فصلنامه علمی امنیت ملی
سال دوازدهم، شماره چهل‌وپنجم، پاییز ۱۴۰۱
مقاله سوم از صفحات ۱۰۰-۶۹

مقاله پژوهشی: ارائهٔ مدلی برای ارزیابی امنیت سایبری جمهوری اسلامی ایران

۲۰.۱۰۰۱.۱.۳۳۲۹۲۵۳۸.۱۴۰۱.۱۲.۴۵.۳.۶

محمدرضا کریمی قهرودی [۱]، حافظ محمدی [۲] و امیر مسعود سعادتمند [۳]

تاریخ دریافت: ۱۳۹۹/۰۸/۰۶ **تاریخ پذیرش: ۱۴۰۰/۰۳/۲۹**

چکیده

موقعیت راهبردی جمهوری اسلامی ایران در منطقه و نظام بین‌الملل و ناکامی نظام سلطه در عرصهٔ تهدیدهای سخت و هزینه‌بر بودن آن موجب تغییر راهبرد دشمنان نظام اسلامی و استفاده از ظرفیت‌های موجود در فضای سایبری

به‌منظور تقابل با جمهوری اسلامی ایران گردیده است. 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 کشورها در حوزه‌های مختلف شده و با برنامه‌ریزی و ارایهٔ راهبردهای لازم در نهایت موجب ارتقاء آن می‌گردد؛ در همین راستا هدف این پژوهش دستیابی به مدل بومی ارزیابی امنیت سایبری جمهوری اسلامی ایران است؛ بر این اساس با استناد به فرامین و تدابیر مقام معظم رهبری، اسناد بالادستی در حوزهٔ سایبر و اسناد مؤسسات جهانی و با به‌کارگیری فن خوشه‌بندی در تحلیل محتوا و روش دلفی، پنج مفهوم حکمرانی، حقوقی و قانونی، توانمندسازها و ظرفیت‌سازی، دفاعی- امنیتی و اجتماعی-فرهنگی به‌عنوان ابعاد اساسی مدل ارزیابی امنیت سایبری مورد شناسایی قرار گرفتند؛ سپس مؤلفه‌ها و ذی‌نفعان هر یک از این ابعاد استخراج شدند و در نهایت مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران پس از تأیید خبرگان حوزهٔ سایبر ارایه گردید.

کلیدواژه‌ها: **امنیت سایبری، ارزیابی امنیت سایبری، روش دلفی، فضای سایبری، مدل**

۱. عضو هیئت علمی دانشگاه صنعتی مالک اشتر، m.karimi@sndu.ac.ir
۲. دانشجوی دکتری مدیریت راهبردی فضای سایبر، (نویسندهٔ مسئول)، hafez.mohammadi@sndu.ac.ir
۳. دانشجوی دکتری مدیریت راهبردی فضای سایبر، s.saadatmand@sndu.ac.ir

مقدمه

فضای سایبر به‌عنوان پدیده‌ای نوظهور در زندگی بشر، محصول عملکرد شبکهٔ جهانی اینترنت است که امکان گردآوری، تمرکز، جابجایی، 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، امنیت سایبری، توسعهٔ دانش مربوط به ارزیابی امنیت سایبری در این عرصه را دو چندان نموده است.

با آغاز هزارهٔ سوم، فضای سایبر رشد فزاینده‌ای داشته و این رشد در عرصه‌های مختلف زندگی انسان‌ها تأثیرات غیرقابل انکاری بر جای گذاشته است. با توسعهٔ 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 و ارزیابی منظم و مستمر آن، روز به روز بیشتر احساس می‌شود.

امروزه بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور در کلیهٔ سطوح در فضای سایبر انجام می‌گیرد؛ زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور یا خود بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا کنترل، مدیریت و بهره‌برداری می‌شوند و عمدهٔ اطلاعات حیاتی و حساس کشور نیز به این فضا منتقل و یا اساساً در این فضا شکل گرفته است. عمدهٔ فعالیت‌های رسانه‌ای به این فضا منتقل شده، بیشتر مبادلات مالی از طریق این فضا انجام می‌گیرد و نسبت قابل توجهی از وقت و فعالیت‌های شهروندان صرف تعامل در این حوزه می‌گردد؛ سهم درآمدهای حاصل از کسب و کارهای فضای سایبر در تولید ناخالص ملی افزایش چشمگیر یافته و از میان شاخص‌های تعیین شده برای سنجش میزان توسعه‌یافتگی کشور، شاخص‌های حوزهٔ سایبر، سهم عمده‌ای را به خود اختصاص داده‌اند. بخش قابل توجهی از سرمایه‌های مادی و معنوی کشور صرف این حوزه شده و بخش قابل توجهی از درآمدهای مادی و اکتسابات معنوی شهروندان نیز از این حوزه کسب شده یا تأثیر عمده می‌پذیرد؛ به

عبارت دیگر وجوه مختلف زندگی شهروندان به معنای واقعی با این فضا درآمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، مستقیماً وجوه مختلف زندگی شهروندان را متأثر خواهد نمود (سند راهبردی پدافند سایبری کشور، سازمان پدافند غیر عامل کشور).

بیش از نیمی از جمعیت جهان در حال حاضر برخط هستند؛ مطابق پیش‌بینی ITU[1]، تا سال ۲۰۲۳، ۷۰ درصد نفوذ اینترنت در دنیا وجود خواهد داشت و این امر نیاز به فضای سایبر ایمن‌تر را افزایش می‌دهد (شاخص جهانی امنیت سایبری، ۶،۲۰۱۹).

با توجه به توسعهٔ فناوری اطلاعات و ارتباطات و فراگیرشدن فناوری‌های نوظهور در فضای سایبر و افزایش تعداد کاربران آن می‌توان گفت مهم‌ترین چالش فضای سایبر امروزه موضوع امنیت این فضاست؛ با توجه به افزایش روزافزون جرایم سایبری و نقض امنیت داده‌ها در این فضا، هنوز یک شکاف آشکار بین بسیاری از کشورها از نظر دانش برای اجرای قانون جرایم رایانه‌ای، راهبردهای ملی امنیت سایبری، تیم‌های واکنش سریع رایانه-ای، آگاهی و ظرفیت برای گسترش راهبردها، توانایی‌ها و برنامه‌ها در حوزهٔ امنیت سایبری وجود دارد؛ توسعهٔ پایدار در این حوزه باید از استفادهٔ ایمن و مناسب از فناوری اطلاعات و ارتباطات متناسب با رشد اقتصادی اطمینان حاصل کند.

مروری بر وقایع و حوادث سال‌های اخیر کشور، مؤید این واقعیت است که بخش عمده‌ای از تهدیدهای موجود علیه کشور، به‌ویژه در زیرساخت‌های حیاتی، یا مستقیماً از فضای سایبر نشأت می‌گیرند و یا این فضا را هدف تهدید مستقیم خود قرار می‌دهند؛ بنابراین با توجه به آسیب‌پذیری‌های ذاتی موجود در فضای سایبری و روند رو به رشد مهاجرت از دنیای سنتی به این فضا، ریسک سامانه‌های مبتنی بر فناوری اطلاعات، که برای اقتصاد کشور حیاتی می باشند را، افزایش می‌دهد و پیچیدگی روزافزون و رو به ازدیاد سامانه‌ها و شبکه‌های مبتنی بر فناوری اطلاعات چالش‌های امنیتی را برای کشور در بر دارد (سند راهبردی پدافند سایبری کشور، سازمان پدافند غیر عامل). بررسی‌ها نشان می‌دهد بین رشد و توسعهٔ فناوری اطلاعات و ارتباطات و امنیت

---

۱. International Telecommunication Union

رابطهٔ معنی‌داری وجود دارد (انتظامی،۱۳۹۲:۱۹۷). فضای سایبری در معرض چالش‌ها، آسیب‌ها و تهدیدات الکترونیکی گوناگونی نظیر ارتکاب جرایم سازمان‌یافته، تخریب بانک‌های اطلاعاتی، حملات مختل‌کننده خدمات، جاسوسی، خرابکاری، نقض حریم خصوصی و نقض حقوق مالکیت معنوی قراردارد؛ به‌طوری‌که نپرداختن یا رویکرد نادرست به امنیت این فضا و ارزیابی مستمر آن، مانع بزرگ کاربرد امن فناوری ارتباطات و اطلاعات و ورود به جامعهٔ اطلاعاتی خواهد بود. امنیت فضای تبادل اطلاعات برقراری شرایط و حالتی است که دارایی‌های این فضا از خطرات و تهدیدات مختلف محفوظ بماند و بیم و دغدغه نسبت به تهدید سایر دارایی‌های مادی و معنوی جامعه از این طریق نیز وجود نداشته باشد؛ بر این اساس امنیت فضای تبادل اطلاعات و ایجاد نظام کارآمد امنیت فضای سایبری و ارزیابی مستمر آن در کشور فراتر از فعالیت‌های اجرایی یک یا چند دستگاه است و نیازمند مشارکت همهٔ بخش‌های حاکمیتی و اجرایی کشور، بخش‌های غیردولتی و همچنین آحاد شهروندان جامعه است که این امر خطیر با دستیابی به یک نظام جامع امنیت سایبری و مدل ارزیابی آن قابل تحقق است.

