ای از تجهیزات، داده‌ها و عملیات‌ها
۲۵	راهبرد امنیت سایبری فنلاند	«حوزهٔ سایبری (محیط سایبری) یک حوزهٔ پردازش اطلاعات (داده‌های) الکترونیکی می‌باشد که از یک یا چند زیرساخت فناوری اطلاعات تشکیل می‌شود. این حوزه استفاده از الکترونیک و طیف الکترومغناطیسی جهت ذخیره‌سازی، پردازش و انتقال داده و اطلاعات از طریق شبکه‌های مخابرات را در بر می‌گیرد. منظور از پردازش اطلاعات (داده‌ها) گردآوری، ذخیره، سازماندهی، به‌کارگیری، انتقال، نمایش، بایگانی، پردازش، تلفیق، محافظت، حذف و از بین بردن اطلاعات (داده‌ها) و انجام سایر اقدامات مشابه روی آن‌ها می‌باشد».		
۲٦	راهبرد امنیت سایبری دولت کنیا	«فضای سایبری تنها اینترنت و فناوری‌های اطلاعاتی و ارتباطی را در بر نمی‌گیرد. فضای سایبری حوزه‌ای شبیه حوزه‌های زمین، هوا، دریا و فضا است ولی ویژگی‌ها و چالش‌های خاص خود را دارد. مشخصهٔ حوزهٔ سایبری ذخیره‌سازی، پردازش و تبادل داده از طریق سامانه‌های شبکه‌شده می‌باشد. این حوزه توسط زیرساخت‌های اطلاعاتی حیاتی پشتیبانی می‌شود و دارای ابعاد ملی و بین‌المللی‌ای است که صنعت، تجارت، مالکیت فکری، امنیت، فناوری، فرهنگ، سیاست و دیپلماسی را در بر می‌گیرند. از این رو، فضای سایبری نقش مهمی در اقتصاد جهانی ایفا می‌کند».		
۲۷	راهنمای تالین پیرامون قوانین بین‌المللی قابل اعمال در جنگ سایبری	«محیطی متشکل از عناصر فیزیکی و غیرفیزیکی که استفاده از رایانه‌ها و طیف الکترومغناطیسی جهت ذخیره‌سازی، پردازش و تبادل اطلاعات از طریق شبکه‌های رایانه‌ای را در بر می‌گیرد».		
۲۸	راهبرد امنیت سایبری بریتانیا: حفاظت و ارتقاء بریتانیا در دنیای دیجیتال	«فضای سایبری انواع مختلف فعالیت‌های دیجیتال شبکه‌ای را در بر می‌گیرد. این فضا محتوا و فعالیت‌هایی که از طریق شبکه‌های دیجیتال انجام می‌شوند را شامل می‌شود».		
۲۹	راهبرد امنیت سایبری بریتانیا: ایمنی، امنیت و تاب‌آوری در فضای سایبری	«فضای سایبری یک حوزهٔ تعاملی متشکل از شبکه‌های دیجیتال است که جهت ذخیره‌سازی، پردازش و انتقال اطلاعات به کار برده می‌شود. فضای سایبری از اینترنت و همچنین سایر سامانه‌های اطلاعاتی که به تجارت، زیرساخت‌ها و خدمات کمک می‌کنند تشکیل می‌شود».		

