فصلنامه علمی امنیت ملی
سال یازدهم، شماره چهلم، تابستان ۱۴۰۰
مقاله دوم از صفحات ٦٦-۳۷

مقاله پژوهشی: تعیین شاخص‌های ارزیابی امنیت سایبری به روش مطالعه تطبیقی

20.1001.1.33292538.1400.11.40.2.8

امیرمسعود سعادتمند[۱]، محمدرضا کریمی قهرودی[۲]، حافظ محمدی[۳]، محمد بابک[۴]

تاریخ دریافت: ۱۳۹۹/۰۱/۲۵ **تاریخ پذیرش: ۱۴۰۰/۰۴/۱۳**

چکیده

با توسعه و گسترش فضای سایبر، وجوه مختلف زندگی شهروندان به‌گونه‌ای روشن با این فضا درآمیخته و هرگونه ناامنی و چالش در این فضا به‌طور مستقیم یا غیرمستقیم بر زندگی و رفتار شهروندان تأثیر خواهد گذاشت؛ بنابراین امنیت فضای سایبری یکی از مؤلفه‌های امنیت ملی است که باید به‌طور جدی مورد توجه واقع شده و به‌صورت پیوسته مورد ارزیابی قرار گیرد. ارزیابی مناسب امنیت سایبری باعث شناسایی نقاط قوت و ضعف سیستم‌ها و شبکه‌ها در حوزه‌های مختلف می‌شود و با برنامه‌ریزی و ارائه راهبردهای لازم، درنهایت موجب ارتقاء امنیت سایبری می‌گردد. بر این اساس، نیازمند تبیین و به‌کارگیری شاخص‌هایی به‌منظور انجام ارزیابی هستیم. بررسی تطبیقی شاخص‌های ارزیابی امنیت سایبری می‌تواند ضمن توسعه ادبیات و ارتقاء دانش و فهم مشترک ابعاد و مؤلفه‌ها و احصاء ویژگی‌های آن‌ها، در تدوین شاخص‌های بومی ارزیابی امنیت سایبری کشورمان مورد استفاده قرار گیرد. در همین راستا، هدف این تحقیق انجام مطالعه تطبیقی به‌منظور ارائه مهم‌ترین شاخص‌های ارزیابی امنیت سایبری مطرح در سطح جهان و منطقه است. این پژوهش از نوع کاربردی بوده و با استفاده از روش مطالعه تطبیقی و استناد به منابع کتابخانه‌ای، به بررسی گزارش‌های ارائه‌شده از سوی مراجع بین‌المللی معتبر در حوزه ارزیابی امنیت سایبری پرداخته است و درنهایت با انتخاب هفت الگوی ارزیابی معتبر و مقایسه تطبیقی معیارهای آن‌ها نظیر حوزه تمرکز، اهداف، ابعاد و رویکرد نتایج حاصل در قالب مجموعه شاخص‌های ارزیابی امنیت سایبری ارائه شده‌اند.

کلیدواژه‌ها: امنیت سایبری، امنیت ملی، فضای سایبر، مطالعه تطبیقی

۱.دانشجوی مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران- ایران (نویسنده مسئول). a.saadatmand@sndu.ac.ir

۲.عضو هیئت علمی دانشگاه مالک اشتر، m-karimi@mut.ac.ir

۳ دانشجوی مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی.

٤ دانشجوی مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی.

مقدمه و بیان مسئله

با آغاز هزاره سوم، فضای سایبر رشد فزاینده‌ای داشته و این رشد در عرصه‌های مختلف زندگی انسان‌ها تأثیرات غیرقابل انکاری بر جای گذاشته است. فضای سایبر به‌عنوان پدیده‌ای نوظهور در زندگی بشر، امکان گردآوری، تمرکز، جابه‌جایی، پردازش و کاربری اطلاعات را با استفاده از فناوری اطلاعات و ارتباطات بین کاربران اینترنت و بازیگران فضای مجازی در سراسر جهان فراهم می‌کند. اهمیت روزافزون فضای سایبر و در پی آن، مخاطرات به‌وجودآمده در این زیست‌بوم شرایطی را به وجود آورده است که سازمان‌ها برای انجام موفقیت‌آمیز مأموریت‌های خود همواره به دنبال حفظ، استمرار و ارتقاء امنیت سایبری در حوزه‌های مختلف می‌باشند.

با توسعه فضای سایبر و خلق فناوری‌های نوظهور در آن، میزان تأثیرگذاری این فناوری به‌صورت تصاعدی افزایش یافته است. پیشرفت روزافزون فناوری‌های مرتبط با فضای سایبر، موجب گسترش تهدیدات سایبری شده و اهمیت موضوع امنیت سایبری با توجه به تهدیدات متنوع در آن، روزبه‌روز بیشتر احساس می‌شود.

بیش از نیمی از جمعیت جهان در حال حاضر برخط هستند. در پایان سال ۲۰۱۸ میلادی، ۵۱,۲ درصد از افراد، معادل ۳,۹ میلیارد نفر، از اینترنت استفاده کرده‌اند. این گامی مهم به‌سوی جامعه اطلاعاتی فراگیر جهانی است و در عین حال نیاز مهمی به افزایش حفاظت اینترنتی نیز دارد. مطابق پیش‌بینی ITU[1] تا سال ۲۰۲۳ میلادی، ۷۰ درصد نفوذ اینترنت در دنیا وجود خواهد داشت و این امر نیاز به فضای سایبری امن‌تری را افزایش می‌دهد (شاخص جهانی امنیت سایبری، ۲۰۱۹: ٦). این موضوع با شیوع و همه‌گیری ویروس کرونا و افزایش تمایل و از سویی اجبار در به‌کارگیری اینترنت و ارتباطات بر خط در حوزه‌های آموزش مجازی، اقتصاد کسب‌وکارهای دیجیتال، بیش‌ازپیش نمایان گردیده است.

بررسی‌ها نشان می‌دهد بین رشد و توسعه فناوری اطلاعات و ارتباطات و امنیت رابطه معنی‌داری وجود دارد (انتظامی،۱۳۹۲:۱۹۷). با توجه به توسعه فناوری اطلاعات و ارتباطات و

1. International Telecommunication Union.

فراگیر شدن فناوری‌های نوظهور در فضای سایبر و افزایش تعداد کاربران آن می‌توان گفت مهم‌ترین چالش فضای سایبر امروزه موضوع امنیت این فضا است، با توجه به افزایش روزافزون جرائم سایبری و نقض امنیت داده‌ها در این فضا، هنوز یک شکاف آشکار بین بسیاری از کشورها از نظر دانش برای اجرای قانون جرائم رایانه‌ای، راهبردهای ملی امنیت سایبری، تیم‌های واکنش سریع رایانه‌ای، آگاهی و ظرفیت برای گسترش راهبردها، توانایی ها و برنامه‌ها در حوزه امنیت سایبری وجود دارد. برای توسعه پایدار در این حوزه باید استفاده ایمن و مناسب از فناوری اطلاعات و ارتباطات متناسب با رشد اقتصادی در شرایط اطمینان‌بخشی باشد.

فضای سایبری در معرض چالش‌ها، آسیب‌ها و تهدیدات الکترونیکی گوناگونی نظیر ارتکاب جرائم سازمان‌یافته، تخریب بانک‌های اطلاعاتی، حملات مختل‌کننده خدمات، جاسوسی، خرابکاری، نقض حریم خصوصی و نقض حقوق مالکیت معنوی قرار دارد؛ به‌طوری که نپرداختن یا رویکرد نادرست به امنیت این فضا، مانع بزرگی در به‌کارگیری امن فناوری اطلاعات و ارتباطات و ورود به جامعه اطلاعاتی خواهد بود. امنیت فضای تبادل اطلاعات برقراری شرایط و حالتی است که دارایی‌های این فضا از خطرات مختلف محفوظ بماند و بیم و دغدغه نسبت به تهدید سایر دارایی‌های مادی و معنوی جامعه از این طریق نیز وجود نداشته باشد (انتظامی،۱۳۹۲:۱۹۸). بر این اساس، امنیت فضای تبادل اطلاعات فراتر از فعالیت‌های اجرایی یک یا چند دستگاه است و نیازمند مشارکت همه بخش‌های حاکمیتی و اجرایی کشور، بخش‌های غیردولتی و همچنین آحاد شهروندان جامعه است.

با توسعه و گسترش فضای سایبری، اکنون حجم بالایی از امور و دادوستدهای اقتصادی، فرهنگی، اجتماعی و دفاعی در کلیه سطوح اعم از فردی، دولتی و بخش خصوصی در این فضا انجام می‌شود. به عبارتی، وجوه مختلف زندگی شهروندان به‌گونه‌ای روشن با این فضا درآمیخته و هرگونه ناامنی و چالش در این فضا به‌طور مستقیم یا غیرمستقیم بر زندگی و رفتار شهروندان تأثیر خواهد گذاشت (راهنمای تدوین راهبرد ملی امنیت سایبری، ۱۳۹۵: ۱۰) طی سال‌های اخیر حملات سایبری به شکل فوق‌العاده‌ای افزایش پیدا

کرده‌اند؛ به‌طوری که مهاجمان به پیشرفت‌های زیادی در به‌کارگیری ابزارهای مختلف حمله به سیستم‌های هدف نائل آمده‌اند. این حملات چه برای شبکه‌های محلی و چه شبکه‌های سراسری تهدیدات جدی و مؤثری محسوب می‌شوند. این حمله‌ها در حال پیچیده‌تر شدن هستند و در برخی از موارد این توانایی را دارند که در زمان‌های بسیار کوتاه گسترش پیدا کنند.

فضای سایبر به‌شدت آسیب‌پذیر است و در سطح ملی می‌تواند از سوی عوامل بیرونی یا درونی مورد تهدید جدی قرار گرفته و صدمه ببیند که این خسارت متوجه حاکمیت، سازمان‌ها و نهادهای دولتی، مؤسسه‌ها، بانک‌ها و درنهایت شهروندان خواهد گردید؛ بنابراین امنیت فضای سایبری یکی از مؤلفه‌های امنیت ملی است که باید به‌طور جدی مورد توجه قرار گرفته و به‌صورت پیوسته مورد ارزیابی واقع شود (همان:۱۱).