بیان مسئله

تهدیدات سایبری از ماهیتی متنوع، گسترده و منحصربه‌فرد برخوردارند. متنوع از آن‌رو که این تهدیدات تمام حوزه‌های زندگی بشر را تحت‌تأثیر قرار داده‌اند و در نتیجه فقدان امنیت در فضای سایبری بسیار بالاست؛ طبیعتاً امنیت در فضای سایبر یکی از مؤلفه‌های اصلی امنیت ملی کشور است (ملائی، ۱۳۹۷). حملات مخرب مهم با تأثیرات گسترده، تهدیدهای سایبری را به‌عنوان یکی از بدترین تهدیدهای منافع ملی به تصویر کشیده است تا جایی‌که ایالات متحدهٔ آمریکا اعلام کرده است که این حملات را به‌عنوان جنگ تلقی کرده و با آن برخورد فیزیکی خواهد کرد (خلیلی‌پور رکن‌آبادی، ۱۳۹۱).

جایگاه خاص جمهوری اسلامی ایران در ترتیبات منطقه‌ای و نظام بین‌الملل سبب شده تا نظام سلطه از فضای سایبری برای تحدید قدرت ملی به شکل فزاینده‌ای بهره‌برداری

نماید؛ در این میان به‌منظور ایجاد سازوکار مناسب برای تضمین امنیت و منافع ملی در این فضا، شناخت ابعاد مختلف این مسئله به دغدغهٔ بسیاری از صاحبنظران این حوزه تبدیل شده است (تقی‌پور و اسماعیلی، ۱۳۹۷)؛ به عبارت دیگر فضای سایبر به شدت 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 در نهایت 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. (راهنمای تدوین راهبرد ملی امنیت سایبری، ۱۳۹۵: ۱۱)

برای ارزیابی صحیح امنیت در فضای سایبری لازم است که یک چارچوب برای امنیت سایبری وجود داشته باشد؛ چنین چارچوبی شامل مجموعهٔ فعالیت‌های اصلی بخش دولتی و خصوصی برای تضمین سطح قابل قبولی از امنیت سایبری است؛ امنیت فضای سایبر ملی، نه یک هدف نهایی؛ بلکه به‌عنوان ابزاری برای دستیابی به مؤلفه‌های ملی 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 پتانسیل‌های 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 شده تا با برنامه‌ریزی‌های کوتاه‌مدت و بلندمدت نسبت به ارتقاء امنیت سایبری اقدام نمایند؛ در همین راستا جمهوری اسلامی ایران نیز، با توجه به تقابل دائمی آن با نظام سلطه و ضرورت حفاظت و صیانت از فضای مجازی کشور نیازمند یک مدل بومی برای ارزیابی امنیت سایبری خود متناسب با این مقتضیات می‌باشد؛ نظر به اینکه مدل مفهومی ارزیابی امنیت سایبری در کشور طراحی نگردیده و از سویی چیستی و ارتباط میان ابعاد و

مؤلفه‌های تشکیل دهندهٔ آن مشخص نیست؛ می‌بایست نسبت به تعریف و طراحی این مدل مفهومی اقدام لازم صورت پذیرد. الگوی مفهومی موصوف از بایسته‌های سازمان معنایی نظام امنیت سایبری کشور خواهد بود.

اهمیت تحقیق: ارایهٔ مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران و اجرای آن موجب رصد و پایش مستمر امنیت در فضای سایبر کشور شده و در نهایت منجر به ارتقاء امنیت این فضا خواهد شد؛ ضمن اینکه ابزار و راهنمایی مناسب برای مدیریت و سیاست‌گذاری در حوزهٔ امنیت فضای سایبر کشور بوده و زمینهٔ همدلی و وفاق در حوزهٔ امنیت فضای مجازی کشور از طریق ایجاد گفتمان و تعاریف مشترک را به وجود خواهد آورد؛ طراحی این الگوی ارزیابی با استفاده از روش علمی دقیق، می‌تواند باعث جلوگیری از اعمال سلایق شخصی و تصمیمات غیرکارشناسی در این حوزه گردد.

ضرورت تحقیق: فقدان مدل بومی ارزیابی امنیت سایبری در کشور با توجه به رشد فزایندهٔ تهدیدات سایبری در فضای مجازی منجر به عدم وجود معیارهای مشخص سنجش امنیت در فضای مجازی کشور، اجرایی‌نشدن سیاست‌های کلان در حوزهٔ امنیت فضای مجازی کشور و عدم ارتقاء امنیت سایبری خواهد گردید.

بدیع بودن این تحقیق در قالب ارایهٔ مدل برای نخستین بار در حوزهٔ ارزیابی امنیت فضای سایبر کشور با بهره‌گیری از گفتمان مقام معظم رهبری (مدظله‌العالی) و اسناد بالادستی و استفاده از تجربیات مؤسسات جهانی در زمینهٔ الگوی ارزیابی امنیت سایبری با در نظر گرفتن مقتضیات فضای مجازی و زیست‌بوم سایبری کشور، دارای اهمیت به‌سزایی است و از آنجا که تاکنون در خصوص طراحی و ارایهٔ مدل ارزیابی در این حوزه اقدامی نشده است، انجام این تحقیق ضرورت دارد.

هدف اصلی، دستیابی به مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران و **هدف فرعی**، دستیابی به ابعاد، مؤلفه‌ها و ذی‌نفعان مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران می‌باشد.

سؤال اصلی، مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران کدام است؟

سؤال فرعی، ابعاد و مؤلفه‌ها و ذی‌نفعان مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران کدامند؟

پیشینهٔ پژوهش

با توجه به موضوع تحقیق، بررسی‌های مختلفی بر روی پژوهش‌های علمی مرتبط با موضوع تحقیق صورت پذیرفت که در زیر به برخی از مهم‌ترین موضوعات که در مؤلفه‌ها و متغیرهایی با موضوع تحقیق مشترک هستند؛ اشاره شده است.

در سال ۱۳۹۶ رساله‌ای با عنوان «طراحی الگوی راهبردی بومی امنیت فضای مجازی کشور» توسط احسان شهیر در دانشگاه عالی دفاع ملی انجام گرفت که در این رساله مدل مفهومی راهبردی بومی امنیت فضای مجازی کشور برگرفته از چهار بعد اصلی (حوزهٔ تأمین‌کنندگان و عوامل عملیاتی امنیت فضای مجازی، بستر، آسیب پذیری‌های امنیت فضای مجازی، روش، تاروپود، رویکرد بومی‌سازی، ارزش‌ها و اهداف، کنترل و فرماندهی) به دست آمده است: (شهیر،۱۳۹۶)

مقاله‌ای با عنوان «الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح» در سال ۱۳۹۷، توسط محمودزاده و همکاران ارایه شد که نتایج این تحقیق نشان می‌دهد که الگوی راهبردی صیانت امنیتی، دارای ۳ بعد و ۱۱ مؤلفه است که ابعاد ارایه شده شامل اهداف امنیتی، اقدامات و راهکارهای صیانت و عوامل اصلی فضای سایبر نیروهای مسلح می‌باشند.

نصرت‌آبادی و همکاران مقاله‌ای با عنوان «ارایهٔ الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران» در سال ۱۳۹۸، ارایه نمودند که نتایج این تحقیق نشان می‌دهد که الگوی راهبردی ارزیابی قدرت سایبری، دارای ۳ بعد است که ابعاد ارایه شده شامل آفند، پدافند و تاب‌آوری می‌باشند.

مقاله‌ای با عنوان «الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران» توسط تقی‌پور و همکاران در سال ۱۳۹۷، ارایه شد که نتایج این

تحقیق نشان می‌دهد که الگوی راهبردی صیانت امنیتی، دارای چهار بعد و هجده مؤلفه است که ابعاد ارایه شده شامل حکمروایی، حقوقی و مدیریت امنیت و عملیات می‌باشند.

«طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران» عنوان مقاله‌ای بود که در سال ۱۳۹۷ توسط تقی‌پور و همکاران ارایه شد که نتایج این تحقیق نشان می‌دهد که الگوی ارایه شده دارای ابعاد قابلیت بازدارندگی، قابلیت پدافند و قابلیت برگشت‌پذیری می‌باشند.

در سال ۱۳۹۸ مقاله‌ای با عنوان «ارائهٔ الگوی راهبردی ارزیابی شبکهٔ ملی اطلاعات» توسط نصرت‌آبادی و همکاران ارایه شد که نتایج این تحقیق نشان می‌دهد که الگوی ارایه شده دارای ابعاد امنیتی، فناورانه و مدیریتی می‌باشد.

علاوه بر موارد یاد شده و در راستای استفاده از تجارب سایر کشورها در تدوین شاخص‌های ارزیابی امنیت سایبری، اسناد مرتبط با این موضوع در قالب مقاله‌ای علمی پژوهشی با عنوان مطالعهٔ تطبیقی شاخص‌های ارزیابی امنیت سایبری توسط محققین این پژوهش مورد بررسی قرار گرفته که در ادامه به ارایهٔ نتایج این تحقیق در بخش مبانی و مفاهیم نظری خواهیم پرداخت.