۳۰	راهبرد امنیت سایبری اتریش	«فضای سایبری عبارت است از فضای مجازی تمام سامانه‌های فناوری اطلاعاتی که در مقیاس جهانی در سطح داده به یکدیگر متصل هستند. اینترنت به عنوان یک شبکهٔ جهانی و عمومی برای ارتباط و انتقال که می‌توان با استفاده از شبکه‌های دادهٔ اضافی آن را توسعه بخشید اساس فضای سایبری را تشکیل می‌دهد. فضای سایبری به شبکهٔ جهانی زیرساخت‌های مستقل و مختلف فناوری اطلاعات، شبکه‌های مخابرات و سامانه‌های رایانه‌ای نیز اطلاق می‌شود. در حوزهٔ اجتماعی، استفاده از این شبکهٔ جهانی افراد را به تعامل، تبادل نظر، انتشار اطلاعات، حمایت اجتماعی، انجام فعالیت‌های اقتصادی، کنترل فعالیت‌ها، خلق آثار هنری و رسانه‌ای، بازی، مشارکت در بحث‌های سیاسی و بسیاری موارد دیگر قادر می‌سازد».	تجهیزات + داده‌ها + نقش‌ها و عملیات (مجموعه چهار عنصر)	فضای سایبری به عنوان مجموعهٔ جامعی از تجهیزات، داده‌هجموعه چهار عنصر)، افراد و عملیات‌ها
۳۱	راهبرد امنیت فضای سایبری ملی چین	«در پی توسعهٔ گستردهٔ انقلاب اطلاعاتی، یک فضای سایبری متشکل از اینترنت، شبکه‌های مخابرات، سامانه‌های رایانه‌ای، سامانه‌های کنترل خودکار، تجهیزات دیجیتال و کاربردها، خدمات و داده‌های آن‌ها، در حال ایجاد تغییرات اساسی در روش‌های تولید و زندگی مردم و اثرگذاری عمیق بر فرآیند رشد اجتماعی تاریخی بشر است».		
۳۲	رهنمودهای سیاستی کلمبیا پیرامون امنیت سایبری و دفاع سایبری	«محیطی فیزیکی و مجازی متشکل از رایانه‌ها، سامانه‌های رایانه‌ای، برنامه‌ها (نرم‌افزارهای) رایانه‌ای، شبکه‌های مخابرات، داده‌ها و شبکه‌های اطلاعاتی که در آن کاربران به تعامل با یکدیگر می‌پردازند».		
۳۳	سیاست امنیت سایبری ملی هند	«فضای سایبری محیطی پیچیده متشکل از تعامل‌های بین افراد و خدمات می‌باشد که توسط ابزارها و شبکه‌های فناوری‌های اطلاعاتی و ارتباطی در سطح جهان پشتیبانی می‌شود».		
۳٤	راهبرد امنیت سایبری لتونی برای سال ۲۰۱٤ تا ۲۰۱۸	«فضای سایبری یک محیط تعاملی می‌باشد که از کاربران، شبکه‌ها، فناوری‌های رایانشی، نرم‌افزارها، فرآیندها، اطلاعات ذخیره‌شده یا در حال انتقال، برنامه‌ها، خدمات و سامانه‌هایی که می‌توان آن‌ها را به طور مستقیم یا غیرمستقیم به اینترنت، شبکه‌های مخابرات و شبکه‌های رایانه‌ای متصل کرد تشکیل می‌شود».		
۳۵	راهبرد امنیت سایبری ملی مونته‌نگرو برای سال ۲۰۱۳ تا ۲۰۱۷	«هر چیز مرتبط با یا دربرگیرندهٔ رایانه‌ها یا شبکه‌های رایانه‌ای از قبیل اینترنت. فضای سایبری فراتر از اینترنت است. فضای سایبری نه تنها سخت‌افزارها، نرم‌افزارها و سامانه‌های اطلاعاتی بلکه افراد و تعامل‌های اجتماعی در این شبکه‌ها را نیز در بر می‌گیرد».		
۳٦	سیاست حفاظت از فضای سایبری جمهوری لهستان	«فضایی برای پردازش و تبادل اطلاعات که از سامانه‌های اطلاعاتی و ارتباطی، پیوندهای بین آن‌ها و روابط با کاربران تشکیل می‌شود».		
۳۷	راهبرد امنیت سایبری رومانی و طرح اقدام در زمینهٔ توسعهٔ نظام امنیت اطلاعات ملی	«فضایی مجازی که توسط زیرساخت‌های سایبری ایجاد می‌گردد و پردازش، ذخیره‌سازی یا انتقال اطلاعات و عملیات‌های کاربران در این فضا را در برمی‌گیرد».		
۳۸	دیدگاه‌های ادراکی در مورد فعالیت‌های نیروهای مسلح فدراسیون روسیه در فضای اطلاعاتی	«فضای اطلاعاتی: یک حوزهٔ فعالیت که به تشکیل، ایجاد، تغییر، انتقال، به‌کارگیری و ذخیره‌سازی اطلاعات مربوط می‌شود و بر موارد متعددی از جمله آگاهی فردی و جمعی، زیرساخت‌های اطلاعاتی و خود اطلاعات تأثیر می‌گذارد».		
۳۹	راهبرد ادراکی برای امنیت سایبری فدراسیون	«فضای سایبری: یک حوزهٔ فعالیت در فضای اطلاعاتی که توسط مجاری ارتباطی اینترنت و سایر شبکه‌های مخابرات و زیرساخت‌های		

	روسیه	فناوری که عملکرد مؤثر آن را تضمین می‌کنند و هر گونه دادهٔ مربوط به فعالیت‌هایی که افراد، نهادها و کشورها در آن انجام می‌دهند ایجاد می‌گردد».		
٤٠	پروژه بررسی مفاهیم پایه و بنیادی حوزه‌های سایبری و کارگروه سایبری ن.م	به شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه شده (جاگذاری شده)، کنترل‌کننده‌های صنایع، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات گفته می‌شود که ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد		

