فصلنامه
سیاست‌نامهٔ علم و فناوری
دورهٔ ۱۵، شمارهٔ ۲، تابستان ۱۴۰۴

مقالهٔ مروری
صفحات ۹۶-۱۱۴

مروری بر مدل‌های لایه‌بندی فضای سایبری و پیشنهاد مدلی جدید

: 20.1001.1.24767220.1404.15.2.5.3

احسان خوشحال‌پور[۱]

چکیده

امروزه فضای سایبری به جزئی جدایی‌ناپذیر از زندگی بشر تبدیل شده است و بسیاری از نیازمندی‌های زندگی بشر در قالب امکانات مختلفی که این فنّاوری فراهم می‌آورد تأمین می‌شود. این تحول فنّاورانه با داشتن مزیت‌هایی نظیر سرعت، سادگی و دقت در ارائهٔ خدمات مختلف به کاربران مسائلی را نیز متوجه حاکمیت‌ها کرده است. از مهم‌ترین لوازم مدیریت مؤثر فضای سایبری درک اجزای مختلف فضای سایبری و چگونگی ترکیب آن‌ها در کنار یکدیگر است که این مهم جز با ساده‌سازی و محدود کردن فضای سایبری در قالب یک مدل دست‌یافتنی نیست. مدل‌های لایه‌بندی، اجزای تشکیل‌دهنده را عموماً در ساختاری عمودی و به‌صورت لایه‌هایی وابسته به یکدیگر نشان می‌دهند. هدف این پژوهش مروری روایی بر مدل‌های لایه‌بندی ارائه‌شده برای فضای سایبری به‌منظور شناسایی مدلی جامع و ساده‌فهم برای مدیریت و حاکمیت فضای سایبری است. بدین منظور با جست‌وجو در پایگاه‌های معتبر برخط، ۵۷ مقاله و کتاب یافت شده و مورد مطالعه قرار گرفته است و ۱۹ مدل لایه‌بندی منحصربه‌فرد شناسایی شده است. مدل‌های لایه‌بندی شناسایی، تفکیک و در ۴ دسته دسته‌بندی شده‌اند و مقایسهٔ مدل‌ها براساس میزان پوشش مؤلفه‌های فضای سایبری و نیز سطح هم‌پوشانی لایه‌های مدل‌های مختلف با یکدیگر صورت گرفته است. نتایج این پژوهش حاکی از آن است که مدل‌های لایه‌بندی شناسایی‌شده برای مدیریت مؤثر فضای سایبری جامعیت کافی ندارند و مدل جدید پیشنهادی در این مقاله به رفع این خلأ کمک می‌کند.

واژگان کلیدی: فضای سایبری، مدل لایه‌بندی، مدیریت فضای سایبری

تاریخ دریافت: ۱۹ آبان ۱۴۰۳ **تاریخ بازنگری: ۱ اسفند ۱۴۰۳** **تاریخ پذیرش: ۸ اسفند ۱۴۰۳**

۱. کارشناس ارشد مهندسی فنّاوری اطلاعات-امنیت اطلاعات، دانشگاه صنعتی مالک اشتر، تهران، ایران (نویسندهٔ مسئول)؛ khoshhalpour@chmail.ir

مقدمه

گسترش روزافزون به‌کارگیری قابلیت‌های فضای سایبری در جنبه‌های مختلف زندگی بشر، در کنار تسهیلات و مزیت‌هایی که برای آسایش بیشتر بشر فراهم کرده است (همچون رفع محدودیت‌های مکانی و زمانی، افزایش سرعت و سهولت)، موجب مسائل و مخاطراتی برای حکومت‌ها در عرصهٔ مدیریت این فضا و حفظ حاکمیت ملی شده است؛ درنتیجه به‌موازات گسترش به‌کارگیری فضای سایبری و انتقال خدمات مختلف به بستر فضای سایبری، توجه به مسائل مربوط به مدیریت و حاکمیت فضای سایبری نیز امری اجتناب‌ناپذیر شده است.

مدیریت فضای سایبری نیازمند ساده‌سازی ماهیت پیچیده و چندوجهی این فضا برای آگاهی از همهٔ جنبه‌های این پدیده است که این کار از طریق محدود کردن فضای سایبری در قالب مدل به دست می‌آید. درواقع برای مدیریت مؤثرِ چیزی باید حدود آن مشخص شود و ترکیب آن به‌درستی درک شود. بدین منظور محققان معمولاً فضای سایبری را در قالب مدلی شامل لایه‌های وابسته به یکدیگر نشان می‌دهند. منظور از لایه، مجموعه‌ای از اجزای فضای سایبری است که هدف و عملکرد مشترکی دارند و خدماتی را به دیگر لایه‌ها ارائه می‌دهند و یا از آن‌ها خدماتی را دریافت می‌کنند. مدل لایه‌بندی، عمدتاً ساختاری عمودی است که در آن لایه‌ها روی یکدیگر قرار می‌گیرند و لایه‌های بالاتر بدون لایه‌های پایین‌تر نمی‌توانند کار کنند (Limonier et al., 2021)؛ به‌عبارت‌دیگر لایه‌های پایین‌تر خدماتی را فراهم می‌کنند که لایه‌های بالاتر بدون آن‌ها قادر به عملکرد نیستند و لایه‌های بالاتر مستقل از آنکه خدمات لایه‌های پایین‌تر چگونه پیاده‌سازی می‌شوند از آن خدمات بهره می‌برند.

درک جامع جنبه‌های مختلف فضای سایبری، روشن‌کنندهٔ نقش‌ها و تسهیل‌گر همکاری عوامل مختلف در مدیریت این فضاست. مدیریت مؤثر فضای سایبری نیازمند همکاری و هماهنگی همهٔ عواملی است که بر فضای سایبری تأثیر دارند و یا از آن تأثیر می‌پذیرند و همکاری عوامل نیازمند درک مشترک آن‌ها از فضای سایبری است. این درک مشترک باعث می‌شود هر عامل مسائلی که دیگر عوامل با آن‌ها مواجه‌اند را نیز درک کرده و هرکدام بتوانند نقش خود را در قالب همکاریِ مشارکتی مشخص کنند. و همهٔ عوامل و ذی‌نفعان خود را در قبال تأثیر تصمیم‌ها و اقدام‌هایشان در حوزهٔ فضای سایبری مسئول بدانند (Gleason and Friedman, 2005).

آنچه در فضای سایبری رخ می‌دهد صرفاً جنبهٔ فنی و ماشینی ندارد؛ بلکه تصمیم‌ها و اقدام‌های مختلف کاربران، طراحان و حاکمان انسانی این فضا نیز در چگونگی شکل‌گیری این فضا تأثیرگذار است. مهم است که به‌غیر از توسعه‌دهندگان، دیگر عوامل نیز درک کافی از فضای سایبری داشته باشند تا آن‌ها هم خود را در قبال تصمیم‌هایشان درخصوص فضای سایبری مسئول بدانند. این امر نیازمند مدلی از فضای سایبری است که به اندازهٔ کافی جامع و فهم‌پذیر باشد تا همهٔ عوامل به‌خوبی متوجه نقش خود و تأثیر تصمیم‌هایشان بر این فضا باشند (Gleason and Friedman, 2005).

مدل لایه‌بندی فضای سایبری تمایز میان بخش‌های مختلف این فضا را آشکار می‌سازد و درنتیجه امکان برنامه‌ریزی برای توسعه و تکامل جداگانهٔ بخش‌های مختلف فضای سایبری را فراهم می‌کند (Kademi and Koltuksuz, 2017). اساساً مدل لایه‌بندی فضای سایبری ساختاری است که به تسهیل مدیریت و برنامه‌ریزی درخصوص این فضا کمک می‌کند (Bush, 2021).

برای پاسخ‌گویی به این نیاز، برخی محققان به ارائهٔ مدل لایه‌بندی فضای سایبری پرداخته‌اند؛ اما تاکنون اتفاق‌نظر بر یک مدل شکل نگرفته است؛ این درحالی است که، همان‌طور که بیان شد، بدون یک مدل جامع و مورد اتفاق‌نظر میان همهٔ عوامل، امکان تحقق همکاری لازم میان عوامل تأثیرگذار بر یا تأثیرپذیر از فضای سایبری وجود ندارد. کریمی قهرودی[1] (2023) در این زمینه می‌گوید: «سازمان‌ها، مراکز و نهادهای علمی و پژوهشی کشورهای مختلف تاکنون تعریف‌ها و توصیف‌های گوناگونی برای فضای سایبری و عناصر اصلی آن ارائه داده‌اند. برداشت‌ها، توصیف‌ها و تعریف‌های نسبتاً متنوع در کشورها سبب ایجاد ابهام، ضعف زبان مشترک، بروز مشکلات، ناهماهنگی و تعارض‌هایی در سیاست‌گذاری‌ها، تقنین، تقسیم‌کار ملی، برنامه‌ریزی‌ها و توسعهٔ فضای سایبری و امنیت فضای سایبری و ... شده است. سازمان‌دهی نامناسب، موازی‌کاری‌ها، پراکنده‌کاری‌ها، ضعف در قاعده‌گذاری‌ها و بروز اختلاف‌ها در تقسیم‌کار ملی از جمله شواهد این مسئله است.»

سؤال اصلی پژوهش حاضر این است که کدام مدل لایه‌بندی فضای سایبری امکان اتفاق‌نظر میان عوامل عرصهٔ مدیریت فضای سایبری و همکاری مؤثرتر آنان را فراهم می‌کند؟ در این پژوهش با درک ضرورت وجود مدلی جامع و ساده‌فهم به‌منظور تسهیل مدیریت فضای سایبری، مدل‌های لایه‌بندی مختلف ارائه‌شده برای فضای سایبری شناسایی و مرور شده‌اند. سپس با مقایسهٔ مدل‌ها با یکدیگر ضعف مدل‌های ارائه‌شده در زمینهٔ ایجاد نگاه جامع و ساده‌فهم لازم برای مدیریت مؤثر فضای سایبری روشن شده و با انطباق لایه‌های متناظر در مدل‌های مختلف، یک مدل لایه‌بندی جدید برای فضای سایبری پیشنهاد می‌شود.

در ادامه در بخش ۱ روش‌شناسی پژوهش بیان می‌شود. در بخش ۲ دسته‌بندی و مرور مدل‌های مختلف ارائه‌شده برای

1. Karimi Ghohroudi

فضای سایبری ارائه می‌شود. سپس در بخش ۳ مقایسه‌ای بین این مدل‌ها صورت می‌گیرد و مدل لایه‌بندی جدیدی پیشنهاد می‌شود. درنهایت با جمع‌بندی مطالب بیان‌شده پیشنهادهایی در این زمینه مطرح می‌شود.

