فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره اول، زمستان ۱۴۰۰، صفحات ۱۰۲-۶۷

ارائه مدل مفهومی تحلیل امنیت در فضای سایبر ملی کشورها

رضا تقی‌پور[۱]، مهراب رامک[۲]

تاریخ دریافت: ۱۴۰۰/۰۴/۰۲ **تاریخ پذیرش: ۱۴۰۰/۰۹/۱۱**

چکیده

فضای سایبر ملی یا فضای سایبر ملی، قلمرو حاکمیتی هر کشور در فضای سایبر محسوب می‌گردد و به‌منظور تحقّق امنیت در این فضا لازم است وضعیت امنیت این فضا و تمامی عوامل تأثیرگذار بر آن، مورد رصد، شناسایی، ارزیابی و تحلیل مداوم قرار گیرد تا در صورت بُروز هرگونه اختلال، اقدامات لازم انجام گیرد که پیش‌نیاز این مهم، وجود مدل مناسبی برای تحلیل امنیت در فضای سایبر ملی است که پژوهش توسعه‌ای – کاربردی حاضر، این مهم را مورد توجه قرار داده و از طریق جستجوی اینترنتی، مطالعات کتابخانه‌ای و بهره‌گیری از نظرات خبرگان، مبانی نظری، مدل‌های علمی، استانداردهای ملی یا بین‌المللی مرتبط با این موضوع را جمع‌آوری و مورد مطالعه قرار داده است. با توجه به ماهیت مستندات پژوهش از روش کیفی و مبتنی بر خبرگی استفاده شد و با بهره‌گیری از عقل، منطق، غور و اندیشه، اسناد، مدارک و اطلاعات جمع‌آوری‌شده مورد بررسی و تحلیل محتوا قرار گرفت و با جمع‌بندی یافته‌ها، ساختار کلانی بری مدل مورد نظر تنظیم گردید. با بررسی دقیق‌تر عوامل احصاشده و تلفیق موارد همسان به‌منظور رفع همپوشانی‌ها موجود، ابعاد، مؤلفه‌ها و زیر مؤلفه‌های قابل توجه در مدل مفهومی استخراج و مدل مفهومی تحلیل امنیت در فضای سایبر ملی کشورها ترسیم و ارائه گردید. نتایج پژوهش نشان داد که کشورها، برای تحلیل امنیت فضای سایبر ملی خود باید، زیرساخت‌ها و نیازمندی‌های امنیتی از قبیل فناوری‌های امنیت، فرایندهای اجرایی امنیت، منابع عملیاتی کردن امنیت، توانمندی منابع انسانی و تشکیلات (نهادهای متولی، مسئول و پاسخگو) خود را از دیدگاه‌های شناختی، خدماتی و زیرساختی مورد توجه قرار دهند و در این راستا نیز ابزارهایی همانند سیاست‌گذاری و برنامه‌ریزی، نظارت و ارزیابی مستمر، هماهنگی و همکاری در زمینه امنیت را مورد استفاده قرار دهند.

کلید واژه‌ها: مدل مفهومی، تحلیل امنیت، فضای سایبر ملی

۱.دکتری علوم پیشرفته مدیریت – هیئت علمی و استاد دانشگاه عالی دفاع ملی
۲.دکتری مدیریت راهبردی فضای سایبر (امنیت سایبری) – دانشگاه عالی دفاع ملی (نویسنده مسئول)
m.ramak@sndu.ac.ir

مقدمه

فضای سایبر ملی یا فضای سایبر ملـی، قلمـرو حـاکمیتی هـر کشـور در فضـای سـایبر محسوب می‌گردد و معطوف به اجزاء فیزیکیِ پراکنده تحت حاکمیت یا تأمین‌کننـده منـافع آن کشور، ساختار و معماری منطقیِ این اجزا، محتوا و خدماتِ ارائه‌شده توسط این اجـزا و هویت‌های مرتبط‌کننده تعامل میان انسان و این محیط، است. به‌منظور تحقّق امنیـت در ایـن فضا لازم است از یک‌سو، شبکه‌ای بر اساس نگرش سامانمند و با رعایـت کامـل اصـول و الزامات امنیتی یا مبتنی بر یک مدل علمی ایجاد یا توسعه داده شود که پیش‌نیاز تحقـق ایـن امر، تعیین و ارائه اصول و الزامات امنیتی این شبکه، در قالب مدل مفهومی است و از سوی دیگر، وضعیت امنیت این شبکه و تمامی عوامل تأثیرگذار بـر آن، مـورد رصـد، شناسـایی، ارزیابی و تحلیل مداوم قرار گیرد تا در صورت بُـروز هرگونـه اخـتلال در سـطح مطلـوب امنیت این شبکه، مواجهه‌ی لازم با عوامل بُروز این اختلال، انجام گیرد که پیش‌نیـاز تحقـق ارزیابی و تحلیل وضعیت امنیت این شبکه، وجـود معمـاری تحلیـل امنیـت مناسـب بـرای فضای سایبر ملی است که حداقل حاوی یک روش نظام‌مند، بـه همـراه ابعـاد، مؤلفـه‌هـا و شاخص‌های سنجش وضعیت امنیت این شبکه باشد. پـژوهش حاضـر، ایـن مهـم را مـورد توجه قرار داده و با جمع‌آوری، مطالعه و جمع‌بندی مدل‌های علمی و استانداردهای ملی یـا بین‌المللی موجود، تلاش می‌نماید که مدل مفهومی معمـاری تحلیـل امنیـت مناسـب بـرای فضای سایبر ملی را پیشنهاد نماید.

۱. مبانی نظری

در این بخش، مبانی نظری مرتبط با موضوع پژوهش را مورد بررسـی دقیـق‌تـری قـرار می‌دهیم.

فضای سایبر

بر اساس تعریف مشترک ارائه‌شده در واژه‌نامه دوجانبه اصطلاحات حیاتی امنیت فضای سایبر توسط انستیتو شرق-غرب آمریکا و انستیتو امنیت اطلاعات دانشـگاه دولتـی مسـکو،

فضـای سـایبر، محـیط الکترونیکـی اسـت کـه اطلاعـات در آن تولیـد، ارسـال، دریافـت، ذخیره‌سازی، پردازش و حذف می‌گردد (Rauscher & Yaschenko, 2011: 10). سـند تئـوری جنگ و راهبرد دانشگاه جنگ ارتش آمریکا، فضای سایبر را شـامل شـبکه‌هـای وابسـته بـه یکـدیگر، از زیرسـاخت‌هـای فنـاوری اطلاعـات، اعـم از اینترنـت، شـبکه‌هـای ارتبـاطی، سامانه‌های رایانه‌ای، پردازنده‌های جاگذاری شده و کنترل‌کننده‌های صنایع حیـاتی مـی‌دانـد (Bartholomees, 2012: 19). در سند راهبرد امنیت فضای سایبر کابینه انگلیس، فضای سایبر، تمامی حالات فعالیت‌های رقومی شبکه‌ای، شـامل محتـوای و فعالیـت‌هـای انجـام‌شـده در داخل شبکه‌های دیجیتال را در برمی‌گیرد (Great Britain & Cabinet Office, 2009: 19) و بر اساس این تعریف، محتوا و رفتار کاربران نیز جزئی از فضـای سـایبر قـرار گرفتـه اسـت و فضای سایبر، شامل اینترنت و سایر سامانه‌هـای اطلاعـاتی کـه زیرسـاخت، سـرویس‌هـا و کسب‌وکار را پشتیبانی می‌کنند نیز می‌شود (Great Britain & Home Office, 2010: 34). سـند راهبرد امنیت فضای سایبر وزارت کشور دولت فدرال آلمـان، فضـای سـایبر را متشـکل از تمامی سامانه‌های فناوری اطلاعات پیوندیافته به یکدیگر، در لایـه داده، در مقیـاس جهـانی می‌داند که در آینده با هر تعداد از شـبکه‌هـای جدیـد داده، قابـل توسـعه اسـت؛ بنـابراین، سامانه‌های فناوری اطلاعاتی که در فضای مجـازی منفـرد و مجـزا قـرار دارنـد، بخشـی از فضای سـایبر محسـوب نمـی‌شـوند (Federal Ministry of the Interior, 2011: 14). در سـند راهبرد امنیت فضای سایبر دولت کانادا، فضای سایبر، دنیای الکترونیکی ایجادشـده توسـط شـبکه‌هـای فنـاوری اطلاعـات متصـل بـه یکـدیگر و اطلاعـات موجـود در آن شـبکه‌هـا اسـت(Goverment of Canada, 2010: 18). در سـند راهبـردی امنیـت فضـای سـایبر دولـت اسـترالیا، فضـای سـایبر، معـادل ارتباطـات و فنـاوری اطلاعـات تعریـف شـده است(Commonwealth of australia, 2009: 27). بر اساس تعریف ارائه‌شـده در سـند راهبـرد امنیت فضای سایبر دولت نیوزیلند، فضای سایبر، شبکه جهانی از زیرسـاخت‌هـای فنـاوری اطلاعات دارای وابستگی متقابل، شبکه‌های ارتباطی و سامانه‌های پـردازش رایانـه‌ای اسـت که در آن‌ها، امکان ارتباط برخط، تعبیه شده باشد (New Zealand Government, 2011: 12).

فضای سایبر ملی

فضای سایبر ملی که از آن با عناوینی همچون شبکه ملی، شبکه داخلی، شبکه ملی سایبری یا قلمرو سایبری کشور نیز یاد می‌شود، بخشی از فضای سایبر است که منتسب به یک کشور مشخص باشد، اما درواقع چنین نیست و فضای سایبر ملی، بخشی از شبکه ملی سایبری یک کشور است که ویژگی‌های خاصی را داشته باشد. در کتاب جغرافیای سیاسی فضای مجازی (حافظ نیا، ۱۳۹٤: ۱۸)، وجه بارز یک کشور، حکومت و نظام سیاسی معرفی‌شده است که به نمایندگی از مردم آن سرزمین، به وجود می‌آید و انجام وظایفی از قبیل اداره امور عمومی، تأمین امنیت فردی شهروندان، تأمین امنیت عمومی، تنظیم روابط ملّت، تدارک و تأمین نیازهای اساسی افراد ملّت، حفاظت از حقوق و حیثیت ملی، توسعه و ارتقای مستمر ابعاد مادی و معنوی و فکری آن جامعه را بر عهده دارد. این کتاب تأکید دارد که همین مفاهیم و کارکردها در فضای سایبر نیز مطرح بوده و از اهمیت بسیار زیادی برخوردار است. به عبارت دیگر، اعمال حاکمیت و تنظیم روابط بین ذی‌نفعان فضای سایبر، همانند دنیای واقعی، در فضای سایبر نیز ضرورت دارد. بر همین اساس، در فضای سایبر اولین مفهومی که از نظر ملی برای کشورها و دولت‌ها اهمیت دارد، مفهوم قلمرو حاکمیتی است و موضوعاتی باید در آن مورد توجه قرار گیرد:

ـ مفهوم مرز: برای انتساب فضای سایبر به یک کشور، لازم است پارامترهای تعیین‌کننده‌ی مرز در این فضا را شناسایی نمود. نقش مرز در فضای سایبر، توسط چند پارامتر ایفا می‌شود. یکی از این پارامترها، نام دامنه است. تخصیص نام دامنه‌های سطح اوّل به کشورها و سازمان‌ها یا اتحادیه‌های منطقه‌ای نیز بر همین مبنا صورت گرفته و بیانگر قلمروسازی و ایجاد حریم سایبری برای فعالیت‌ها و نقش‌های بازیگران این حوزه است. البته در کنار این نام‌های دامنه، دسته‌ی دیگری از نام‌های دامنه سطح اوّل نیز مانند .com، .edu، .gov، .mil و .ac وجود دارند که واگذاری آن‌ها فارغ از قلمرو کشورها در فضای سایبر انجام می‌گیرد.