٤-٤. گروه‌بندی کشورهای منتخب براساس گونه‌های شناسایی شده

همانطور که در جدول دو مشاهده شد، مبنای گونه‌شناسی بر اساس تعاریف مستخرج از اسناد راهبردی کشورها بود(ستون دوم جدول دو)، حال اگر در جدول شماره یک به جای عنوان سند نام کشور مربوطه را قرار دهیم در این‌صورت نگاشتی از کشورها به گونه‌ها به دست می‌آید، یعنی مشخص می‌شود که هر کشور در کدام گونه قرار دارد. در گام آخر با با کنار هم قراردادن و مرتب کردن سطرهای این جدول بر اساس گونه‌ها به نگاشت کشورهای منتخب به گونه‌ها می‌رسیم، یعنی می‌توانیم کشورها را بر اساس گونه‌شناسی انجام شده دسته‌بندی و گروه‌بندی نمود. نتایج این کار در جدول دو آمده است. این جدول نشان می‌دهد که هر کدام از کشورهای منتخب بر چه گونه‌ای از فضای سایبر تمرکز نموده‌اند.

جدول ۲. گروه‌بندی کشورها بر اساس گونه‌های شناسایی شده (منبع، جمع‌بندی مولفان)

ردیف	کشورها	گونه‌های مفهوم فضای سایبر	عنوان گونه
۱	افغانستان	فضای سایبری به عنوان یک زیرساخت اطلاعاتی و ارتباطی(تجهیزات)	گونه اول
۲	فرانسه		
۳	ژاپن		
٤	لیتوانی ۲۰۱۱ تا ۲۰۱۹		
٥	نیوزیلند		
٦	عربستان سعودی		
۷	سوئیس		
۸	ترکیه ۲۰۱٤-۲۰۱۳		
۹	آمریکا[1]		
۱۰	بلژیک	فضای سایبری به عنوان یک زیرساخت اطلاعاتی و ارتباطی و داده‌های موجود در آن (تجهیزات و داده‌ها)	گونه شماره ۲
۱۱	کانادا		
۱۲	آلمان		
۱۳	مجارستان		
۱٤	آمریکا [2]		
۱٥	هلند		
۱٦	ایتالیا		
۱۷	ژاپن	فضای سایبری به عنوان مجموعه‌ای از تجهیزات، داده‌ها و افراد	گونه شماره ۳
۱۸	رژیم صهیونیستی		
۱۹	آفریقای جنوبی		
۲۰	قطر		
۲۱	اسپانیا		
۲۲	چک	فضای سایبری به عنوان مجموعه‌ای از تجهیزات، داده‌ها و عملیات	گونه شماره ٤
۲۳	فنلاند		
۲٤	کنیا		
۲٥	تالین		
۲٦	بریتانیا		
۲۷	اتریش	فضای سایبری به عنوان مجموعهٔ جامعی از تجهیزات، داده‌ها، افراد و عملیات	گونه شماره ٥
۲۸	چین		
۲۹	کلمبیا		
۳۰	هند		
۳۱	لتونی ۲۰۱٤ تا ۲۰۱۸		
۳۲	مونته‌نگرو ۲۰۱۳ تا ۲۰۱۷		
۳۳	لهستان		

[1] . براساس اسناد راهبرد ملی ایمن‌سازی فضای سایبری آمریکا، طرح ملی مشاغل و مطالعات امنیت سایبری آمریکا گزارش سیاست فضای سایبری: تضمین قابل اطمینان و تاب‌آور بودن زیرساخت‌های ارتباطی آمریکا

[2] . براساس سند فرهنگ واژه‌های نظامی و مرتبط با حوزهٔ نظامی وزارت دفاع

ردیف	کشورها	گونه‌های مفهوم فضای سایبر	عنوان گونه
۳٤	رومانی		
۳۵	روسیه		

۵. جمع‌بندی و نتیجه‌گیری

مفهوم و عناصر اصلی فضای سایبری در یک سیر تاریخی توسعه و تکامل یافته‌اند. همچنین سازمان‌ها، مراکز و نهادهای علمی کشورهای مختلف تاکنون تعاریف و توصیف‌های گوناگونی برای این مفهوم و عناصر اصلی آن ارایه داده‌اند. مفهومی که در دهه ۱۹۸۰ پدید آمد، در ابتدا فضای کاملاً مجزا از دنیای فیزیکی تلقی می‌شد، در ادامه برخی از اندیشمندان بر این که این فضا کاملاً فیزیکی است تمرکز نموده‌اند. در حال حاضر فضای سایبر بخش جدایی‌ناپذیر از این زندگی فردی و اجتماعی را تشکیل می‌دهد و با امتزاج این دو فضا، جهان به سرعت و شتاب روزافزون به سمت جامعه سایبری- فیزیکی یا جامعه الحاقی در حرکت است و مردم نقاط مختلف جهان از طریق مجموعه‌ای از پیوندهای شبکه شده به تعامل، همکاری و رقابت با یکدیگر می‌پردازند.