برای ارزیابی صحیح امنیت در فضای سایبری لازم است چارچوبی برای امنیت سایبری وجود داشته باشد. چنین چارچوبی شامل مجموعه فعالیت‌های اصلی بخش دولتی و خصوصی برای تضمین سطح قابل قبولی از امنیت سایبری است. امنیت فضای سایبر ملی، نه یک هدف انتهایی، بلکه به‌عنوان ابزاری برای دستیابی به مؤلفه‌های ملّی اعم از امنیت ملی، اقتصاد ملی یا منافع ملی است. بسیاری از کشورها، هدف راهبردی ایمنی و امنیت فضای سایبر را تعریف می‌کنند تا بتوانند آرامش و اطمینان را بر فضای سایبر خود حاکم نموده و ظرفیت‌های اقتصادی خود را در کامل‌ترین حالت، به ظهور و بُروز برسانند و شهروندان خود را در مقابل انواع مختلف مخاطرات سایبری و غیرسایبری در این فضا محافظت نمایند.

با توجه به اهمیت بالای موضوع امنیت سایبری لازم است تا وضعیت کشورها توسط شاخص‌هایی سنجیده شده و نقاط قوت و ضعف آن‌ها در حوزه‌ها و ابعاد گوناگون مشخص گردد تا با برنامه‌ریزی‌های کوتاه‌مدت و بلندمدت نسبت به ارتقا امنیت سایبری اقدام نمایند و در این راستا تعدادی از مؤسسات بین‌المللی در این حوزه، نسبت به معرفی ابعاد، مؤلفه‌ها و شاخص‌های ارزیابی امنیت سایبری اقدام نموده‌اند و وضعیت امنیت سایبری کشورها را مورد ارزیابی قرار داده‌اند.

بنابراین، در این راستا این پژوهش درصدد آن است که با استفاده از روش تحقیق مطالعات تطبیقی، ضمن بررسی اسناد و گزارش‌های مؤسسات بین‌المللی، مطالعه تطبیقی بر روی شاخص‌های ارزیابی امنیت سایبری را انجام داده و ضمن مقایسه شاخص‌ها و شناسایی نقاط قوت و ضعف آن‌ها، نتایج حاصل را ارائه نماید که این نتایج می‌تواند علاوه بر استفاده در تدوین سند بومی، در ارزیابی وضعیت امنیت سایبری کشورمان مورد استفاده قرار گیرد. همچنین معیاری برای ارزیابی امنیت سایبری ملی مشخص می‌شود و از طرفی تصمیم‌سازان و تصمیم‌گیران می‌توانند نسبت به تدوین راهبردها و برنامه‌های عملیاتی در راستای ارتقاء امنیت سایبری در سطح ملی اقدام نمایند؛ ضمن اینکه فقدان آن می‌تواند باعث بروز چالش‌های اساسی و تصمیم‌گیری نادرست در مورد به‌کارگیری شاخص‌های امنیت سایبری، افول قدرت تصمیم‌سازی در حوزه امنیت سایبری و همچنین افول قدرت ارزیابی امنیت سایبری ملی باشد؛ بنابراین پرسش اصلی تحقیق این است: مهم‌ترین شاخص‌های جهانی و منطقه‌ای ارزیابی امنیت سایبری چیست؟ و پرسش‌های فرعی عبارت‌اند از: ابعاد، مؤلفه‌ها، ارکان و معیارهای این شاخص‌ها کدام‌اند؟ و مقایسه این شاخص‌ها چه آموزه‌هایی برای کشورمان دارد؟

۱. مبانی نظری

در این تحقیق ضمن بررسی جدیدترین الگوهای ارزیابی امنیت سایبری در سطح منطقه و جهان، تعداد هفت منبع از معتبرترین ارائه‌دهندگان شاخص‌های ارزیابی امنیت سایبری انتخاب و از نظر معیارهایی مثل مرجع و سال انتشار، تعداد کشورهای تحت پوشش، تعداد ابعاد و مؤلفه‌ها، اهداف اصلی ارزیابی، ابعاد اصلی ارزیابی، روش ارزیابی، شیوه رتبه‌بندی و رویکرد دفاعی/ غیردفاعی و ترکیبی مورد مقایسه و بررسی قرار گرفتند. مهم‌ترین ارائه‌کنندگان شاخص‌های ارزیابی امنیت سایبری منتخب در این تحقیق عبارت‌اند از:

۱. شاخص جهانی ارزیابی امنیت سایبری اتحادیه بین‌المللی مخابرات[1]

شاخص جهانی امنیت سایبری[2]، یک شاخص مرکب است که توسط اتحادیه بین‌المللی مخابرات، تولید، تحلیل و منتشر شده و از آن به‌منظور سنجش تعهد کشورهای عضو اتحادیه بین‌المللی ارتباطات به امنیت سایبری و افزایش آگاهی عمومی نسبت به امنیت سایبری استفاده می‌شود. پایه و اساس این ارزیابی، دستور کار امنیت سایبری جهانی[3] اتحادیه بین‌المللی مخابرات است که در سال ۲۰۰۷ میلادی به وجود آمد و دارای پنج رکن اصلی شامل اقدامات قانونی، فنی، سازمان‌دهی، ظرفیت‌سازی و همکاری است. درواقع شاخص جهانی امنیت سایبری، میزان تعهد ۱۹٤ کشور عضو سازمان ملل متحد (ازجمله کشور فلسطین) به ابعاد عنوان‌شده را مورد نظارت و ارزیابی قرار داده و گزارش آن را به‌صورت سالیانه منتشر می‌کند. ابعاد اصلی شاخص جهانی امنیت سایبری بر پنج رکن زیر تمرکز دارد:

۱-۱. اقدامات قانونی: اقدامات مبتنی بر وجود نهادهای حقوقی، قانونی، چارچوب مربوط به امنیت سایبری و جرائم اینترنتی است. اقدامات قانونی به دولت‌های ملی اجازه می‌دهد تا سازوکارهای واکنش اساسی را از طریق تحقیقات و پیگیری جنایات و اعمال تحریم برای عدم انطباق یا نقض قانون وضع کند. یک چارچوب قانونی، حداقل پایه رفتاری را تعیین می‌کند که قابلیت‌های امنیتی سایبری بیشتری را می‌توان بنا نهاد. دراصل، هدف داشتن قوانین کافی به‌منظور هماهنگی اعمال در سطح منطقه‌ای / بین‌المللی و هماهنگ‌سازی مبارزه بین‌المللی بر ضد جرائم رایانه‌ای است. زمینه قانونی بر اساس تعداد نهادهای قانونی و چارچوب‌های مربوط به امنیت سایبری و جرائم رایانه‌ای مورد ارزیابی قرار می‌گیرد.

۲-۱. اقدامات فنی: اقدامات مبتنی بر وجود نهادهای فنی و چارچوب مربوط به امنیت سایبری را شامل می‌شود. فناوری، مرز اصلی دفاعی در برابر تهدیدهای سایبری است.

1. ITU.
2. Global Cybersecurity Index (GCI).
3. Global Cybersecurity Agenda (GCA).

بدون مهارت‌های فنی مناسب برای شناسایی و پاسخ به حملات سایبری، کشورهای عضو همچنان آسیب‌پذیر باقی می‌مانند. توسعه و استفاده مؤثر از فناوری اطلاعات و ارتباطات می‌تواند تنها در محیط اعتماد و امنیت موفق باشد؛ بنابراین کشورهای عضو نیاز به ساخت و نصب معیارهای حداقلی و برنامه‌های اعتبارگذاری برای نرم‌افزارها و سیستم‌های نرم-افزاری دارند. این تلاش‌ها باید با ایجاد یک گروه ملی با هدف برخورد با حوادث سایبری، یک نهاد دولتی مقتدر و یک چارچوب ملی برای نظارت، هشدار دادن و واکنش به حوادث کامل شود. عناصر فنی بر اساس تعداد سازوکارهای عملی برای مقابله با امنیت سایبری، ارزیابی می‌شوند.

۱-۳. سازمان‌دهی: اقدامات مبتنی بر وجود مؤسسات هماهنگ سیاست‌گذاری و راهبردهای توسعه سایبری در سطح ملی می‌باشند. معیارهای سازمانی برای اجرای مناسب هرگونه ابتکار ملی ضروری هستند. اهداف راهبردی گسترده باید توسط دولت ملی، همراه با یک برنامه فراگیر در تدوین، اجرا و ارزیابی ایجاد شود. نهادهای ملی باید برای اجرای این راهبرد و ارزیابی نتیجه آماده باشند. بدون یک راهبرد ملی، مدل اداره و هیئت نظارت، تلاش‌ها در بخش‌های مختلف در تضاد هستند و از تحقق تلاش‌ها برای به دست آوردن یک هماهنگی مؤثر در توسعه امنیت سایبری جلوگیری می‌کنند. ساختارهای سازمانی بر اساس حضور مؤسسات و راهبردهای مربوط به توسعه امنیت سایبری در سطح ملی ارزیابی می‌شوند.

۱-٤. ظرفیت‌سازی: اقدامات مبتنی بر وجود برنامه‌های تحقیق و توسعه، آموزش و مهارت‌افزایی، مراجع صدور مجوزها و سازمان‌های دولتی که از ایجاد ظرفیت حمایت می‌کنند. ظرفیت‌سازی برای سه رکن اول (قانونی، فنی و سازمانی) وجود دارد. امنیت سایبری اغلب از دیدگاه فنی مورد بحث قرار می‌گیرد، اگرچه مفاهیم اجتماعی – اقتصادی و سیاسی متعددی وجود دارد. ایجاد ظرفیت سازمانی برای بالا بردن سطح آگاهی و دانش در سراسر بخش‌ها، برای راه‌حل‌های نظام‌مند و مناسب و ارتقای دانش متخصصان واجد شرایط ضروری است. ظرفیت‌سازی بر اساس تعداد تحقیقات و توسعه، برنامه‌های آموزشی، تربیتی و متخصصان مورد تأیید و سازمان‌های بخش دولتی ارزیابی می‌شود.