مبانی و مفاهیم نظری تحقیق

در این تحقیق جدیدترین الگوهای ارزیابی امنیت سایبری در سطح منطقه و جهان مورد بررسی قرار گرفته و هفت نمونه از آن‌ها منتخب گردیدند؛ مهم‌ترین شاخص‌های ارزیابی امنیت سایبری منتخب در این تحقیق عبارتند از:

۱. شاخص جهانی ارزیابی امنیت سایبری اتحادیهٔ بین‌المللی مخابرات (ITU)

شاخص جهانی امنیت سایبری (GCI[۱])، یک شاخص مرکب است که توسط اتحادیهٔ بین‌المللی مخابرات، تولید، تحلیل و منتشر شده و از آن به‌منظور سنجش تعهد کشورهای

۱. Global Index Cybersecurity

عضو اتحادیهٔ بین‌المللی ارتباطات به امنیت سایبری و افـزایش آگـاهی عمـومی نسـبت بـه امنیت سایبری استفاده می‌شود؛ پایـه و اسـاس ایـن ارزیـابی، دسـتور کـار امنیـت سـایبری جهانی(GCA) اتحادیهٔ بین‌المللی مخابرات است که در سال ۲۰۰۷ منتشر شـد و دارای پـنج رکن اصلی شامل: اقدامات قانونی، فنی، سازمان‌دهی، ظرفیت‌سـازی و همکـاری مـی‌باشـد؛ درواقع شاخص جهانی امنیت سایبری، میزان تعهد ۱۹۴ کشور عضو سازمان ملل متحـد (از جمله کشور فلسطین) به ابعاد عنوان شده را مورد نظارت و ارزیابی قرار داده و گـزارش آن را به‌صورت سالیانه منتشر می‌کند؛ ابعاد اصلی شاخص جهانی امنیت سایبری بر پـنج رکـن تمرکز دارد که اساس

شاخص‌های جهانی امنیت سایبری اتحادیهٔ بین‌المللـی مخـابرات را تشـکیل مـی‌دهنـد. جدول شمارهٔ ۲۵،۲ شاخص جهانی ارزیابی امنیت سایبری اتحادیهٔ بین‌المللـی مخـابرات در سال ۲۰۱۸ بر مبنای ۵ ستون دستور کار امنیت سایبری جهانی را ارایـه مـی‌نمایـد. (شـاخص جهانی امنیت سایبری، ۲۰۱۹)

جدول شمارهٔ۱: شاخص جهانی امنیت سایبری اتحادیهٔ بین‌المللی مخابرات در سال ۲۰۱۸

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 زمینهٔ امنیت سایبری
اقدامات فنی	تیم واکنش به حوادث سایبری		برنامه‌های ملی آموزش و دروس دانشگاهی
	چارچوب استانداردهای امنیت سایبری		برنامه‌های تحقیق و توسعهٔ امنیت سایبری
	استانداردسازی		راهکارهای تشویقی
	مکانیسم‌های فنی و پرداختن به اسپم		صنعت امنیت سایبری در حال رشد
	استفاده از فناوری ابر در امنیت سایبری	همکاری	توافق‌نامه‌های امنیت سایبری دو جانبه
	مکانیسم‌های محافظت از کودکان برخط		توافق‌های امنیت سایبری چند جانبه
سازماندهی	راهبرد ملی امنیت سایبری		مشارکت در سازمان‌ها و انجمن‌های بین‌المللی
	ادارهٔ مسئول و پاسخگو		مشارکت و همکاری بخش عمومی و خصوصی
	معیارهای امنیت سایبری		مشارکت‌های درون و بین‌سازمانی
			استفاده از بهترین تجربیات در امنیت سایبری

۱ Global Cybersecurity Agenda

۲. شاخص ارزیابی امنیت سایبری اتحادیهٔ اروپا

شاخص ارزیابی امنیت سایبری اتحادیهٔ اروپا، توسط ادارهٔ امنیت شبکه و اطلاعات اتحادیهٔ اروپا[۱] ارایه گردیده است؛ این اداره مرکز تخصصی امنیت شبکه و اطلاعات این اتحادیه است که توصیه‌هایی را در مورد عملکرد مناسب در زمینهٔ امنیت اطلاعات ارائه می‌دهد تا کشورهای عضو در اجرای قوانین مربوطه و بهبود تاب‌آوری زیرساخت‌ها و شبکه‌های مهم اطلاعاتی فعالیت نمایند (شاخص ارزیابی امنیت سایبری اتحادیهٔ اروپا،۲۰۱۴).

جدول ۲: شاخص‌های ارزیابی امنیت سایبری اتحادیهٔ اروپا

ابعاد	مولفه ها
سیاست دفاعی و قابلیت‌های سایبری	اختصاص یک برنامهٔ ملی راهبردی برای دفاع سایبری (دکترین، مفاهیم، ذی‌نفعان، مسئولیت‌های خاص)
	میزان مشارکت کشور در ابتکارات اتحادیهٔ اروپا (ایجاد توانمندی)
	شناسایی و ایجاد گروه واکنش به حوادث سایبری نظامی
	وجود آموزش (بر اساس نیاز کارکنان) و ارزیابی میزان اثربخشی آن
	قابلیت‌های همکاری
	افزایش تاب‌آوری از طریق همکاری و به‌کارگیری فناوری‌ها جهت مقابله با حملات سایبری نظامی
تاب‌آوری سایبری	راه‌اندازی تیم‌های واکنش به حوادث سایبری و یا سازمان‌های امنیت ملی
	وجود یا راه‌اندازی مشارکت‌های خصوصی- عمومی در امنیت سایبری
	شناسایی چشم‌انداز ریسک‌ها و تهدیدات
	وجود مأموریت‌های سازمان ملی امنیت سایبری
	افزایش توانمندی‌ها: آموزش‌های سازمان‌یافته برای بخش عمومی و خصوصی، فعالیت‌های یادگیری متقابل
	فعالیت‌های آگاهی‌رسانی برای کاربران نهایی (محتوی، کمپین‌ها، رویدادها)
	هماهنگی ملی در میان همهٔ فعالان ملی عرصهٔ امنیت سایبری (ادارات امنیت ملی)
	افزایش توانایی پاسخ‌گویی (طرح‌های بهبود واکنش، سامانه‌های هشداردهنده اولیه و غیره)
جرایم سایبری	چارچوب سازمانی ملی برای کاهش جرائم سایبری
	تجزیه و تحلیل خلاءها، شناسایی نیازها، دارایی‌های فنی، استفاده از بهترین شیوه‌ها
	وجود سازوکارهای همکاری با سازمان‌های بین‌المللی
	قطعنامه‌های مربوط به موارد جرایم سایبری
	همکاری‌های بین‌المللی
	فضای امن‌تر برای همهٔ کاربران

۱. European Union Agency for Network and Information Security(ENISA)

ابعاد	مولفه ها
صنعت و فناوری امنیت سایبری	پشتیبانی از استانداردسازی و توسعهٔ برچسب‌های اعتماد و ایمنی
	حمایت مالی از طریق برنامه‌های تحقیقاتی ملی و اتحادیهٔ اروپا
	در حال توسعهٔ اقدامات جدید در مورد تقاضای ملی در سطح ملی
	نوآوری در تجارت الکترونیک و اثربخشی هزینه
	دسترسی بیشتر مصرف‌کنندگان به تکنولوژی امن
زیرساخت‌های اطلاعاتی حیاتی	شناسایی زیرساخت‌های اطلاعات بحرانی یعنی دارایی‌های بحرانی، آسیب‌پذیری‌ها، وابستگی‌ها و خطرات
	ارزیابی ریسک و رویه‌های مدیریت ریسک/ طرح‌ها
	راه‌اندازی گزارش‌دهی حوادث و روش اطلاع‌رسانی نقض
	طراحی و پیاده‌سازی ابزارها
	بازیابی فرایندها و برنامه‌ها برای زیرساخت‌های حیاتی
	به اشتراک‌گذاری اطلاعات موفقیت‌آمیز و همکاری قابل اعتماد بین فعالان مختلف
	پاسخ سریع‌تر و کارآمدتر در صورت وقوع حادثه در سطح ملی
	شفافیت و پاسخگویی سامانه‌ها
عمومی	ارزیابی راهبرد ملی امنیت سایبری در سطح برنامه
	ارزیابی اجرایی
	تعهدات قانونی بین‌المللی و ملی
	بودجه
	همکاری با توجه به هنجارهای مشترک در فضای مجازی؛ حمایت از ارزش‌های مشترک در فضای مجازی

۳. مدل بلوغ امنیت سایبری دانشگاه آکسفورد[۱]

این مدل توسط دانشگاه آکسفورد در سال ۲۰۱۴ ارایه شده و اهداف آن توسعهٔ 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 تحقق فضای سایبری که بتواند به رشد و نوآوری در حمایت از رفاه، حقوق بشر و شکوفایی برای همه ادامه دهد؛ ابعاد این مدل به‌شرح جدول ذیل می‌باشد.

۱. Cyber Security Capability Maturity Model (CMM)

جدول۳: شاخص‌های مدل بلوغ امنیت سایبری دانشگاه آکسفورد

ردیف	ابعاد	مؤلفه‌ها
۱	سیاست و راهبرد امنیت سایبری	راهبرد ملی امنیت سایبری
۲		پاسخ به حوادث
۳		حفاظت از زیرساخت‌های حیاتی
۴		مدیریت بحران
۵		دفاع سایبری
۶		افزونگی ارتباطات
۷	جامعه و فرهنگ	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	امنیت سایبری، تربیت، آموزش و مهارت-آموزی	افزایش آگاهی
۱۳		چارچوبی برای تربیت امنیت سایبری
۱۴		چارچوب آموزش حرفه‌ای
۱۵	چارچوب‌های قانونی و نظارتی	چارچوب‌های قانونی
۱۶		سیستم عدالت کیفری
۱۷		چارچوب‌های همکاری رسمی و غیررسمی برای مبارزه با جرایم سایبری
۱۸	استانداردها، سازمان‌ها و فن‌آوری‌ها	پیروی از استانداردها
۱۹		تاب‌آوری زیرساخت‌های اینترنت
۲۰		کیفیت نرم افزار
۲۱		کنترل‌های امنیتی فنی
۲۲		کنترل‌های رمزنگاری
۲۳		بازار امنیت سایبری

این مدل، ارزیابی امنیت سایبری را در پنج سطح کیفی بلوغ شامل سطوح آغازین، شکل‌دهی شده، تأسیس شده، راهبردی و پویا رتبه‌بندی می‌کند (مدل بلوغ توانمندی امنیت سایبری،۲۰۱۴).