این مطالعه نشان می‌دهد که برخی از تعاریف ارایه شده بر عنصر فناوری (شامل تجهیزات ذخیره‌سازی، پردازش و تبادل اطلاعات و زیرساخت ارتباطی و اطلاعاتی و کنترل‌کننده‌ها) تمرکز دارند و به عنصر انسانی و اجتماعی فضای سایبری توجهی ندارند، درحالی‌که برخی دیگر بر کاربران انسانی توجه و تمرکز بیشتری نموده‌اند. اگرچه تعاریف گوناگون برای فضای سایبر ارائه شده ولی بیشتر این تعاریف یک بعد مشترک دارند، هسته فضای سایبر از سخت‌افزار و نرم‌افزارهای بین‌المللی متصل به هم و داده‌های مربوط به آن تشکیل می‌شود و بعلاوه افراد می‌توانند به این فضا متصل شوند و هنگام استفاده از اینترنت، افراد و فضای سایبر در هم آمیخته می‌شوند.

جمع‌بندی این مطالعه نشان می‌دهد که در یک نگاه جامع فضای سایبر چهار عنصر اصلی شامل تجهیزات (حامل، زیرساخت)، داده‌ها (اشیاء، بار)، نقش‌ها (سوژه‌ها و کاربران) و عملیات (فعالیت‌ها و رفتار) را دربرمی‌گیرد. می‌توان گفت حامل‌های انواع مختلف بار (سیگنال، داده، اطلاعات و غیره) حکم «تجهیزات» را دارند چرا که همهٔ آن‌ها در فضای سایبری ویژگی‌های یکسانی دارند که تمام آن‌ها به «حمل کردن» مربوط می‌شوند. عنصر «داده» به نشان‌های دیجیتالی اطلاق می‌شود که بیانگر اطلاعاتی از قبیل نور، برق، خاصیت مغناطیسی، کوانتوم (و حتی ذره-های کوچک‌تری که ممکن است در آینده پدید آیند) و غیره در فضای سایبری هستند و حکم «بار» در تعریف «شبکه» را دارد همچنین، داده‌ها نتایج پردازش‌شده و همچنین انعکاس هدف یک فعالیت مشخص می‌باشند. عنصرِ «تجهیزات» و «داده‌ها» به سطح فناوری مربوط می‌شوند، ویژگی‌های «شبکه» را منعکس می‌کنند و معمولاً به‌مثابه نقاط اقدامی هستند که مدیریت می‌گردند. عنصرِ «نقش‌ها» تمام نقش‌ها و کاربران در فضای سایبری را در برمی‌گیرد. در این فضا، انسان‌ها نقش‌ها می‌باشند. افزون بر این، سازمان‌ها، وسایل، نرم‌افزارها، پایگاه‌های اینترنتی، انسان‌های مجازی (ربات‌ها)، وسایل شبکه (مسیریاب) و غیره نیز می‌توانند نقش‌های اصلی باشند که قادر به تولید اطلاعات هستند. هم «نقش‌ها» و هم «عملیات» به سطوح اجتماعی تعلق دارند و ویژگی‌های «فضا» را منعکس می‌کنند. در فضای سایبری، «نقش‌ها» و «عملیات» از اهمیت زیادی برخوردار هستند.

با توجه به این که مفهوم فضای سایبر از سال ۲۰۰۹ تا ۲۰۱۹ در یک سیر تکاملی توسعه یافته است پیشنهاد مولفان، تمرکز کشور به گونه پنجم مفاهیم احصا شده یعنی فضای سایبری به عنوان مجموعهٔ جامعی از تجهیزات،

داده‌ها، افراد و عملیات است و با توجه به ویژگی خاص جامعه اسلامی توجه بیشتر به سطوح اجتماعی این فضا در کشور یعنی نقش‌ها و عملیات مورد تاکید است. در این پژوهش ۴۰ سند راهبرد (امنیت) سایبری ۳۵ کشور منتخب طی سال‌های ۲۰۰۹ تا ۲۰۱۹ مورد بررسی و نهایتاً براساس عناصر شکل‌دهنده‌ی فضای سایبر ۵ گونه مختلف از مفهوم فضای سایبری شناسایی و دسته‌بندی شد. این ۵ گونه شامل فضای سایبری به عنوان یک زیرساخت اطلاعاتی و ارتباطی(تجهیزات)؛ فضای سایبری به عنوان یک زیرساخت اطلاعاتی و ارتباطی و داده‌های موجود در آن؛ فضای سایبری به عنوان مجموعه‌ای از تجهیزات، داده‌ها و افراد؛ فضای سایبری به عنوان مجموعه‌ای از تجهیزات، داده‌ها و عملیات؛ فضای سایبری به عنوان مجموعهٔ جامعی از تجهیزات، داده‌ها، افراد و عملیات‌ها است. همچنین نگاشتی از کشورهای مختلف به این ۵ گونه ارائه شد.