۱. روش‌شناسی

هدف این پژوهش کاربردی و شیوهٔ گردآوری اطلاعات روش مطالعهٔ کتابخانه‌ای و اسنادی است. برای گردآوری اطلاعات عبارت‌های زیر در پایگاه علمی گوگل اسکالر[1] جست‌وجو شدند:

layers of cyberspace, layer model of cyberspace, cyber world model, conceptual model + cyber-space

۵۷ مقاله و کتاب یافت و مطالعه شد که ۱۹ مدل لایه‌بندی معتبر و منحصربه‌فرد در آن منابع شناسایی شد. هر مدل فیش‌برداری شد و اطلاعات هر مدل شامل نام ارائه‌دهنده، سال ارائه، زمینهٔ موضوعی، هدف از ارائهٔ مدل، عنوان لایه‌ها و توضیحات مربوط به هرکدام از لایه‌های مدل ثبت شد و سپس اطلاعات جمع‌آوری‌شده با روش کیفی تحلیل شد. در این تحلیل، اتصال و الهام‌گیری مدل‌های مختلف از یکدیگر شناسایی شده است و همچنین تشابه مفهومی میان مدل‌های مختلف علی‌رغم تفاوت‌ها در واژه‌های استفاده‌شده در مدل‌ها مورد تحلیل قرار گرفته است.

۲. مدل‌های لایه‌بندی فضای سایبری

مدل‌های ارائه‌شده برای فضای سایبری هرکدام از منظری خاص ارائه شده‌اند و هر محقق با نگاهی متفاوت و در بستر موضوعی خاصی به ارائهٔ دیدگاه خود درخصوص مدل لایه‌بندی فضای سایبری پرداخته است.در کنار محققانی که از نقطه‌نظر تشریح عوامل مطرح در مدیریت و حاکمیت بر فضای سایبری مدل خود از این فضا را ارائه داده‌اند، برخی محققان از منظر تشریح عوامل مؤثر در تأثیرگذاری بر کاربران فضای سایبری مدل خود را ارائه داده‌اند. گروهی دیگر از محققان از نظر تشریح عوامل مؤثر در طرح‌ریزی و اجرای عملیات سایبری و دسته‌ای دیگر از محققان از منظر تشریح عوامل مؤثر در تأمین امنیت فضای سایبری به ارائهٔ مدل‌های پیشنهادی برای این فضا پرداخته‌اند.

هر چند پژوهش حاضر بر حوزهٔ مدیریت و حاکمیت فضای سایبری تمرکز دارد، اما باید توجه داشت که علی‌رغم دیدگاه‌های مختلف به فضای سایبری، این فضا دارای ماهیتی واحد بوده و با وجود برخی تفاوت‌ها در ادبیات علمی مطرح در زمینه‌های موضوعی مختلف دربردارندهٔ مؤلفه‌ها و اجزای واحدی است؛ درنتیجه امکان بهره‌گیری از محتوای مدل‌های هرکدام از دسته‌های چهارگانه در دستهٔ دیگر به‌تناسب نیاز وجود دارد. بر همین اساس برای دستیابی به مدلی مناسب برای حوزهٔ مدیریت و حاکمیت فضای سایبری لازم است در ابتدا فارغ از زمینهٔ موضوعی ارائهٔ هر مدل، مدل‌های مختلف لایه‌بندی فضای سایبری شناسایی و مرور شود و سپس به‌تناسب نیاز زمینهٔ موضوعی موردتمرکز مدل مطلوب معرفی شود. در این بخش انواع مدل‌های ارائه‌شده ذیل هرکدام از منظرهای چهارگانه با رعایت ترتیب زمانی ارائهٔ مدل‌ها تشریح می‌شود.

۲-۱. مدل‌های تشریح‌کنندهٔ عوامل مطرح در مدیریت و حاکمیت بر فضای سایبری

یوچای بنکلر فضای سایبری را محیط اطلاعاتی دیجیتالی معرفی کرد و بر لزوم تنظیم‌گری حاکمیت‌ها بر این محیط اطلاعاتی تأکید کرد. در این راستا او با یکی دانستن لایه‌های فضای سایبری و لایه‌های محیط اطلاعاتی، در یکی از ابتدایی‌ترین مدل‌های ارائه‌شده، فضای سایبری را شامل ۳ لایه معرفی کرد: ۱) لایهٔ زیرساخت فیزیکی[2] شامل سیم‌ها، کابل‌ها، طیف فرکانس رادیویی؛ ۲) لایهٔ زیرساخت منطقی[3] شامل نرم‌افزار و ۳) لایهٔ محتوا شامل اطلاعات (Benkler, 2000).

لاورنس فریدمن لزوم مسئولیت‌پذیری عوامل مختلف در قبال اثرات تصمیم‌های آن‌ها بر فضای سایبری را مورد توجه قرار داد و بر لزوم توجه به جوانب انسانی فضای سایبری در کنار جنبه‌های فنی این فضا تأکید کرد. او ضمن اشاره به اینکه مدل OSI[4] ــ که یک مدل ۷ لایهٔ ارائه‌شده در سال ۱۹۸۰ برای توصیف ارتباطات در شبکه‌های رایانه‌ای است (Zimmermann, 1980) ــ صرفاً از جانب مهندسان توسعه داده شده است، به‌منظور تعمیم دادن آن و رفع ضعف این مدل در پرداختن به مسائل انسانی فضای سایبری، افزودن ۳ لایه را به مدل OSI ــ لایه‌های ۸ تا ۱۰ــ پیشنهاد کرد: ۸) لایهٔ رابط کاربری، ۹) لایهٔ تفسیر و ۱۰) لایهٔ تأثیر. از نظر فریدمن، لایهٔ رابط کاربری، اطلاعات رایانه‌ای را برای کاربر انسانی ادراک‌پذیر می‌کند؛ سپس در لایهٔ تفسیر این اطلاعات با توجه به سطح دانش و تجربهٔ فرد و یا متأثر از ترتیب نمایش آن‌ها می‌تواند به ایجاد معانی مختلف برای افراد مختلف بینجامد؛ شکل‌گیری تصمیم‌های مختلف در کاربر یا سازمان دریافت‌کنندهٔ آن اطلاعات نیز در لایهٔ تأثیر مورد توجه قرار می‌گیرد (Gleason and Friedman, 2005).

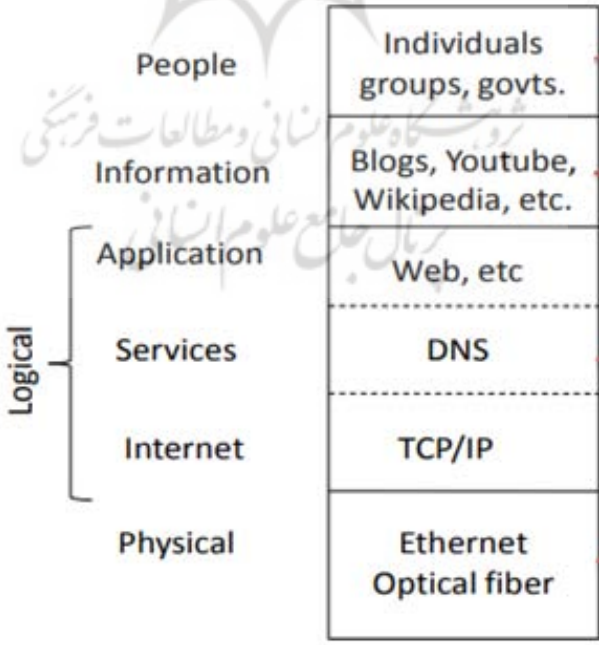
1. Google Scholar

2. Physical
3. Logical
4. Open System Interconnection

الیهو زیمت، ایجاد جوامع مجازی در فضای سایبری و نیز تأثیرات تصمیم‌گیری‌های حاکمیتی بر این فضا را مورد توجه قرار داد و مدلی ۴ لایه‌ای از فضای سایبری برای درک بهتر این موارد پیشنهاد داد: ۱) لایهٔ سیستمی، ۲) لایهٔ محتوا و برنامهٔ کاربردی، ۳) لایهٔ اجتماعی و مردم و ۴) لایهٔ حاکمیت؛ زیمت برنامه‌های کاربردی مورداستفادهٔ کاربران و همچنین اطلاعاتی که بر بستر آن برنامه‌ها مبادله می‌شوند را در لایهٔ محتوا و برنامهٔ کاربردی و تمامی نیازمندی‌های زیرین آن شامل سخت‌افزارها، نرم‌افزارهای سیستمی و نیز پروتکل‌های ارتباطی و ذخیره‌سازی و حتی منابع تغذیهٔ موردنیاز را در لایهٔ سیستمی در نظر می‌گیرد. او ارتباطات اجتماعی افراد با یکدیگر که به ایجاد جوامع مجازی می‌انجامد را در لایهٔ اجتماعی و مردم مورد توجه قرار داده است و تمامی چارچوب‌های مربوط به حاکمیت بر فضای سایبری اعم از تعیین مشخصه‌های فنی لایهٔ سیستمی و یا استانداردهای مبادلهٔ اطلاعات در لایهٔ محتوا و برنامهٔ کاربردی و یا الزامات قانونی و حقوقی ارتباطی در لایهٔ اجتماعی و مردم را ذیل لایهٔ حاکمیت قرار داده است (Zimet and Skoudis, 2009).

دیوید کلارک نقش مردم را در شکل دادن به فضای سایبری و اعمال کنترل آن‌ها بر این فضا برجسته و تأکید کرد که با تغییرِ مردم از یک منطقه به منطقهٔ دیگر فضای سایبری متفاوتی شکل می‌گیرد، زیرا مردم هر منطقه الگوهای متفاوتی در تعامل با لایه‌های مختلف این فضا داشته و تصمیم‌گیری‌های متفاوتی در این موارد خواهند داشت. براین‌اساس او فضای سایبری را مطابق شکل «۱» شامل ۴ لایهٔ ۱) فیزیکی، ۲) منطقی، ۳) اطلاعات و ۴) مردم معرفی می‌کند که لایهٔ فیزیکی شامل تمام اجزا و مباحث فیزیکی نظیر رایانه‌ها و کانال‌های ارتباطی، لایهٔ منطقی شامل منطق عملکرد اجزای فیزیکی از قبیل پروتکل‌ها و حتی برنامه‌های کاربردی، لایهٔ اطلاعات شامل هر گونه اطلاعاتی که پردازش و یا مبادله می‌شود و لایهٔ مردم شامل استفاده و تعامل افراد با لایه‌های زیرین است (Clark, 2010).