۴. شاخص آمادگی سایبری مؤسسهٔ پوتومک[۱]

این شاخص توسط مؤسسهٔ مطالعات سیاسی پوتومک[۲] در سال ۲۰۱۵ ارایه 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 عبارتند از:

جدول ۴: شاخص‌های آمادگی سایبری مؤسسهٔ پوتومک

ردیف	ابعاد	ردیف	ابعاد
۱	راهبرد ملی	۵	سرمایه‌گذاری در تحقیقات و توسعه
۲	واکنش به حوادث	۶	دیپلماسی و تجارت
۳	جرایم الکترونیکی و الزامات قانونی	۷	دفاع و پاسخ بحران
۴	به اشتراک‌گذاری اطلاعات	شاخص آمادگی سایبری-۲۰۱۵- مؤسسهٔ پوتومک	

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 مؤسسهٔ پوتومک، ۲۰۱۵).

۵. چارچوب ارزیابی امنیت سایبری سازمان مخابرات کشورهای مشترک‌المنافع[۳]

این شاخص توسط سازمان مخابرات کشورهای مشترک‌المنافع در سال ۲۰۱۵ ارایه شده که در زمینهٔ فناوری اطلاعات و ارتباطات و در جهت کمک به اعضای آن برای

۱. CYBER READINESS INDEX 2/0 (CRI 2.0)
۲. potomac
۳. Commonwealth Telecommunications Organization (CTO)

بهره‌برداری از این فناوری برای توسعهٔ اجتماعی اقتصادی فعالیت می‌کند؛ ابعاد و مؤلفه‌های اصلی ارزیابی امنیت سایبری ارائه شده؛ توسط این سازمان عبارتند از:

جدول۵: چارچوب ارزیابی امنیت سایبری سازمان مخابرات کشورهای مشترک‌المنافع

ابعاد	مؤلفه‌ها	ابعاد	مؤلفه‌ها
چارچوب قانونی و مقررات گذاری	وضع، اصلاح و رفع تزاحم قوانین جرایم سایبری	قابلیت‌های فنی	اولویت‌بندی تحقیق و توسعهٔ سایبری
	بازنگری قوانین حمایت از زیرساخت‌های حیاتی		هماهنگی تحقیق و توسعهٔ ملی و بین‌المللی.
	تدوین قوانین به اشتراک‌گذاری اطلاعات		پیوند بین نتایج تحقیق و توسعهٔ سیاست‌ها
	حفاظت از مالکیت معنوی		هماهنگی تحقیق و توسعه در سطح ملی
واکنش به حوادث	ایجاد شبکه‌ای CERT		سرمایه‌گذاری در تحقیقات دانشگاهی
	تقویت مدیریت حوادث با اهمیت ملی		اهمیت مالکیت معنوی برای افراد
	اعتمادسازی برای به اشتراک‌گذاری اطلاعات	ظرفیت‌سازی	طراحی برنامه‌های ظرفیت‌سازی
	تمرین‌های سایبری		استخراج نیازمندی‌های آموزشی مؤسسات
	ارزیابی توانایی پاسخگویی سازمان‌ها به حملات		شناسایی کارکنان ماهر مورد نیاز و تحلیل نیازها
آگاهی رسانی			تعریف مهارت‌ها در مشاغل، حفظ و استخدام

۶. چارچوب ارزیابی بلوغ سایبری در منطقهٔ آسیا- اقیانوسیه

این چارچوب ارزیابی بلوغ سایبری توسط مؤسسهٔ خط‌مشی‌گذاری راهبردی استرالیا با گسترهٔ 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 ارایه گردیده است؛ مؤسسهٔ مذکور در سال ۲۰۰۱ به‌عنوان یک اندیشکدهٔ مستقل تشکیل شد و هدف اصلی آن ارایهٔ 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 سایبر و مشاورهٔ نزدیک با دولت، صاحبان کسب و کار و جامعهٔ مدنی انجام می‌شود؛ ابعاد اصلی ارزیابی امنیت سایبری در این چارچوب عبارتند از:

۱ Australian Strategic Policy Institute (ASPI)

جدول۶: شاخص‌های ارزیابی بلوغ سایبری در منطقهٔ آسیا- اقیانوسیه

ردیف	ابعاد	مؤلفه‌ها
۱	حکمرانی	ساختار سازمانی
۲		قانون / مقررات‌گذاری
۳		تعامل بین‌المللی
۴		تیم‌های پاسخ به حوادث سایبری
۵	جرایم سایبری مالی	جرایم سایبری مالی
۶	نیروی نظامی	کاربردهای نظامی
۷	اقتصاد و تجارت دیجیتال	گفتگوی دولت با صاحبان مشاغل
۸		اقتصاد دیجیتال
۹	تعامل اجتماعی	آگاهی عمومی
۱۰		استفاده از اینترنت

۷. شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک[۱]

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[۲] ارایه شده است؛ این آکادمی یک سازمان دانش‌بنیان و مشاوره است که برای ایجاد و انتقال دانش و بهترین تجربیات در زمینهٔ مدیریت الکترونیکی، دموکراسی الکترونیکی، امنیت سایبری ملی و توسعهٔ جوامع اطلاعاتی آزاد ایجاد شده است؛ ابعاد اصلی ارزیابی آمادگی امنیت سایبری عبارتند از:

جدول۷: شاخص‌های ملی امنیت سایبری آکادمی حکمرانی الکترونیک

ردیف	شاخص‌ها	ردیف	شاخص‌ها
۱	سیاست و خط مشی امنیت سایبری	۷	خدمات شناسایی و اعتماد الکترونیکی
۲	تحلیل و اطلاع‌رسانی تهدیدات سایبری	۸	محافظت از اطلاعات شخصی
۳	آموزش و تربیت امنیت سایبری	۹	تیم واکنش به حوادث سایبری
۴	مشارکت در امنیت سایبری جهانی	۱۰	مدیریت بحران سایبری
۵	حمایت از خدمات دیجیتال	۱۱	پلیس مبارزه با جرایم سایبری
۶	حمایت از خدمات حیاتی	۱۲	عملیات سایبری نظامی

۱. National Cyber Security Index 2018 (NCSI)
۲. e-Governance Academy (eGA)

روش‌شناسی تحقیق

این پژوهش با توجه به این‌که مدلی به‌منظور ارزیابی امنیت سایبری کشور ارائه می‌نماید که می‌تواند در ارتقاء آن مؤثر باشد و نیز به‌عنوان ابزار و راهنمایی برای خط‌مشی‌گذاری در حوزهٔ امنیت سایبری عمل نماید، کاربردی است و با توجه به ارایهٔ مدل ارزیابی امنیت سایبری ج.ا.ا. و توسعهٔ دانش در این زمینه توسعه‌ای محسوب می‌شود؛ بنابراین این پژوهش با توجه به موضوع و هدف تحقیق، از نوع کاربردی- توسعه‌ای است و روش تحقیق به کار گرفته شده در این پژوهش، روش آمیخته است.

این پژوهش برای دستیابی به مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران در سه گام صورت گرفته است؛ در ابتدا با توجه به تعدد اسناد و مدارک مرتبط در بخش مطالعات کتابخانه‌ای با استفاده از روش تحلیل محتوای کیفی، ابعاد و مؤلفه‌های مدل ارزیابی امنیت سایبری احصاء گردید؛ پس از آن با استفاده از تکنیک دلفی ابعاد بدست آمده در مرحلهٔ اول با اجماع نظر خبرگان اصلاح و تکمیل گردیدند و در ادامه به‌منظور نهایی نمودن مدل ارایه شده، پرسشنامه‌ای محقق ساخته، تهیه و با اخذ نظرات کارشناسان حوزهٔ امنیت سایبری، صحت مدل مورد تأیید قرار گرفت؛ در ادامه هریک از گام‌های سه‌گانهٔ روش‌های تحقیق به‌کار گرفته شده در این پژوهش توضیح داده خواهد شد:

۱. تحلیل محتوای کیفی: در این پژوهش به تحلیل محتوای کیفی تدابیر و رهنمودهای مقام معظم رهبری (مدظله‌العالی)، اسناد بالادستی، مطالعات تطبیقی و مقالات علمی و پژوهشی داخلی پرداخته شد و با تکنیک خوشه بندی، کلید واژه‌های مؤثر در امنیت سایبری استخراج شدند و بر اساس فراوانی کلیدواژه‌ها؛ ابعاد و مؤلفه‌های اصلی مدل ارزیابی امنیت سایبری مورد بازشناسی قرار گرفتند.