ـ نقش مراکز داده: اگر محتوای اینترنتی متعلق به یک کشور، در داخل مرکز داده اینترنتی قرار گیرد که از نظر جغرافیایی، خارج از مرزهای جغرافیایی آن کشور و در داخل

کشور دیگری قرار دارد، جزء فضای سایبر کشور مالک محتوای اینترنتی است. همان‌طور که در دنیای واقعی نیز سفارت یک کشور در داخل کشور دیگر، بخشی از خاک کشور مالک سفارت‌خانه تلقی شده و قوانین و مقررات همان کشور بر محل سفارت حاکم است.

ـ **اعمال حاکمیت:** از طریق تخصیص نام دامنه به کشورها، اعمال کنترل و مدیریت بر کارکردهای فضای سایبر توسط حکومت‌ها و از طریق آمایش و ساماندهی ابعاد سخت‌افزاری و نرم‌افزاری فضای سایبر به‌عنوان زیرساخت‌های این فضا، توسط دولت‌ها انجام می‌گیرد. ایجاد، توسعه و اعمال حاکمیت بر این زیرساخت‌ها که خود، بخشی از فضای سایبر را تشکیل می‌دهند، توسط دولت‌ها صورت می‌گیرد. بر اساس این دیدگاه، قلمرو یک کشور در فضای سایبر، مشتمل بر بخشی از فضای سایبر است که توسط و با هزینه‌ی آن کشور ایجاد شده است و کنترل و مدیریت آن بخش نیز توسط همان کشور انجام می‌شود.

به این ترتیب، بین فضای سایبر و فضای واقعی، ارتباط متقابل وجود دارد و انطباق مفهوم و ابعاد قلمرو در دو فضای واقعی و سایبری توسط دولت‌ها انجام می‌گیرد. بر اساس این دیدگاه، شبکه ملی سایبری یک کشور، قلمرو حاکمیتی آن کشور در فضای سایبر محسوب می‌شود و جایگاه و اهمیت آن، قابل مقایسه با سایر قلمروهای حاکمیتی در عرصه‌های زمینی، هوایی، دریایی و فضایی است و مشتمل بر بخشی از فضای سایبر بین‌المللی است که:

۱. با نام دامنه متعلق به کشور مورد نظر، قابل دسترس باشد.

۲. محتواهای سایبری متعلق به کشور مورد نظر، در آن اقامت داشته باشند.

۳. توسط و با هزینه‌ی کشور مورد نظر توسعه یافته باشد.

٤. کنترل و مدیریت این فضا، توسط حاکمیت کشور مورد نظر، اعمال گردد.

درواقع، هر بخشی از فضای سایبر که مؤلفه‌ی جغرافیایی آن در محدوده‌ی قلمرو حاکمیتی یا منافع ملی یک کشور قرار گیرد، «فضای سایبر ملی» آن کشور تلقی شده و به‌طورکلی نُه کارکرد را می‌توان برای آن در نظر گرفت:

ـ شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی و سامانه‌های رایانه‌ای.

ـ پیش‌ران توسعه اقتصادی، اجتماعی و سیاسی کشورها.

ـ محیط شکل‌گیری کسب‌وکار دیجیتال و ابزار دیجیتالی کردن کسب‌وکار سنّتی.

ـ زیست‌بوم اطلاعات و دانش یک ملّت که در پرتو نظم مبتنی بر اصول و ارزش‌های آن ملّت اداره می‌شود.

ـ یک محیط انجام فعالیت‌های سایبری «تأثیرگذار بر» و یا «تأثیرپذیر از» محیط فعالیت‌های فیزیکی بشر بوده و بر این اساس، یک محیط تعاملی برای انجام فعالیت‌های مجرمانه تلقّی می‌شود.

ـ یکی از مؤلفه‌های کلیدی امنیت ملی و تأثیرگذار بر سایر مؤلفه‌ها از قبیل اقتصاد ملی، منافع ملی، روابط بین‌المللی، اقتدار ملی، انسجام ملی، اعتماد عمومی و سلامت عمومی است.

ـ زیرساخت حیاتی ارتباطات و فناوری اطلاعات، از بارزترین مصداق سرمایه ملی سایبری است.

ـ بخشی کلیدی از قلمرو حاکمیتی هر کشور، در فضای سایبر ملی آن کشور قرار دارد و با هزینه‌ی آن کشور، کنترل و مدیریت شده و با نام دامنه متعلق به آن کشور، قابل دسترس است.

ـ پس از زمین، هوا، دریا و فضا، پنجمین محیط عملیات نظامی محسوب می‌شود؛ بنابراین، قدرت سایبر نیز یکی از مؤلفه‌های تشکیل‌دهنده‌ی قدرت نظامی هر کشور محسوب می‌شود.

امنیت در فضای سایبر ملی

راهنمای راهبرد امنیت سایبر ملی اتحادیه بین‌المللی مخابرات[1]، امنیت سایبر ملی را به‌صورت «مجموعه‌ی ابزارها، خط‌مشی‌ها، مفاهیم، حفاظ‌های امنیتی، راهنماها، رویکردهای مدیریت مخاطره، اقدامات، آموزش‌ها و فناوری‌هایی که می‌توانند برای محافظت از محیط سایبر و سرمایه‌های سازمان و کاربران، استفاده شوند»، توصیف نموده است (ITU, 2011).

1. International Telecommunication Union (ITU)

در کتاب راهنمای چارچوب امنیت سایبر ملی مرکز مشارکتی نخبگان دفاع سایبری ناتو[1]، امنیت سایبر ملی، به‌صورت «به‌کارگیری متمرکز اهرم‌های حاکمیتی ویژه و اصول تضمین اطلاعات[2]، برای سامانه‌های ارتباطی و فناوری اطلاعات عمومی، خصوصی و بین‌المللی و محتوای درآمیخته با آن‌ها، در حالی که این سامانه‌ها، مستقیماً بر امنیت ملی، اثرگذارند» تعریف شده است (Klimburg & NATO, 2012). بر این اساس، امنیت در فضای سایبر ملی را می‌توان «بهره‌گیری از کلیه امکانات سایبری و غیر سایبری کشور، به‌منظور ایجاد مصونیت (تأمین محرمانگی، صحت، دسترس‌پذیری، تصدیق هویت، کنترل دسترسی، عدم انکار، امنیت ارتباط و حریم خصوصی) و تضمین تداوم آن (پیش‌گیری، ممانعت از انجام، تشخیص به‌موقع، کنترل ابعاد، مقابله مؤثر و بازدارنده) در مقابل هرگونه تهدید سایبری (قابلیت، نیّت یا اقدام احتمالی سایبری جهت نقض این مصونیت و تأثیرگذاری بر امنیت ملی، منافع ملی یا اقتصاد ملی، وجهه و روابط بین‌المللی، سلامت، ایمنی و اطمینان عمومی، باورهای دینی و ملی یا اداره‌ی امور کشور)» تعریف نمود. بر این اساس، ویژگی‌های کلیدی فضای سایبر ملی را می‌توان این‌گونه برشمرد:

ـ وابستگی زیرساخت‌های حیاتی، حساس و مهم کشور به زیرساخت شبکه ملی سایبری.

ـ تعارض گمنامی و بی‌مرزی با استنادپذیری.

ـ قابلیت ایجاد پیامدهای جنبشی، اعم از فیزیکی (جنگ فیزیکی) و اجتماعی (جنگ نرم).

ـ توانایی تأثیرگذاری بر اداره امور کشورها، به‌واسطه وابستگی شدید زیرساخت‌ها به این فضا.

ـ توانایی تأثیرگذاری بر امنیت، اقتصاد و منافع ملّی، سلامت و اعتماد عمومی و باورهای ملّی، دینی و قومی.

1. NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE).
2. Information Assurance (IA).

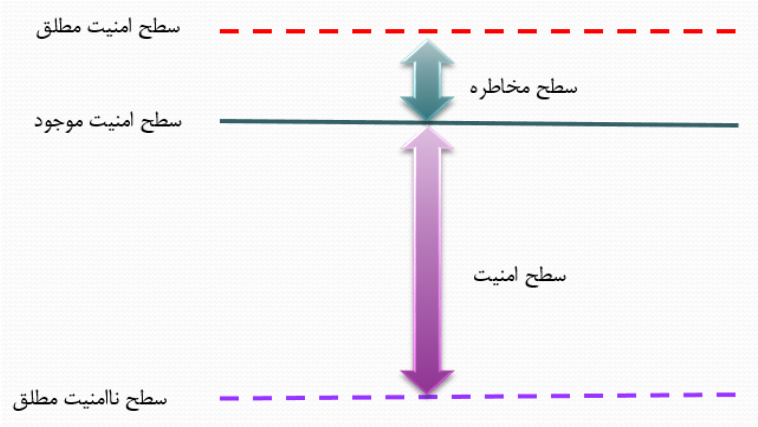
تحلیل امنیت در فضای سایبر ملی

تحلیل به معنی دسته‌بندی، مرتب کردن و خلاصه کردن داده‌ها به‌منظور دست‌یابی به پاسخ پرسش‌ها است و تحلیل‌گر نیز، مجموعه‌های وسیع، پیچیده و حتی غیرقابل درک داده‌ها را به واحدها، الگوها و شاخص‌های قابل درک و استفاده در مسائل پژوهشی، تبدیل می‌نماید. تفسیر[1]، به معنای رسیدن به استنباط درباره‌ی روابط بین متغیرهای مورد مطالعه و استخراج نتایج روابط بر مبنای یافته‌های حاصل از تحلیل است. درواقع می‌توان گفت که تفسیر، محصول تحلیل است و همه‌ی تحلیل‌ها به تفسیر یعنی رسیدن به استنباط و نتایجی درباره‌ی روابط مورد مطالعه می‌انجامد. از این رو می‌توان گفت، اساس تحلیل بر دو پایه استوار است:

ـ اول: جزء نمودن یک موضوع کلان (شکستن یک موضوع کلان، به موضوعات خرد تشکیل‌دهنده‌ی آن)

ـ دوم: فهم ویژگی‌های هر جزء و روابط موجود بین اجزا

امنیت، واژه‌ای نسبی است. سطح امنیت، بین دو سطح ناامنی مطلق و امنیت مطلق تعریف می‌شود. مطابق شکل ۱، فاصله‌ی بین سطح امنیت موجود با سطح ناامنی مطلق با عنوان سطح امنیت و فاصله‌ی بین سطح امنیت موجود با سطح امنیت مطلق، سطح مخاطره نامیده می‌شود.



شکل ۱: سطح امنیت و سطح مخاطره

1. Explanation

سطح امنیت، خروجی فعالیتی با عنوان تحلیل امنیت یا تحلیل وضعیت امنیت است و سطح امنیت هر موجودیت را می‌توان با تعیین یا تخمین سطح مخاطره‌ی موجود بر ضد آن موجودیت به دست آورد، به این ترتیب که سطح مخاطره را از ۱۰۰ درصد (سطح امنیت مطلق) کم می‌کنیم تا سطح امنیت به دست بیاید. سطح مخاطره یک موجودیت، خروجی فعالیتی با عنوان تحلیل مخاطره است که در آن:

۱. تهدیدهای موجود بر ضد موجودیت مورد نظر، شناسایی می‌شوند.