فن بینشینگ نیز به فضای سایبری از دیدگاه مدیریت و حاکمیت بر این فضا نگریسته است و با جدا کردن مفهوم سایبر از فضا و درواقع تفکیک لایه‌های فنی سایبر از لایه‌های انسانی فضا، سایبر را شامل دو بخش زیرساخت و داده دانسته و فضای حاصل از استفادهٔ افراد از سایبر را نیز شامل دو بخش شخصیت مجازی[1] و فعالیت‌های افراد در این فضا معرفی می‌کند و درنتیجه فضای سایبری را شامل ۴ بخش معرفی می‌کند: ۱) زیرساخت یا امکانات محاسباتی و ارتباطی که پایانه‌ها، رایانه‌ها و تجهیزات شبکه را شامل می‌شود؛ ۲) داده یا باری که در زیرساخت‌ها محاسبه یا مبادله می‌شود؛ ۳) شخصیت‌های مجازی که منعکس‌کنندهٔ ارادهٔ کاربران انسانی در فضای سایبری‌اند و ۴) عملیات که همان اقدام‌ها یا رفتارهایی است که کاربران در فضای سایبری انجام می‌دهند ازجمله ارتباط کاربران با یکدیگر (Binxing et al., 2016).



شکل ۱: مدل لایه‌بندی فضای سایبری دیوید کلارک (Choucri and Clark, 2012)

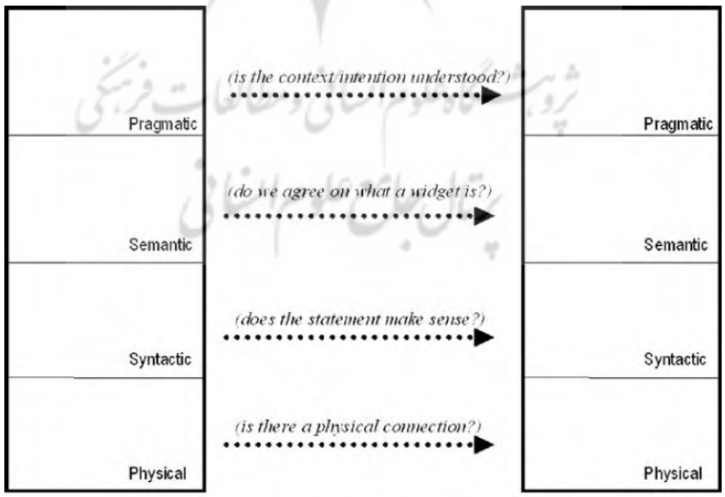
1. Virtual character

۲-۲. مدل‌های تشریح‌کنندهٔ عوامل مؤثر در تأثیرگذاری بر کاربران فضای سایبری

مارتین لیبیکی با هدف تشریح چگونگی تأثیرگذاری فضای سایبری بر مخاطبان انسانی، نگاهی زبان‌شناسانه به ارتباطات انسانی در این فضا ارائه داد و با نشان دادن مسائل مربوط به نیت فرستنده و برداشت مخاطب پیام مدلی ۴ لایه‌ای برای فضای سایبری مطابق شکل «۲» معرفی کرد. او لایه‌های زبان انسانی را شامل واج‌شناسی[1]، نحوی[2]، معنایی[3] و عمل‌گرایانه[4] معرفی می‌کند و با فضای سایبری را راهکاری جدید برای ارتباطات انسانی دانسته و این فضا را شامل لایه‌های ۱) فیزیکی، ۲) نحوی، ۳) معنایی و ۴) عمل‌گرایانه مورد بحث قرار می‌دهد: لایه‌های فیزیکی، نحوی و معنایی این مدل به‌ترتیب متناظر با لایه‌های فیزیکی، منطقی و اطلاعات در مدل کلارک است با این تفاوت که لیبیکی در لایهٔ معنایی، علاوه‌بر خود اطلاعات قوانین لازم برای تولید دانش از آن اطلاعات برای استفادهٔ کاربران در کاربردهای سطح بالا را نیز در نظر می‌گیرد. لیبیکی پس از این سه لایه، لایهٔ عمل‌گرایانه را مطرح می‌کند و در آن به مباحث برون‌زبانی ارتباطات افراد و چگونگی تأثیرگذاری افراد بر هم می‌پردازد و هدف و نیت ضمنی فرستنده از ارسال پیام و نیز تفسیری که از آن پیام برای مخاطب ایجاد می‌شود را مورد توجه قرار می‌دهد (Libicki, 2007).

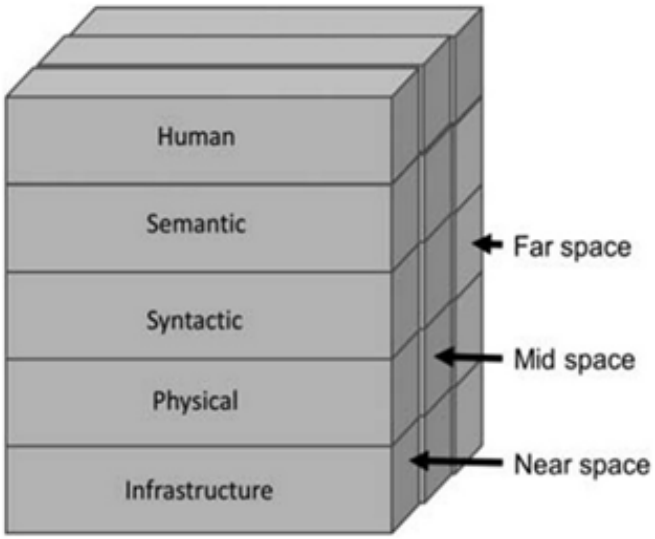
جان شلدون مدل لیبیکی را مبنای کار خود قرار داد و از آن برای بیان چگونگی تأثیرگذاری عملیات سایبری بر تصمیم‌گیران راهبردی کشورِ هدف استفاده کرد. او لایهٔ عمل‌گرایانهٔ مدل لیبیکی که شاید مهم‌ترین لایه برای تشریح موضوع موردنظر او بود را حذف کرد و صرفاً برای برجسته کردن اهمیت مباحث طیف الکترومغناطیسی با تغییر نام لایهٔ فیزیکی مدل لیبیکی به لایهٔ زیرساخت یک لایه به نام لایهٔ فیزیکی شامل مباحث الکترومغناطیسی ارتباطات به این مدل افزود. درواقع او زیرساخت‌های سخت‌افزاری نظیر رایانه‌ها و کابل‌ها را در لایهٔ زیرساخت و مباحث الکترومغناطیسی شامل الکترون‌ها و فرکانس‌ها را در لایهٔ فیزیکی مدل خود در نظر گرفت. براساس مدل شلدون، فضای سایبری از ۴ لایه تشکیل شده است: ۱) لایهٔ زیرساخت، ۲) لایهٔ فیزیکی، ۳) لایهٔ نحوی و ۴) لایهٔ معنایی (Sheldon, 2011).

آدریان ونابلز موضوع موردتوجه لیبیکی یعنی چگونگی تأثیرگذاری فضای سایبری بر مخاطبان انسانی را دوباره مورد توجه قرار داد و لایهٔ عمل‌گرایانهٔ مدل لیبیکی را که شلدون از آن صرف‌نظر کرده بود با تغییر نام آن لایه به لایهٔ انسان مجدد به این مدل افزود و مدل ۵ لایه‌ای شامل لایه‌های ۱) زیرساخت، ۲) فیزیکی، ۳) نحوی، ۴) معنایی و ۵) انسان ارائه داد که در شکل «۳» مشاهده می‌شود. ونابلز با طرح لایهٔ انسان سعی در برجسته کردن نقش انسان در فضای سایبری دارد و بر این واقعیت تأکید می‌کند که اولاً فضای سایبری در ایجاد، نگهداری، بهره‌برداری و درنهایت تخریب نیازمند دخالت انسان است؛ ثانیاً چگونگی تفسیر اطلاعات لایهٔ معنایی از سوی کاربر انسانی و تأثیرپذیری از آن را متناسب با نیازهای آن کاربر و متأثر از عواملی مانند زبان و



شکل ۲: مدل لایه‌بندی فضای سایبری مارتین لیبیکی (Libicki, 2007)

1. Phonology
2. Syntactic
3. Semantics
4. Pragmatics

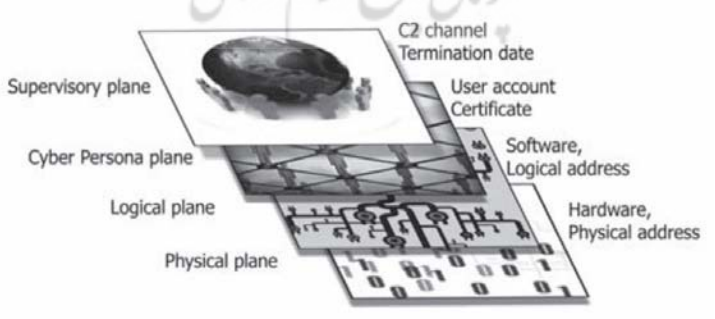


شکل ۳: مدل لایه‌بندی فضای سایبری آدریان ونابلز (Venables et al., 2015)

فرهنگ او می‌داند. ونابلز همچنین با نگاهی عملیاتی و جغرافیایی به فضای سایبری بعد دومی را هم در قالب سه لایهٔ عمودی شامل فضای نزدیک، فضای میانه و فضای دور در مدل خود در نظر می‌گیرد و با این کار بر تمایز میان فضای محلی یک شرکت یا کشور، فضای متعلق به کشور یا شرکت رقیب او و نیز فضای بین این دو فضا تأکید می‌کند (Venables et al., 2015).