۲. تکنیک دلفی: در این مرحله با استفاده از روش دلفی، ابعاد بازشناسی شده در گام اول برای طراحی مدل مفهومی امنیت سایبری با اجماع نظر خبرگان اصلاح گردیدند. جمعیت نمونهٔ تکنیک دلفی در این پژوهش، پانزده نفر از جامعهٔ آماری اساتید و اعضای گروه مطالعاتی، متخصصین حوزهٔ امنیت فضای سایبر، پژوهشگران، مدیران و متصدیان

اجرایی در حوزهٔ فناوری اطلاعات و فضای سایبری کشور هستند که با استفاده از روش نمونه‌گیری قضاوتی انتخاب گردیدند.

۳. پرسشنامهٔ باز: در گام سوم، پرسشنامه‌ای شامل سؤالات باز به‌منظور ارزیابی مدل ارایه شده تهیه گردید و با توجه به جامعهٔ آماری دوم که به‌صورت تمام شمار ۲۳ نفر از متخصصین امنیت فضای سایبر بودند صحت مدل مورد تأیید قرار گرفت.

تجزیه و تحلیل و یافته‌های تحقیق

در این مرحله؛ با تجزیه و تحلیل مفاهیم امنیت و امنیت سایبری و همچنین بررسی تدابیر و رهنمودهای مقام معظم رهبری (مدظله‌العالی) در این حوزه، اسناد بالادستی، ادبیات تحقیق، مطالعات تطبیقی و مقالات علمی و پژوهشی، ابعاد و مؤلفه‌های ارزیابی امنیت سایبری جمهوری اسلامی ایران را شناسایی و در نهایت مدل ارزیابی آن را ارایه خواهیم نمود.

ابعاد ارزیابی امنیت سایبری

با تحلیل محتوای مفهوم امنیت و نیز امنیت سایبری و همچنین بررسی تدابیر و رهنمودهای مقام معظم رهبری(مدظله‌العالی)، اسناد بالادستی، ادبیات تحقیق، مطالعات تطبیقی و مقالات علمی و پژوهشی داخلی با استخراج کلید واژه‌های مهم این تعاریف مبتنی بر تکنیک خوشه‌بندی و دریافت اجماع نظر خبرگان درباره این کلیدواژه‌ها از طریق تکنیک دلفی، ابعاد حکمرانی، حقوقی و قانونی، توانمندسازها و ظرفیت‌سازی، دفاعی- امنیتی و اجتماعی- فرهنگی به‌عنوان ابعاد ارزیابی امنیت سایبری منتخب گردیدند و نتایج در قالب جدول شمارهٔ ۸ ارایه گردیده است.

حکمرانی: حکمروایی در شاخص ENISA شامل تعیین نهاد راهبر، ارایهٔ چارچوب‌ها، تعیین ساختار مدیریتی، تعیین نقش‌ها و مسئولیت‌ها متمرکز بوده و در شاخص ASPI بر مفاهیمی نظیر ساختار سازمانی، قانون و مقررات‌گذاری، تعامل بین‌المللی و تیم پاسخ به

حوادث اشاره دارد؛ همچنین در اسناد کشورهای مختلف با مباحثی نظیر سیاست‌گذاری، راهبری، نگاشت نهادی، همکاری‌های سایبری، ظرفیت‌سازی و مدیریت شرایط بحران بیان شده است؛ همچنین در استاندارد COBIT در فناوری اطلاعات و ارتباطات طبق مدل DEM، مؤلفه‌های حکمرانی شامل جهت‌دهی، ارزشیابی و نظارت می‌باشد؛ لیکن پس از مشورت با خبرگان و بررسی‌های لازم مؤلفه‌های بعد حکمروایی شامل سیاست‌گذاری، راهبرد و هماهنگ‌سازی، نظارت و ارزیابی تعیین گردید.

حقوقی و قانونی: نظامات (توافقنامه‌های جامع حقوقی مانند DURSA در امریکا و IGSOC در انگلیس) نقش مهمی در حفاظت و امنیت سایبری دارند؛ بر این اساس مؤلفه‌های قانون‌گذاری و نظارت و مقررات‌گذاری به‌عنوان مؤلفه‌های این بعد پس از اجماع با خبرگان مورد پذیرش قرار گرفتند.

توانمندسازها و ظرفیت‌سازی: شاخص ITU شامل چارچوب استانداردهای امنیت سایبری سازمان‌ها، استانداردسازی، استفاده از فن‌آوری ابر به‌منظور امنیت سایبری، ظرفیت‌سازی و سازماندهی و در شاخص CTO شامل اولویت‌بندی تحقیق و توسعهٔ سایبری، هماهنگی تحقیق و توسعهٔ ملی و بین‌المللی، پیوند بین نتایج تحقیق و توسعهٔ سیاست‌ها، هماهنگی تحقیق و توسعه در سطح ملی، سرمایه‌گذاری در تحقیقات دانشگاهی و مالکیت معنوی برای افراد بود که نهایتاً مؤلفه‌های تحقیق و توسعه، استانداردها، ظرفیت‌سازی، سازماندهی، مشارکت و فناوری منتخب گردیدند.

دفاعی- امنیتی: دفاع سایبری در شاخص ENISA شامل برنامهٔ ملی راهبردی دفاع سایبری، شناسایی و ایجاد گروه واکنش به حوادث سایبری نظامی، وجود آموزش و ارزیابی میزان اثربخشی آن، قابلیت‌های همکاری و افزایش تاب‌آوری از طریق همکاری و به‌کارگیری فناوری‌ها جهت مقابله با حملات سایبری نظامی می‌باشند؛ همچنین در شاخص NCSI پلیس مبارزه با جرایم سایبری و عملیات سایبری نظامی و در شاخص ASPI نیروی نظامی و در شاخص CMM به دفاع سایبری اشاره شده است؛ بر این اساس و پس از

مشورت با خبرگان مؤلفه‌های دفاع از زیرساخت‌های حیاتی، سایبری انتظامی، سایبری دفاعی، رصد و پایش و پاسخ به رویدادها مورد پذیرش قرار گرفتند.

اجتماعی-فرهنگی: شاخص CMM دانشگاه آکسفورد جامعه و فرهنگ را به‌عنوان یک بعد ارزیابی امنیت سایبری ارایه نموده که شامل مؤلفه‌های فرهنگ امنیت سایبری، رسانه‌های اجتماعی می‌باشد؛ همچنین در چارچوب ارزیابی بلوغ سایبری توسط مؤسسهٔ خط‌مشی‌گذاری راهبردی استرالیا (ASPI[1]) اقتصاد و تجارت دیجیتال را به‌عنوان یکی از مؤلفه‌های اصلی ارزیابی امنیت سایبری معرفی نموده است؛ بر این اساس و پس از مشورت با خبرگان و بررسی‌های لازم و با توجه به زیست‌بوم فضای مجازی کشور و ضرورت تولید محتوای فاخر و بومی، مؤلفهٔ محتوای بومی نیز به مؤلفه‌های یاد شده اضافه گردید

جدول شمارهٔ ۸: استنتاج ابعاد ارزیابی امنیت سایبری جمهوری اسلامی ایران

ابعاد	اسناد	مضامین
حکمرانی	تدابیر و رهنمودها	- اشراف کامل و بروز نسبت به فضای مجازی - مواجههٔ فعال و خردمندانه - ارتقاء ج.ا.ا به قدرت سایبری در تراز قدرت‌های تأثیرگذار جهانی
	اسناد بالادستی	- حضور مؤثر و هدفمند در تعاملات بین‌المللی فضای مجازی، افزایش ظرفیت‌های قدرت نرم و دفاع سایبری (سیاست‌های کلی برنامهٔ ششم توسعهٔ کشور)
	مطالعات تطبیقی	- حکمرانی (مؤسسهٔ خط‌مشی‌گذاری راهبردی استرالیا- چارچوب ارزیابی بلوغ سایبری در منطقهٔ آسیا- اقیانوسیه) - سیاست‌ها و ظرفیت‌های دفاع سایبری (ادارهٔ امنیت شبکه و اطلاعات اتحادیهٔ اروپا- شاخص ارزیابی امنیت سایبری) - تدوین سیاست و راهبرد سایبری (دانشگاه آکسفورد- مدل بلوغ امنیت سایبری) - راهبرد ملی (مؤسسهٔ پوتومک- شاخص آمادگی سایبری) - سیاست و خط‌مشی سایبری (آکادمی حکمرانی الکترونیک- شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک)
	مقالات علمی و پژوهشی	- حکمروایی (الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران- ۱۳۹۷)