۱-۵. همکاری: اقدامات مبتنی بر وجود مشارکت، چارچوب همکاری و شبکه‌های به اشتراک‌گذاری اطلاعات را شامل می‌شود. جرم سایبری یک مسئله جهانی و نامحدود به مرزهای ملی یا تمایزات بخشی است. به این ترتیب، مقابله با جرائم اینترنتی نیازمند یک رویکرد چند ذی‌نفعی با ورودی‌ها از تمام بخش‌ها و رشته‌ها (ازجمله توافق‌نامه‌های چندجانبه، مشارکت مجامع بین‌المللی / انجمن‌ها، مشارکت‌های دولتی - خصوصی، شراکت‌های دولتی، بهترین تجربه‌ها[1] و ...) نیاز دارد. همکاری بیشتر می‌تواند باعث توسعه بیشتر توانایی‌های امنیتی سایبری، کمک به بازدارندگی پایدار و مداوم تهدیدات برخط شود. همکاری ملی و بین‌المللی بر اساس تعداد مشارکت‌ها، چارچوب‌های مشارکتی و شبکه‌های تسهیم اطلاعات مورد ارزیابی قرار می‌گیرد.

پنج بُعد ذکرشده، اساس شاخص‌های جهانی امنیت سایبری اتحادیه بین‌المللی مخابرات را تشکیل می‌دهند، زیرا آن‌ها زیربنای ذاتی و بنیادی ساختار فرهنگ ملی امنیت سایبری می‌باشند.

جدول شماره یک، ۲۵ مؤلفه جهانی ارزیابی امنیت سایبری اتحادیه بین‌المللی مخابرات در سال ۲۰۱۸ میلادی که بر مبنای پنج بُعد دستور کار امنیت سایبری جهانی تنظیم گردیده را ارائه می‌نماید.

جدول شماره ۱- ابعاد و مؤلفه‌های جهانی امنیت سایبری اتحادیه بین‌المللی مخابرات

ابعاد	مؤلفه‌ها	ابعاد	مؤلفه‌ها
اقدامات قانونی	قوانین مجازات جرائم سایبری	ظرفیت سازی	کمپین‌های آگاه‌سازی عمومی
	مقررات‌گذاری امنیت سایبری		استانداردهای امنیت سایبری و صدور گواهی‌نامه‌ها
	قوانین مهار و محدود کردن اسپم		دوره‌های آموزش حرفه‌ای در زمینه امنیت سایبری
اقدامات فنی	تیم واکنش به حوادث سایبری		برنامه‌های ملی آموزش و دروس دانشگاهی
	چارچوب استانداردهای امنیت سایبری سازمان		برنامه‌های تحقیق و توسعه امنیت سایبری

1. Best Practices.

ابعاد	مؤلفه‌ها	ابعاد	مؤلفه‌ها
	استانداردسازی		راهکارهای تشویقی
	سازوکارهای فنی و توانمندی پرداختن به هرزنامه[1]		صنعت امنیت سایبری در حال رشد
	استفاده از فناوری ابر به‌منظور امنیت سایبری		توافق‌نامه‌های امنیت سایبری دوجانبه
	سازوکارهای محافظت از کودکان برخط		توافق‌های امنیت سایبری چندجانبه
سازمان‌دهی	راهبرد ملی امنیت سایبری	همکاری	مشارکت در سازمان‌ها و انجمن‌های بین‌المللی
	اداره مسئول و پاسخگو		مشارکت و همکاری بخش عمومی و خصوصی
	معیارهای امنیت سایبری		مشارکت‌های درون و بین سازمانی
منبع: ابعاد و مؤلفه‌های جهانی امنیت سایبری اتحادیه بین‌المللی مخابرات-۲۰۱۸			استفاده از بهترین تجربیات در امنیت سایبری

۲. شاخص ارزیابی امنیت سایبری اتحادیه اروپا

شاخص ارزیابی امنیت سایبری اتحادیه اروپا، توسط اداره امنیت شبکه و اطلاعات اتحادیه اروپا[2] ارائه گردیده است. این اداره مرکز تخصصی امنیت شبکه و اطلاعات این اتحادیه است که توصیه‌هایی را در مورد عملکرد مناسب در زمینه امنیت اطلاعات ارائه می‌دهد تا کشورهای عضو در اجرای قوانین مربوطه و بهبود تاب‌آوری زیرساخت‌ها و شبکه‌های مهم اطلاعاتی فعالیت نمایند. این اداره درصدد است در زمینه بهبود امنیت شبکه و اطلاعات در سراسر اتحادیه اروپا، مهارت‌های موجود در کشورهای عضو را ارتقاء بخشد. همچنین هسته اصلی سند ارائه‌شده توسط این اداره جهت ارزیابی امنیت سایبری، یک چارچوب ارزیابی شامل شاخص‌های کلیدی عملکرد[3] است که در سال ۲۰۱٤ میلادی ارائه گردیده است.

1.Spam.
2. European Union Agency for Network and Information Security (ENISA).
3. key performance indicator (KPI).

ابعاد اصلی شاخص ارزیابی امنیت سایبری ارائه‌شده توسط این اداره به شرح جدول زیر است:

جدول ۲: شاخص ارزیابی امنیت سایبری اتحادیه اروپا

ردیف	شاخص‌ها
۱	توسعه سیاست و قابلیت‌های دفاع سایبری
۱-۱	اختصاص یک برنامه ملی راهبردی برای دفاع سایبری (دکترین، مفاهیم، ذی‌نفعان، مسئولیت‌های خاص)
۱-۲	میزان مشارکت کشور در ابتکارات اتحادیه اروپا (ایجاد توانمندی)
۱-۳	شناسایی و ایجاد گروه واکنش به حوادث سایبری نظامی
۱-٤	وجود آموزش (بر اساس نیاز کارکنان) و میزان اثربخشی آن
۱-٥	قابلیت‌های همکاری
۱-٦	افزایش تاب‌آوری از طریق همکاری و به‌کارگیری فناوری‌ها جهت مقابله با حملات سایبری نظامی
۲	دستیابی به تاب‌آوری سایبری
۲-۱	راه‌اندازی تیم‌های واکنش به حوادث سایبری یا سازمان‌های امنیت ملی
۲-۲	وجود یا راه‌اندازی مشارکت‌های خصوصی- عمومی در امنیت سایبری
۲-۳	شناسایی چشم‌انداز خطرات و تهدیدات
۲-٤	وجود مأموریت‌های سازمان ملی امنیت سایبری
۲-٥	افزایش توانمندی‌ها: آموزش‌های سازمان‌یافته برای بخش عمومی و خصوصی، فعالیت‌های یادگیری متقابل
۲-٦	فعالیت‌های آگاهی‌رسانی برای کاربران نهایی (محتوی، کمپین‌ها، رویدادها)
۲-۷	هماهنگی ملی در میان همه فعالان ملی عرصه امنیت سایبری (ادارات امنیت ملی)
۲-۸	افزایش توانایی پاسخگویی (طرح‌های بهبود واکنش، سامانه‌های هشداردهنده اولیه و ...)
۲-۹	افزایش ایمنی سامانه‌های عمومی فناوری اطلاعات
۳	کاهش جرائم سایبری
۳-۱	چارچوب سازمانی ملی برای کاهش جرائم سایبری
۳-۲	تجزیه‌وتحلیل خلأها، شناسایی نیازها، دارایی‌های فنی، استفاده از بهترین شیوه‌ها
۳-۳	وجود سازوکارهای همکاری با سازمان‌های بین‌المللی
۳-٤	قطعنامه‌های مربوط به موارد جرائم سایبری
۳-٥	همکاری‌های بین‌المللی
۳-٦	فضای امن‌تر برای همه کاربران
٤	حمایت از صنعت در زمینه امنیت سایبری

ردیف	شاخص‌ها
٤-١	پشتیبانی از استانداردسازی و توسعه برچسب‌های اعتماد و ایمنی
٤-٢	حمایت مالی از طریق برنامه‌های تحقیقاتی ملی و اتحادیه اروپا
٤-٣	در حال توسعه اقدامات جدید در مورد تقاضای ملی در سطح ملی (برای مثال در تهیه)
٤-٤	نوآوری در تجارت الکترونیک (و اثربخشی هزینه)
٤-٥	مصرف‌کنندگان دسترسی بیشتری به فناوری امن دارند
٥	امن‌سازی زیرساخت‌های اطلاعاتی حیاتی
٥-١	شناسایی زیرساخت‌های اطلاعات بحرانی، یعنی دارایی‌های بحرانی، آسیب‌پذیری‌ها، وابستگی‌ها و خطرات
٥-٢	ارزیابی خطر و رویه‌های مدیریت خطر/ طرح‌ها
٥-٣	راه‌اندازی گزارش‌دهی حوادث و روش اطلاع‌رسانی نقض
٥-٤	طراحی و پیاده‌سازی ابزارها (PPP[1]، قوانین افشای نقض)
٥-٥	بازیابی فرایندها و برنامه‌ها برای زیرساخت‌های حیاتی
٥-٦	به اشتراک‌گذاری اطلاعات موفقیت‌آمیز و همکاری قابل اعتماد بین فعالان مختلف
٥-٧	پاسخ سریع‌تر و کارآمدتر در صورت وقوع حادثه در سطح ملی
٥-٨	شفافیت و پاسخگویی سامانه‌ها
٦	ارزیابی عمومی
٦-١	ارزیابی راهبرد ملی امنیت سایبری در سطح برنامه
٦-٢	ارزیابی اجرایی
٦-٣	تعهدات قانونی بین‌المللی و ملی
٦-٤	بودجه
٦-٥	همکاری با توجه به هنجارهای مشترک در فضای مجازی؛ حمایت از ارزش‌های مشترک در فضای مجازی

٣. مدل بلوغ قابلیت امنیت سایبری دانشگاه آکسفورد[2]

این مدل توسط دانشگاه آکسفورد در سال ٢٠١٤ میلادی ارائه شده و اهداف آن توسعه اثربخش ساختار و ظرفیت‌های امنیت سایبری، در بریتانیا و سطح بین‌المللی و انتقال دانش به دولت‌ها، جوامع و سازمان‌ها به‌منظور افزایش ظرفیت سایبری جهت کسب اطمینان و

1. Public Private Partnership (PPP).
2. Cyber Security Capability Maturity Model (CMM).

تحقق فضای سایبری که بتواند به رشد و نوآوری در حمایت از رفاه، حقوق بشر و شکوفایی برای همه ادامه دهد. در این مدل، ارزیابی امنیت سایبری در پنج بُعد عمده و مؤلفه‌های مربوطه مورد بررسی قرار گرفته است:

جدول ۳: ابعاد و مؤلفه‌های مدل بلوغ امنیت سایبری دانشگاه آکسفورد

ردیف	ابعاد	مؤلفه‌ها
۱	خط‌مشی و راهبرد امنیت سایبری	راهبرد ملی امنیت سایبری
۲		پاسخ به حوادث
۳		حفاظت از زیرساخت‌های حیاتی
٤		مدیریت بحران
٥		دفاع سایبری
٦		افزونگی ارتباطات
۷	فرهنگ سایبری جامعه	طرز تفکر امنیت سایبری
۸		اعتماد و اطمینان به اینترنت
۹		درک کاربر از حفاظت از اطلاعات شخصی به‌صورت آنلاین
۱۰		مکانیزم‌های گزارش‌دهی
۱۱		رسانه و رسانه‌های اجتماعی
۱۲	آموزش، تربیت و مهارت‌آموزی امنیت سایبری	افزایش آگاهی
۱۳		چارچوبی برای تربیت امنیت سایبری
۱٤		چارچوب آموزش حرفه‌ای
۱٥	چارچوب‌های حقوقی و تنظیم مقررات	چارچوب‌های قانونی
۱٦		سیستم عدالت کیفری
۱۷		چارچوب‌های همکاری رسمی و غیررسمی برای مبارزه با جرائم سایبری
۱۸	استانداردها، سازمان‌ها و فناوری‌ها	پیروی از استانداردها
۱۹		تاب‌آوری زیرساخت‌های اینترنت
۲۰		کیفیت نرم‌افزار
۲۱		کنترل‌های امنیتی فنی
۲۲		کنترل‌های رمزنگاری
۲۳		بازار امنیت سایبری

٤. شاخص آمادگی سایبری[1] مؤسسه پوتومَک[2]

این شاخص توسط مؤسسه مطالعات سیاسی پوتومک در سال ۲۰۱۵ میلادی ارائه شده و رهبران ملی را در مورد اقداماتی که باید برای محافظت از کشورهای خود از نظر بلوغ، الزام و تعهد به امنیت و تاب‌آوری سایبری انجام دهند، مطلع می‌نماید. شاخص آمادگی سایبری برای ارزیابی امنیت سایبری ۱۲۵ کشور در حوزه‌های ارزیابی بلوغ و تعهد هر کشور برای امنیت سایبری و زیرساخت‌ها و خدمات به کار گرفته می‌شود. روش‌های مورد استفاده در تدوین این شاخص شامل ارزیابی بلوغ و تعهد هر کشور نسبت به امنیت سایبری و تاب‌آوری آن با تمرکز بر رشد اقتصادی است.

ابعاد اصلی ارزیابی امنیت سایبری در این مدل عبارت‌اند از:

٤-١. راهبرد ملی

مهم‌ترین حوزه آمادگی سایبری یک کشور، بیان و انتشار یک راهبرد ملی امنیت سایبری است که چشم‌انداز اقتصادی را با الزامات امنیتی ملی آن، همسو می‌کند. راهبرد ملی امنیت جامع سایبری باید تهدیدات کشور را از نظر اقتصادی توصیف کند و مراحل، برنامه‌ها و ابتکارات لازم را تشریح کند. این راهبرد را باید زیربنای ظرفیت اقتصادی اینترنت و پذیرش فناوری اطلاعات و ارتباطات دانست.

٤-٢. واکنش در برابر حادثه

دومین عنصر آمادگی سایبری یک کشور شامل ایجاد و حفظ توانایی مؤثر در واکنش به حوادث ملی است. اغلب، این توانایی به‌صورت یک یا چند تیم ملی پاسخ به حوادث امنیت رایانه‌ای[3] یا تیم‌های واکنش اضطراری رایانه[4] است. عملیاتی کردن یک تیم ملی پاسخ به حوادث امنیت رایانه‌ای، یک مؤلفه اصلی راهبرد کلی یک کشور برای تأمین امنیت و حفظ خدمات و زیرساخت‌هایی است که برای امنیت ملی و رشد اقتصادی حیاتی است.

1. Cyber Readiness Index (CRI).
2. Potomac.
3. National Computer Security Incident Response Teams (NCSIRTs).
4. Computer Emergency Response Team (CERT).

٤-٣. جرائم الکترونیکی و اجرای قانون

سومین عنصر آمادگی سایبری یک کشور از طریق تعهد آن کشور برای حمایت از جامعه خود در برابر جرائم سایبری، معرفی شده است. بیشتر اوقات، این آمادگی به‌صورت تعامل و همکاری با مجامع بین‌المللی تعیین شده برای پرداختن به موضوعات بین‌المللی در مورد جرائم سایبری و همچنین ایجاد مکانیزم‌های مقررات‌گذاری و قانونی داخلی برای مقابله با جرائم سایبری صورت می‌گیرد.

٤-٤. به اشتراک‌گذاری اطلاعات

چهارمین عنصر آمادگی سایبری یک کشور، توانایی آن در ایجاد و نگهداری مکانیسم‌های به‌اشتراک‌گذاری اطلاعات است که امکان تبادل اطلاعات عملی یا اطلاعات بین دولت‌ها و بخش‌های صنعت را فراهم می‌کند. اکثر دولت‌ها و سازمان‌ها برای درک بهتر خطرات ناشی از بازیگران دولتی و غیردولتی برنامه‌هایی را برای به اشتراک گذاشتن اطلاعات ایجاد کرده‌اند.

٤-٥. سرمایه‌گذاری در تحقیقات و توسعه

پنجمین عنصر آمادگی سایبری یک کشور، تعیین اولویت ملی و سرمایه‌گذاری در تحقیقات سایبری و تحقیقات کاربردی فناوری اطلاعات و ارتباطات به‌طور گسترده در زمینه امنیت سایبری است. نوآوری‌ها رشد اقتصادی را به دنبال دارد و می‌تواند امنیت را ارتقا بخشد و شرایط را برای ایجاد امنیت پایدار فراهم کند.

٤-٦. دیپلماسی و تجارت

ششمین عنصر آمادگی سایبری از طریق تعامل در موضوعات سایبری به‌عنوان بخشی از سیاست خارجی یک کشور نشان داده شده است. به‌طور اساسی دیپلماسی سایبری در پی یافتن راه‌حل‌های قابل قبول برای چالش‌های مشترک است. موضوعات سایبری در بسیاری از زمینه‌های مختلف روابط بین‌الملل ازجمله حقوق بشر، توسعه اقتصادی، توافق‌های تجاری، کنترل اسلحه و فناوری‌های استفاده دوگانه، امنیت، ثبات و صلح و حل مناقشه در حال ظهور است.

٤-۷. دفاع و واکنش به رویداد

هفتمین و آخرین عنصر آمادگی سایبری، توانایی نیروهای مسلح یک کشور یا آژانس دفاعی مرتبط برای دفاع از کشور در برابر تهدیدات ناشی از فضای مجازی است. کشورهایی که علاقه‌مند به این نوع توانایی‌ها هستند نیروهای دفاعی خود را برای ایجاد ظرفیت یا تخصص برای پاسخگویی به تهدیدات و حملات سایبری هدایت می‌کنند.

این شاخص، ارزیابی امنیت سایبری را در سه سطح کیفی بلوغ شامل سطوح شواهد ناکافی، تا حدی عملیاتی و کاملاً عملیاتی رتبه‌بندی می‌کند (شاخص آمادگی سایبری مؤسسه پوتومک، ۲۰۱۵).

۵. چارچوب ارزیابی امنیت سایبری سازمان ارتباطات کشورهای مشترک‌المنافع[1]

این شاخص توسط سازمان ارتباطات کشورهای مشترک‌المنافع در سال ۲۰۱۵ میلادی ارائه شده که در زمینه فناوری اطلاعات و ارتباطات و در جهت کمک به اعضای آن برای بهره‌برداری از این فناوری برای توسعه اجتماعی اقتصادی فعالیت می‌کند. ابعاد اصلی ارزیابی امنیت سایبری ارائه‌شده توسط این سازمان عبارت‌اند از:

۵-۱. چارچوب قانونی، مقررات‌گذاری و نظارتی

چارچوب قانونی و نظارتی، پایه و اساس هرگونه توانایی ملی امنیت سایبری، به‌ویژه برای فعالیت‌های اجرای قانون است و باید به‌صورت مستمر به‌منظور حفظ کارآمدی آن به‌روز شود تا منعکس‌کننده تهدیدات و فرصت‌های جهان امروزی ناشی از رشد سریع فضای مجازی باشد. در این بخش، راهبرد امنیت سایبر ملی باید چگونگی دستیابی دولت به این هدف را به‌صورت گسترده و بدون توصیف برنامه قانون‌گذاری، توصیف کند.

۵-۲. ظرفیت‌سازی

با توجه به اینکه امنیت سایبری یک زمینه جدید بوده و در حال تحول است، راهبردهای امنیت سایبری ملی باید به دستیابی به مهارت‌های لازم بپردازند. کاملاً محتمل

1. Commonwealth Telecommunications Organization (CTO).

است که در بسیاری از حوزه‌ها و ازجمله تمام ذی‌نفعان این مجموعه، کمبود مهارت وجود داشته باشد. با توجه به طیف وسیعی از ذی‌نفعان و مؤسسات درگیر، ارزیابی نیازهای آموزشی، ازجمله مواردی است که لازم است در ابتدا در دستور کار امنیت سایبری قرار گیرند، به‌منظور تدوین برنامه‌های مناسب و جامع برای ایجاد ظرفیت در این حوزه، توصیه می‌شود با توجه به سرعت و ماهیت غیرقابل پیش‌بینی تحولات در فضای سایبری، نیاز به آموزش‌ها به‌صورت مداوم احصاء و ارزیابی گردد.

۵-۳. آگاهی‌رسانی

با توجه به تأثیرگذاری فضای سایبر بر عموم مردم، افزایش آگاهی در کلیه بخش‌ها و سطوح جامعه یک مؤلفه مهم هر راهبرد امنیت سایبری است. فرایند آگاهی‌رسانی باید به‌گونه‌ای طراحی شود که در کنار فعالیت‌های ظرفیت‌سازی قرار بگیرد تا بتواند پیام مورد نظر را برای مخاطبان بسیار وسیعی منتقل کند.