۲-۳. مدل‌های تشریح‌کنندهٔ عوامل مؤثر در طرح‌ریزی عملیات سایبری

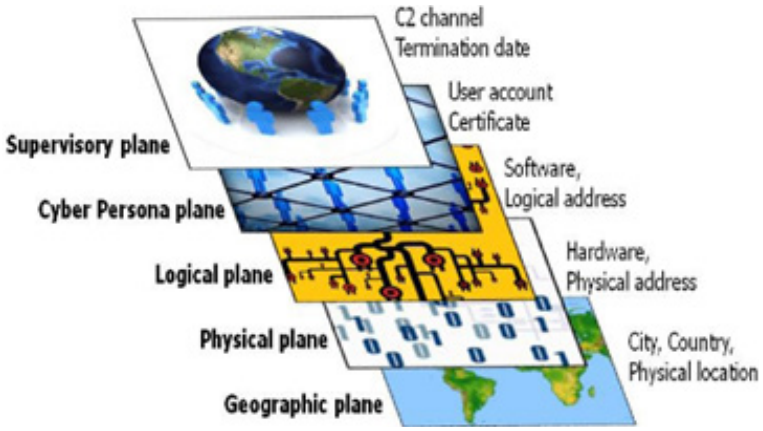
رابرت فنلی به‌منظور تشریح چگونگی کنترل اثرات ناخواسته در عملیات سایبری تهاجمی، برای اولین‌بار مباحث مربوط به هویت‌های سایبری افراد را در مدل فضای سایبری مطرح کرد. او لایه‌ای به نام کاربرنمای سایبری[1] در مدل خود قرار داد که بیانگر هویت‌های کاربران در فضای سایبری ازجمله حساب‌های کاربری و گواهینامه‌های دیجیتال است. لایه‌های مختلف مدل پیشنهادی او مطابق شکل ۴ عبارت‌اند از: ۱) سطح فیزیکی: این سطح ویژگی‌های سخت‌افزاری، ویژگی‌های عملیاتی و ویژگی‌های محیط فیزیکی دستگاه‌ها را شامل می‌شود؛ ۲) سطح منطقی: این سطح مشخصات نرم‌افزارها و همچنین پیکربندی‌های آن‌ها را شامل می‌شود؛ ۳) سطح کاربرنمای سایبری: این سطح بیانگر هویت‌های کاربران در فضای سایبری شامل حساب‌های کاربری (محلی، راه‌دور و یا رایانامه)، مجوزهای نرم‌افزارها و گواهینامه‌های دیجیتال و نیز داده‌های بیومتریک ذخیره‌شده از کاربران است؛ ۴) سطح نظارتی[2]: تصمیم‌ها و فرمان‌های کاربران انسانی و نیز رویدادهای از پیش تعریف‌شده که موجب شروع، توقف و یا تغییر در عملیات می‌شوند و نیز زمان‌بندی موردنظر برای انجام عملیات یا ابقای اثرات آن در این سطح مورد توجه قرار می‌گیرند (Fanelli and Conti, 2012).



شکل ۴: مدل لایه‌بندی فضای سایبری رابرت فنلی (Fanelli and Conti, 2012)

1. Cyber persona

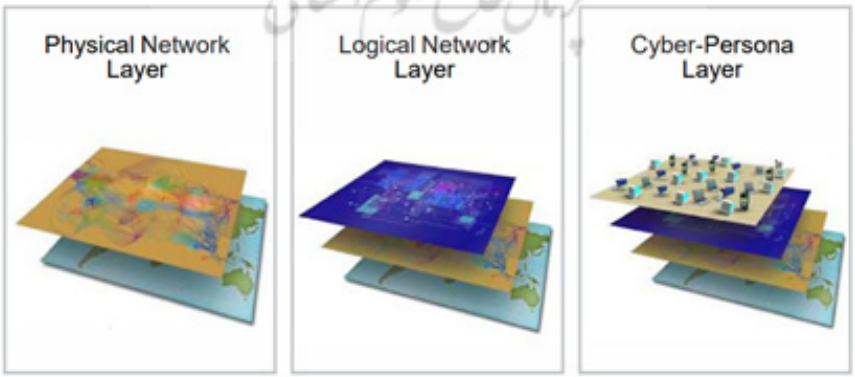
2. Supervisory



شکل ۵: مدل لایه‌بندی فضای سایبری دیوید ریموند (Raymond et al., 2013)

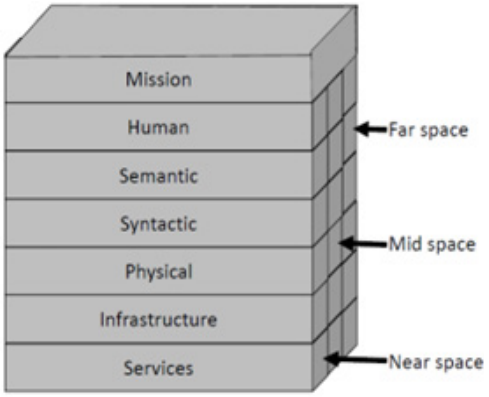
دیوید ریموند با تمرکز بر محدود کردن آسیب‌های جانبی عملیات سایبری تهاجمی، مدل فنلی را بازنگری کرد و موقعیت جغرافیایی اجزای فیزیکی و وابستگی‌های فیزیکی این اجزا را که در مدل فنلی مغفول بود به آن افزود و مدلی ۵ لایه‌ای از فضای سایبری ارائه داد که در شکل «۵» مشاهده می‌شود: ۱) سطح جغرافیایی[1]، ۲) سطح فیزیکی، ۳) سطح منطقی، ۴) سطح کاربرنمای سایبری و ۵) سطح نظارتی. ریموند یک سطح جغرافیایی قبل از سطوح چهارگانهٔ مدل فنلی در نظر می‌گیرد که موقعیت جغرافیایی اجزای فیزیکی و وابستگی‌های محیطی آن‌ها نظیر زیرساخت برق و ساختمان محل قرارگیری اجزا را در این لایه لحاظ می‌کند. توجیه ریموند در افزودن این لایه این است که در طراحی عملیات سایبری تهاجمی تحت حمایت یک دولت، مسئلهٔ جغرافیا بسیار مهم است و عبور بسته‌های حمله از کشور ثالث بی‌طرف می‌تواند عواقبی در پی داشته باشد؛ درنتیجه بی‌توجهی به تأثیر جغرافیا بر عملیات می‌تواند پرهزینه باشد (Raymond et al., 2013).

نیروی مسلح ایالات متحدهٔ امریکا به‌منظور تسهیل طرح‌ریزی عملیات سایبری مدل فنلی را مبنا قرار داد و با افزودن خود افراد به لایهٔ کاربرنمای سایبری مدلی ۳ لایه‌ای ارائه داد که در شکل «۶» مشاهده می‌شود: این مدل شامل ۳ لایهٔ ۱) شبکهٔ فیزیکی، ۲) شبکهٔ منطقی، ۳) کاربرنمای سایبری است که به‌ترتیب متناظر با سطوح فیزیکی، منطقی و کاربرنمای سایبری در مدل فنلی هستند، با این تفاوت که در این مدل همچون مدل ریموند به موقعیت جغرافیایی اجزای فیزیکی نیز توجه شده که البته در اینجا نه در قالب لایه‌ای مستقل بلکه ذیل لایهٔ شبکهٔ فیزیکی در نظر گرفته شده است؛ تفاوت دیگر آنکه در لایهٔ کاربرنمای سایبری علاوه‌بر هویت‌های افراد در فضای سایبری خود افراد که گردانندگان آن هویت‌ها هستند نیز ذیل این لایه در نظر گرفته شده‌اند تا به‌این‌ترتیب استفادهٔ منحصربه‌فرد یا اشتراکی افراد از هر هویت سایبری مورد توجه قرار گیرد (U.S. Joint Chiefs of Staff, 2013).

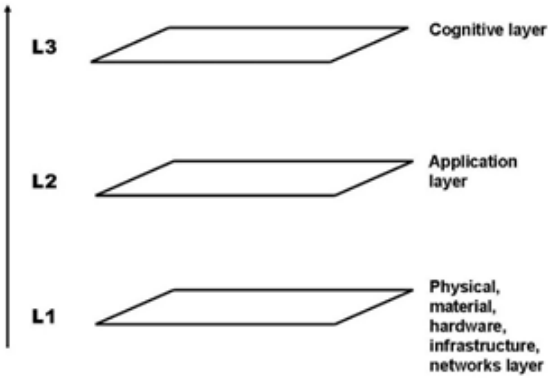


شکل ۶: مدل لایه‌بندی فضای سایبری نیروی مسلح ایالات متحده امریکا (U.S. Joint Chiefs of Staff, 2013)

1. Geographic



شکل ۷: مدل لایه‌بندی فضای سایبری آدریان ونابلز (Venables et al., 2015a)



شکل ۸: مدل لایه‌بندی فضای سایبری دنیل ونتره (Ventre, 2012)

تیم گرانت بر لزوم توجه به مباحث جغرافیایی در طرح‌ریزی عملیات سایبری تأکید کرد و همچنین اهمیت توجه به روابط سازمانی میان کاربران درگیر در عملیات سایبری را در مدل پنج‌لایه‌ای‌خود نشان داد. ۳ لایهٔ ۱) جغرافیایی، ۲) فیزیکی و ۳) اطلاعاتی این مدل متناظر با سطوح جغرافیایی، فیزیکی و منطقی مدل ریموند است، در عین حال گرانت دو لایهٔ ۴) شناختی[1] و ۵) اجتماعی‌ـسازمانی را نیز به آن‌ها افزوده است. در لایهٔ شناختی، آگاهی و شناخت ایجادشده در نتیجهٔ دریافت اطلاعات برای افراد مورد توجه قرار گرفته است. هدف لایهٔ اجتماعی‌ـسازمانی هم نشان دادن روابط اجتماعی و سازمانی میان افراد درگیر در اقدامات سایبری نظامی یا غیرنظامی است (Grant, 2014).