۲. آسیب‌پذیری‌های موجودیت مورد نظر، از طریق آزمون، ممیزی یا جمع‌آوری، شناسایی می‌شوند.

۳. احتمال بهره‌برداری تهدیدها از آسیب‌پذیری‌های آن موجودیت، شدّت پیامد احتمالی ناشی از این بهره‌برداری و درنتیجه، سطح مخاطره موجودیت تعیین می‌شود.

استاندارد مدیریت مخاطرات امنیت اطلاعات، در داخل متدولوژی ارائه‌شده برای مدیریت مخاطرات سایبری که بخش اول آن را ارزیابی مخاطرات سایبری تشکیل می‌دهد، ذیل فعالیت ارزیابی مخاطره، ابتدا فعالیت تحلیل مخاطره و بعد سنجش مخاطره را قرار داده است. در این متدولوژی، تحلیل مخاطره شامل دو فعالیت شناسایی و تخمین مخاطره عنوان شده است (Fahrurozi, Tarigan, Tanjung, & Mutijarsa, 2020: 59). در تحلیل محیط‌های راهبردی، عوامل باید از منظر ابعاد سیاسی[1]، اقتصادی[2]، اجتماعی[3]، فناورانه[4]، حقوقی[5] (قانونی)، زیست‌محیطی[6]، جمعیتی[7]، نظامی[8]، فرهنگی[9]، حاکمیتی[10] و ... مورد توجه قرار گیرند.

1. Political.
2. Economical
3. Social
4. Technical
5. Legal
6. Legal
7. Demographic
8. Military
9. Cultural
10. Governmental

امنیت در فضای سایبر ملی برخی از کشورها (مطالعات تطبیقی)

به‌منظور دست‌یابی به مدل مفهومی مورد نظر، وضعیت امنیت فضای سایبر ملی برخی از کشورها را طبق مستندات مربوطه مورد بررسی قرار می‌دهیم.

ایالات‌متحده آمریکا

در ایالات‌متحده آمریکا، مسئولیت امنیت فضای سایبر ملی، بر عهده وزارت امنیت داخلی است و مؤسسه استاندارد و فناوری ایالات‌متحده نیز استانداردها و الگوهای مناسب برای این حوزه را تعیین و منتشر می‌نماید. بر این اساس، سه الگوی منتشرشده توسط مؤسسه مذکور که مجموعاً دید کاملی در خصوص الگوی معماری و تحلیل امنیت فضای سایبر ملی را ترسیم می‌نمایند، مورد بررسی قرار خواهیم داد.

چارچوب بهبود امنیت سایبری زیرساخت‌های حیاتی (مؤسسه استاندارد آمریکا)

در راستای تحقق برنامه محافظت از زیرساخت‌های حیاتی ایالات‌متحده آمریکا، مؤسسه استاندارد و فناوری این کشور[1]، اقدام به ارائه چارچوبی جهت بهبود وضعیت امنیت سایبری در زیرساخت‌های حیاتی این کشور، ارائه نموده است. این چارچوب با همکاری و هماهنگی وزارت امنیت داخلی[2] و در راستای اهداف پیش‌بینی‌شده برای برنامه ملی امنیت فضای سایبر ایالات‌متحده منتشر شده است که متولی آن وزارت امنیت داخلی این کشور است. رویکرد کلی این چارچوب، مبتنی بر مدیریت مخاطرات موجود در زیرساخت‌های حیاتی است و در سه بخش هسته‌ی چارچوب[3] (وظایف، دسته‌ها، زیر دسته‌ها و مراجع اطلاعاتی)، ردیف‌های پیاده‌سازی چارچوب[4] (اقداماتِ بخشی در لایه ۱، اقدامات آگاهی‌دهنده[5] در لایه ۲، اقدامات تکرارپذیر[6] در لایه ۳ و اقدامات تطبیق‌پذیر[7] در لایه ٤) و

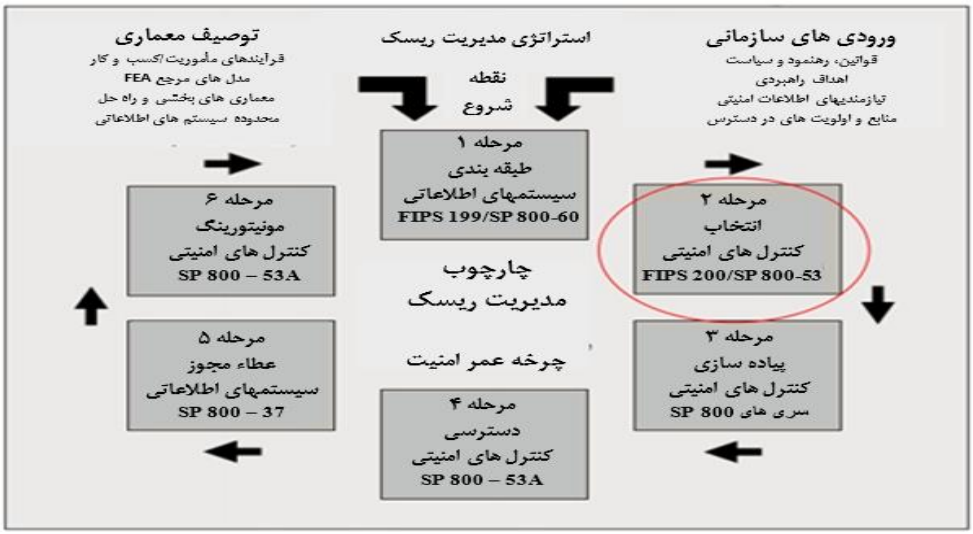
1. NIST.
2. Department of Homeland Security (DHS).
3. Framework Core.
4. Framework Implementation Tiers.
5. Informed.
6. Repeatable.
7. Adaptive.

رخ‌نماهای چارچوب[1] (نمایش‌دهنده‌ی خروجی‌های مبتنی بر نیازهای کسب‌وکاری است که یک سازمان، باید از دسته‌ها و زیر دسته‌های پنج دسته فعالیت ارائه‌شده در بخش هسته‌ی چارچوب، انتخاب کند) است.

معماری مرجع امنیت رایانش ابری (مؤسسه استاندارد آمریکا)

مؤسسه استاندارد ایالات‌متحده آمریکا در سال ۲۰۱۳ میلادی پیش‌نویس استاندارد شماره NIST SP 500-299 با عنوان مرجع معماری امنیت رایانش ابری را منتشر نمود. در این استاندارد، معماری امنیت برای معماری خدمات ابری ارائه‌شده در راهبرد رایانش ابری فدرال ارائه شده است. در این معماری، ارائه خدمات ابری در سه لایه‌ی زیرساخت به‌عنوان خدمت[2]، سکو به‌عنوان خدمت[3] و نرم‌افزار به‌عنوان خدمت[4] انجام می‌گیرد و برای برای مدل توسعه‌ی خدمات نیز از مدل عمومی، خصوصی، ترکیبی و جامعه که بهترین نوع پوشش را برای مأموریت‌های کسب‌وکار و نیازمندی‌های امنیتی مشتری ایجاد می‌کند، استفاده شده است. همچنین دیدگاه‌های تمامی بازیگران ارائه این خدمات، شامل مشتری، تأمین‌کننده، واسطه (دلال)، حمل‌کننده و ممیّز نیز مورد توجه قرار می‌گیرند (Group & others, 2013). این استاندارد، پس از شناسایی و طبقه‌بندی سرمایه‌های خدمات ابری، بر اساس چارچوب مدیریت مخاطرات امنیتی ارائه‌شده در استاندارد NIST SP 800-37 (Ross & others, 2010, p. 55) و مطابق گام دوّم این متدولوژی که در شکل ۲ نمایش داده شده است، اقدام به انتخاب کنترل‌های امنیتی نموده است.

1. Framework Profiles.
2 Infrastructure as a Service (IaaS)
3. Platform as a Service (PaaS)
4. Software as a Service (SaaS)



شکل ۲: چارچوب مدیریت مخاطرات

مهندسی امنیت سامانه‌ها–رویکرد یکپارچه برای تولید سامانه‌ی مطمئن انعطاف‌پذیر (مؤسسه استاندارد ایالات‌متحده)

در ادامه‌ی بهره‌گیری از مهندسی امنیت به‌منظور تأمین امنیت پایدار در سامانه‌های اطلاعاتی، مؤسسه استاندارد ایالات‌متحده نیز در سال ۲۰۱٤ میلادی اقدام به انتشار توصیه‌نامه شماره NIST SP 800-160 با عنوان مهندسی امنیت سامانه‌ها – رویکرد یکپارچه‌شده برای تولید سامانه‌های مطمئن انعطاف‌پذیر نموده است (Ross, Oren, & McEvilley, 2014). بر این اساس، مهندسی امنیت سامانه در چهار حوزه‌ی نیازهای محافظت، روابط امنیت، قابلیت اعتماد و اعتماد و مدیریت مخاطره امنیت، نسبت به مهندسی سامانه، ایجاد ارزش‌افزوده می‌نماید.

اتحادیه اروپایی

آژانس امنیت اطلاعات و شبکه اروپا[1]، به‌عنوان مرکز مدیریت راهبردی حوزه‌ی امنیت فضای سایبر در اتحادیه اروپایی عمل می‌کند و بر این اساس، نقش هماهنگی و مدیریت کلان در حوزه امنیت فضای سایبر کشورها عضو این اتحادیه را بر عهده دارد. این آژانس،

1. European Network and Information Security Agency (ENISA).

دو سند مکمل یکدیگر را منتشر نموده است که به‌صورت توأمان، بیانگر الگوی معماری و تحلیل امنیت فضای سایبر ملی کشورهای عضو این اتحادیه است.

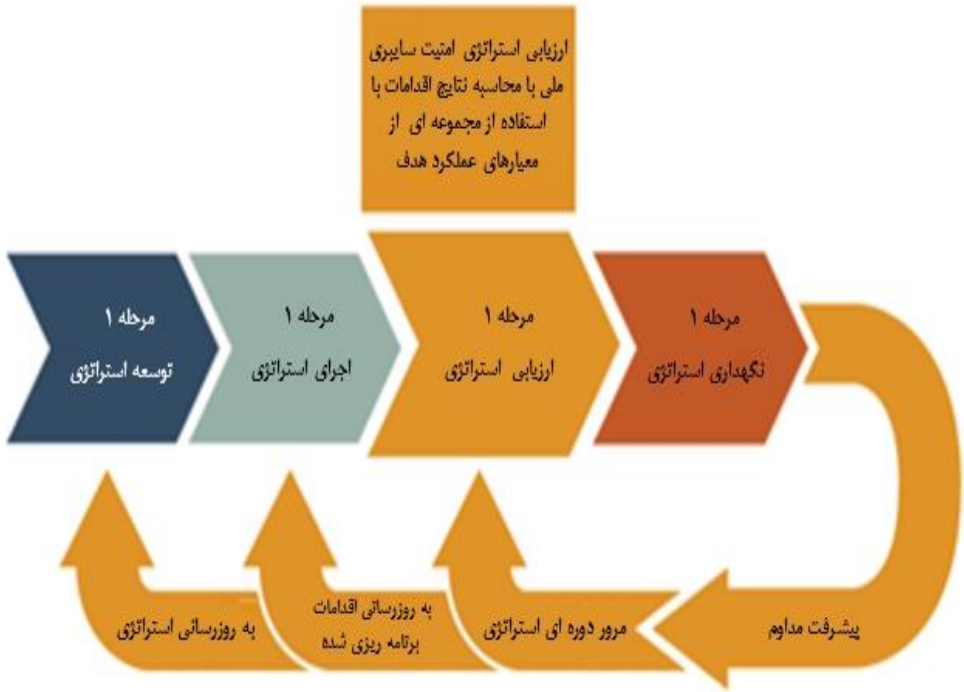
راهنمای توسعه و اجرای راهبردهای امنیت فضای سایبر ملی

آژانس امنیت اطلاعات و شبکه اروپا، در راستای تحقق راهبرد اروپا برای امنیت فضای سایبر، در سال ۲۰۱۲ میلادی اقدام به انتشار راهنمای توسعه و اجرای راهبردهای امنیت فضای سایبر ملی برای کشورهای عضو این اتحادیه نموده است. در این راهنما، مؤلفه‌های کلیدی دست‌یابی و تحقق یک راهبرد امنیت فضای سایبر در سطح ملی کشورهای عضو، در دو محور اصلی، توسعه و اجرای راهبرد امنیت فضای سایبر ملی[1] و ارزیابی و تنظیم نمودن راهبرد امنیت فضای سایبر ملی ارائه شده است (Falessi, Gavrila, Klejnstrup, & Moulinos, 2012) و در آن، برای هر یک از اقدامات، ضمن تشریح جزئیات و نحوه‌ی انجام، نمونه‌هایی که در متن راهبرد امنیت فضای سایبر ملی کشورهای عضو این اتحادیه وجود دارد نیز ارائه شده است. در جمع‌بندی ارائه‌شده در انتهای این راهنما، انجام مجموعه‌ای از ۲۰ اقدام یکپارچه‌ی فوق، به سیاست‌گذاران کشورها پیشنهاد شده است.