۵-٤. قابلیت‌های فنی بومی

هر کشوری به متخصصان فنی بومی در زمینه امنیت سایبری نیاز دارد تا به دولت در انجام مأموریت و هنگام قرارداد با سایر سازمان‌ها مشاوره دهد. تحقیقات و توسعه، به‌عنوان مثال در دانشگاه‌ها، نقش مهمی در توسعه ظرفیت برای امنیت سایبری دارد و به‌عنوان یکی از ستون‌های اصلی راهبردهای امنیت سایبری شناخته شده است. فضای مجازی به‌سرعت در حال توسعه است و ابزارهای جدیدی برای تأمین نیازمندی‌های امنیتی آن باید با سرعت مناسب تولید شود و انگیزه برای تحقیق و توسعه در فضای مجازی ایجاد کند.

۵-۵. واکنش به حوادث

امروزه نمی‌توان سازوکارهای دفاعی لازم را ایجاد کرد تا تضمین شود که هیچ‌گاه حادثه‌ای برای به خطر انداختن امنیت و تاب‌آوری استفاده از فضای مجازی روی نخواهد داد؛ بنابراین ضروری است راهبردهای امنیت سایبری برای مقابله با این حوادث برنامه‌ریزی شوند. این حوادث اغلب به طیف وسیعی از ذی‌نفعان نیاز دارد تا دانش و

مهارت‌های خود را به کار گیرند تا بتوانند سریع عمل کنند. شبکه واکنش به رویدادهای سایبری، پایه و اساس توانایی واکنش به حملات و تهدیدات را تشکیل می‌دهد که می‌تواند با سازوکارهای مدیریت بحران کشور ایجاد شود که از قبل ارتباطات حیاتی با مسئولان را برای تأمین امنیت لازم برای اقدام در شرایط اضطراری دارند (چارچوب ارزیابی امنیت سایبری کشورهای مشترک‌المنافع برای توسعه راهبردهای ملی امنیت سایبری،۲۰۱۵).

٦. چارچوب ارزیابی بلوغ سایبری در منطقه آسیا- اقیانوسیه

این چارچوب ارزیابی بلوغ سایبری توسط مؤسسه خط‌مشی‌گذاری راهبردی استرالیا[1] با گستره وسیع جغرافیایی و اقتصادی، شامل ۲۵ کشور از جنوب، شمال و جنوب شرقی آسیا، اقیانوس آرام جنوبی و آمریکای شمالی بوده و در سال ۲۰۱۷ میلادی ارائه گردیده است. مؤسسه مذکور در سال ۲۰۰۱ میلادی به‌عنوان یک اندیشکده مستقل تشکیل شد و هدف اصلی آن ارائه ایده‌های تازه به دولت استرالیا در امور دفاعی، امنیتی و سیاسی راهبردی است. موضوع امنیت سایبری و ارزیابی آن توسط مرکزی در ذیل این مؤسسه با عنوان مرکز بین‌المللی خط‌مشی‌گذاری سایبری ASPI، با مأموریت، خط‌مشی‌گذاری، تفاهم در مورد موضوعات سایبری و مشاوره نزدیک با دولت، صاحبان کسب‌وکار و جامعه مدنی انجام می‌شود.

ابعاد اصلی ارزیابی امنیت سایبری در این چارچوب عبارت‌اند از:

٦-١. حکمرانی

موضوع حکمرانی، رویکرد سازمانی دولت به مسائل سایبری، ازجمله ترکیب آژانس‌های دولتی درگیر در این موضوعات را مورد توجه قرار می‌دهد. قصد و توانایی قانون‌گذاری دولت و مشارکت دولت در موضوعات بین‌المللی سیاست سایبری مانند حاکمیت اینترنت، اعمال قوانین بین‌المللی و تدوین هنجارها یا اصول. این شاخص‌ها

1. Australian Strategic Policy Institute (ASPI).

راهنمایی‌هایی را برای مشارکت‌های دیپلماتیک، دولتی، توسعه، اجرای قانون و بخش خصوصی در کشورهای آسیا و اقیانوسیه ارائه می‌دهند.

٦-٢. جرائم سایبری مالی

جرائم سایبری مالی یک موضوع مهم برای همه دولت‌های آسیا و اقیانوسیه است. تأثیر جرائم سایبری بر مردم عادی منطقه قابل توجه است و خسارات مالی قابل توجهی را شامل می‌شود. درک ظرفیت دولت برای پرداختن به جرائم سایبری مالی می‌تواند مشارکت در اجرای قانون را هدایت کند، ازجمله از طریق اشتراک‌گذاری اطلاعات و کمک به توسعه توانایی بخش‌های دولتی و خصوصی.

٦-٣. نیروی نظامی

این موضوع به ساختار سازمانی ارتش ایالت (در صورت وجود) مربوط به فضای سایبر و دیدگاه‌های شناخته شده دولت در مورد استفاده از فضای مجازی توسط نیروهای مسلح خود می‌پردازد. این می‌تواند تعامل نظامی به نظامی بین کشورها و همچنین تعامل دیپلماتیک و سیاسی- نظامی را هدایت کند. استفاده‌های نظامی از فضای مجازی، به‌ویژه قابلیت‌های ملی، موضوعی حساس برای همه کشورهای آسیا و اقیانوسیه است.

٦-٤. اقتصاد و تجارت دیجیتال

اینکه دولت اهمیت فضای سایبر و اقتصاد دیجیتال را درک کند و چگونه آن‌ها را از نظر اقتصادی مهم می‌داند، نشانگر بلوغ سایبری است. این موضوع می‌تواند مشارکت در ایجاد ظرفیت، پیوندهای تجاری منطقه‌ای و تعامل بین دولت و تجارت در زمینه امنیت سایبری را هدایت و تقویت کند.

٦-٥. تعامل اجتماعی

آگاهی عمومی و مشارکت در مورد موضوعات سایبری، مانند حاکمیت اینترنت، سانسور اینترنت و جرائم سایبری، نشانگر بلوغ گفتمان عمومی بین دولت و شهروندان آن

است. برنامه‌های آموزشی در زمینه فناوری اطلاعات و ارتباطات و سایبر نیز می‌تواند نشانگر سطح بالایی از درک فنی و مسائل مبتنی بر موضوعات باشد.

جدول ٤: شاخص‌های ارزیابی بلوغ سایبری در منطقه آسیا- اقیانوسیه

ردیف	ابعاد	مؤلفه‌ها
۱	حکمرانی	ساختار سازمانی
		قانون / مقررات‌گذاری
		تعامل بین‌المللی
		تیم‌های پاسخ به حوادث سایبری
۲	جرائم سایبری مالی	جرائم سایبری مالی
۳	نیروی نظامی	کاربردهای نظامی
٤	اقتصاد و تجارت دیجیتال	گفتگوی دولت با صاحبان مشاغل
		اقتصاد دیجیتال
٥	تعامل اجتماعی	آگاهی عمومی
		استفاده از اینترنت

این چارچوب، ارزیابی امنیت سایبری کشورها را در سه سطح کیفی بلوغ شامل سطوح بلوغ تعامل، تعامل و توسعه و توسعه رتبه‌بندی می‌کند (چارچوب ارزیابی بلوغ سایبری در منطقه آسیا- اقیانوسیه، ۲۰۱۷).

۷. شاخص ملی امنیت سایبری[1] آکادمی حکمرانی الکترونیک[2]

شاخص امنیت سایبری ملی یک شاخص جهانی است که آمادگی کشورها را برای جلوگیری از تهدیدهای سایبری و مدیریت حوادث سایبر اندازه‌گیری می‌کند و در حال حاضر فهرست ۱۰۰ کشور در لیست رتبه‌بندی آن قرار دارد. این شاخص توسط آکادمی حکمرانی الکترونیک ارائه شده است. این آکادمی یک سازمان دانش‌بنیان و مشاوره است

1.National Cyber Security Index (NCSI).
2. e-Governance Academy (eGA).

که برای ایجاد و انتقال دانش و بهترین تجربیات در زمینه مدیریت الکترونیکی، دموکراسی الکترونیکی، امنیت سایبری ملی و توسعه جوامع اطلاعاتی آزاد ایجاد شده است.

ابعاد اصلی ارزیابی آمادگی امنیت سایبری عبارت‌اند از:

جدول ٥: شاخص‌های ملی امنیت سایبری آکادمی حکمرانی الکترونیک

ردیف	شاخص‌ها	ردیف	شاخص‌ها
١	سیاست و خط‌مشی امنیت سایبری	٧	خدمات شناسایی و اعتماد الکترونیکی
٢	تحلیل و اطلاع‌رسانی تهدیدات سایبری	٨	محافظت از اطلاعات شخصی
٣	آموزش و تربیت امنیت سایبری	٩	تیم واکنش به حوادث سایبری
٤	مشارکت در امنیت سایبری جهانی	١٠	مدیریت بحران سایبری
٥	حمایت از خدمات دیجیتال	١١	پلیس مبارزه با جرائم سایبری
٦	حمایت از خدمات حیاتی	١٢	عملیات سایبری نظامی

روش‌شناسی تحقیق

روش تحقیق مورد استفاده در این پژوهش مقایسه تطبیقی است، مطالعات تطبیقی شناخت یک پدیده در پرتو مقایسه است که با توصیف و تبیین نقاط اشتراک و نقاط اختلاف انجام می‌پذیرد. در مطالعات تطبیقی، صِرف مقایسه کردن هدف نیست، بلکه از کشف موارد تشابه و اختلاف باید به ملاک تشابه یا اختلاف رسیده شود و بر اساس آن مسئله‌ای حل شود (قرا ملکی،١٣٩٥: ٥٣)؛ بنابراین می‌توان نتیجه گرفت روش تحقیق مطالعات تطبیقی مقایسه‌ای، راهبرد عقلایی جهت استفاده از تجارب دیگران است و می‌توان با هماهنگ کردن اطلاعات و برنامه‌های مدون ایشان با شرایط مالی و ملاحظات بومی کشورمان برنامه‌هایی با کیفیت بهتر تنظیم کرد و از منابع انسانی و مالی موجود استفاده بهینه نمود. فرایند مطالعه تطبیقی شامل تدوین مسئله، تعیین دامنه تحقیق، تدوین فرضیه، استقصای موارد شباهت و تفاوت، توصیف و تبیین موارد وفاق و خلاف است (همان،٥٥). مطابق با فرایند یادشده و پس از تبیین مسئله، دامنه پژوهش در بررسی شاخص‌های ارزیابی امنیت سایبری در سطح ملی در نظر گرفته شد و با بررسی صورت گرفته و تجارب

موجود درعمل فرضیه اولیه‌ای توسط محققین پیشنهاد یا استنباط نگردید. در ادامه با استفاده از روش جمع‌آوری اطلاعات کتابخانه‌ای و اینترنتی، مجموعه اسناد و اطلاعات مرتبط با شاخص‌های ارزیابی امنیت سایبری ملی رایج منتشرشده در سطوح جهانی و منطقه‌ای مورد بررسی جامعی قرار گرفت و جدیدترین و معتبرترین این شاخص‌ها در قالب هفت شاخص اصلی با استفاده از پنل خبرگی و با حضور دوازده نفر از کارشناسان و خبرگان حوزه امنیت سایبری مورد بررسی قرار گرفت و درنهایت به‌عنوان شاخص‌های منتخب جهت انجام مقایسه تطبیقی انتخاب گردیدند. در ادامه این تحقیق موارد مشابه و تفاوت شاخص‌های ارزیابی امنیت سایبری ملی بر اساس مرجع و سال انتشار، تعداد کشورهای تحت پوشش، تعداد ابعاد و مؤلفه‌ها، اهداف و ابعاد اصلی ارزیابی، روش ارزیابی، شیوه رتبه‌بندی و رویکرد دفاعی/ غیردفاعی و ترکیبی مورد مقایسه تطبیقی قرار گرفته و نتایج آن در قالب در جدول شماره ٦ جمع‌بندی و درنهایت موارد تشابه و تفاوت آن‌ها با یکدیگر مقایسه، تبیین و نتیجه‌گیری به عمل آمد.