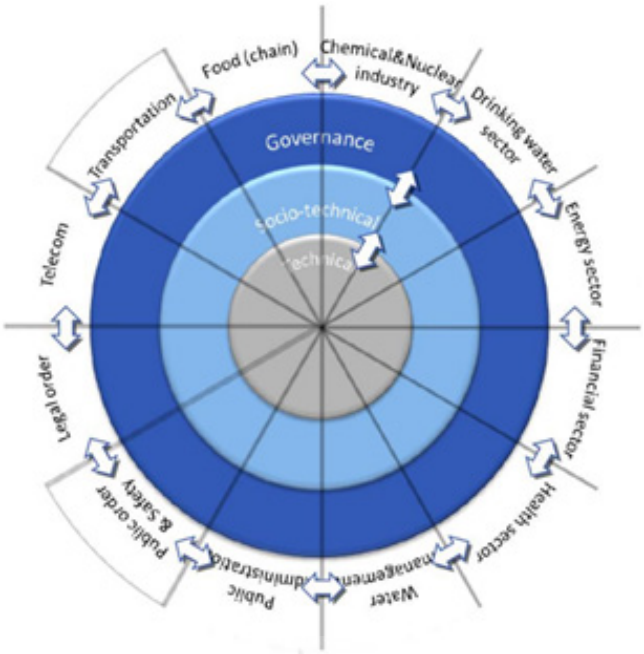
آدریان ونابلز با هدف تشریح عناصر ضروری موردنیاز برای دستیابی، حفظ و اندازه‌گیری قدرت در انجام عملیات سایبری مدل پیشین خود (Venables et al., 2015b) را به‌روزرسانی کرد و همان‌طور که در شکل «۷» مشاهده می‌شود دو لایهٔ خدمات و مأموریت را به این مدل افزود. لایهٔ خدمات که قبل از لایهٔ زیرساخت قرار دارد، بر وابستگی‌های اجزای لایهٔ زیرساخت که این اجزا را قادر به کار کردن می‌کند تأکید دارد. این وابستگی‌ها شامل منابع تغذیه، تجهیزات خنک‌کننده، تهویهٔ مطبوع و حتی امنیت فیزیکی ساختمان‌هایی که اجزای فیزیکی شامل رایانه‌ها، کارگزارها و تجهیزات شبکه در آنجا قرار دارند می‌شود. مدل ونابلز تنها مدلی است که با اختصاص لایه‌ای منحصربه‌فرد، این‌گونه وابستگی‌های اجزای فیزیکی ــ که در سایر مدل‌ها توجه چندانی به آن‌ها نشده است ــ را برجسته می‌کند. لایهٔ مأموریت که بعد از لایهٔ انسانی اضافه شده و بالاترین لایه در مدل است، بر چگونگی رابطه‌ای که کاربران با فضای سایبری دارند حاکم است و ماهیت مصنوعی این فضا را نشان می‌دهد. درواقع این لایه مشخص می‌کند که فضای سایبری برای تحقق هدفی مشخص طراحی و ساخته می‌شود و هر تعاملی که کاربر انسانی یا دستگاه خودکار با این محیط تعاملی انجام می‌دهد برای انجام نقشی است و در پس هر رویداد هدفی وجود دارد (Venables et al., 2015a).

۲-۴. مدل‌های تشریح‌کنندهٔ عوامل مؤثر در تأمین امنیت فضای سایبری

دنیل ونتره به بررسی چگونگی تأمین امنیت فضای سایبری از طریق درک چگونگی اثرگذاری بر یک لایه از فضای سایبری از طریق اقدام در لایه‌های دیگر این فضا پرداخت. او به موضوع جنگ سایبری از منظر جنگ اطلاعاتی نگریست و ضمن الهام از «ادوارد والتز» ــ که در سال ۱۹۹۸ «فضای سایبری» را سطح میانی از سه سطح مطرح در جنگ اطلاعاتی در نظر گرفت ــ فضای سایبری را شامل ۳ لایه مطابق شکل «۸» معرفی کرد: ۱) لایهٔ فیزیکی شامل اجزا و زیرساخت فیزیکی نظیر رایانه‌ها و مخابرات و نیز وابستگی‌های آن‌ها نظیر برق و کنترل‌های محیطی است؛ ۲) لایهٔ کاربرد شامل نرم‌افزارها و اطلاعاتی است که مورداستفادهٔ کاربران انسانی قرار می‌گیرد و یا برای کنترل عملکرد اجزای فیزیکی به کار گرفته می‌شود؛ و ۳) لایهٔ شناخت بیانگر تأثیر اطلاعات دریافتی بر ادارک و تصمیم‌گیری کاربران انسانی است (Ventre, 2012; Waltz, 1998).

یان وندربرگ با رویکرد تدوین دانش لازم برای آموزش متخصصان امنیت سایبری، مدلی ۳ لایه‌ای از فضای سایبری مطابق شکل «۹» ارائه داد و در آن بر تعامل‌های اجتماعی‌ـفنی موجود در این فضا تأکید کرد: ۱) لایهٔ فنی شامل تمامی اجزای سخت‌افزاری و نرم‌افزاری مبادلهٔ اطلاعات میان اجزای شبکه است؛ ۲) لایهٔ اجتماعی‌ـفنی بیانگر هر گونه برنامهٔ کاربردی

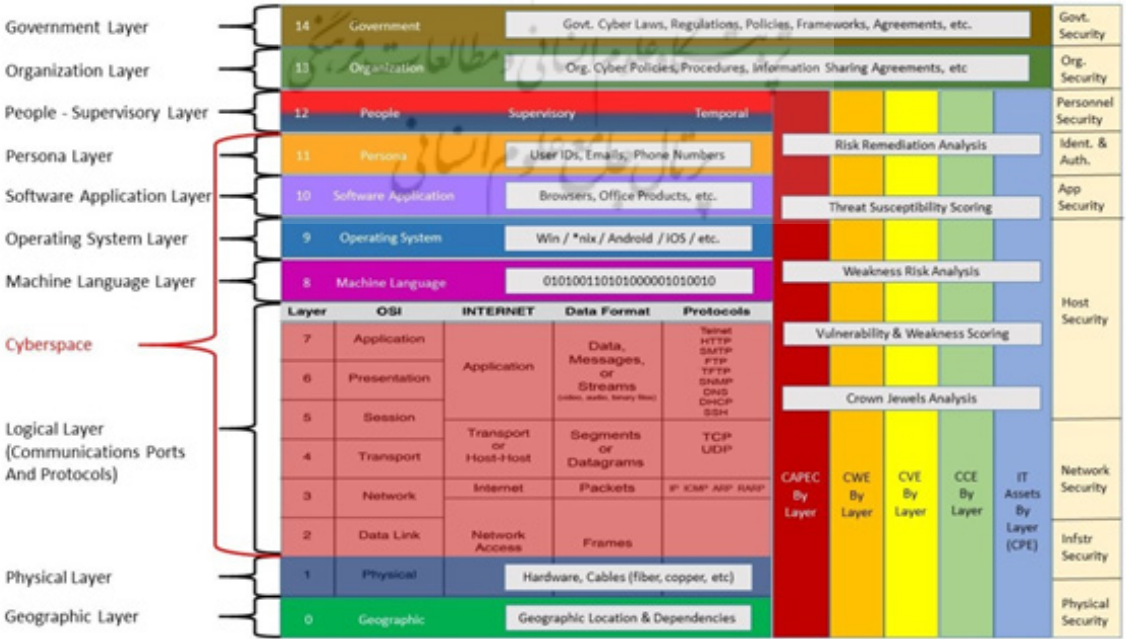
1. Cognitive



شکل ۹: مدل لایه‌بندی فضای سایبری یان وندربرگ (Van den Berg et al., 2014)

تسهیل‌گر تعامل بین انسان‌ها نظیر ارتباطات اجتماعی برخط، تماشا و گوش دادن به محتوای برخط و یا تراکنش‌های مالی است؛ و ۳) لایهٔ حاکمیتی در مدل بر این تأکید دارد که دو لایهٔ زیرین به‌وسیلهٔ طیف عظیمی از عوامل و سازمان‌های انسانی اداره می‌شوند (Van den Berg et al., 2014).

شون رایلی با تمرکز بر تأمین امنیت سایبری به‌دنبال مدلی بود که به‌کمک آن تمام لایه‌هایی که تحت‌تأثیر از عملیات سایبری قرار می‌گیرند را توضیح دهد. او مدل ریموند (Raymond et al., 2013) را مبنا قرار داد و لایه‌هایی را به‌منظور تأکید بر برخی مباحث فنی و نیز توجه به مباحث سازمانی فضای سایبری به آن افزود. بدین منظور ۵ لایهٔ زبان ماشین، سیستم‌عامل، نرم‌افزار کاربردی، سازمان و حاکمیت به مدل ریموند اضافه شدند. همان‌طور که در شکل «۱۰» مشاهده می‌شود، ۳ لایهٔ نخست قبل از لایهٔ کاربرنمای سایبری و ۲ لایهٔ دیگر بعد از لایهٔ نظارتی



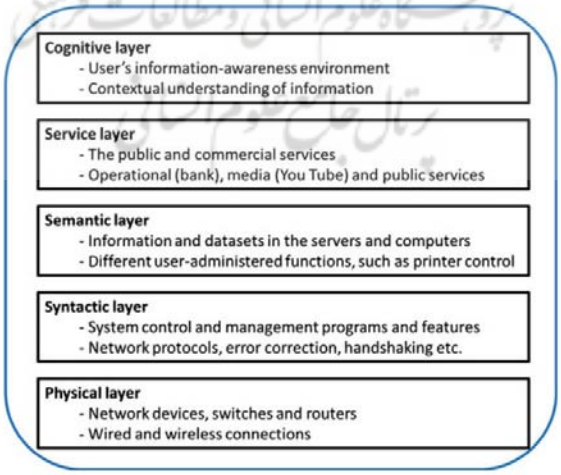
شکل ۱۰: مدل لایه‌بندی فضای سایبری شون رایلی (Riley, 2014)

قرار می‌گیرند. رایلی با ذکر لایهٔ زبان ماشین تمام کدهای موردنیاز برای عملکرد رایانه‌ها ازجمله کتابخانه‌های BIOS ،DLL و سخت‌افزارهای[1] دستگاه‌های مختلف نظیر کارت گرافیک یا دستگاه ذخیره‌سازی را مورد توجه قرار می‌دهد. او همچنین سیستم‌عامل‌های استفاده‌شده در رایانه‌ها و نیز برنامه‌های کاربردی مورداستفادهٔ کاربران که روی این سیستم‌عامل‌ها نصب می‌شوند را به‌ترتیب در لایهٔ سیستم‌عامل و لایهٔ نرم‌افزار کاربردی در نظر می‌گیرد. همچنین لایهٔ سازمان بیانگر سیاست‌ها، فرایندها و رویه‌های سازمان استفاده‌کننده از فضای سایبری است و لایهٔ حاکمیت نیز قوانین، مقررات، سیاست‌ها و چارچوب‌هایی که از سوی حاکمیت بر سایر لایه‌های فضای سایبری وضع می‌گردد در بر می‌گیرد (Riley, 2014).

مارتی لهتو مطابق شکل «۱۱» یک لایه به مدل مارتین لیبیکی (Libicki, 2007) افزود تا با در نظر گرفتن انواع خدمات فنّاوری اطلاعات موردنیاز سازمان‌ها در مدل بهتر بتواند تهدیدهای مطرح در لایه‌های مختلف فضای سایبری را توضیح دهد. درواقع همان‌طور که در شکل «۱۱» مشاهده می‌شود لایهٔ نحوی مدل لیبیکی در این مدل در قالب دو لایهٔ نحوی و خدمت بیان شده است. لهتو در لایهٔ نحوی فقط برنامه‌های سیستمی و پروتکل‌های لازم برای تعامل دستگاه‌های شبکه با هم را مورد توجه قرار می‌دهد و درعین‌حال انواع خدمات فنّاوری اطلاعات مورداستفادهٔ کاربران نظیر خدمات رسانه‌های اجتماعی و خدمات بانکی را در لایهٔ خدمت در نظر می‌گیرد (Lehto, 2015).