۱. Australian Strategic Policy Institute (ASPI)

ابعاد	اسناد	مضامین
حقوقی و قانونی	تدابیر و رهنمودها	– شکل‌دهی به قواعد و قوانین مرتبط با فضای مجازی (حکم انتصاب دورهٔ اول و دوم اعضای جدید شورای عالی فضای مجازی) – تدوین و تصویب نظام‌های مورد نیاز فضای مجازی(حکم انتصاب دورهٔ اول و دوم اعضای جدید شورای عالی فضای مجازی)
	اسناد بالادستی	– ... حفظ و توسعهٔ امنیت فضای تولید و تبادل اطلاعات و ارتباطات و تهیهٔ پیش‌نویس قوانین موردنیاز... (سیاست‌های کلی نظام در بخش افتا) – توسعهٔ نظام حقوقی و تعاملات بین‌المللی درحوزهٔ دفاع سایبری (سند راهبردی پدافند سایبری کشور) –تدوین قوانین و مقررات، دستورالعمل‌ها درحوزهٔ دفاع سایبری(سند راهبردی پدافند سایبری کشور)
	مطالعات تطبیقی	– اقدامات حقوقی و قانونی (اتحادیهٔ بین‌المللی مخابرات– شاخص جهانی ارزیابی امنیت سایبری) – چارچوب قانونی، مقررات و نظارت (سازمان کشورهای مشترک‌المنافع– چارچوب ارزیابی امنیت سایبری) – ایجاد چارچوب‌های مؤثر قانونی و نظارتی (دانشگاه آکسفورد– مدل بلوغ امنیت سایبری)
	مقالات علمی و پژوهشی	– قوانین و مقررات (الگوی راهبردی ارزیابی شبکهٔ ملی اطلاعات –نصرت‌آبادی و همکاران–۱۳۹۸) – حقوقی (الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران–تقی‌پور و همکاران– ۱۳۹۷) – حقوق سایبری (ارایهٔ الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح جمهوری اسلامی ایران– نصرت‌آبادی و همکاران–۱۳۹۷)
دفاعی– امنیتی	تدابیر و رهنمودها	– اشراف کامل و بروز نسبت به فضای مجازی – مواجههٔ فعال و خردمندانه (حکم انتصاب دورهٔ اول و دوم اعضای جدید شورای عالی فضای مجازی)
	اسناد بالادستی	– رصد، پایش، مراقبت و تشخیص و هشدار تهدیدات وحملات سایبری، توسعهٔ قابلیت‌های صیانت از اطلاعات، افراد و سرمایه‌های سایبری، درک هوشمندانه و پیش‌دستانه تهدیدات، نفوذناپذیری و استحکام و ایمنی زیرساخت‌های حیاتی و حساس (سند راهبردی پدافند سایبری کشور) – پایش، پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هرگونه تهدید در حوزهٔ فناوری اطلاعات و ارتباطات (سیاست‌های کلی نظام در بخش افتا) – حفظ و پایدارسازی زیرساخت‌های حیاتی و حساس کشور در مقابل تهدیدات و حملات سایبری (سند راهبردی پدافند سایبری کشور)
	مطالعات تطبیقی	– نیروی نظامی (مؤسسهٔ خط‌مشی‌گذاری راهبردی استرالیا– چارچوب ارزیابی بلوغ سایبری در منطقهٔ آسیا– اقیانوسیه) – عملیات سایبری نظامی، تیم واکنش به حوادث سایبری و حمایت از خدمات حیاتی (آکادمی حکمرانی الکترونیک– شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک) – دفاع و پاسخ به بحران (مؤسسهٔ پوتومک– شاخص آمادگی سایبری) – واکنش به حوادث (سازمان کشورهای مشترک‌المنافع– چارچوب ارزیابی امنیت سایبری) – تیم واکنش به حوادث (مؤسسهٔ خط‌مشی‌گذاری راهبردی استرالیا– چارچوب ارزیابی بلوغ سایبری در منطقهٔ آسیا– اقیانوسیه) – امن‌سازی زیرساخت‌های اطلاعاتی حیاتی (ادارهٔ امنیت شبکه و اطلاعات اتحادیهٔ اروپا– شاخص ارزیابی امنیت سایبری)
	مقالات علمی و پژوهشی	– عملیات (اقدامات واکنشی و بازیابی، مدیریت حوادث)، (الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران– تقی‌پور و همکاران– ۱۳۹۷)

ابعاد	اسناد	مضامین
توانمندسازها و ظرفیت‌سازی	تدابیر و رهنمودها	– سازمان مناسبی را ... جهت انجام جنگ الکترونیک در محدودهٔ فاوا (پیشگیری از نفوذ، تخریب و فریب) پیش‌بینی و در سیر مراحل تصویب قرار دهد (۹۲/۱/۱۵)
	اسناد بالادستی	– افزایش ظرفیت‌های قدرت نرم و دفاع سایبری و تأمین پدافند و امنیت سایبری برای زیرساخت-های کشور در چارچوب سیاست‌های کلی مصوب (برنامهٔ ششم توسعهٔ کشور) – ایجاد، تکمیل و توسعهٔ شبکهٔ ملی اطلاعات و تأمین امنیت آن، افزایش ظرفیت‌های قدرت نرم و دفاع سایبری (سیاست‌های کلی برنامهٔ ششم توسعهٔ کشور) – استانداردهای بومی درحوزهٔ دفاع سایبری (سند راهبردی پدافند سایبری کشور) – ارتقاء سطح دانش و ظرفیت‌های علمی، پژوهشی، آموزشی و صنعتی کشور برای تولید علم و فناوری مربوط به امنیت فضای اطلاعاتی و ارتباطی (سیاست‌های کلی نظام در افتا)
	مطالعات تطبیقی	– اقدامات فنی، سازماندهی و ظرفیت‌سازی (اتحادیهٔ بین‌المللی مخابرات– شاخص جهانی ارزیابی امنیت سایبری) – قابلیت‌های فنی بومی، ظرفیت‌سازی، آگاهی‌رسانی (سازمان کشورهای مشترک‌المنافع– چارچوب ارزیابی امنیت سایبری) –آموزش و تربیت امنیت سایبری (آکادمی حکمرانی الکترونیک– شاخص ملی امنیت سایبری آکادمی حکمرانی الکترونیک) – سرمایه‌گذاری در تحقیق و توسعه، دیپلماسی سایبری (مؤسسهٔ پوتومک– شاخص آمادگی سایبری)
اجتماعی-فرهنگی	تدابیر و رهنمودها	– اهتمام ویژه به سالم‌سازی و حفظ امنیت همه‌جانبهٔ فضای مجازی کشور و نیز حفظ حریم خصوصی آحاد جامعه و مقابلهٔ مؤثر با نفوذ و دست‌اندازی بیگانگان در این عرصه. – ترویج هنجارها، ارزش‌ها و سبک زندگی اسلامی ایرانی و ممانعت از رخنه‌ها و آسیب‌های فرهنگی و اجتماعی در این عرصه و مقابلهٔ مؤثر با تهاجم همه‌جانبهٔ فرهنگی – احراز جایگاه و سهم مناسب برای اقتصاد دانش‌بنیان در فضای مجازی در چارچوب سیاست‌های اقتصاد مقاومتی کشور و برنامه‌ریزی همه‌جانبه برای بهبود شرایط کسب و کار مرتبط با فناوری‌های مجازی و بهره‌گیری از فرصت‌های اشتغال‌زایی و نیز رونق محتوا، خدمات و تجارت در این عرصه. – توسعهٔ محتوا و خدمات کارآمد و رقابتی منطبق بر ارزش‌ها و فرهنگ اسلامی ایرانی در تمامی قلمروهای مورد نیاز جامعه (حکم انتصاب دورهٔ دوم اعضای جدید شورای عالی فضای مجازی)
	اسناد بالادستی	– ایجاد تناسب وکفایت سرمایه‌های انسانی، فرهنگ سازی و توسعهٔ مفاهیم دفاع سایبری (سند راهبردی پدافند سایبری کشور)
	مطالعات تطبیقی	– تدوین سیاست و راهبرد سایبری، تشویق فرهنگ مسئولیت‌پذیری سایبری در جامعه (دانشگاه آکسفورد– مدل بلوغ امنیت سایبری)

مؤلفه‌های ارزیابی امنیت سایبری

به‌منظور استخراج مؤلفه‌های امنیت سایبری، مضامین مرتبط با امنیت سایبری، با مطالعهٔ ادبیات پژوهش و تحلیل کیفی تدابیر و رهنمودهای مقام معظم رهبری (مدظله‌العالی) و اسناد بالادستی شامل حکم انتصاب دورهٔ اول و دوم اعضای جدید شورای عالی فضای مجازی، ابلاغ سیاست‌های کلی به مجمع در حوزهٔ خودکفایی دفاعی و امنیتی، سیاست‌های کلی برنامهٔ ششم توسعهٔ کشور، سیاست‌های کلی نظام در بخش افتا، اهداف و سیاست‌های مرکز ملی فضای مجازی، سند راهبردی پدافند سایبری کشور و مطالعهٔ تطبیقی الگوهای ارزیابی امنیت سایبری در سطح منطقه و جهان صورت پذیرفت و سپس با تکنیک خوشه‌بندی و بر اساس فراوانی تکرار واژه‌ها، مؤلفه‌های اصلی مورد بازشناسی اولیه قرار گرفتند و این مؤلفه‌ها از طریق تکنیک دلفی با اجماع نظر خبرگان اصلاح گردیدند که نتایج در جدول شمارهٔ ۹ ارایه شدند.

جدول شمارهٔ ۹ : ابعاد و مؤلفه‌های ارزیابی امنیت سایبری ملی

ابعاد	مولفه‌ها
حکمرانی	سیاست‌گذاری، راهبرد، هماهنگ‌سازی، نظارت و ارزیابی، دیپلماسی
حقوقی و قانونی	قانون‌گذاری، نظارت، مقررات‌گذاری
توانمندسازها و ظرفیت‌سازی	تحقیق و توسعه، استانداردها، نیروی انسانی، سازماندهی، مشارکت، علم و نوآوری، بودجه و اعتبارات
دفاعی- امنیتی	زیرساخت‌های حیاتی، سایبری انتظامی، سایبری دفاعی، رصد و پایش، پاسخ به رویدادها
اجتماعی- فرهنگی	فرهنگ امنیت سایبری، محتوای بومی، رسانه‌های اجتماعی، اقتصاد و تجارت دیجیتال، حریم خصوصی

ذی‌نفعان فضای سایبری ج.ا.ایران

با توجه به اینکه مدل ارایه شده در این تحقیق به‌منظور ارزیابی امنیت سایبری جمهوری اسلامی ایران پیشنهاد شده است، در گام بعد ذی‌نفعان امنیت فضای سایبر ملی به تفکیک لایه‌های فضای مجازی و نیز براساس ابعاد مدل ارایه شده در این تحقیق با اقتباس از سند راهبردی افتا استخراج و مطابق با مندرجات جدول شمارهٔ ۱۰ و ۱۱ معرفی گردیدند.