چارچوب ارزیابی برای راهبردهای امنیت فضای سایبر ملی

آژانس امنیت اطلاعات و شبکه اروپا[2]، پس از آنکه در سال ۲۰۱۲ میلادی اقدام به انتشار «راهنمای توسعه و اجرای راهبردهای امنیت فضای سایبر ملی» (Falessi et al., 2012, p. 22) نمود، در سال ۲۰۱٤ میلادی، اقدام به انتشار «چارچوب ارزیابی برای راهبردهای امنیت فضای سایبر ملی» کرد. این راهنما، جایگاه ارزیابی در چرخه‌ی حیات راهبرد امنیت فضای سایبر ملی را مطابق شکل ۳ پس از مراحل طراحی و اجرای راهبرد، در مرحله‌ی سوم این چرخه، یعنی فاز ارزیابی راهبرد معرفی نموده است.

1. National Cyberspace Security Strategy (NCSS).
2. ENISA.



شکل ۳: چرخه‌ی حیات یک راهبرد امنیت فضای سایبر ملی

همچنین ارزیابی راهبرد امنیت فضای سایبر ملی در این راهنما، از طریق ارزیابی مؤلفه‌های ذیل، توسط مجموعاً ۸۷ نشانگر، پیشنهاد شده است (ارزیابی اهداف[1] در قالب ۱۹ نشانگر، ارزیابی اهداف ویژه[2] (مناطق تمرکز فعالیت‌ها[3]) در قالب نُه نشانگر، ارزیابی ورودی‌ها در قالب ده نشانگر، ارزیابی فعالیت‌ها[4]، ارزیابی خروجی‌های فعالیت‌ها در قالب ۱۳ نشانگر، ارزیابی نتایج[5] (نتایج کوتاه‌مدت و میان‌مدت) و پیامدها[6] (نتایج بلندمدت) در قالب ۲۷ نشانگر، ارزیابی فرایند ارزیابی[7] در قالب نُه نشانگر).

1. Objectives.
2. Specific objectives.
3. Focal areas of actions.
4. Activities.
5. Outcomes.
6. Impacts.
7. Evaluation Process.

سازمان پیمان آتلانتیک شمالی (ناتو)

در پی تهاجم سایبری گسترده‌ای که در سال ۲۰۰۷ میلادی بر ضد کشور استونی انجام گرفت و برخی از آن با عنوان جنگ سایبری یاد می‌کنند، سازمان پیمان آتلانتیک شمالی[1] در سال ۲۰۰۸ میلادی، با هدف بهبود توانمند ناتو در عملیات دفاع سایبری و کمک به اعضا در مقابل جنگ سایبری، اقدام به تأسیس مرکز مشارکتی نخبگان دفاع سایبری ناتو[2] نمود که محل استقرار آن در شهر تالین[3]، پایتخت کشور استونی است. ازجمله اقدامات انجام‌شده توسط این مرکز، انتشار کتب و راهنماهای متعدد در زمینه‌های امنیت و دفاع سایبری برای استفاده اعضا است. کتاب راهنمای چارچوب امنیت فضای سایبر ملی، در سال ۲۰۱۲ میلادی توسط این مرکز منتشر شد (Schmitt, 2013, p. 46) و سه بُعد، دولتی، ملی و بین‌المللی را برای امنیت شبکه ملی سایبری در نظر گرفت که از پنج منظر یا دیدگاه مجزا، قابل بررسی است:

ـ دیدگاه اوّل: فضای سایبر به‌عنوان محیط عملیات نظامی

ـ دیدگاه دوّم: فضای سایبر به‌عنوان محیط عملیات مجرمانه (جرم سایبری)

ـ دیدگاه سوّم: فضای سایبر به‌عنوان محیط جاسوسی و ضد جاسوسی

ـ دیدگاه چهارم: فضای سایبر به‌عنوان زیرساخت حیاتی و سرمایه ملی

ـ دیدگاه پنجم: فضای سایبر به‌عنوان محیط حکمرانی و دیپلماسی

در این راهنما، پنج معمای دشوار[4] نیز برای شبکه ملی سایبری عنوان شده است:

ـ معمّای اوّل: انگیزش (تحریک) اقتصاد، در مقابل بهبود امنیت ملی

ـ معمّای دوّم: مدرن‌سازی زیرساخت در مقابل محافظت از زیرساخت

ـ معمّای سوّم: بخش خصوصی در مقابل بخش عمومی

ـ معمّای چهارم: محافظت از داده[5] در مقابل به اشتراک‌گذاری اطلاعات[6]

ـ معمّای پنجم: آزادی بیان[7] در مقابل پایداری سیاسی

1. NATO.
2. CCD-COE.
3. Tallinn.
4. Dilemma.
5. Data Protaction.
6. Information Sharing.
7. Freedom of Expression.

اتحادیه بین‌المللی مخابرات

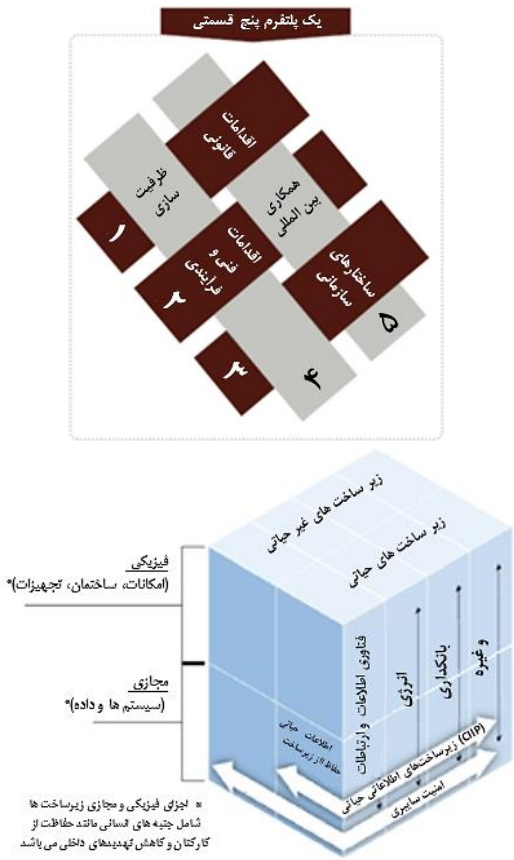
اتحادیه بین‌المللی مخابرات، اولین نسخه از راهنمای راهبرد امنیت سایبر ملی را در سال ۲۰۰۸ میلادی و نسخه‌ی اصلاح‌شده‌ی این راهنما را در سال ۲۰۱۱ میلادی منتشر نمود (ITU, 2011). راهنمای راهبرد امنیت سایبر ملی، تمامی اِلمان‌های تشکیل‌دهنده‌ی یک برنامه‌ی امنیت فضای سایبر ملی را به همراه سازوکار ارزیابی و تحلیل وضعیت امنیت فضای سایبر ملی ارائه نموده است و از این طریق، امکان طراحی، اجرا، سنجش، ارزیابی و اعلام وضعیت امنیت فضای سایبر ملی برای اعضای اتحادیه بین‌المللی مخابرات را فراهم نموده است. راهنمای راهبرد امنیت سایبر ملی، ده اِلمانِ یک برنامه امنیت فضای سایبر ملی را مطابق جدول ۱ اعلام نموده است.

جدول ۱: المان‌های یک برنامه امنیت فضای سایبر ملی

ردیف	عنوان	ردیف	عنوان
۱	مرجع عالی دولتی پاسخ‌گویی	۲	هماهنگ‌کننده‌ی ملی
۳	نقطه کانونی ملی	٤	معیارهای قانونی (قوانین و مقررات)
٥	چارچوب (نیازها و الزامات)	٦	تیم پاسخ به حوادث سایبری (CERT ملی)
۷	آگاهی‌رسانی و آموزش امنیت فضای سایبر ملی	۸	مشارکت بخش خصوصی-عمومی
۹	برنامه مهارت‌ها و آموزش امنیت فضای سایبر ملی	۱۰	همکاری‌های بین‌المللی

بر اساس این راهنما، تعیین و اختیار دهی به متولیان یا مراجع پاسخ‌گویی، هماهنگ‌کننده، نقطه کانونی و پاسخ به حوادث سایبری بخش قابل توجهی از یک برنامه امنیت فضای سایبر ملی را تشکیل می‌دهد. اِلمان بعدی این برنامه را فعالیت‌های فناورانه ازجمله تدوین و ابلاغ نیازمندی‌ها و الزامات تأمین امنیت فضای سایبر ملی (امن‌سازی) به همراه مقابله با حوادث سایبری (تضمین تداوم امنیت) تشکیل می‌دهند. معیارهای قانونی یا قوانین و مقررات حوزه‌ی امنیت فضای سایبر و همکاری‌های بین‌المللی، دو دسته‌ی بعدی از المان‌ها و نهایتاً ظرفیت‌سازی جهت مشارکت همه‌ی بخش‌های دولتی، عمومی و خصوصی در اجرای برنامه و توانمندسازی عموم مخاطبین، شامل آگاهی‌رسانی و آموزش مهارتی و تخصصی نیز آخرین دسته از المان‌های این برنامه را تشکیل می‌دهند. راهنمای

راهبرد امنیت سایبر ملی، ارکان پنج‌گانه یک برنامه امنیت فضای سایبر ملی (معیارهای قانونی، معیارهای فنی و فرایندی، ساختارهای سازمانی، ظرفیت‌سازی و همکاری‌های) و بافتار امنیت فضای سایبر جهانی پیشنهاد نموده است (**Error! Reference source not found.**).