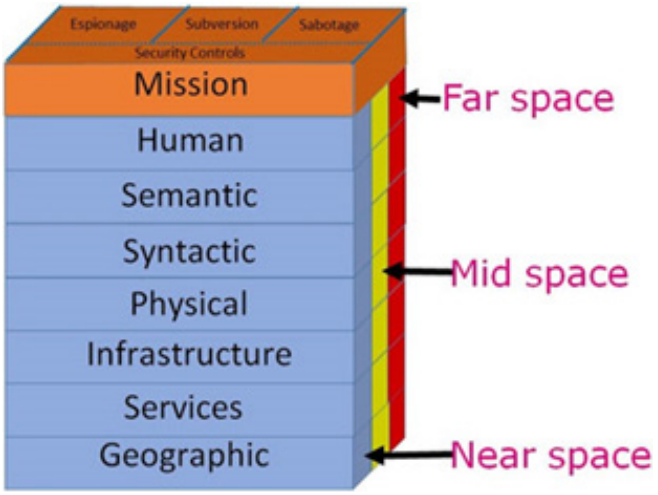
ایکوو روث بر پیش‌بینی و هشدار زودهنگام حملات سایبری تمرکز کرد و تأکید داشت که مدل فضای سایبری باید در کنار ابعاد فنی و انسانی، ابعاد سیاسی، اجتماعی و اقتصادی رویدادهای سایبری را نیز لحاظ کند. بدین منظور او مدلی ۳ لایه‌ای از این فضا ارائه داد: ۱) لایهٔ فضای فیزیکی، ۲) لایهٔ فضای اجتماعی و ۳) لایهٔ اقتصادی. اجزای فیزیکی، منطق عملکرد اجزای فیزیکی و نیز موقعیت جغرافیایی آن اجزا همه در لایهٔ فضای فیزیکی مورد توجه قرار می‌گیرند. لایهٔ فضای اجتماعی، از سویی هویت‌های سایبری افراد مانند آدرس رایانامه و آدرس IP و از سوی دیگر ویژگی‌های واقعی افراد در دنیای واقعی مانند سن و آدرس محل سکونت آن‌ها را شامل می‌شود. لایهٔ اقتصادی نیز دربردارندهٔ اطلاعات منتشرشده از رویدادهای دنیای واقعی در منابع رسانه‌ای و نیز وضعیت بازارهای واقعی مالی و تجاری است تا بدین‌وسیله این موضوع را نشان دهد که چگونه فعالیت‌های اقتصادی و سیاسی دنیای واقعی بر رویدادها و حمله‌های سایبری تأثیر می‌گذارد و بالعکس (Ruth, 2017).

آدریان ونابلز با به‌روزرسانی مجدد دو مدل قبلی خود (Ven-ables et al., 2015a, 2015b)، این بار به تبیین تمام عوامل تأثیرگذار بر تأمین امنیت سایبری پرداخت و مطابق شکل «۱۲» یک لایه و نیز یک بعد به مدل خود اضافه کرد. لایهٔ جغرافیایی که نخستین لایه و قبل از لایهٔ زیرساخت افزوده شده است، بیانگر اهمیت در نظر گرفتن منطقهٔ جغرافیایی است که دستگاه و سخت‌افزار فیزیکی در آنجا واقع است و درنتیجه شرایط خاصی از نظر طبیعت محیطی، ملاحظات سیاسی و یا سطح سرمایه‌گذاری توسعهٔ زیرساختی در آن منطقه را بر فضای سایبری تحمیل می‌کند. در کنار افزودن این لایه بعد سومی نیز به مدل اضافه شده است. این بعد بر جنبه‌های امنیتی و چگونگی کاهش



شکل ۱۱: مدل لایه‌بندی فضای سایبری مارتی لهتو (Lehto, 2015)

1. Firmware



شکل ۱۲: مدل لایه‌بندی فضای سایبری آدریان ونابلز (Venables, 2021)

مخاطرات امنیتی مربوط به تهدیدهای مختلف امنیتی تمرکز دارد و انگیزه‌ها و مهارت‌های مهاجمان سایبری را از یک سو و آموزش‌ها و کنترل‌های امنیتی موردنیاز برای مدافعان سایبری را از سوی دیگر به عنوان بعدی مهم در امنیت سایبری مورد توجه قرار می‌دهد (Venables, 2021).

۳. بحث و بررسی و مقایسهٔ مدل‌ها

در میان مدل‌های لایه‌بندی فضای سایبری، فقط ۵ مورد از آن‌ها از منظر مدیریت و حاکمیت بر این فضا ارائه شده‌اند. این مدل‌ها عبارت‌اند از مدل‌های بنکلر، فریدمن، زیمت، کلارک و بینشینگ. به‌منظور بررسی جامعیت این مدل‌ها ابتدا مقایسهٔ مدل‌ها براساس مؤلفه‌های تشکیل‌دهندهٔ فضای سایبری صورت می‌گیرد و در گام بعد میزان هم‌پوشانی لایه‌های متناظر در مدل‌های مختلف دسته‌بندی چهارگانه با یکدیگر ارزیابی می‌شود.

عبارت فضای سایبری از ترکیب دو واژهٔ فضا و سایبر ساخته شده است. سایبر واژه‌ای است که ریشه در مفهوم سایبرنتیک دارد؛ واژهٔ سایبرنتیک برگردان لاتین واژهٔ یونانی κυβερνητικός است که در یونان باستان به معنای هنر هدایت کشتی به کار می‌رفت. با ارائهٔ کتاب *سایبرنتیک؛ کنترل و ارتباطات در حیوان و ماشین* نوشتهٔ نوبرت وینر[1]، این ریاضی‌دان برجستهٔ آمریکایی در سال ۱۹۴۸ میلادی، علم جدیدی را با نام سایبرنتیک که مکانیسم‌های کنترل خودکار در سیستم‌های پیچیدهٔ حیوانی و ماشینی را تشریح می‌کند معرفی کرد (Godwin III et al., 2014). در سال ۱۹۸۴ میلادی ویلیام گیبسون[2]، نویسندهٔ آمریکایی، با به کار بردن عبارت فضای سایبری در داستان‌های علمی ـ تخیلی این واژه را بر سر زبان‌ها انداخت (Ning, 2022).

فضای سایبری به معنای ارتباطات متقابل کامل انسان‌ها از طریق رایانه و مخابرات بدون توجه به جغرافیای فیزیکی آن‌ها معنا می‌شود (Blane, 2001). به تعبیر دیگر فضای سایبری بستر جدید ارتباطات انسان‌ها با واسطهٔ شبکه‌های رایانه‌ای است. درواقع فضای سایبری با ایجاد تعاملی پیچیده میان انسان‌ها و سیستم‌های رایانه‌ای ایجاد می‌شود و به معنای شکل‌گیری یک سیستم انسان‌ـماشین گسترده در جهان واقعی است، درنتیجه می‌توان سه مؤلفهٔ ماشینی، انسانی و محیطی را در تحلیل این فضا مورد ملاحظه قرار داد. در توضیح مؤلفهٔ محیطی باید گفت که هرکدام از مؤلفه‌های انسانی یا ماشینی فضای سایبری در موقعیتی جغرافیایی و ذیل یک محیط حاکمیتی قرار دارند و از آن متأثر می‌شوند که لازم است در قالب دو مؤلفهٔ جغرافیایی و حاکمیتی مورد توجه قرار گیرند.

مدل‌هایی که برای فضای سایبری ارائه شده‌اند، هرکدام با تأکید بر یک یا چند مورد از مؤلفه‌های ماشینی، انسانی، جغرافیایی و حاکمیتی این فضا ارائه شده‌اند که در جدول «۱» آمده است. برخی مدل‌ها صرفاً مؤلفه‌های فنی و ماشینی فضا را مورد توجه قرار داده‌اند و وجوه انسانی و محیطی فضای سایبری در آن‌ها مغفول است. مؤلفه‌های فنی شامل سخت‌افزارهای فیزیکی، امواج الکترومغناطیسی، پروتکل‌های پردازش، ذخیره‌سازی و مبادلهٔ اطلاعات، نرم‌افزارهای سیستمی و کاربردی و نیز اطلاعات می‌شود. مدل بنکلر تنها مدلی است که با این نگاه محدود ارائه شده است. برخی دیگر از مدل‌ها در کنار مؤلفه‌های ماشینی به مؤلفه‌های انسانی فضا نیز توجه کرده‌اند، اما همچنان توجه به مؤلفه‌های محیطی در آن‌ها دیده نمی‌شود. مؤلفه‌های انسانی شامل افراد، هویت‌های سایبری آن‌ها و ارتباطات اجتماعی میان آن‌ها در فضای سایبری است. مدل‌های فریدمن، لیبیکی، لهتو، شلدون، بینشینگ، کلارک و ونتره با همین نگاه ارائه شده‌اند.

1. Norbert Wiener
2. William Gibson

جدول ۱: پوشش مؤلفه‌های فضای سایبری در مدل‌های لایه‌بندی

مدل‌های لایه‌بندی	مؤلفهٔ ماشینی	مؤلفهٔ انسانی	مؤلفهٔ محیطی
	بنکلر		
		فریدمن لیبیکی لهتو شلدون بینشینگ کلارک ونتره	
		فنلی ریموند نیروی مسلح امریکا رایلی گرانت وندربرگ زیمت روث ونابلز	

دستهٔ دیگر از مدل‌ها ضمن توجه به مؤلفه‌های ماشینی و انسانی مؤلفه‌های محیطی مربوط به فضای سایبری را نیز در مدل خود بیان کرده‌اند، ازجمله مدل‌های فنلی، رایلی، گرانت، زیمت، روث و ونابلز. در این مدل‌ها عمدتاً به موقعیت جغرافیایی قرارگیری مؤلفه‌های ماشینی و همچنین وابستگی‌های محیطی آن‌ها نظیر منابع تغذیه، سیستم‌های خنک‌کننده و ساختمان قرارگیری توجه شده است. همچنین الزامات حاکمیتی مثل چارچوب‌های قانونی و حقوقی، فرایندها و روابط سازمانی و مالکیت و مأموریت اجزا کم‌وبیش در این مدل‌ها مورد ملاحظه قرار گرفته است. مدل وندربرگ، از میان مؤلفه‌های محیطی صرفاً به مؤلفهٔ حاکمیتی توجه داشته است و مدل‌های ریموند و نیروی مسلح امریکا نیز از توجه به مؤلفهٔ حاکمیتی غافل بوده و فقط به مؤلفهٔ جغرافیایی توجه داشته‌اند.