جدول شمارهٔ۱۰: ذی‌نفعان امنیت فضای سایبر ملی به تفکیک لایه‌های فضای مجازی

لایه‌ها	نقش ذی‌نفعان	ذی‌نفعان
حکمرانی	تعیین خط‌مشی‌ها، رویه‌ها، قوانین، مقررات استانداردها، طرح‌ها، برنامه‌ها، راهبردها و راهنمائی‌ها، نظارت، حمایت از تحقیق و توسعه.	نهاد رهبری، وزارت ارتباطات و فناوری اطلاعات، هیئت دولت، معاونت برنامهٔ ریاست جمهوری، مجلس شورای اسلامی، وزارت دفاع و پشتیبانی نیروهای مسلح، قو قضاییه، وزارت علوم، تحقیقات و فناوری، مجمع تشخیص مصلحت نظام، سازمان پدافند غیرعامل، شورای‌عالی فضای مجازی کشور، مرکز افتا ریاست جمهوری، ستاد کل نیروهای مسلح، دستگاه‌های نظارتی، وزارت اطلاعات، سازمان تنظیم مقررات و ارتباطات رادیویی، مؤسسهٔ ملی استاندارد و تحقیقات صنعتی.
کاربر	ارتقاء سطح آگاهی، دانش و مهارت‌های مرتبط با امنیت سایبر	وزارت ارتباطات و فناوری اطلاعات، وزارت دفاع و پشتیبانی نیروهای مسلح، وزرات علوم، تحقیقات و فناوری، وزارت اطلاعات، سازمان صدا و سیما ج.ا.ا ، معاونت برنامهٔ ریاست جمهوری، سازمان پدافند غیرعامل، بانک مرکزی جمهوری اسلامی ایران
محتوی	تأمین امنیت و جلوگیری از مخاطرات ناشی از محتوا	وزارت فرهنگ و ارشاد اسلامی (مالکیت فکری)، وزارت علوم تحقیقات و فناوری، سازمان ثبت اسناد و املاک کشور (مالکیت معنوی ـ صنعتی)، سازمان تبلیغات اسلامی، وزارت اطلاعات، بنیاد ملی جوانان، وزارت دادگستری، دفتر تبلیغات حوزهٔ علمیهٔ قم، وزارت ارتباطات و فناوری اطلاعات، سازمان صدا و سیما ج.ا.ا
خدمات	تقویت صنعت و توسعهٔ خدمات و محصولات امنیت فضای سایبر	وزارت صنعت ، معدن و تجارت، وزارت ارتباطات و فناوری اطلاعات، وزارت فرهنگ و ارشاد اسلامی، دانشگاه‌ها و مراکز علمی و پژوهشی کشور، سازمان پدافند غیرعامل
زیرساخت	امن‌سازی زیرساخت‌های حیاتی کشور در قبال حملات الکترونیکی	وزارت اطلاعات، دستگاه‌های متولی زیرساخت‌های حیاتی، وزارت ارتباطات و فناوری اطلاعات، وزارت کشور، وزرات دفاع و پشتیبانی نیروهای مسلح، سازمان پدافند غیرعامل

جدول شمارهٔ۱۱ : ذی‌نفعان مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران

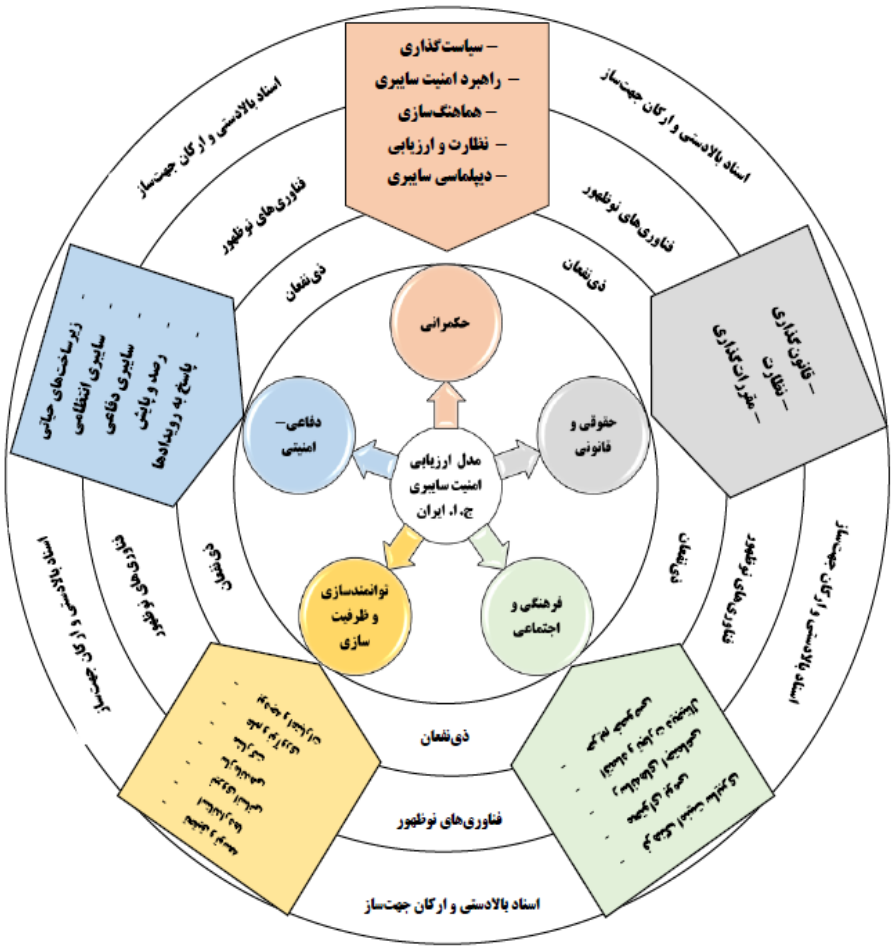
ابعاد	ذی‌نفعان
حکمرانی	نهاد رهبری، هیئت دولت، مجلس شورای اسلامی، مجمع تشخیص مصلحت نظام، شورای‌عالی فضای مجازی کشور، ستاد کل نیروهای مسلح ، وزارت ارتباطات و فناوری اطلاعات، مرکز افتا ریاست جمهوری، سازمان پدافند غیرعامل، معاونت برنامهٔ ریاست جمهوری، وزارت اطلاعات، وزارت دفاع و پشتیبانی نیروهای مسلح
حقوقی و قانونی	هیئت دولت، مجلس شورای اسلامی، قوهٔ قضاییه، دستگاه‌های نظارتی، وزارت ارتباطات و فناوری اطلاعات ، مرکز افتا ریاست جمهوری، معاونت برنامهٔ ریاست جمهوری، سازمان تنظیم مقررات و ارتباطات رادیویی
توانمندسازها و ظرفیت‌سازی	سازمان صدا و سیما ج.ا.ا، وزارت ارتباطات و فناوری اطلاعات، مرکز افتا ریاست جمهوری، پارک‌های علم و فناوری، مؤسسهٔ آموزشی تحقیقاتی ارتباطات و فناوری اطلاعات، سازمان تنظیم مقررات و ارتباطات رادیویی، دانشگاه‌ها و مراکز علمی و پژوهشی کشور، مؤسسهٔ ملی استاندارد و تحقیقات صنعتی، وزارت دفاع و پشتیبانی نیروهای مسلح، وزارت علوم، تحقیقات و فناوری، وزارت صنعت ، معدن و تجارت
دفاعی- امنیتی	سازمان پدافند غیرعامل، وزارت اطلاعات، وزارت ارتباطات و فناوری اطلاعات، وزرات دفاع و پشتیبانی نیروهای مسلح، دستگاه‌های متولی زیرساخت‌های حیاتی، وزارت کشور، پلیس فتا
اجتماعی- فرهنگی	سازمان صدا و سیما ج.ا.ا، سازمان پدافند غیرعامل، مؤسسهٔ آموزشی تحقیقاتی ارتباطات و فناوری اطلاعات، دانشگاه‌ها و مراکز علمی و پژوهشی کشور، وزارت علوم، تحقیقات و فناوری، بانک مرکزی جمهوری اسلامی ایران، وزارت فرهنگ و ارشاد اسلامی (مالکیت فکری)، سازمان ثبت اسناد و املاک کشور (مالکیت معنوی- صنعتی)، سازمان تبلیغات اسلامی، بنیاد ملی جوانان، دفتر تبلیغات حوزهٔ علمیه قم، وزارت صنعت، معدن و تجارت