برای بررسی وجوه اشتراک و افتراق این گونه‌ها توجه به چهار عناصر اصلی فضای سایبر مبنای مناسبی می‌تواند باشد. مهمترین وجه مشترک این پنج گونه توجه به زیرساخت اطلاعاتی و ارتباطی(تجهیزات) به عنوان عنصر پایه فضای سایبر و وجه مشترک گونه‌های دوم تا پنجم توجه به عنصر داده‌ها به عنوان یک عنصر اساسی فضای سایبر است. مهمترین افتراق دو گونه اول با سایر گونه‌ها عدم توجه این دو گونه به سطوح اجتماعی فضای سایبر می‌باشد که از اهمیت زیادی برخوردار است. تعاریف دسته‌بندی شده در گونه پنجم به هر چهار عنصر اصلی فضای سایبر و ابعاد فنی و اجتماعی این فضا پرداخته و لذا کامل‌ترین گونه تعاریف محسوب می‌شوند.

نتایج این پژوهش می‌تواند در توسعه نگاه جامع به فضای سایبر و توجه متوازن به عناصر اصلی آن و تبیین بهتر مفهوم این فضا و ایجاد زبان مشترک و رفع ابهامات، پیچیدگی و ناهماهنگی‌ها، و برخی مشکلات ناشی از ضعف زبان مشترک مورد استفاده دانشجویان، محققان و مراکز مطالعاتی و اجرایی مرتبط قرار گیرد. اصلح است این مراکز در اسناد و تحقیقات خود مشخص نمایند که کدام گونه از تعاریف فضای سایبر و عناصر اصلی آن را مبنای مطالعه و عمل خود قرارداده‌اند.

فهرست منابع و مآخذ فارسی

- خلیلی، احمد. زبردست، اسفندیار و عزیزی، محمد مهدی، (زمستان ۱۳۹٦)، «**گونه‌شناسی سیاست‌های مدیریت شهری در مناطق شهربنیان**»، فصلنامه معماری و شهرسازی آرمان‌شهر، شماره ۲۱، ۲۹۱-۳۰۸.
- دهقان اشکذری، محمدجواد. میرعمادی، طاهره و قاضی نوری، سید سپهر، (زمستان ۱۳۹۷)، «**گونه‌شناسی نظریه‌های بین‌المللی‌سازی نظام‌های نوآوری**»، پژوهش‌های مدیریت عمومی، سال یازدهم، شماره ٤۲، ۳۳-٦۰.
- کریمی قهرودی، محمدرضا و زارعی، وحید، (۱۳۹۹)، «**حاکمیت فضای سایبری اندیشه‌هایی پیرامون جامعه‌ای با آینده مشترک در فضای سایبر**»، انتشارات مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، ۷۵-۱۲۵.
- کریمی قهرودی، محمدرضا و کیان‌خواه، احسان، (تابستان ۱۳۹٤)، «**چالش آفرینی اینترنت اشیا بر ارکان امنیت ملی کشور**»، فصلنامه علمی امنیت ملی، سال چهارم، شماره شانزدهم، ۸۱-۱۰٦.
- کیان‌خواه، احسان، (زمستان ۱۳۹۸)، «**چالش‌های راهبردی حکمرانی با گسترش فضای سایبر**»، فصلنامه علمی امنیت ملی، سال نهم، شماره سی‌وچهارم، ۱۵۳-۱۷٤.
- لطیفی، میثم (زمستان ۱۳۹۷)، «**روش‌شناسی گونه‌شناسی: رهنمونی بر نظریه‌پردازی در دانش مدیریت**»، فصلنامه مطالعات مدیریت دولتی ایران، دوره اول، شماره ۲، ۲۵-۵۲.