همان‌گونه که مشاهده می‌شود از میان ۵ مدلی که از دیدگاه مدیریت و حاکمیت فضای سایبری ارائه شده‌اند فقط مدل زیمت تمام مؤلفه‌های فضای سایبری را پوشش می‌دهد.

مقایسهٔ هم‌پوشانی میان لایه‌های مدل‌های مختلف دسته‌های چهارگانه در جدول «۲» آمده است.

در مقایسهٔ مدل‌ها در جدول «۱» مشاهده شد که فقط مدل زیمت تمام مؤلفه‌های فضای سایبری را پوشش می‌دهد. بااین‌حال مقایسهٔ مدل‌ها در جدول «۲» نشان می‌دهد که مدل زیمت علی‌رغم جامعیت نسبی نتوانسته بیان مناسبی از لایه‌بندی فضای سایبری داشته باشد و نمی‌تواند لایه‌های این فضا را به گونه‌ای ساده و فهم‌پذیر برای همهٔ عوامل انسانی مرتبط با فضای سایبری مشخص کند. علت آن است که تفکیک مناسبی میان اجزای فضای سایبری در لایه‌بندی این مدل رعایت نشده است و برای مثال همهٔ اجزای سخت‌افزاری و نرم‌افزاری این فضا در قالب یک لایهٔ واحد یعنی لایهٔ سیستمی آورده شده‌اند.

از بررسی مدل‌های ارائه‌شده برای فضای سایبری و به کمک جدول‌های «۱ و ۲» می‌توان مدلی برای مدیریت و حاکمیت فضای سایبری پیشنهاد داد که هم از جامعیت برخوردار باشد و مؤلفه‌های چهارگانهٔ جغرافیایی، ماشینی، انسانی و حاکمیتی این فضا را پوشش دهد و هم با بیان تفکیک‌شده‌تر لایه‌ها نسبت به مدل زیمت از طریق ملاحظهٔ لایه‌های متناظر در سایر مدل‌ها مدلی ساده‌تر و فهم‌پذیرتر از این فضا پیشنهاد دهد. براین‌اساس مدل لایه‌بندی مطابق شکل «۱۳» پیشنهاد می‌شود.

جدول ۲: مقایسهٔ هم‌پوشانی مدل‌های لایه‌بندی مختلف ارائه‌شده برای فضای سایبری

مدل‌ها / معیارها	فریدمن	لیبیکی	لهتو	شلدون	وانبلز	بینینگ	بنکلر	کلارک	فنلی	ریموند	نیروی مسلح امریکا	رابلی	گرانت	وتره	وندربرگ	زیمت	روث
جامعیت	لایه‌های OSI	فیزیکی	فیزیکی	فیزیکی	فیزیکی	زیرساخت	زیرساخت فیزیکی	فیزیکی	فیزیکی	جغرافیایی	فیزیکی	جغرافیایی	جغرافیایی	فیزیکی	فنی	سیستمی	فیزیکی
		نحوی	نحوی	نحوی	نحوی							منطقی					
		معنایی	معنایی	معنایی	معنایی	داده	اطلاعات					زبان ماشین	اطلاعات	کاربردی		کاربردی/ محتوا	
	رابط کاربری	رابط کاربری	خدمت		انسان	شخصیت مجازی عملیات	محتوا	مردم	کاربرنمای سایبری نظارتی	کاربرنمای سایبری نظارتی	کاربرنمای سایبری	سیستم‌عامل نرم‌افزار کاربردی			اجتماعی- فنی	مردم/ اجتماعی	اجتماعی
		عمل‌گرایانه	شناختی		مأموریت						سازمانی	نظارتی	سازمانی	شناختی		حاکمیتی	حاکمیتی
	تفسیر تأثیر										حاکمیتی		اجتماعی- سازمانی				اقتصادی

شکل ۱۰: مدل لایه‌بندی پیشنهادی برای فضای سایبری

توضیح رنگ‌های به‌کاررفته در مدل پیشنهادی چنین است: لایه‌های نشان‌داده‌شده با رنگ‌های قهوه‌ای، آبی، سبز و نارنجی به‌ترتیب بیانگر مؤلفه‌های جغرافیایی، ماشینی، انسانی و حاکمیتی فضای سایبری‌اند. تشریح هرکدام از این لایه‌ها در جدول «۳» آمده است.

جدول ۳: تشریح لایه‌های مدل لایه‌بندی پیشنهادی برای فضای سایبری

عنوان	تعریف
لایهٔ حاکمیت	مجوزها، هنجارها، سیاست‌ها، استانداردها و قوانین محلی، ملی و بین‌المللی که ذیل آن‌ها مأموریت‌ها در فضای سایبری امکان ظهور و بروز می‌یابند و بر فضای سایبری تأثیر می‌گذارند و از آن تأثیر می‌پذیرند.
لایهٔ مأموریت	مأموریت و هدفی که هرکدام از سکوهای نرم‌افزاری کاربردی فضای سایبری برای تحقق آن طراحی، ساخته و اداره می‌شود. این لایه مشخص‌کنندهٔ چرایی و چگونگی درگیرشدن موجودیت‌های سکوهای فضای سایبری و همچنین چگونگی طراحی و ساخت لایه‌های مختلف فضای سایبری است.
لایهٔ انسانی	افراد مختلف حقیقی و حقوقی تعامل‌کننده با فضای سایبری ازجمله توسعه‌دهندگان، کاربران و ...
لایهٔ هویت سایبری	هویت‌ها یا شناسه‌های منحصربه‌فردی که فرد با آن‌ها در فضای سایبری شناخته‌شده و از طریق آن‌ها امکان دسترسی و ادراک فضا را می‌یابد.
لایهٔ محتوایی	محتوایی که فرد از فضای سایبری ادراک یا در آن ایجاد می‌کند.
لایهٔ کاربردی	سکوهای نرم‌افزاری کاربردی و رابط کاربری آن‌ها که امکان تعاملات و مبادلهٔ اطلاعات را برای مخاطب فراهم می‌آورند.
لایهٔ نرم‌افزاری	زیرساخت‌های نرم‌افزاری پردازشی، ذخیره‌سازی و ارتباطی لازم برای کارکرد لایه‌های بالاتر دربردارندهٔ منطق و سازوکار پردازشی، ذخیره‌سازی و ارتباطی.
لایهٔ سخت‌افزاری	زیرساخت‌های سخت‌افزاری الکترونیکی، مغناطیسی و الکترومغناطیسی تأمین‌کنندهٔ پردازش، ذخیره‌سازی و ارتباطات لازم برای کارکرد لایه‌های بالاتر.
لایهٔ تأسیساتی	نیازمندی‌ها و ملاحظات تأسیساتی لازم برای حفظ عملکرد سخت‌افزارها شامل منابع تغذیه، سیستم‌های خنک‌کننده و ....
لایهٔ جغرافیایی	محل قرارگیری جغرافیایی سخت‌افزارها در جغرافیای جهان و اقتضائات اقلیمی و سیاسی هر منطقه.

جمع‌بندی و نتیجه‌گیری

مدل لایه‌بندی فضای سایبری ضرورتی برای شناخت جامع این فضا و مدیریت مؤثر آن محسوب می‌شود و به درک بهتر اجزای تشکیل‌دهندهٔ این فضا و همکاری مؤثرتر عوامل مختلف تأثیرگذار یا تأثیرپذیر از فضای سایبری کمک می‌کند. مدل لایه‌بندی فضای سایبری با نمایش اجزای مختلف این فضا در قالب لایه‌های وابسته به یکدیگر در درک بهتر اجزا و تشخیص تمایزات و تعاملات آن‌ها با یکدیگر کمک کرده و نقش‌آفرینی و همکاری عوامل مختلف در کنار یکدیگر برای مدیریت آن را تسهیل می‌کند.

در این پژوهش مدل‌های لایه‌بندی مختلف ارائه‌شده برای فضای سایبری در دسته‌بندی‌های چهارگانه شامل حاکمیت بر فضای سایبری، تأثیرگذاری بر کاربران فضای سایبری، عوامل مؤثر در طرح‌ریزی عملیات سایبری و عوامل مؤثر در تأمین امنیت فضای سایبری دسته‌بندی شد. مقایسهٔ هم‌پوشانی میان لایه‌های مدل‌های مختلف علی‌رغم نام‌های متفاوت آن‌ها در مدل‌ها امکان تلفیق مدل‌های ارائه‌شده ذیل زمینه‌های موضوعی چهارگانه با یکدیگر و ارائهٔ مدل لایه‌بندی جدید را آشکار کرد. براین‌اساس مدل لایه‌بندی جدیدی برای فضای سایبری پیشنهاد شد تا با برخورداری از جامعیت و سادگی در فهم، برای مدیریت و حاکمیت بهتر فضای سایبری به کار گرفته شود.

مدل لایه‌بندی پیشنهادی ضمن پوشش همهٔ مؤلفه‌های جغرافیایی، ماشینی، انسانی و حاکمیتی فضای سایبری بیانی ساده از لایه‌های مختلف این فضا ارائه و نشان می‌دهد که در کنار توجه به اجزای سخت‌افزاری، نرم‌افزاری و حتی کاربران فضای سایبری لازم است به موقعیت جغرافیایی هرکدام از این اجزا و تبعات اقلیمی یا سیاسی مترتب بر آن نیز توجه شود. همچنین لازم است اهدافی که در طراحی هرکدام از سکوهای خدماتی و نرم‌افزارهای کاربردی فضای سایبری نهفته است و نیز قوانین و مقررات و هنجارهایی که این طراحی را تحت‌تأثیر قرار می‌دهند مورد توجه قرار گیرد.

براساس مدل ارائه‌شده لازم است در کنار مباحث فنی، سایر مؤلفه‌های انسانی، حاکمیتی و جغرافیایی در تأمین امنیت سایبری مورد توجه قرار گیرد؛ لذا پیشنهاد می‌شود که محققان حوزهٔ امنیت فضای سایبری و نیز سیاست‌گذاران این حوزه با به‌کارگیری مدل لایه‌بندی پیشنهادی از مغفول واقع‌شدن این مؤلفه‌ها در تحقیقات و سیاست‌گذاری‌ها جلوگیری کنند.