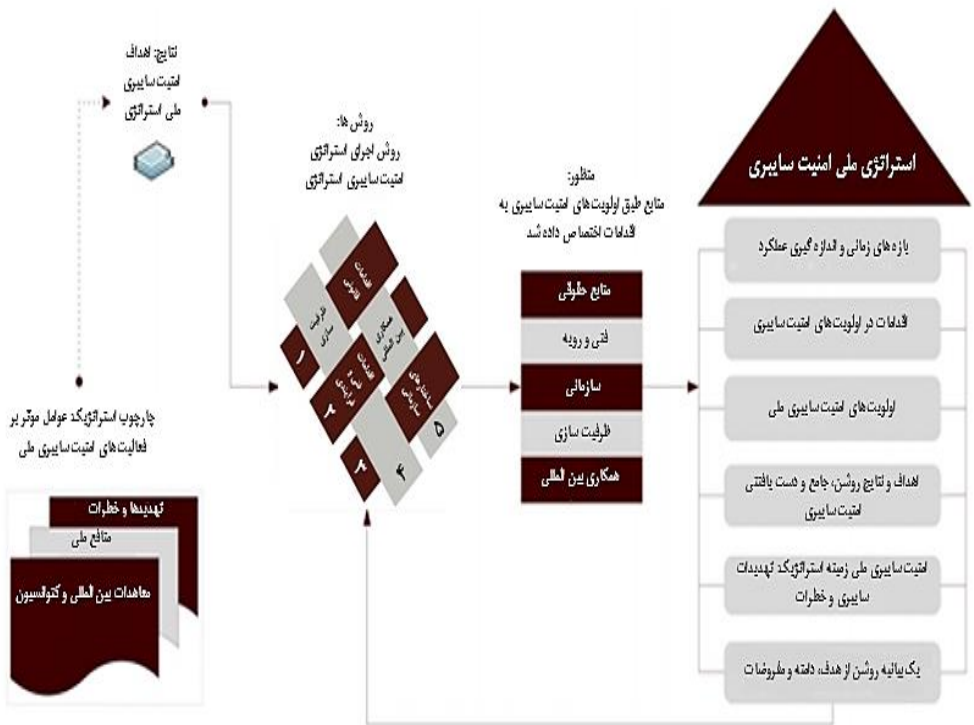


شکل ٤: ارکان یک برنامه امنیت فضای سایبر ملی

بافتار امنیت فضای سایبر ملی

راهنمای فوق، مدل پیشنهادی راهبرد امنیت فضای سایبر ملی (که تأمین‌کننده‌ی دیدگاه کُل‌نگرانه در قلمرو امنیت اطلاعات) را نیز ارائه نموده است و در آن، پنج رکن پیش‌بینی شده که ذیل آن‌ها، حاکمیت هر کشور می‌تواند راهبردهای مورد نظر خود را اتخاذ نموده و

بر آن اساس، فعالیت‌های راهبردی مورد نظر را شناسایی و تعیین نماید. بـرای ایـن منظـور، حاکمیت تعیین می‌کند که منابع خود را در هر یک از ارکان، چگونه استفاده کند تا به نتـایج مطلوب مورد نظر خود، دست یابـد. همچنـین حاکمیـت تعیـین مـی‌کنـد کـه هـر یـک از ذی‌نفعان، از چه منابعی استفاده نموده و انجام کدام مسئولیت را بر عهده داشته باشند. یـک اقدام دیگر حاکمیت که از اهمیت ویژه‌ای برخوردار است، تعیـین نتـایج مطلـوب و میـزان بهبود کارایی مورد انتظار از هر اقدام است (۰).



شکل ۵: مدل راهبرد امنیت فضای سایبر ملی

۲. روش‌شناسی تحقیق

پژوهش توسعه‌ای و کاربردی حاضر، به روش کیفی و مبتنی بر خبرگی انجام می‌شود و از یـک‌سـو، مبـانی و ادبیـات مـرتبط بـا موضـوع پـژوهش و از سـوی دیگـر، مـدل‌هـا و استانداردهای به‌کارگیری شده در جهان را جمـع‌آوری و مـورد مطالعـه، بررسـی و تحلیـل

محتوا قرار می‌دهد و درنهایت مدل مفهومی مناسب را برای تحلیل امنیت در فضای سایبر ملی کشورها ارائه می‌کند. روش تحقیق مورد استفاده در این پژوهش، ترکیبی از روش‌های داده‌کاوی، مطالعات میدانی و تحلیل مبتنی بر خبرگی است. اطلاعات این پژوهش، از طریق جستجوی اینترنتی، مطالعات کتابخانه‌ای و بهره‌گیری از نظرات خبرگان انجام گردآوری می‌شود:

ـ اسناد رسمی منتشرشده توسط نهادهای متولی نظام امنیت سایبر کشورها یا اتحادیه‌های منطقه‌ای و بین‌المللی.

ـ استانداردها، توصیه‌نامه‌ها یا راهنماهای منتشرشده توسط مؤسسات استاندارد گذاری ملی و مجامع استاندارد گذاری بین‌المللی.

ـ کتب و مقالات علمی منتشرشده توسط مراجع معتبر.

با توجه به ماهیت و محتوای مستندات پژوهش و اهمیت بالای تمام موارد مطرح‌شده در آن‌ها، لازم است که حداکثر دقت و ظرافت در نظر گرفته شود؛ بنابراین، از روش کیفی و مبتنی بر خبرگی استفاده می‌شود. تحقیقات فراوانی وجود دارد که فاقد جنبه آماری بوده و عمدتاً متکی به اسناد و مدارک و شهود و ادراک و تحلیل عقلانی است و چون تحلیل داده‌های کیفی را نمی‌توان با روش کمّی و آماری انجام داد، باید معیار و مبنای دیگری غیر از روش‌های آماری برای تجزیه‌وتحلیل آن‌ها به کار رود. این مبنا و معیار در تجزیه‌وتحلیل‌های کیفی مشخصاً عقل، منطق، تفکر و استدلال است؛ یعنی محقق با استفاده از عقل و منطق و غور و اندیشه باید اسناد، مدارک و اطلاعات را مورد بررسی و تجزیه‌وتحلیل قرار دهد. تحقیق کیفی اگرچه در مقایسه با تحقیق کمی وقت‌گیرتر است، ولی بعضاً راهی بهتر و مفیدتر و دارای مزیت‌های زیر است:

ـ با تحقیق کیفی، می‌توان پیچیدگی موضوعات اجتماعی، اطلاعاتی و امنیتی را شناسایی و تشریح کرد.

ـ در جایی که تحقیق تجربی نتواند مفید واقع شود می‌توان از تحقیق کیفی استفاده کرد.

ـ تحقیق کیفی روشی است که در آن به‌جای اینکه پاسخی دقیق به پرسشی نادرست داده شود، پاسخی نسبتاً مناسب به پرسشی دقیق داده می‌شود.

به‌منظور بررسی قوانین و مقررات، اسناد راهبردی و سیاست‌های کلان مرتبط با فضای سایبر و امنیت این فضا، ابتدا طی یک مطالعه کتابخانه‌ای، فهرستی از اسناد مرتبط تهیه شد. در ادامه، به‌منظور تشخیص میزان ارتباط و اهمیت این اسناد در موضوع مورد مطالعه، این قوانین مورد بررسی و پایش اولیه قرار گرفت و از مجموع اسناد پیداشده، موارد اصلی و مهم‌تر که حاوی مطالب مهم و ارزشمند در خصوص فضای سایبری و امنیت آن بودند با توجه به معیارهای زیر جدا گردیده و سپس مفاهیم کلیدی متناظر تکرار و تأکید لحاظ شده در مورد آن‌ها جداسازی شده و در نهایت نتایج حاصل مورد تجزیه‌وتحلیل قرار می‌گیرند:

- حوزه تأثیرگذاری سند، کشوری و کلان‌نگر باشد.
- حوزه تعریف سند، اختصاصی نباشد.
- حاوی جدیدترین و به‌روزترین سند در یک موضوع باشد.
- حاوی موارد مرتبط با امنیت یا دفاع سایبری باشد.

۳. تجزیه‌وتحلیل یافته‌ها

به‌منظور دست‌یابی به مدل مفهومی مناسب برای تحلیل امنیت فضای سایبر ملی، لازم است ابتدا معیارهایی را برای مقایسه‌ی مدل‌ها (به دلیل محدودیت حجم مقاله، برخی از مدل‌های مطالعه‌شده به‌صورت مختصر در بخش مبانی نظری آورده شده است) با یکدیگر انتخاب نمود و در ادامه، بر اساس این معیارها، اقدام به مقایسه و دسته‌بندی (طبقه‌بندی) مدل‌های مورد بررسی می‌نماییم. با بررسی مستندات پروژه، معیارهای موضوع مدل، حوزه‌ی قلمرو یا کاربرد مدل، ارتباط مدل با چرخه‌ی حیات، اعتبار مدل، کفایت جزئیات مدل، رویکرد مدل و بلوغ مدل مورد توجه قرار گرفتند و طبق ۰ مقایسه لازم بر روی مدل‌های مطالعه‌شده انجام شد.

جدول۲: مقایسه‌ی مدل‌های معماری و تحلیل امنیت موردبررسی

ردیف	عنوان مدل	منتشرکننده	اعتبار (مرجع)	زمان انتشار	موضوع	قلمرو (کاربرد)	ارتباط با چرخه حیات	کفایت جزئیات	رویکرد	بلوغ	نکته کلیدی
۱	امنیت سایبر ملی	ITU	بین‌المللی	۲۰۱۱	امنیت	فضای سایبر ملی	دارد	٤	کمّی	بالغ	قابل بهره‌برداری
۲	راهنمای چارچوب امنیت فضای سایبر ملی	CCD-COE	منطقه‌ای	۲۰۱۲	امنیت		دارد	۲	کیفی	بالغ	کلیات مؤلفه/شاخص/نشانگر
۳	راهنمای توسعه و اجرای راهبردهای امنیت فضای سایبر ملی	ENISA	منطقه‌ای	۲۰۱۲	امنیت		دارد	۲	کمّی/کیفی	بالغ	ترکیب قابل بهره‌برداری
٤	چارچوب ارزیابی برای راهبردهای امنیت فضای سایبر ملی	ENISA	منطقه‌ای	۲۰۱٤	امنیت		دارد	٤	کمّی/کیفی	بالغ	
۵	مدلی برآورد تهدید سایبری	قرارگاه پدافند سایبری	ملی	۱۳۹۳	امنیت		دارد	۵	کمّی	رشد یافته	جزئیات کافی مؤلفه/شاخص/نشانگر
٦	مدلی ارزیابی و تحلیل وضعیت افتا	مرکز مدیریت راهبردی افتا	ملی	۱۳۸۸	امنیت		دارد	۵	کمّی	بالغ	فقط تحلیل ولی با جزئیات کافی
۷	مدلی معماری امنیت TOGAF				معماری سازمانی	فضای سایبر سازمانی	ندارد	۱	کیفی	بالغ	
۸	مدلی معماری امنیت FEAF				معماری سازمانی		ندارد	۱	کیفی	بالغ	
۹	مدلی معماری امنیت Zachman				معماری سازمانی		ندارد	۱	کیفی	بالغ	