فهرست منابع و مآخذ انگلیسی

- ۲٦ Years After Gibson, Pentagon Defines ‘Cyberspace’. https://www. wired.com/۲۰۰۸/۰۵/pentagon-define/ [۲۰۱٦-۹-۷].
- afieldfile/۲۰۱۳/۱۲/۱۷/NSS.pdf [۲۰ ۱٦-۹-۲٤].
- against_cyber_risksEN.pdf [۲۰۱٦-۹-۲٤].
- Annex ۱ to Government Decision No. ۱۱۳۹/۲۰۱۳ National Cyber Security Strategy of Hungary, ۲۰۱۳: ۳. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss map/HU_NCSS.pdf [۲۰۱٦-۹-٤].
- Austrian Cyber Security Strategy, ۲۰۱۳: ۲۱. https://www.enisa.euro pa.eu/topics/national-cybersecurity-strategies/ncss-map/AT_NCSS.pdf [۲۰۱٦-۹-۲٤].
- Belgium, Cyber Security Strategy, ۲۰۱۲: ۱۲. https://www.enisa.europa. eu/topics/national-cybersecurity-strategies/ncss-map/belgian-cyber-sec urity-strategy/at_download/file [۲۰۱٦-۹-۲٤].
- Braun, viriginia and Clarke(۲۰۰٦)”using thematic analysis in psychology” Qualititative research , Vol.۳ No.۲:۷٦-۱۰۱ Retrived from: http:eprints.uwe.ac.//۱۱۷۳۵.
- Canada’s Cyber Security Strategy, For a Stronger and More Prosperous Canada, ۲۰۱۰: ۲. http://www.publicsafety.gc.ca/cnt/rsrcs/p blctns/cbr-scrt-strtgy/index-eng.aspx [۲۰۱٦-۹-۲٤].

- Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space, p. ٥. https://ccdcoe.org/ strategies/Russian_Federation_unofficial_translation.pdf ,٢٠١٦.
- Cyber Security Strategy for Germany, ٢٠١١: ٩. http://www.cio.bund. de/SharedDocs/Publikationen/DE.
- Cyber Security Strategy of Latvia ٢٠١٤-٢٠١٨, ٢٠١٤.https://www.enisa. europa.eu/topics/national-cyber-security-strategies/n css-map/lv-ncss [٢٠١٦-٩-٢٤]. r%٢٠Montenegro.pdf [٢٠١٦-٩-٢٤].
- Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space, ٢٠٠٩:٧. https://www.gov.uk/government/ uploads/system/uploads/attachment_data/file/٢٢٨٨٤١/٧٦٤٢.pdf [٢٠١٦-٢٤].
- Cybersecurity Strategy: Towards a world-leading, resilient and vigorous cyberspace, ٢٠١٣: ٥. http://www.nisc.go.jp/active/kihon/pdf/ cybersecuritystrategy-en.pdf [٢٠١٦-٩-٢٤].
- Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, ٢٠٠٩: III. https://ww w.smartgrid.gov/files/Cyberspace_Policy_Review _Assuring_ Trusted_ Resilient_Informat_٢٠٠٩٠٨.pdf [٢٠١٦-٩-٢٤].
- Cyberspace Protection Policy of the Republic of Poland, ٢٠١٣: ٥. https: //www.enisa.europa.eu/topics.
- Cyberspace: Definition and Implications. https://ccdcoe.org/multime dia/cyberspace-definitionand-implications.html [٢٠١٦-٩-٦].
- Czech Republic, Draft Act on Cyber Security and Change of Related Acts (Act on Cyber Security), ٢٠١٤: ٢. https://www.govcert.cz/downlo ad/legislativa/container-nodeid-١١٦٨/draftactcybersecurity-١٣٠٤١٥.pdf [٢٠١٦-١٢-٣١].
- Denmark A, Mulvenon J (٢٠١٠) Contested commons. Contested commons: the future of American power in a multi-polar world, pp ٣-٤٨. https://s٣.amazonaws.com/files.cnas.org/documents/CNAS-Contest ed-Commons_١.pdf [٢٠١٦-١٢-٣١].
- Department of Communications, Notice of Intention to Make South African National Policy, ٢٠١٠: ١٢. http://www.gov.za/sites/www.gov. za/files/٣٢٩٦٣_١١٨_٠.pdf [٢٠١٦-٩-٢٤].
- Developing National Information Security Strategy for the Kingdom of Saudi Arabia, NISS, DRAFT ٧: A- http://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repositoy/ SaudiArabia_NISS_Draft_٧_EN.pdf ٢٠١٦-١٢-٣١].
- Discussion on origin and translation of cyberspace. http://www.٣٦٠doc. com/content/١٦/٠١١٥/١٩/٢١٩٦٦٢٦٧ _ ٥٢٨٢٢٠٣٧٢.shtml [٢٠١٦-١٢-٣١].
- Finland´s Cyber Security Strategy. http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/٤٠-finlandas-cyber-security-strategy [٢٠١٦-٩-٢٥].
- Finland’s Cyber Security Strategy Government Resolution ٢٤ Jan ٢٠١٣. https://ccdcoe.org/cyberdefinitions .html [٢٠١٦-٩-١٠.
- Government of Kenya Cybersecurity Strategy, ٢٠١٤: ٢. http://www.ict a.go.ke/wp-content/uploads/٢٠١٤ /٠٣/ GOK-national-cybersecurity-strat egy.pdf [٢٠١٦-٩-٢٥].
- Government of the Republic of Lithuania Resolution No. ٧٩٦ of ٢٩ June ٢٠١١ on the approval of the programme for the development of electronic information security (cyber-security) for ٢٠١١-٢٠١٩, ٢٠١١: ٣. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National Strategies _Repository/ Lithuania_ ٢٠١١_ EIS(KS)PP_٧٩٦_٢٠١١-٠٦-٢٩_E N_PATAIS.pdf [٢٠١٦-٩-٢٤].
- Hotărârea nr. ٢٧١/٢٠١٣ pentru aprobarea Strategiei de securitate Cibernetică a României şi a Planului de Acţiune la Nivel Naţional Privind Implementarea Sistemului Naţional de Securitate.