برنامه‌ریزی برای توسعهٔ اجزای مختلف فضای سایبری مطابق با مدل لایه‌بندی پیشنهادی از ضروریات دستیابی و حفظ سطح قابل‌قبول از قدرت سایبری در مقایسه با رقبای تجاری یا نظامی است. براین‌اساس لازم است با مورد توجه قرار دادن لایه‌های مختلف مدل پیشنهادی و اندازه‌گیری توانمندی‌ها و قابلیت‌های موجود در هرکدام از لایه‌ها برنامه‌ریزی به‌منظور ارتقای متوازن توانمندی‌ها در تمامی لایه‌ها صورت پذیرد.

باید توجه داشت که براساس مدل پیشنهادی در کنار توسعهٔ قابلیت‌های فنی، توانایی قانون‌گذاری و تدوین استانداردهای لازم برای فضای سایبری از لوازم حکمرانی مؤثر و حفظ استقلال کشورها در فضای سایبری است. لذا پیشنهاد می‌شود که فعالان حوزهٔ حکمرانی، سیاست‌گذاری و قانون‌گذاری فضای سایبری با اتکا به مدل پیشنهادی بتوانند درک همه‌جانبه‌تری از فضای سایبری به دست آورده و از این مدل به‌منظور تدوین سیاست‌ها، قوانین و استانداردهای متقن استفاده کنند تا در پرتو برخورداری از نگاه جامع به فضای سایبری، پذیرش، اتفاق‌نظر و اثربخشی بیشتری را در زمینهٔ قوانین وضع‌شده در حوزهٔ فضای سایبری شاهد باشیم.

منابع

Benkler, Y. (2000). "From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access. "*Federal Communications Law Journal*, 25(3), pp. 561–579.

Binxing, F., Peng, Z., and Shibing, Z. (2016). "Research on Cyberspace Sovereignty." *Strategic Study of Chinese Academy of Engineering Description*, 18(6).

Blane, J. V. (2001). *Cyberwarfare: Terror at a Click*. Nova Science Pub Inc.

Bush, J. E. (2021). *Cyberspace for the Operational Artist: Every Planner has the Tools to Understand the Cyber Domain*.

Choucri, N., and Clark, D. D. (2012). "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma." *ECIR Working Paper* No. 2012-3.

Clark, D. (2010). *Characterizing Cyberspace: Past, Present, and Future* (ECIR Working Paper No. 2010-3). MIT Political Science Department.

Fanelli, R., and Conti, G. (2012). "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict." *4th International Conference on Cyber Conflict* (CYCON 2012), pp. 319–331.

Gleason, D. H., and Friedman, L. (2005). "Proposal for an Accessible Conception of Cyberspace." *Journal of Information, Communication and Ethics in Society*, 3(1), pp. 15–23.

Godwin III, J. B., Kulpin, A., Rauscher, K. F., and Yaschenko, V. (2014). *Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations 2*. New York and Moscow: EastWest Institute and Moscow State University. https://www.files.ethz.ch/isn/178418/terminology2.pdf

Grant, T. (2014). "On the Military Geography of Cyberspace." *9th International Conference on Cyber Warfare and Security* (ICCWS 2014), pp. 66–76.

Kademi, A., and Koltuksuz, A. (2017). "Formal Characterization of Cyberspace for Cyber Lexicon Development." *ECCWS 2017 16th European Conference on Cyber Warfare and Security*.

Karimi Ghohroudi M.R, Moeinazad, Sh., and Karimi Ghohroudi E. (2023). “Typology of the Concept and Main Elements of Cyberspace in National Cyber Security Strategy of Selected Countries”. *National Security,* 13(47), pp. 9-36. {In Persian}

Lehto, M. (2015). "Phenomena in the Cyber World. In Martti Lehto and Pekka Neittaanmäki.” *Cyber Security: Analytics, Technology and Automation* (pp. 3–29). Springer.

Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press.

Limonier, K., Douzet, F., Pétiniaud, L., Salamatian, L., and Salamatian, K. (2021). "Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine." *First Monday*, *26*(5).

Ning, H. (2022). *A Brief History of Cyberspace*. CRC Press (Auerbach Publications).

Raymond, D., Conti, G., Cross, T., and Fanelli, R. (2013). "A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons." *5th International Conference on Cyber Conflict* (CYCON 2013), pp. 1–16.

Raymond, D., Conti, G., Cross, T., and Nowatkowski, M. (2014). "Key Terrain in Cyberspace: Seeking the High Ground." *6th International Conference on Cyber Conflict* (CyCon 2014), pp. 287–300.

Riley, S. (2014, October 7). *Cyber Terrain: A Model for Increased Understanding of Cyber Activity* [Blogspot Article]. http://cyber-analysis.blogspot.com/2014/10/cyber-terrain-model-for-increased.html

Ruth, I. (2017). "Multi-dimensional structural data integration for proactive cyber-defence." *International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (Cyber SA), pp. 1–9.

Sheldon, J. B. (2011). "Deciphering Cyberpower: Strategic Purpose in Peace and War." *Strategic Studies Quarterly*, 5(2), pp. 95–112.

U.S. Joint Chiefs of Staff. (2013). *Cyberspace Operations* (Joint Publication (JP) 3-12(R)).

Van den Berg, J., van Zoggel, J., Snels, M., van Leeuwen, M., Boekee, S., van de Koppen, L., van der Lubbe, J., van den Berg, B., and de Bos, T. (2014). "On (The Emergence of) Cyber Security Science and Its Challenges for Cyber Security Education." *Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium*.

Venables, A. (2021). "Modelling Cyberspace to Determine Cybersecurity Training Requirements." *Frontiers in Education*, 6(768037).

Venables, A., Shaikh, S. A., and Shuttleworth, J. (2015a). "A Model for Characterizing Cyberpower." *9th International Conference on Critical Infrastructure Protection* (ICCIP), pp. 3–16.

Venables, A., Shaikh, S. A., and Shuttleworth, J. (2015b). "The projection and measurement of cyberpower." *Security Journal*, 30(3), 1000–1011.

Ventre, D. (2012). *Cyber Conflict: Competing National Perspectives*. Wiley-ISTE.

Waltz, E. (1998). *Information Warfare Principles and Operations*. Artech House.

Zimet, E., and Skoudis, E. (2009). "A Graphical Introduction to the Structural Elements of Cyberspace". In Kramer, F. D., Starr, S. H. and Wentz, L. K., *Cyberpower and National Security* (pp. 91–112). University of Nebraska Press, Potomac Books.

Zimmermann, H. (1980). "OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection." *IEEE Transactions on Communications*, 28(4), pp. 425–432.

Science and Technology Pole
icy Letters
15, Issue 2, summer 2025

A Review of Layered Models of Cyberspace and and Proposal of a New Model

Ehsan Khosshalpour[1]

Abstract

In today's world, cyberspace has become an integral part of human life, fulfilling many of humanity's needs through the various capabilities provided by this technology. This technological transformation, while offering advantages such as speed, simplicity, and accuracy in delivering diverse services to users, has also posed challenges for governments. One of the most critical requirements for effective management of cyberspace is the understanding of its various components and how they interconnect. This understanding can only be achieved by simplifying and constraining cyberspace within a model. A layered model typically represents the constituent components in a vertical structure as interdependent layers. This paper aims to provide a narrative review of the layered models proposed for cyberspace, to identify a comprehensive and easily understandable model for managing and governing cyberspace. For this purpose, a search of reputable online databases yielded 57 papers or books, which were studied, and 19 unique layered models were identified. The identified layered models were categorized into four groups, and the models have been compared based on the coverage of cyberspace components and the level of overlap between the layers of different models. The results of this research suggest that the existing layered models are insufficiently comprehensive to provide effective management of cyberspace, and the proposed new model could help address this gap.

Keywords: Cyberspace, Layered model, Cyberspace Management

1. Master of Information Technology Engineering - Information Security, Malek Ashtar University of Technology, Tehran, Iran. khoshhalpour@chmail.ir

نقش‌نامه و فرم تعارض منافع

الف) نقش نامه

پدیدآورندگان	احسان خوشحال‌پور
نقش	نویسندهٔ مسئول
نگارش متن	تمامی فعالیت‌های نگارش و بازنگری متن
ویرایش متن و ...	تمامی فعالیت‌های ویرایش متن، کامنت‌دهی و پاسخ به داوران
طراحی / مفهوم‌پردازی	طراحی و مفهوم‌پردازی
گردآوری داده	مطالعات کتابخانه‌ای و گردآوری داده‌ها
تحلیل / تفسیر داده	تفسیر و تحلیل کیفی داده‌ها

ب) اعلام تعارض منافع

در جریان انتشار مقالات علمی تعارض منافع به این معنی است که نویسنده یا نویسندگان، داوران و یا حتی سردبیران مجلات دارای ارتباطات شخصی و یا اقتصادی می‌باشند که ممکن است به طور ناعادلانه‌ای بر تصمیم‌گیری آن‌ها در چاپ یک مقاله تأثیرگذار باشد. تعارض منافع به خودی خود مشکلی ندارد بلکه عدم اظهار آن است که مسئله‌ساز می‌شود.

بدین وسیله نویسندگان اعلام می‌کنند که رابطه مالی یا غیرمالی با سازمان، نهاد یا اشخاصی که موضوع یا مفاد این تحقیق هستند ندارند، اعم از رابطه و انتساب رسمی یا غیررسمی. منظور از رابطه و انتفاع مالی از جمله عبارت است از دریافت پژوهانه، گرنت آموزشی، ایراد سخنرانی، عضویت سازمانی، افتخاری یا غیررسمی، اشتغال، مالکیت سهام، و دریافت حق اختراع، و البته محدود به این موارد نیست. منظور از رابطه و انتفاع غیرمالی عبارت است از روابط شخصی، خانوادگی یا حرفه‌ای، اندیشه‌ای یا باورمندانه، و غیره.

چنانچه هر یک از نویسندگان تعارض منافعی داشته باشد (و یا نداشته باشد) در فرم زیر تصریح و اعلام خواهد کرد:

مثال: نویسندهٔ الف هیچ‌گونه تعارض منافعی ندارد. نویسندهٔ ب از شرکت فلان که موضوع تحقیق بوده است گرنت دریافت کرده است. نویسندگان ج و د در سازمان فلان که موضوع تحقیق بوده است سخنرانی افتخاری داشته‌اند و در شرکت فلان که موضوع تحقیق بوده است سهام‌دارند.

اظهار (عدم) تعارض منافع: با سلام و احترام؛ به استحضار می‌رساند نویسندگان مقاله هیچ‌گونه تعارض منافعی ندارد.

نویسندهٔ مسئول: احسان خوشحال‌پور

تاریخ: ۱۴۰۳/۰۸/۱۶