تجزیه‌وتحلیل یافته‌ها

با بررسی و مقایسه تطبیقی شاخص‌های هفت‌گانه منتخب در حوزه‌های امنیت سایبری، مطابق با جدول ٦ یافته‌هایی به شرح زیر حاصل گردید.

۱. مطابق با مندرجات ردیف اول جدول شماره ٦، کلمات کلیدی به‌کاررفته در عناوین این شاخص‌ها شامل امنیت سایبری، مدل بلوغ، شاخص آمادگی و چارچوب ارزیابی است.

۲. مطابق با مندرجات سطر دوم جدول شماره ٦، مأموریت مراجع منتشرکننده شاخص‌های ارزیابی امنیت سایبری به‌طور عمده راهبردی، خط‌مشی‌گذاری، آموزشی، تحقیقاتی و حکمرانی است.

۳. مطابق با مندرجات ردیف سوم جدول شماره ٦، از نظر سال انتشار، شاخص‌های ارزیابی امنیت سایبری در بازه زمانی ۲۰۱٤ الی ۲۰۱۸ میلادی منتشر شده و در این میان شاخص‌های سازمان‌های اتحادیه بین‌المللی مخابرات و آکادمی حکمرانی الکترونیک مربوط به سال ۲۰۱۸ میلادی بوده و از سایر شاخص‌ها جدیدتر می‌باشند.

٤. مطابق با مندرجات ردیف چهارم جدول شماره ٦، از نظر تعداد کشورهای تحت پوشش، اتحادیه بین‌المللی مخابرات با ۱۹٤ کشور، بیشترین کشورها را تحت پوشش دارد و شاخص آمادگی سایبری مؤسسه پوتومک و شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک به ترتیب با ۱۲۵ و ۱۰۰ کشور در رده‌های بعدی قرار دارند. بر این اساس شاخص ارائه‌شده توسط اتحادیه بین‌المللی مخابرات طیف وسیع‌تری از کشورها را در مقایسه با سایر شاخص‌ها تحت پوشش قرار داده است. همچنین با تولید نسخه‌های جدید شاخص‌های ارزیابی، تعداد کشورهای تحت پوشش در طول زمان افزایش یافته است.

۵. مطابق با مندرجات ردیف پنجم جدول شماره ٦، از نظر تعداد ابعاد اصلی ارزیابی امنیت سایبری، چارچوب ارزیابی بلوغ سایبری در منطقه آسیا- اقیانوسیه نسبت به معرفی تعداد دوازده شاخص ارزیابی امنیت سایبری اقدام نموده که در مقایسه با سایر شاخص‌ها بیشترین تعداد ابعاد را شامل می‌گردد و سایر شاخص‌ها به ترتیب در رتبه‌های بعدی قرار دارند. همچنین شاخص آمادگی سایبری مؤسسه پوتومک، مدل بلوغ امنیت سایبری دانشگاه آکسفورد و شاخص ارزیابی امنیت سایبری اتحادیه اروپا به ترتیب با تعداد ۷۰،٤٦ و ۳۹ شاخص دارای بیشترین تعداد مؤلفه‌های ارزیابی می‌باشند.

٦. مطابق با مندرجات ردیف ششم جدول شماره ٦، از نظر اهداف اصلی ارزیابی امنیت سایبری، اغلب مؤسسات با رویکرد ایجاد انگیزش مناسب به‌منظور ارتقاء امنیت سایبری، کمک به ارتقاء فرهنگ امنیت سایبری، افزایش سطح امنیت سایبری با احصاء خلأها و چالش‌های موجود در فضای سایبر نسبت به تدوین شاخص‌ها اقدام نموده‌اند.

۷. مطابق با مندرجات ردیف هفتم جدول شماره ٦، از نظر ابعاد اصلی ارزیابی امنیت سایبری، اغلب شاخص‌ها نسبت به معرفی اقدامات حقوقی و قانونی، سازمان‌دهی، ظرفیت‌سازی، اقدامات فنی و همکاری‌های ملی، منطقه‌ای و بین‌المللی اقدام نموده‌اند. همچنین در شاخص ارزیابی امنیت سایبری اتحادیه اروپا به موضوع ارزیابی امنیت سایبری که منبعث از راهبرد ملی امنیت سایبری این اتحادیه است، پرداخته شده است. در

شاخص های ارزیابی امنیت سایبری اتحادیه اروپا، آمادگی سایبری مؤسسه پوتومک، چارچوب ارزیابی بلوغ سایبری در منطقه آسیا- اقیانوسیه و شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک به مقوله دفاع نظامی سایبری به‌عنوان یکی از ابعاد اصلی امنیت سایبری کشورها صراحتاً پرداخته شده است.

۸. مطابق با مندرجات ردیف هشتم جدول شماره ٦، از نظر روش ارزیابی امنیت سایبری به غیر از اتحادیه بین‌المللی مخابرات که در بخشی از فرایند ارزیابی از خوداظهاری برخط استفاده می‌کند، اغلب شاخص‌های ارزیابی بر اساس جمع‌آوری اطلاعات باز و با مشورت خبرگان و تعامل با طیف وسیعی از ذی‌نفعان با لحاظ نمودن قابل اندازه‌گیری بودن شاخص‌ها تدوین گردیده و گاهی قبل از به‌کارگیری عملیاتی شاخص‌ها، ارزیابی آن‌ها در یک محیط عملیاتی کوچک مورد بررسی و اعتبارسنجی قرار گرفته است.

۹. مطابق با مندرجات ردیف هشتم جدول شماره ٦، از نظر وضعیت رتبه‌بندی کشورها، اتحادیه بین‌المللی مخابرات، شاخص آمادگی سایبری مؤسسه پوتومک، چارچوب ارزیابی بلوغ سایبری در منطقه آسیا- اقیانوسیه و شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک، نسبت به رتبه‌بندی کشورها اقدام نموده‌اند و رتبه‌بندی اتحادیه بین‌المللی مخابرات با توجه به انجام این رتبه‌بندی شفاف، وسیع، تجربه‌شده و ممتاز در سه سطح و در مقیاس جهانی و منطقه‌ای کامل‌تر است.