ردیف	عنوان مدل	منتشرکننده	اعتبار (مرجع)	زمان انتشار	موضوع	قلمرو (کاربرد)	ارتباط با چرخه حیات	کفایت جزئیات	رویکرد	بلوغ	نکته کلیدی
۱۰	مدلی معماری امنیت Gartner				معماری سازمانی		ندارد	۱	کیفی	بالغ	
۱۱	مدلی معماری امنیت SABSA				معماری سازمانی		ندارد	۳	کیفی	بالغ	ساختار ماتریسی
۱۲	سیستم مدیریت امنیت اطلاعات (۲۷۰۰۱ و ۲۷۰۰۲)	ISO	بین‌المللی	۲۰۱۳	امنیت		دارد	۵	کمّی	بالغ	ترکیب قابل بهره‌برداری
۱۳	سنجش مدیریت امنیت اطلاعات (۲۷۰۰٤)	ISO	بین‌المللی	۲۰۰۹	امنیت		دارد	۳	کمّی	بالغ	
۱٤	مدیریت مخاطرات امنیت اطلاعات (۲۷۰۰۵)	ISO	بین‌المللی	۲۰۱۱	امنیت		ندارد	۱	کمّی	بالغ	
۱۵	راهنمای مدیریت امنیت اطلاعات برای نهادهای مخابراتی	ITU	بین‌المللی	۲۰۰۸	امنیت		دارد	۵	کمّی	بالغ	
۱٦	مدلی معماری امنیت برای ارتباطات انتها-به-انتها	ITU	بین‌المللی	۲۰۰۳	امنیت	شبکه ارتباطی	ندارد	۳	کیفی	بالغ	نیازمندی امنیتی و ساختار ماتریسی
۱۷	چارچوب بهبود امنیت سایبری زیرساخت‌های حیاتی	NIST	ملی	۲۰۱٤	امنیت		دارد	٤	کمّی	بالغ	قابل بهره‌برداری

ردیف	عنوان مدل	منتشرکننده	اعتبار (مرجع)	زمان انتشار	موضوع	قلمرو (کاربرد)	ارتباط با چرخه حیات	کفایت جزئیات	رویکرد	بلوغ	نکته کلیدی
۱۸	مهندسی امنیت سامانه – مدل تعالی قابلیت	ISO	بین‌المللی	۲۰۰۲	امنیت	سامانه اطلاعاتی	دارد	۳	کیفی	بالغ	
۱۹	مهندسی امنیت سامانه‌ها – رویکرد یکپارچه‌شده برای تولید سامانه‌های مطمئن انعطاف‌پذیر	NIST	ملی	۲۰۱٤	امنیت		دارد	۳	کیفی	بالغ	تلفیق چرخه حیات، نیازهای امنیتی و دیدگاه عوامل درگیر

جمع‌بندی نتایج مقایسه نشان داد که:

۱) هیچ‌یک از مدل‌ها، قابلیت بهره‌برداری مستقیم یا غیرمستقیم به‌عنوان مدل تحلیل امنیت فضای سایبر ملی ندارند ولی می‌توان از ترکیب آن‌ها استفاده نمود:

ـ راهنمای راهبرد امنیت سایبر ملی

ـ ترکیب «راهنمای توسعه و اجرای راهبردهای امنیت فضای سایبر ملی» و «چارچوب ارزیابی برای راهبردهای امنیت فضای سایبر ملی»

ـ سیستم مدیریت امنیت اطلاعات[1] مشتمل بر استانداردهای ISO/IEC 27001، ISO/IEC 27002، ISO/IEC 27004 و ISO/IEC 27005 و توصیه‌نامه ITU-T X.1051 وابسته به آن

ـ مدلی ارزیابی و تحلیل وضعیت افتا (جزئیات)

ـ مدلی برآورد تهدید سایبری (جزئیات)

ـ راهنمای چارچوب امنیت فضای سایبر ملی (کلیات)

1 ISMS)

۲) در خصوص نیازمندی‌های امنیتی و طبقه‌بندی مبتنی بر ساختار ماتریسی، استفاده از مدل‌های زیر نیز مفید است:

- مدلی معماری امنیت برای ارتباطات انتها-به-انتها
- مدلی معماری امنیت SABSA
- مدلی معماری امنیت گارتنر

۳) نکته‌ی کلیدی تلفیق چرخه حیات، نیازمندی‌های امنیتی و دیدگاه عوامل درگیر، از مرجع زیر، در ساختار معماری، مورد توجه جدی قرار گیرد:

- استاندارد مهندسی امنیت سامانه‌ها-رویکرد یکپارچه‌شده برای تولید سامانه‌های مطمئن انعطاف‌پذیر

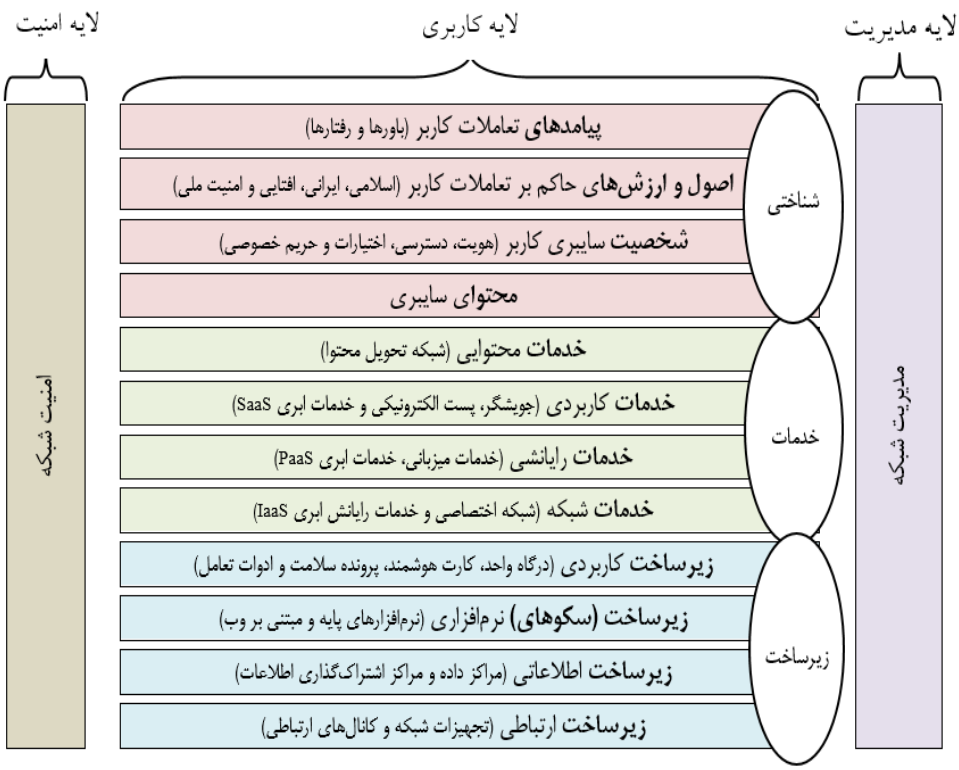
طبق جمع‌بندی، ذی‌نفعان همچون حاکمیت، متولیان زیرساخت‌های حیاتی، دستگاه‌های دولتی و مؤسسات خصوصی و عمومی، کسب‌وکارها (صنعت، خدمت، تجارت)، عموم شهروندان، حوزه‌ی انتظامی-قضایی و حوزه‌ی دفاعی-امنیتی، در فضای سایبر ملی شناسایی شد که اهداف امنیتی کارکردی زیر باید برای آن‌ها تأمین شود:

۱) مأمن ارتباطی برای کاربران عمده
۲) ایجاد اعتماد برای توسعه
۳) ایجاد اعتبار برای حوزه‌ی کسب‌وکار
٤) اطمینان و آرامش برای جامعه
۵) مصونیت برای زیرساخت‌های حیاتی
٦) تشخیص جرائم سایبری (قضائی-پلیسی)
۷) اشراف برای امنیت ملی
۸) بازدارندگی برای دفاع ملی
۹) اقتدار ملی برای حاکمیت

بر این اساس، کارکردهای نه‌گانه‌ی فضای سایبر ملی نیز استخراج گردید:

۱) بستر ارتباطات و فناوری اطلاعات
۲) محرّک توسعه کشور
۳) فضای کسب‌وکار
٤) زیست‌بوم سایبری
۵) زیرساخت حیاتی و سرمایه ملی
٦) محیط عملیات مجرمانه
۷) مؤلفه‌ی امنیت ملی
۸) محیط عملیات نظامی
۹) قلمرو حاکمیتی

فضای سایبر ملی را طبق مدل توسعه‌یافته در استاندارد ITU-T X.805، می‌توان شبکه‌ای با سه لایه‌ی مدیریت، کنترل و کاربر انتهایی و سه سطح زیرساخت، خدمات و کاربرد در نظر گرفت که به سه سطح کلان زیرساخت (زیرساخت ارتباطی، زیرساخت اطلاعاتی، زیرساخت نرم‌افزاری و زیرساخت کاربردی)، خدمات (خدمات شبکه، خدمات رایانشی، خدمات کاربردی و خدمات محتوایی) و شناختی (محتوا، شخصیت سایبری کاربر، اصول و ارزش‌های حاکم بر تعاملات کاربر و پیامدهای تعاملات کاربر) تفکیک شده است (INTERNATIONAL TELECOMMUNICATION UNION, 2004, p. 37). همچنین لایه‌های شبکه با عناوین مدیریت، امنیت و کاربری نام نهاده شده‌اند. لایه‌های مدیریت و امنیت به‌موازات لایه‌ی کاربری ترسیم شده و به ازای هر سطح از این لایه، این دولایه نیز باید سطح متناظری داشته باشند. علاوه بر این، لایه‌های مدیریت و امنیت خودشان باید یکدیگر را نیز پوشش دهند یعنی مدیریت امنیت و امنیت مدیریت نیز موضوعیت خواهند داشت (۰).



شکل ٦: مدل توسعه‌یافته در استاندارد ITU-T X.805 بر اساس لایه‌ای افقی-عمودی

به‌منظور پیش‌بینی کنترل‌های همه‌جانبه، باید چرخه‌ی امنیت، به‌صورت کامل توسط مأموریت‌های عملیاتی امنیت سایبری، پوشش داده شود. این چرخه، حاوی مأموریت‌هایی با رویکردهای پیشگیرانه، پیش‌بینانه، تشخیص‌گرانه، واکنش‌گرایانه، پس‌نگرانه و مأموریت‌های عملیاتی امنیت سایبری، شامل موارد زیر است:

۱) رصد، پایش و برآورد تهدید سایبری

۲) استخراج و رفع آسیب‌پذیری سایبری

۳) تحلیل، تشخیص و مقابله با حملات سایبری

٤) رسیدگی (ارزیابی، بازیابی، تحلیل و ریشه‌یابی) حوادث سایبری

۵) امن‌سازی (تأمین محرمانگی، صحت، دسترس‌پذیری و...) و ارتقای آمادگی امنیت سایبری

٦) بازدارندگی و تولید قدرت پاسخ به تهدید سایبری

این مأموریت‌ها در قالب مدل تعالی (چرخه‌ی حیات) امنیت سایبری، شامل مراحل ظهور، رشد، بلوغ و فعالیت، رشد یافته و به تکامل می‌رسند. در این راستا نیز، تهدیدهای سایبری عمدی همانند دولت‌ها یا نهادهای بین‌المللی، ارتش سایبری کشورها، سرویس امنیتی کشورها، تروریست‌های سازمان‌یافته، بازیگران چندملیتی، تبهکاران سازمان‌یافته، هکرها (خودی، سیاسی و ...) و غیرعمدی همانند خرابی و خطای غیر عمد و عوامل طبیعی بر ضد فضای سایبر ملی نیز باید مورد توجه قرار گیرند و بر این اساس، اصول زیر باید به‌منظور تحقق امنیت پایدار در فضای سایبر ملی رعایت شود:

۱) یکپارچگی امنیت با چرخه‌ی حیات شبکه

۲) فراگیری (همه‌جانبه بودن) کنترل‌های امنیتی

۳) تحقق گام‌به‌گام امنیت، در مدل تعالی

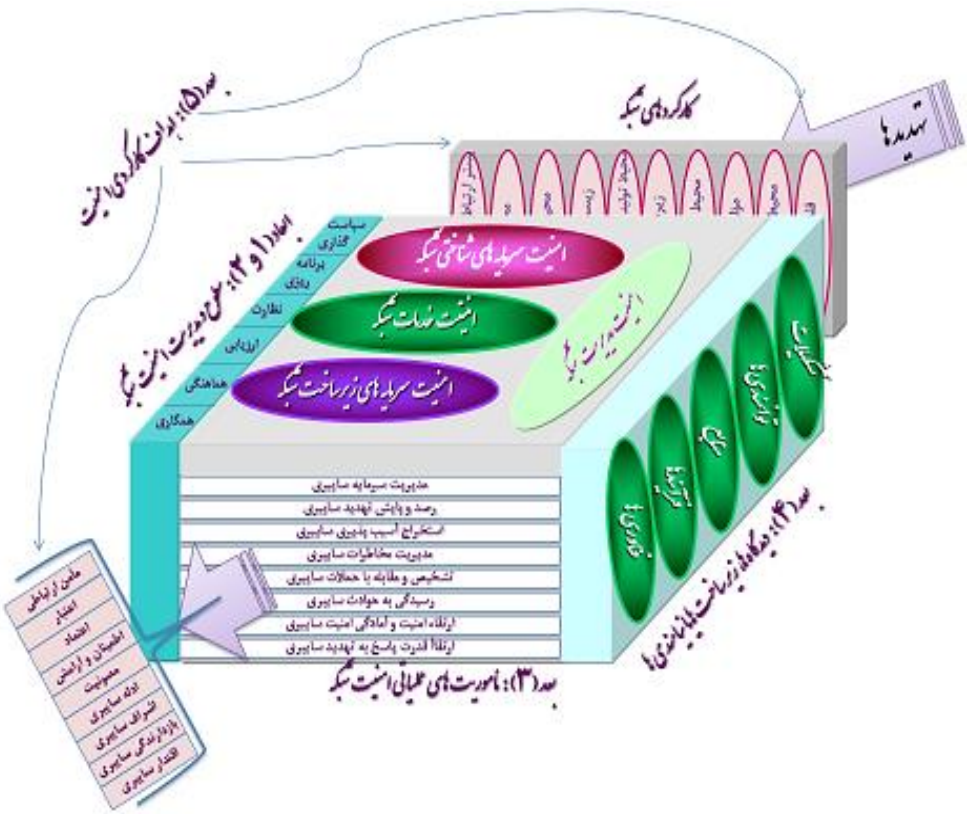
٤) مشارکت جمعی در اجرای امنیت

۵) نظام‌مندی در اجرای امنیت

٦) تمرکز در مدیریت امنیت

ساختار احصاشده برای مدل مفهومی تحلیل امنیت در فضای سایبر ملی کشورها

با توجه به نتایج، ساختار کلانی مشتمل بر پنج بُعد را می‌توان برای تحلیل امنیت در فضای سایبر ملی کشورها مورد توجه قرار داد (۰):



شکل ۷: ساختار کلان احصاشده برای تحلیل امنیت در فضای سایبر ملی کشورها (ترسیم سه‌بعدی)

بُعد اوّل: سطوح امنیت

با توجه به اینکه تمامی اجزا یا موجودیت‌های حاضر در این شبکه، نیازمند تأمین سازوکارهای امنیتی می‌باشند، امنیت فضای سایبر ملی نیز در قالب سه سطح با عناوین زیر، قابل طبقه‌بندی است (۰):

جدول ۳: مؤلفه و زیر مؤلفه‌های سطوح امنیت

مؤلفه	زیر مؤلفه
امنیت مؤلفه‌های سطح زیرساخت	امنیت زیرساخت ارتباطی امنیت زیرساخت اطلاعاتی امنیت زیرساخت (سکوهای) نرم‌افزاری امنیت زیرساخت کاربردی
امنیت مؤلفه‌های سطح خدمت	امنیت خدمات شبکه امنیت خدمات رایانشی امنیت خدمات کاربردی امنیت خدمات محتوایی
امنیت مؤلفه‌های سطح شناختی	امنیت محتوا امنیت شخصیت سایبری امنیت (صیانت از) اصول و ارزش‌ها امنیت پیامدهای تعاملات کاربر

بُعد دوّم: مدیریت امنیت

با توجه به اینکه تمامی اجزا یا موجودیت‌های حاضر در این شبکه، نیازمند تأمین سازوکارهای امنیتی می‌باشند، امنیت فضای سایبر ملی در قالب سه لایه با عناوین زیر، قابل طبقه‌بندی است:

۱) لایه امنیت کاربری: متشکل از سه سطح کلان امنیت زیرساخت، امنیت خدمات و امنیت سرمایه‌های شناختی است که مجموعاً از ۱۲ سطح، تشکیل می‌شوند.

۲) لایه امنیت مدیریت: ساختار لایه مدیریت را می‌توان متناسب با لایه‌بندی سرمایه‌های شبکه انجام داد. در ضمن یکی از اصول تحقق امنیت پایدار، اجرای توزیع‌شده ولی نظام‌مند امنیت است.

۳) لایه مدیریت (حاکمیت) امنیت: از آنجا که یکی از اصول حاکم مدیریت متمرکز است، پس مدیریت امنیت به اپراتورها واگذار نشده و توسط حاکمیت انجام می‌گیرد. بر این اساس، شکست لایه مدیریت امنیت، به‌صورت زیر انجام می‌شود که قابلیت اجرا به‌صورت متمرکز را داشته باشد:

ـ سیاست‌گذاری امنیت
ـ برنامه‌ریزی امنیت
ـ نظارت بر اجرای برنامه‌های امنیت
ـ ارزیابی و تعالی مستمر
ـ هماهنگی امنیت سایبری
ـ همکاری امنیت سایبری

بُعد سوّم: مأموریت‌های عملیاتی امنیت شبکه

مأموریت‌های عملیاتی امنیت شبکه، بر اساس چرخه‌ی امنیت، عبارت است از:
۱) رسیدگی به (طبقه‌بندی و ارزش‌گذاری) سرمایه‌های سایبری شبکه
۲) مواجهه با (رصد، پایش و برآورد) تهدید سایبری شبکه
۳) مواجهه با (استخراج و رفع) آسیب‌پذیری سایبری شبکه
٤) مواجهه با (تحلیل، ارزیابی، تخمین و مقابله با) مخاطرات سایبری شبکه
۵) مواجهه با (تحلیل، تشخیص و مقابله با) حملات سایبری
٦) رسیدگی به (ارزیابی، بازیابی، تحلیل و ریشه‌یابی) حوادث سایبری
۷) ارتقای امنیت و آمادگی امنیت سایبری
۸) ارتقای توانایی (قدرت) پاسخ به تهدید سایبری

بُعد چهارم: دیدگاه‌ها، زیرساخت‌ها یا نیازمندی‌های تحقق امنیت شبکه

دیدگاه‌های تحقق امنیت شبکه، بر اساس مدل‌های سازمانی، عبارت است از:
دیدگاه (۱): فناوری‌های (دانش، فناوری و محصول) امنیت شبکه
دیدگاه (۲): فرایندهای اجرایی (قوانین، مقررات، دستورالعمل‌ها و آئین‌نامه‌ها) امنیت شبکه
دیدگاه (۳): منابع (انسانی و مالی) عملیاتی کردن امنیت شبکه
دیدگاه (٤): توانمندی (آگاهی، مهارت و تخصص) منابع انسانی
دیدگاه (۵): تشکیلات (نهادهای) متولی، مسئولیت و پاسخ‌گویی آن‌ها

بُعد پنجم: اهداف کارکردی امنیت شبکه

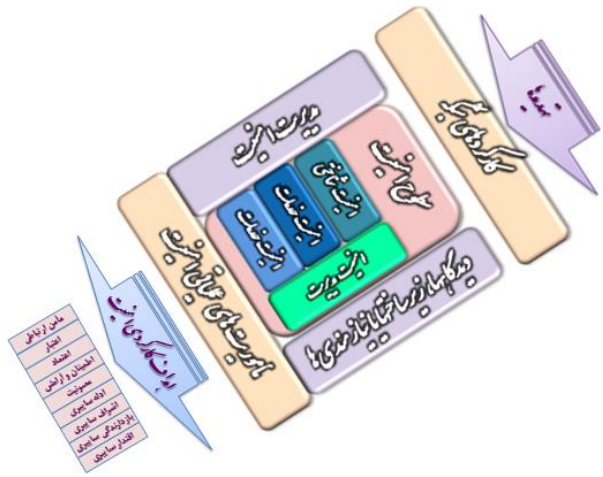
تهدیدهای امنیتی برای هر یک از کارکردهای فضای سایبر ملی متفاوت بوده و بر همین اساس، اهداف امنیتی که باید محقق شوند نیز متناسب با کارکرد شبکه تغییر خواهد کرد. به‌منظور تحقق هر یک از اهداف امنیتی، باید ابتدا اهداف امنیتی مقدم بر آن، محقق شده باشند. به عبارت دیگر، مادامی که بستر ارتباطی امن محقق نشده باشد، نمی‌توان در آن بستر، کسب‌وکار سایبری بنا نهاده و برای آن اعتبار تأمین نمود (۰).

جدول ٤: اهداف امنیتی با کارکرد شبکه

کارکرد شبکه	تهدیدهای سایبری											اهداف کارکردی امنیت شبکه
	دولت‌ها یا نهادهای بین‌المللی	ارتش سایبری	سرویس امنیتی	تروریست سازمان‌یافته	بازیگران چندملیتی	تبهکاران سازمان‌یافته	هکرهای سیاسی	هکرها	هکرهای خودی	خرابی و خطای غیرعمدی	عوامل محیطی	
بستر ارتباطات و فناوری اطلاعات								✓	✓	✓	✓	مأمن ارتباطات و فناوری اطلاعات
فضای کسب‌وکار								✓	✓	✓	✓	اعتبار برای کسب‌وکار سایبری
محرک توسعه‌ی کشور								✓	✓	✓	✓	اعتماد برای سرمایه‌گذاری
زیست‌بوم سایبری								✓	✓	✓	✓	اطمینان و آرامش عمومی
محیط تولید و تبادل محتوای سالم سایبری					✓	✓	✓	✓				صیانت فرهنگی-اجتماعی محتوای سایبری (پالایش محتوای سایبری)
زیرساخت حیاتی و سرمایه ملی					✓	✓	✓	✓	✓			مصونیت سایبری
محیط عملیات مجرمانه					✓	✓	✓	✓				ادلّه‌ی سایبری تشخیص جرم
مؤلفه‌ی امنیت ملی			✓	✓			✓					اشراف سایبری
محیط عملیات نظامی		✓										بازدارندگی سایبری
قلمرو حاکمیتی	✓											اقتدار سایبری

٤. نتیجه‌گیری

در پژوهش توسعه‌ای و کاربردی حاضر، با هدف ارائه مدل مفهومی مناسب برای تحلیل امنیت در فضای سایبر ملی کشورها به روش کیفی و مبتنی بر خبرگی، مبانی و ادبیات مرتبط با موضوع، مدل‌ها و استانداردهای به‌کارگیری شده در جهان، از طریق جستجوی اینترنتی، مطالعات کتابخانه‌ای جمع‌آوری و مورد مطالعه و بررسی قرار گرفت. به‌منظور تجزیه‌وتحلیل یافته‌ها، معیارهایی (موضوع مدل، حوزه‌ی قلمرو یا کاربرد مدل، ارتباط مدل با چرخه‌ی حیات، اعتبار مدل، کفایت جزئیات مدل، رویکرد مدل و بلوغ مدل) برای مقایسه‌ی مدل‌ها (به دلیل محدودیت حجم مقاله، برخی از مدل‌های مطالعه‌شده به‌صورت مختصر در بخش مبانی نظری آورده شده است) با یکدیگر انتخاب و بر آن اساس، مقایسه و دسته‌بندی (طبقه‌بندی) لازم انجام شد و ساختار قابل توجه، طبق ۰ ترسیم گردید (ترسیم ۳ بعدی ساختار فوق در ۰ قابل مشاهده است).