Cibernetică,۲۰۱۳:۷.https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncssmap/.
- Information Systems Defence and Security: France's Strategy, ۲۰۱۱: ۲۱. http://www.ssi.gouv.fr /uploads / IMG /pdf/۲۰۱۱-۰۲-۱۵_Information_ system_defence_and_security_-_France_s_strategy. pdf [۲۰۱٦-۹-۲٤].
- International Organization for Standardization, ISO/IEC۲۷۰۳۲:۲۰۱۲, Information technology Security techniques - Guidelines for cyber security. https://www.iso.org/obp/ui/#iso:std:iso-iec:۲۷۰۳۲:ed-۱:v۱:en [۲۰۱٦-۹-۱۹].
- Israel, Resolution No. ۳٦۱۱: Advancing National Cyberspace Capabilities, ۲۰۱۱: http://www.itu.int /en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Israel_۲۰۱۱_Advancing %۲۰National %۲۰ Cyberspace%۲۰Capabilities.pdf [۲۰۱٦-۹-۲٤].
- Japan, National Security Strategy, ۲۰۱۳: ۹.http://japan.kantei.go.jp/۹٦_abe/documents/۲۰۱۳/__icsFiles.
- Joint Publication ۳-۱۲(R): Cyberspace Operation. http://www.dtic.mil/ doctrine/new_pubs/jp۳_۱۲R.pdf [۲۰۱٦-۹-٥].
- Ministry of Communication and Information Technolory, India, National Cyber Security Policy-۲۰۱۳ (NCSP-۲۰۱۳), ۲۰۱۳: ۱. http:// meity.gov.in/sites/upload_files/dit/files/National%۲۰ Cyber%۲۰Security %۲۰Policy%۲۰(۱).pdf [۲۰۱٦-۹-۲٤].
- National Cyber Security Strategy for Montenegro ۲۰۱۳-۲۰۱۷, ۲۰۱۳: ٥. http://www.mid.gov.me/ ResourceManager/FileDownload.aspx?rid=۱٦٥٤۱٦&rType=۲&file=Cyber%۲۰Security%۲۰Strategy%۲۰fo.
- National Cyber Security Strategy of Afghanistan, ۲۰۱٤.http://nic.af/Content/files/National %۲۰Cybersecurity%۲۰ Strategy%۲۰of%۲۰Afghanistan%۲۰(November۲۰۱٤).pdf [۲۰۱٦-۹-۲٥].
- National Cyberspace Security Strategy. http://www.cac.gov.cn/۲۰۱٦-۱۲/۲۷/c_۱۱۲۰۱۹٥۹۲٦.htm [۲۰۱٦].
- National Initiative for Cybersecurity Careers and Studies, Explore Terms: A Glossary of Common Cybersecurity Terminology. https://def inedterm.com/a/download/document/۱۱۱۲۸ [۲۰۱٦-۹-۲٤].
- National strategy for the protection of Switzerland against cyber risks, ۲۰۱۲: ٥. https://www.enisa.europa .eu / topics/national-cybersecuritystrategies/ncssmap/National_strategy_for_the protection_of_Switzerland.
- national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf [۲۰۱٦-۹-۲٤].
- Netherlands, The Defence Cyber Strategy, ۲۰۱۲: ٤. https://ccdcoe.org/ strategies/Defence_Cyber_Strategy_ NDL .pdf [۲۰۱٦-۹-۲٤].
- New Zealand's Cyber Security Strategy, ۲۰۱۱: ۱۲. http://www.dpmc. govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-۲۰۱۱ _۰.pdf [۲۰۱٦-۹-۲٤].
- Qatar National Cyber Security Strategy, ۲۰۱٤: ۲۳. https://www.itu.int /en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Qatar_۲۰۱٤_national_cyber_security_strategy.pdf [۲۰۱٦-۹-۲٥].
- Rattray G, Evans C, Healey J. Chapter V: American security in the cyber commons. https://s۳.amazonaws.com/files.cnas.org/documents/ CNAS-Contested-Commons_۱.pdf [۲۰۱٦-۱۲-۳۱].
- Republic of Colombia, National Planning Department, Policy Guidelins for Cybersecurity and Cyberdefense, ۲۰۱۱: ۳٤. https://www.sites.oas.org/cyber/Documents/Colombia%۲۰-%۲۰National%۲۰ Cybersecurity%۲۰and%۲۰Cyberdefense%۲۰Policy.pdf [۲۰۱٦-۹-۲٤].
- Series X: Data Networks, Open System Communications and Security. Telecommunication security. Overview of cybersecurity. http://www. itu.int/rec/T-REC-X.۱۲۰٥-۲۰۰۸۰٤-I [۲۰۱٦-۱۲-۳۱].