جدول ٦: مقایسه تطبیقی معیارهای کلی و محتوایی شاخص‌های ارزیابی امنیت سایبری

ردیف		ITU	CTO	ENISA	CMM	CRI	ASPI	eGA
۱	عنوان شاخص	شاخص جهانی ارزیابی امنیت سایبری اتحادیه بین‌المللی مخابرات	چارچوب ارزیابی امنیت سایبری سازمان مخابرات کشورهای مشترک‌المنافع	شاخص ارزیابی امنیت سایبری اتحادیه اروپا	مدل بلوغ امنیت سایبری دانشگاه آکسفورد	شاخص آماده‌گی سایبری مؤسسه پوتومک	چارچوب ارزیابی بلوغ سایبری در منطقه آسیا - اقیانوسیه	شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک
۲	سازمان مرجع	اتحادیه بین‌المللی مخابرات راه دور	سازمان مخابرات کشورهای مشترک‌المنافع	اداره امنیت شبکه و اطلاعات اتحادیه اروپا	دانشگاه آکسفورد	مؤسسه پوتومک	موسسه خط‌مشی‌گذاری راهبردی استرالیا	آکادمی حکمرانی الکترونیک
۳	سال انتشار	۲۰۱۸	۲۰۱۵	۲۰۱٤	۲۰۱٤	۲۰۱۵	۲۰۱۷	۲۰۱۸
٤	تعداد کشورهای تحت پوشش	۱۹٤ کشور	-	۲۸ کشور	بریتانیا و سایر کشورها	۱۲۵ کشور	۲۵ کشور	۱۰۰ کشور
۵	تعداد ابعاد/مؤلفه‌ها	۵/۲۵	۵/-	۵/۳۹	۵/۲۰/٤٦	۷/۷۰	۱۰/-	۱۲/٤٦
٦	اهداف اصلی ارزیابی امنیت سایبری	۱-ایجاد انگیزه مناسب برای کشورها که تلاش‌های آن ها را در زمینه امنیت سایبری شدت بخشد. ۲-کمک به پرورش فرهنگ جهانی امنیت سایبری و ادغام آن در همه فناوری‌های اطلاعات و ارتباطات. ۳-کمک به کشورها برای شناسایی زمینه هایی برای بهبود در حوزه امنیت سایبری در محیط ملی خود. ٤-کمک به افزایش سطح کلی امنیت سایبری در سراسر جهان	۱-کمک به اعضای سازمان مخابرات کشورهای مشترک‌المنافع جهت بهره‌برداری از فناوری اطلاعات و ارتباطات برای توسعه اجتماعی- اقتصادی. ۲- محافظت از زیرساخت فضای سایبر، محتوای آن و کاربران. ۳- شناسایی و تعیین اولویت ها و اهداف ملی و ایمن‌سازی آن‌ها. ٤- نقش‌ها و مسئولیت.	۱-تمرین رویکردهای فعلی مورد استفاده برای انجام ارزیابی راهبردهای ملی امنیت سایبری. ۲-ارائه توصیه‌ها و شناسایی شیوه‌های خوب در پیاده‌سازی و ارزیابی راهبردهای سایبری. ۳-طراحی و توسعه چارچوب ارزیابی برای انطباق به نیازهای مختلف کشورها در سطوح مختلف بلوغ در برنامه‌ریزی راهبردی آن‌ها. ٤-ارتقاء مهارت های کشورهای اتحادیه اروپا در بهبود مقاومت زیرساخت ها و شبکه‌های مهم اطلاعات اروپا	۱- توسعه اثربخش ساختار و ظرفیت های امنیت سایبری، در بریتانیا و سطح بین‌المللی. ۲- انتقال دانش به دولت ها، جوامع و سازمان‌ها به‌منظور افزایش ظرفیت سایبری جهت کسب اطمینان و تحقق فضای سایبری که بتواند به رشد و نوآوری در حمایت از رفاه، حقوق بشر و شکوفایی برای همه ادامه دهد.	رهبران ملی را در مورد اقداماتی که باید برای محافظت از کشورهای خود که از نظر ارتباطات به صورت افزایشی در حال اتصال هستند و نیز ظرفیت رشد تولید ناخالص داخلی به وسیله ارزیابی هدفمند هر کشور از نظر بلوغ و الزام و تعهد به امنیت و انعطاف پذیری سایبری مطلع می‌نماید.	۱-برای اندازه‌گیری آماده‌گی کشورها برای جلوگیری از تهدیدات سایبری و مدیریت رویدادهای سایبری. ۲-ابزار سنجش امنیت سایبری که اطلاعات دقیق و به روز را در مورد امنیت سایبری ملی فراهم می‌کند. ۳-برنامه های مختلف برای تحلیل و توسعه امنیت سایبری ملی توسعه خواهند یافت
۷	ابعاد اصلی ارزیابی امنیت سایبری	۱-حقوقی و قانونی (۰/۲) ۲-سازمان‌دهی (۰/۲) ۳-ظرفیت‌سازی (۰/۲) ٤- فنی (۰/۲) ۵- همکاری (۰/۲)	۱-چارچوب قانونی، مقررات گذاری و نظارت ۲- ظرفیت‌سازی ۳-آگاهی‌رسانی ٤-قابلیت‌های فنی بومی ۵-واکنش به حوادث	۱-سیاست‌ها و ظرفیت‌های دفاع سایبری ۲-تاب‌آوری سایبری ۳-مقابله با جرائم سایبری ٤-حمایت از صنعت در زمینه امنیت سایبری ۵-امن‌سازی زیرساخت های اطلاعاتی حیاتی	۱-تدوین سیاست و راهبرد سایبری ۲-تشویق فرهنگ مسئولیت‌پذیری سایبری در جامعه ۳- ایجاد مهارت های سایبری در نیروی کار و کارفرمایان ٤-ایجاد چارچوب های مؤثر قانونی و نظارتی ۵-کنترل ریسک از طریق سازمان دهی، استانداردها و فناوری	۱-راهبرد ملی ۲-واکنش به حوادث سایبری ۳-جرائم الکترونیکی و الزامات قانونی ٤- به اشتراک‌گذاری اطلاعات ۵-سرمایه‌گذاری در تحقیقات و توسعه ٦-دیپلماسی و تجارت سایبری ۷-دفاع و پاسخ به بحران	۱-حکمرانی ۱-۱- ساختار سازمانی (۸) ۲-۱- قانون/مقررات (۷/۸) ۳-۱- تعاملات بین‌المللی (۷) ٤-۱- تیم واکنش به حوادث (۸) ۲-جرائم سایبری مالی (۷/۸) ۳-نیروی نظامی (٦/۸) ٤-اقتصاد و تجارت دیجیتال ٤-۱-گفتگوی دولت- مشاغل (۷/۸) ۲-٤- اقتصاد دیجیتال (۷/۷) ۵-تعامل اجتماعی ۵-۱- آگاهی عمومی (٦) ۳-۵- استفاده از اینترنت (۷)	۱- سیاست و خط‌مشی امنیت سایبری ۲- اطلاع‌رسانی تهدیدات سایبری ۳- آموزش و تربیت امنیت سایبری ٤- مشارکت در امنیت سایبری جهانی ۵- حمایت از خدمات دیجیتال ٦- حمایت از خدمات حیاتی ۷- شناسایی و اعتماد الکترونیکی ۸- محافظت از اطلاعات شخصی ۹- تیم واکنش به حوادث سایبری ۱۰- مدیریت بحران سایبری ۱۱- پلیس مبارزه با جرائم سایبری ۱۲- عملیات سایبری نظامی
۸	روش ارزیابی امنیت سایبری	۱- خوداظهاری برخط توسط نقاط تماس کشورها به تعداد ۵۰ سؤال مرتبط با ابعاد پنج‌گانه و ارزش گذاری شده توسط خبرگان که حداکثر ۵۰ درصد امتیاز یک کشور را تعیین می‌نماید. ۲- راستی آزمایی اقدامات کشورها توسط تیم ارزیاب، در رابطه با شاخص‌های ۲۵ گانه از طریق جمع‌آوری داده‌های مرتبط با کشورها، با هدف افزایش دقت ارزیابی. ۳- رتبه بندی کشورها و احصاء امتیاز کلی.	این مدل توصیه هایی را برای اجرای امنیت سایبری پیشنهاد و در قالب راهبرد ملی امنیت سایبری، اجرا می‌کند.	۱- تجزیه وتحلیل ۱۸ راهبرد ملی امنیت سایبری کشورهای عضو اتحادیه اروپا و هشت راهبرد غیر اتحادیه اروپا. ۲- تدوین و توصیف فهرستی از شاخص های کلیدی عملکرد مبنعث از راهبرد ملی امنیت سایبری کشورها. ۳- غلرسنجی با صاحب‌نظران در خصوص طبقه بندی، قابلیت اندازه گیری بودن، ارزش گذاری و ... شاخص‌ها ٤- بررسی کارکرد مدل ارزیابی در یک محیط عملیاتی واقعی و در عین حال با مقیاس کوچک جهت نهایی نمودن آن و احصاء نقصان و عیوب مربوطه.	۱- استفاده از محتـوای تولیدشـده در ارزیابی امنیت سایبری توسط سازمان های بین‌المللی (ITU، ENISA و ...). ۲- جمـع‌آوری اطلاعـات متعـدد از ذی‌نفعان متنوع. ۳- غنی‌سـنجی بـا صـاحب‌نظـران در خصوص طبقه بندی، قابلیت اندازه گیری بودن، ارزش گذاری و ... شاخص‌ها ٤- بررسی کارکرد مدل ارزیابی در یک محیط عملیاتی واقعی و در عین حال با مقیاس کوچک جهت نهایی نمودن آن و احصاء نقصان و عیوب مربوطه.	در این مدل ارزیابی، تعداد ۷۰ شاخص کلیدی عملکرد منبعث از ابعاد هفت‌گانه را به منظور اول اطلاع رسانی به رهبران ملی در مورد مراحلی که باید برای محافظت از کشورهای خود جهت دستیابی به بلوغ عینی و تاب آوری امنیت سایبری طی نمایند و دوم تعریف آماده‌گی امنیت سایبری یک کشور و مؤلفه‌های اصلی آن را به عنوان یک طرح عملی که می‌بایست توسط کشورها دنبال شود، مورد بررسی و ارائه قرار می‌دهد.	شاخص های عملکردی در این ارزیابی توسط تعدادی از خبرگان منطقه آسیا - اقیانوسیه و بر اساس جمع آوری اطلاعات باز تدوین گردیده است. هر کشور بر اساس ده عامل، رتبه بندی شده و نعرات کلی نسبت به به درصد بالاترین امتیاز ممکن اندازه‌گیری می‌شوند. (۱۰۰) بلوغ، در این گزارش، اجرای مؤثر و چهره‌برداری از ساختارها، خط مشی‌ها، قوانین و سازمان های مربوط به امنیت سایبری معرفی شده است و دارای بالاترین امتیاز است.	۱- شناسایی تهدیدات سایبری سطح ملی. ۲- شناسایی اقدامات و ظرفیت‌های امنیتی سایبری. ۳- انتخاب جنبه‌های مهم و قابل اندازه‌گیری. ٤- توسعه شاخص‌های امنیتی سایبری. ۵- گروه‌بندی شاخص‌های امنیت سایبری. ٦- امتیازدهی شاخص‌ها توسط خبرگان.
۹	شیوه رتبه‌بندی	کمی - کیفی (سه سطحی) (بالا، متوسط و پایین در مقیاس جهانی و منطقه‌ای)	-	کیفی سطح‌بندی کشورها بر مبنای بررسی شواهد	کیفی (۵ سطحی) (آغازین، شکل‌دهی شده، تأسیس‌شده، راهبردی و پویا)	کیفی (سه سطحی) شواهد ناکافی، تا حدی عملیاتی کاملاً عملیاتی	کمی (رتبه‌بندی هر کشور بر اساس ده بُعد ارزش‌گذاری شده)	کمی - کیفی (سه سطحی) (توسعه، تعامل و توسعه، بلوغ تعامل) همراه با کد‌گذاری رنگی
۱۰	رویکرد دفاعی/غیر دفاعی/ترکیبی	غیرنظامی	غیرنظامی	ترکیبی	غیرنظامی	ترکیبی	ترکیبی	ترکیبی

١٠. مطابق با مندرجات ردیف نهم جدول شماره ٦، از نظر نوع ارزش‌گذاری کمی/کیفی شاخص‌های ارزیابی امنیت سایبری، شاخص ارزیابی امنیت سایبری اتحادیه اروپا، مدل بلوغ امنیت سایبری دانشگاه آکسفورد و شاخص آمادگی سایبری مؤسسه پوتومک از نوع کیفی بوده و مدل چارچوب ارزیابی بلوغ سایبری در منطقه آسیا- اقیانوسیه از نوع کمی و مدل‌های اتحادیه بین‌المللی مخابرات و شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک از نوع کمی - کیفی می‌باشند. با توجه به اینکه شاخص‌های اتحادیه بین‌المللی مخابرات و آکادمی حکمرانی الکترونیک جدیدترین مدل‌های ارزیابی امنیت سایبری می‌باشند؛ بنابراین مزیت نسبی رویکرد ارزیابی کمی- کیفی نسبت به سایر رویکردها در مقوله ارزیابی امنیت سایبری در جدیدترین شاخص‌های ارزیابی ارائه‌شده مورد توجه قرار گرفته است.