شکل ۷: ساختار کلان احصاشده برای تحلیل امنیت در فضای سایبر ملی کشورها (ترسیم دوبعدی)

با بررسی دقیق روابط حاکم بر ابعاد ساختار کلان احصاشده برای تحلیل امنیت در فضای سایبر ملی، همپوشانی‌های متعددی در بُعد پنجم و مؤلفه‌های مربوطه مشاهده گردید که با تلفیق و ساماندهی آن‌ها، ابعاد، مؤلفه‌ها و زیر مؤلفه‌های قابل توجه در مدل مفهومی مورد نظر، طبق ۰ احصا گردید.

جدول ۵: ابعاد، مؤلفه‌ها و زیر مؤلفه‌های قابل توجه در مدل مفهومی

ابعاد	مؤلفه‌ها	زیر مؤلفه‌ها
سطوح امنیت	امنیت شناختی	امنیت پیامدهای تعاملات کاربر – امنیت (صیانت از) اصول و ارزش‌ها – امنیت شخصیت سایبری – امنیت محتوای سایبری
	امنیت خدمات	امنیت خدمات محتوایی – امنیت خدمات کاربردی – امنیت خدمات رایانشی – امنیت خدمات شبکه
	امنیت زیرساخت‌ها	امنیت زیرساخت‌های کاربردی – امنیت زیرساخت‌های (سکوهای) نرم‌افزاری– امنیت زیرساخت‌های اطلاعاتی – امنیت زیرساخت‌های ارتباطی
مدیریت امنیت	سیاست‌گذاری و برنامه‌ریزی امنیت	مأمن ارتباطات و فناوری اطلاعات – اعتبار برای کسب‌وکارهای سایبری – اشراف سایبری – اعتماد برای سرمایه‌گذاری‌ها
	نظارت و ارزیابی مستمر امنیت	ادلّه‌هایی سایبری تشخیص جرم – اطمینان و آرامش عمومی – صیانت فرهنگی–اجتماعی محتوای سایبری
	هماهنگی و همکاری در زمینه امنیت	مصونیت سایبری – اقتدار سایبری – بازدارندگی سایبری
مأموریت‌های عملیاتی	رسیدگی	رسیدگی به سرمایه‌های سایبری (طبقه‌بندی و ارزش‌گذاری) – رسیدگی به حوادث سایبری (ارزیابی، بازیابی، تحلیل و ریشه‌یابی)
	مواجهه	مواجهه با تهدیدهای سایبری (رصد، پایش و برآورد) – مواجهه با آسیب‌پذیری‌های سایبری (استخراج و رفع) – مواجهه با مخاطرات سایبری (تحلیل، ارزیابی، تخمین و مقابله) – مواجهه با حملات سایبری (تحلیل، تشخیص و مقابله)
	ارتقا	ارتقای امنیت و آمادگی امنیت سایبری –ارتقای توانایی (قدرت) پاسخ به تهدید سایبری
زیرساخت‌ها و نیازمندی‌ها	فناوری‌های امنیت	دانش – فناوری – محصول
	فرایندهای اجرایی امنیت	قوانین – مقررات – دستورالعمل‌ها – آئین‌نامه‌ها
	منابع عملیاتی کردن امنیت	انسانی – مالی
	توانمندی منابع انسانی	آگاهی – مهارت – تخصص
	تشکیلات (نهادهای متولی، مسئول و پاسخگو)	ساختار سازمانی – روابط سازمانی

طبق ابعاد، مؤلفه‌ها و شاخص‌های احصاشده، مدل مفهومی تحلیل امنیت فضای سایبر ملی طبق • ترسیم و ارائه گردید. طبق مدل مفهومی فوق، تحلیل امنیت فضای سایبر ملی

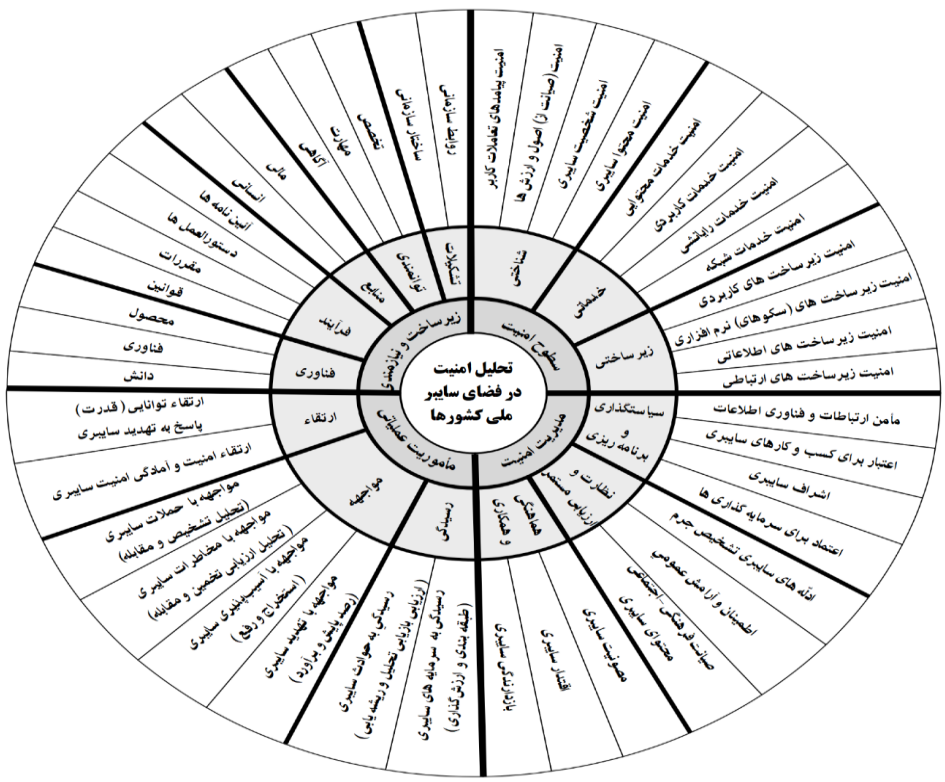
باید از چهار بُعد سطوح امنیت، مدیریت امنیت، مأموریت‌های عملیاتی و زیرساخت‌ها و نیازمندی‌ها مورد توجه قرار گیرد:

ـ بُعد سطوح امنیت: مؤلفه‌های امنیت شناختی، امنیت خدمات و امنیت زیرساخت و زیر مؤلفه‌های آن‌ها مورد توجه است.

ـ بُعد مدیریت امنیت: مؤلفه‌های سیاست‌گذاری و برنامه‌ریزی امنیت، نظارت و ارزیابی مستمر امنیت و هماهنگی و همکاری در زمینه امنیت و زیر مؤلفه‌های آن‌ها مورد توجه است.

ـ بُعد مأموریت‌های عملیاتی: مؤلفه‌های رسیدگی، مواجهه و ارتقا و زیر مؤلفه‌های آن‌ها مورد توجه است

ـ بُعد زیرساخت‌ها و نیازمندی‌ها: مؤلفه‌های فناوری‌های امنیت، فرایندهای اجرایی امنیت، منابع عملیاتی کردن امنیت، توانمندی منابع انسانی و تشکیلات (نهادهای متولی، مسئول و پاسخگو) و زیر مؤلفه‌های آن‌ها مورد توجه است.



شکل ۸: مدل مفهومی تحلیل امنیت در فضای سایبر ملی کشورها

پیشنهاد

طبق نتایج پژوهش، زمینه‌های مطالعاتی زیر بـه منظـور انجـام پـژوهش‌هـایی جـامع‌تـر پیشنهاد می‌گردد:

۱) پژوهش در خصوص سطح امنیتی در فضای سایبر ملی کشورها.

۲) پژوهش به منظور تعیین زیرساخت‌هـای حیـاتی، حسـاس و مهـم در بسـتر فضـای سایبر ملی کشورها.

۳) پژوهش در خصوص مأموریت‌های عملیاتی در بسـتر فضـای سـایبر ملـی کشـورها (حوزه‌های شناختی، خدماتی و زیرساختی).

٤) پژوهش در خصوص شیوه‌های نوین مدیریت امنیت فضای سایبر ملی در کشورها.

۵) پژوهش در خصوص کنترل، نظارت و ارزیابی امنیت سایبری، منطبق بـا نیـاز شـبکه ملی اطلاعات کشور.

فهرست منابع و مآخذ

الف. منابع فارسی

- تقی‌پور، رضا؛ خالقی، محمود و رامک، مهراب (۱۳۹۹)، ۹۸۱۱۰۹-نهایی-الگوی معماری و تحلیل امنیت شبکه ملی سایبری جمهوری اسلامی ایران .docx.دانشگاه عالی دفاع ملی: دانشگاه عالی دفاع ملی.
- حافظ‌نیا، محمدرضا (۱۳۹٤)، جغرافیای سیاسی فضای مجازی. سمت.

ب. منابع لاتین

- Bartholomees, J. Boone (ed.). (2012). U.S. Army War College guide to national security issues Volume 2 (5th ed, Vol. 2). Carlisle, PA: Strategic Studies Institute, U.S. Army War College.
- Commonwealth of australia. (2009). Cyber Security Strategy. australian government.
- Fahrurozi, Muhammad; Tarigan, Soli Agrina; Tanjung, Marah Alam; & Mutijarsa, Kusprasapta. (2020). The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). In 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE) (pp. 86–91). IEEE.
- Falessi, N; Gavrila, R; Klejnstrup, MR; & Moulinos, K. (2012). National cyber security strategies: practical guide on development and execution. European Network and Information Security Agency (ENISA) Publication.
- Federal Ministry of the Interior. (2011). Cyber Security Strategy for Germany. Federal Ministry of the Interior.
- Goverment of Canada. (2010). Canada's cyber security strategy: for a stronger and more prosperous Canada. Canada: Goverment of Canada.
- Great Britain; & Cabinet Office. (2009). Cyber security strategy of the United Kingdom: safety, security and resilience in cyber space. London: Stationery Office.
- Great Britain; & Home Office. (2010). Cyber crime strategy. London: Stationery Office.
- Group, NIST Cloud Computing Security Working; & others. (2013). NIST cloud computing security reference architecture. National Institute of Standards and Technology.
- INTERNATIONAL TELECOMMUNICATION UNION. (2004). ITU-T Recommendation X.805: Security architecture for systems providing end-to-end communications. INTERNATIONAL TELECOMMUNICATION UNION.
- ITU, Frederick Wamala. (2011). ITU NATIONAL CYBERSECURITY STRATEGY GUIDE.
- Klimburg, Alexander; & NATO. (2012). National cyber security framework manual.

- New Zealand Government. (2011). NEW ZEALAND'S CYBER SECURITY STRATEGY. New Zealand Government.
- Rauscher, Karl Frederick; & Yaschenko, Valery. (2011). Russia–US Bilateral on Cyber Security: Critical Terminology Foundations. New York, USA: EastWest Institute.
- Ross, Ron; Oren, Janet; & McEvilley, Michael. (2014). Systems security engineering: An integrated approach to building trustworthy resilient systems. National Institute of Standards and Technology.
- Ross, Ron; & others. (2010). NIST SP 800-37, Revision 1. Guide for Applying the Risk Management Framework to Federal Information Systems.
- Schmitt, Michael N. (ed.). (2013). Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge□; New York: Cambridge University Press.