- Some Principles of Cyber Strategy—Analysis—Eurasia Review. ISN Security Watch, ۲۰۱٤. http://maritimesecurity.asia/free-۲/sea-lines-of-co mmunication/some-principles-of-cyber-strategyanalysis-eurasia-review/ [۲۰۱٦-۹-٦].
- Spain, National Cyber Security Strategy, ۲۰۱۳: ۹. https://www.enisa. europa.eu/topics/nationalcyber-security-strategies/ncssmap/NCSS_ESe n.pdf [۲۰۱٦-۹-۲٤].
- Strate L (۱۹۹۹) The varieties of cyberspace: problems in definition and delimitation. Western J Commun ٦۳(۳):۳۸۲–٤۱۲].
- StrategiaDeSecuritateCibernetica%۲۰ARomaniei.pdf [۲۰۱٦-۱۲-۳۱].
- Strategische-Themen/css_engl_download.pdf? __blob=publicationFile [۲۰۱٦-۹-۲٤].
- The NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare, ۲۰۱۳: ۲۱۱. http://www.jku.at/intlaw/content/e۲۷٥۸۳۱/e۲۷٥۸۳٦/e۲۷٦٦۲۹/Talli nn_Manual_CW.pdf [۲۰۱٦-۹-.
- Turkey, National Cyber Security Strategy and ۲۰۱۳–۲۰۱٤ Action Plan, ۲۰۱۳: ۸. https://www.enisa.europa.eu/topics/national-cyber-security-str ategies/ncss-map/national-cybersecurity-strategyand-۲۰۱۳-۲۰۱٤-action -plan/at_download/file [۲۰۱٦-۹-۲٤].
- United Kingdom, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, ۲۰۱۱:۱۱. https://www.gov.uk/ government/uploads/system/uploads/attachment_data/file/٦۰۹٦۱/uk-cy ber-security-strategy-final.pdf [۲۰۱٦-۹-۲٤].
- White House, and United States of America. The National Strategy to Secure Cyberspace. https://www.us-cert.gov/sites/default/files/publicat ions/cyberspace_strategy.pdf [۲۰۱٦-۹-۱۷].
- Wiener N (۱۹٤۸) Cybernetics or control and communication in the animal and the machine, Vol ۲٥. MIT press. http://www.allen-riley.com/ utopia/cybernetics.pdf [۲۰۱٦-۹-۲٤].
- William G (۱۹۸٤) Neuromancer, Vol ٤. Phantasia Press Edition, Bloomfield, MI. http://www.taodocs .com/p- ٤۰٤٦۰۷۹.html [۲۰۱٦-۱۲-۳۱].
- William G. BURNING CHROME. http://dinhe.net/*aredridel/.notmine /www.digipromo.com/vruz/ebooks /scifi/William%۲۰Gibson-Burning %۲۰Chrome.rtf [۲۰۱٦-۱۱-۳۰].
- Wolff HVH (۲۰۱۳) Territorial sovereignty and neutrality in cyberspace. Intl L Stud Ser US Naval War ۸۹:i. https://www.usnwc. edu/getattachment/ff۹٥۳۷ce-۹٤d٦-٤۹a۸-٥۱e۳۳٥۱۲٦c۱e/vonHeinegg.aspx [۲۰۱٦-۹-۲٤].
- Wolff HVH (۲۰۱۳) Territorial sovereignty and neutrality in cyberspace. Intl L Stud Ser US Naval War ۸۹:i. https://www.usnwc. edu/getattachment/ff۹٥۳۷ce-۹٤d٦--a۹ef-٥۱e۳۳٥۱۲٦c۱e/vonHeine gg.aspx[۲۰۱٦-۹-۲٤].
- Yannakogeorgos P (۲۰۰۹) Technogeopolitics of militarization and security in cyberspace. https://rucore.libraries.rutgers.edu/rutgers-lib/۲ ٦۱۱۸/PDF/۱/ [۲۰۱٦-۹-۲٤].
- Концепция Стратегии Кибербезопасности Российской Федерации, p. ۲. http://council.gov.ru/media/ files/٤۱d٤b۳dfbdb۲٥cea۸a۷۳.pdf [۲۰۱٦-۹-۲٤].