١١. مطابق با مندرجات ردیف دهم جدول شماره ٦، از نظر رویکرد دفاعی/ غیردفاعی/ ترکیبی شاخص‌های ارزیابی امنیت سایبری، اتحادیه بین‌المللی مخابرات، سازمان مخابرات کشورهای مشترک‌المنافع و مدل بلوغ امنیت سایبری دانشگاه آکسفورد دارای رویکرد غیردفاعی هستند، اما شاخص ارزیابی امنیت سایبری اتحادیه اروپا، شاخص آمادگی سایبری مؤسسه پوتومک، چارچوب ارزیابی بلوغ سایبری در منطقه آسیا- اقیانوسیه و شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک دارای رویکرد ترکیبی به مقوله امنیت سایبری می‌باشند.

٤. نتیجه‌گیری

١- در تدوین سؤالات ارزیابی امنیت سایبری مؤسسات فوق، بر بهره‌گیری از دانش و تخصص طیف وسیعی از خبرگان با سلایق مختلف و حتی از مناطق جغرافیایی متفاوت تأکید شده است. همچنین بر مشارکت ذی‌نفعان مختلف در مراحل تدوین سؤالات، ارزش‌گذاری آن‌ها و درنهایت اعتبارسنجی آن‌ها در یک محیط عملیاتی محدود به‌منظور رفع نقایص احتمالی و افزایش کارایی آن‌ها تأکید ویژه‌ای به عمل آمده است.

۲. در مراحل ارزیابی امنیت سایبری، بر تعیین نقاط تماس در کشورها و ارتباط برخط با آن‌ها، خوداظهاری نمایندگان کشورها در پاسخ به سؤالات مطرح‌شده، بررسی و جمع‌آوری اطلاعات میدانی توسط ارزیابان جهت افزایش دقت ارزیابی و درنهایت رتبه‌بندی کشورها به‌عنوان فرایند ارزیابی معرفی شده است.

۳. در بخش عمده‌ای از این شاخص‌ها، اهداف، چشم‌انداز و بیانیه ارزش‌های راهبرد ملی امنیت سایبری کشورها به‌عنوان مبنای اصلی جهت ارزیابی امنیت سایبری در نظر گرفته شده است. بر این اساس قبل از پرداختن به موضوع ارزیابی امنیت سایبری می‌بایست اسناد بالادستی نظیر راهبرد یا دکترین امنیت سایبری، تدوین و به موازات یا پس از آن در خصوص تدوین چارچوب ارزیابی امنیت سایبری اقدام نمود.

٤. در اغلب این ارزیابی‌ها عنوان گردیده، برخی از شاخص‌های امنیت سایبری قابل اندازه‌گیری نیست یا اندازه‌گیری دقیق آن‌ها با مشکلاتی مواجه است. بر این اساس و به مرور زمان که روش‌های ارزیابی امنیت سایبری تکامل یافته‌اند، علاوه بر ارزیابی کمی، ارزیابی کیفی نیز به‌منظور افزایش دقت نتایج ارزیابی استفاده شده است. بر این اساس روش‌های ارزیابی کمی- کیفی ابعاد و مؤلفه‌های امنیت سایبری، از دقت بالایی برخوردار می‌باشند. همچنین از کدگذاری رنگی جهت ارائه تصویری کلی و سریع از وضعیت امنیت سایبری کشورها به‌منظور تصمیم‌گیری و ارائه اطلاعات مدیریتی استفاده شده است.

۵. با بررسی اجمالی شاخص‌های ارزیابی امنیت سایبری معرفی‌شده، درمی‌یابیم که ابعاد ارائه‌شده توسط اتحادیه بین‌المللی مخابرات، با توجه به ویژگی‌هایی نظیر پوشش‌دهی طیف وسیعی از کشورها، دارا بودن نظام ارزیابی شفاف، تجربه‌شده و ممتاز، مورد توافق اغلب سازمان‌های ارائه‌دهنده شاخص‌های ارزیابی امنیت سایبری یادشده است و عمده تفاوت آن‌ها در ملحوظ نمودن بُعد نظامی امنیت سایبری است که این موضوع با توجه به ماهیت و مأموریت محول‌شده از سوی سازمان ملل متحد به اتحادیه بین‌المللی مخابرات قابل توجیه است.

بی‌شک توانایی نیروهای مسلح و سازمان‌های دفاعی آن برای مصون‌سازی کشور از تهدیدات ناشی از فضای مجازی امری لازم و ضروری بوده و اغلب کشورها نیروهای دفاعی خود را برای ایجاد ظرفیت یا تخصص برای پاسخگویی به تهدیدهای سایبری که به سطح درگیری‌های «سایبری» در سطح ملی منتهی می‌شوند، هدایت می‌کنند.

۶. تجربه چهار دهه اخیر نشان می‌دهد که جمهوری اسلامی ایران به‌واسطه موقعیت ممتاز ژئوپلیتیکی و نیز مختصات سیاسی و ایدئولوژیکی انقلاب اسلامی و نظام سیاسی آن، با طیف وسیعی از تهدیدهای سخت و نرم مواجه بوده (سیاست دفاعی نظام جمهوری اسلامی ایران-۱۳۹۵) و در این راستا تهدیدات سایبری به‌عنوان یکی از مهم‌ترین تهدیدات حال حاضر برای زیرساخت‌های حیاتی، امنیتی و دفاعی کشور محسوب می‌شود؛ بنابراین ارزیابی امنیت سایبری مستلزم به‌کارگیری ابعاد و مؤلفه‌هایی متناسب با زیست‌بوم این فناوری‌ها در کشور و تهدیدات مرتبط با آن است.

پیشنهاد

با توجه به ارائه شاخص‌های ارزیابی امنیت سایبری مطرح‌شده که در این مقاله به آن‌ها اشاره شد، شایسته است:

۱. با استفاده از نتایج این پژوهش و با بهره‌گیری از یافته‌های مطالعه تطبیقی انجام‌شده و سایر اطلاعات و تجارب موجود در این حوزه، تدوین الگوی ارزیابی امنیت سایبری متناسب با زیست‌بوم این فناوری در پاسخ به اهمیت و ضرورت ارتقاء امنیت سایبری کشور در دستور کار قرار گیرد.

۲. بی‌شک فناوری‌های نوظهور فضای مجازی و امنیت سایبری، جزء فناوری‌های پیچیده بوده و در عین حال سطح دانش عمومی جامعه در این حوزه نیازمند فرهنگ‌سازی، آموزش، ارتقاء مهارت‌ها و ... است. شناسایی ابعاد و مؤلفه‌های امنیت سایبری باعث می‌گردد ضمن تبیین و افزایش آگاهی عمومی امنیت سایبری در کشور، راهکارهای لازم به‌منظور ارتقاء امنیت سایبری در کشور احصاء گردیده و درنهایت

منجر به ارتقاء جایگاه حاکمیتی کشور در رتبه‌بندی سازمان‌های جهانی و منطقه‌ای گردد.

۳. با ایجاد مراکز علمی و فناوری با مشارکت ذی‌نفعان مختلف و انجام تحقیقات در حوزه امنیت سایبری و تحلیل نتایج ارزیابی آن، نسبت به ارتقاء تاب‌آوری سایبری جمهوری اسلامی ایران اقدام لازم صورت پذیرد.

٤. در تحقیقات آتی مرتبط با موضوع این پژوهش، پرداختن به شاخص‌های ارزیابی امنیت سایبری حوزه دفاعی و نیز پژوهش در مبانی نظری، اندیشه‌ها و تئوری‌های شکل‌گیری و تدوین شاخص‌های ارزیابی امنیت سایبری می‌تواند افق وسیع‌تری در ادامه این پژوهش بگشاید.

فهرست منابع ومآخذ

الف. منابع فارسی

- فرامرز قراملکی، احد، روش‌شناسی مطالعات دینی، (۱۳۹۵)، دانشگاه علوم اسلامی رضوی.
- کمیته دائمی پدافند غیرعامل کشور، (۱۳۹٤)، سند راهبردی پدافند سایبری کشور.
- مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، (۱۳۹۵)، راهنمای تدوین راهبرد ملی امنیت سایبری.
- انتظامی، حسین، (۱۳۹۲)، افق فناوری اطلاعات و ارتباطات در نگاه امنیت ملی، دانشگاه عالی دفاع ملی، تهران.
- شهیر، احسان، (۱۳۹٦)، طراحی الگوی راهبردی بومی امنیت فضای مجازی کشور، رساله دکتری دانشگاه عالی دفاع ملی.
- محمودزاده، ابراهیم و اسماعیلی، علی، (۱۳۹۷)، الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح، فصلنامه امنیت ملی، سال هشتم، شماره سی‌ام، زمستان، دانشگاه عالی دفاع ملی، تهران.
- عالی‌پور، حسن، (۱۳۹۳)، امنیت سایبری در افق ۱٤۰٤ (چالش‌ها و راهکارهای حقوقی رویارویی با بزه‌های امنیتی سایبری)، تهران، همایش ملی دفاع سایبری.
- تقی‌پور، رضا و اسماعیلی، علی، (۱۳۹۷)، طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران، فصلنامه امنیت ملی، دانشگاه عالی دفاع ملی، تهران.
- سیاست‌های کلی نظام در بخش «امنیت فضای تولید و تبادل اطلاعات».
- حکم انتصاب اعضای جدید شورای عالی فضای مجازی،۱٤ شهریور (۱۳۹٤).
- اهداف و سیاست‌های مرکز ملی فضای مجازی،۱۰ تیر (۱۳۹۵).

ب. منابع انگلیسی

- International Telecommunication Union, Global Cybersecurity Index 2018,2019
- Commonwealth Telecommunications Organisation (Cto), Commonwealth Approach for Developing National Cybersecurity Strategies,2015
- European Union Agency for Network and Information Security, An evaluation Framework for National Cyber Security Strategies,2014
- Global Cyber Security Capacity Centre University of Oxford, Cyber Security Capability Maturity Model (CMM) – V1.2,2014
- Potomac Institute for Policy Studies, CYBER READINESS INDEX 2.0,2015
- Australian Strategic Policy Institute (Aspi), Creating an Asia–Pacific Cyber Maturity Metric,2017
- e-Governance Academy, National Cyber Security Index 2018,2018