فناوری‌های نوظهور فضای سایبری

فناوری‌های نوظهور در فضای سایبر و روندهای فناورانه‌ای که امروزه در قالب انقلاب صنعتی چهارم اروپا و تصویرسازی آیندهٔ اغلب کشورها وجود دارد؛ باعث گردیده این فناوری‌ها در محیط آشوبناک و سرشار از عدم قطعیت فضای سایبر نقش بی-بدیلی داشته و این موضوع مقولهٔ امنیت سایبری را تحت‌تأثیر خود قرار دهد؛ بر این اساس فناوری‌هایی نظیر بلاک‌چین، سامانه‌های سایبر فیزیکی، هوش مصنوعی و رباتیک،

اینترنت اشیاء، پردازش کوانتومی، کلان‌داده‌ها و ...؛ مقوله‌هایی نظیر مالکیت داده، حریم خصوصی، بحران‌سازی و جریان‌سازی‌های سیاسی- امنیتی، مالکیت معنوی و ... را تحت‌تأثیر قرار داده و بر این اساس ضروری است؛ چالش‌هایی نظیر فقدان راهبرد کلان و فرابخشی در این حوزه، عدم چابکی و کارآمدی ساختاری در فرایندهای تصمیم‌گیری، اجرا و نظارت بر عملکرد، عملکرد جزیره‌ای و مجزا از یکدیگر نهادهای تصمیم‌گیر، مقررات‌گذار و بهره‌بردار مرتبط، فقدان یک رابطهٔ پیوسته میان صنعت و نهادهای تحقیقاتی و دانشگاهی، ضعف ارتباط شرکت‌های داخلی توانمند در حوزهٔ الکترونیک، مخابرات و نرم‌افزار با شرکت‌های معتبر بین‌المللی، کندی روند صنعتی‌شدن و استفاده از فناوری‌ها در محیط کسب‌وکار کشور، انفعال در عرصهٔ بین‌الملل به دلیل عدم استفاده از فرصت‌های بین‌المللی، تغییر فرهنگ و سبک زندگی ایرانی-اسلامی مردم، افزایش مواجههٔ کاربران ایرانی با محتواهای ضدفرهنگی، از دست دادن باورهای اعتقادی در مواجههٔ کاربران با جریان‌سازی‌های معاند اعتقادات و نهایتاً خروج اطلاعات کاربران به رسانه‌های اجتماعی خارجی و بهره‌برداری بیگانگان از ذائقهٔ ایرانی، مورد توجه جدی قرار گرفته و ضمن بهره‌برداری از این فناوری‌ها در امنیت سایبری، از آسیب‌های عنوان شده نیز جلوگیری شود.

با توجه به موارد عنوان شده، مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران مطابق با مندرجات شکل شمارهٔ یک ارایه می‌گردد.



شکل شمارهٔ ۱: مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران

مقایسهٔ مدل ارایه شده در این تحقیق و ابعاد ارزیابی امنیت سایبری اتحادیهٔ بین‌المللی مخابرات و سازمان مخابرات کشورهای مشترک‌المنافع نشان می‌دهد که مدل این پژوهش در ابعاد حقوقی و قانونی، توانمندسازها و ظرفیت‌سازی با دو مدل مذکور انطباق کامل داشته و ابعاد حکمرانی و سیاست‌گذاری، دفاع و پاسخ به بحران و بعد فرهنگی و اجتماعی از جامعیت بیشتری نسبت به ابعاد عنوان شده توسط این سازمان‌ها برخوردار می‌باشد؛ به‌ویژه اینکه در ابعاد و مؤلفه‌های اتحادیهٔ بین‌المللی مخابرات با توجه به ماهیت غیرنظامی

این سازمان به مؤلفه‌های دفاعی و انتظامی پرداخته نشده و این موضوع در صورتی است که در مدل ارایه شده در این مقاله، مؤلفه‌های دفاع سایبری و انتظامی معطوف به این موضوع می‌باشد؛ همچنین باید توجه داشت که بعد حکمرانی و سیاست‌گذاری از جامعیت کافی برخوردار بوده و به طریقهٔ اولی شامل سیاست‌گذاری و راهبردهای همکاری و تعامل اعم از همکاری بین‌بخشی، شامل بخش‌های خصوصی و دولتی و همکاری‌های منطقه‌ای و بین‌المللی و دیپلماسی سایبری نیز می‌باشد.

مقایسهٔ بین ابعاد مدل معرفی شده در قالب این مقاله و ابعاد امنیت سایبری ادارهٔ امنیت شبکه و اطلاعات اتحادیهٔ اروپا نشان می‌دهد ابعاد ارایه شده توسط این اداره شامل سیاست‌ها و ظرفیت‌های دفاع سایبری، مقابله با جرایم سایبری، حمایت از صنعت در زمینهٔ امنیت سایبری، امن‌سازی زیرساخت‌های اطلاعاتی حیاتی با ابعاد جامع‌تری به ترتیب شامل حکمرانی و سیاست‌گذاری، حقوقی و قانونی، توانمندسازها و ظرفیت‌سازی، دفاع و پاسخ به بحران جایگزین گردیده و لیکن با توجه به ماهیت امنیت، مبانی نظری و پیشینهٔ مطرح شده در این مقاله، تاب‌آوری به‌عنوان یکی از ابعاد امنیت سایبری قابل جمع و تعریف نیست؛ همچنانکه در تحقیق ارایه شده توسط تقی‌پور و همکاران، ۱۳۹۷، تاب‌آوری به‌عنوان یکی از ابعاد دفاع سایبری و البته با ترجمهٔ برگشت‌پذیری از اصطلاح لاتین Resilience معرفی شده است.

در مقایسه بین ابعاد معرفی شده در قالب این مقاله و ابعاد امنیت سایبری دانشگاه آکسفورد باید گفت، ابعاد تدوین سیاست و راهبرد سایبری، تشویق فرهنگ مسئولیت‌پذیری سایبری در جامعه، ایجاد مهارت‌های سایبری در نیروی کار و کارفرمایان، ایجاد چارچوب-های مؤثر قانونی و نظارتی، کنترل ریسک از طریق سازماندهی، استانداردها و فناوری، به-ترتیب با ابعاد جامع‌تری شامل حکمرانی و سیاست‌گذاری، فرهنگی و اجتماعی، توانمندسازها و ظرفیت‌سازی و نهایتاً بعد حقوقی و قانونی جایگزین گردیده و موضوع کنترل ریسک علاوه بر اینکه از طریق سازماندهی، استانداردها و فناوری مورد تأکید قرار گرفته، در بعد دفاع و پاسخ به بحران به‌صورت کامل مورد توجه قرار گرفته است.

مقایسهٔ بین ابعاد معرفی شده در قالب این مقاله و ابعاد امنیت سایبری مؤسسهٔ پوتومک نشان می‌دهد ابعاد مطرح شده توسط این مؤسسه با جامعیت کامل‌تری در مدل ارایه شده مدنظر قرار گرفته؛ به‌ویژه اینکه ابعاد سرمایه‌گذاری در تحقیقات و توسعه، تجارت سایبری، در ابعاد توانمندسازها و ظرفیت‌سازی، فرهنگی و اجتماعی با توجه به پیشرفت روزافزون این ابعاد مدنظر قرار گرفته است.

مقایسهٔ بین ابعاد معرفی شده در قالب این مقاله و ابعاد امنیت سایبری مؤسسه خط‌مشی‌گذاری راهبردی استرالیا و آکادمی حکمرانی الکترونیک بیانگر آن است که ویژگی عمدهٔ این مدل‌ها منظورنمودن بعد نظامی در مدل ارایه شده است که این موضوع با بعد جامع‌تری با عنوان دفاع و پاسخ به بحران در مدل این تحقیق ارایه شده است؛ همچنین در مدل ارایه شده توسط آکادمی حکمرانی الکترونیک از صیانت از حریم خصوصی به‌عنوان یکی از ابعاد اصلی امنیت سایبری یاد شده که این موضوع به‌عنوان یکی از مؤلفه‌های بعد فرهنگی و اجتماعی در مدل ارایه شده در این مقاله به آن پرداخته شده است.

نتیجه‌گیری و پیشنهاد

الف. نتیجه‌گیری

ابعاد و مؤلفه‌های مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران پس از مطالعه اسناد بالادستی و بررسی شاخص‌های جهانی ارزیابی امنیت سایبری مربوط به هفت مؤسسهٔ بین‌المللی و نیز از طریق مراجعه به آرای خبرگان در حوزه‌های راهبردی و امنیتی فضای سایبر، به‌طور منطقی و مفهومی استنباط گردید و با تجزیه و تحلیل مفاهیم و مضامین به دست آمده و ارتباط و تأثیر و تأثر آن‌ها با یکدیگر و با در نظر گرفتن مقتضیات و زیست‌بوم فضای سایبر کشور به‌صورت مدلی متشکل از ابعاد و مؤلفه‌ها بر اساس تدابیر مقام معظم رهبری(مدظله‌العالی)، اسناد بالادستی و همچنین شاخص‌های ارزیابی امنیت سایبری جهانی و منطقه‌ای با استفاده از روش پژوهش آمیخته استخراج و سپس ذی‌نفعان امنیت فضای سایبر ملی به تفکیک لایه‌های فضای مجازی و همچنین ذی‌نفعان مدل ارزیابی

امنیت سایبری تعیین گردیدند و در ادامه به اهمیت فناوری‌های نوظهور و نقش آن‌ها در امنیت فضای سایبری کشورمان اشاره گردید و در نهایت پس از ارایهٔ مدل ارزیابی امنیت سایبری ج.ا.ایران، مقایسهٔ بین مدل این تحقیق و مدل‌های ارایه‌شده توسط مؤسسات معتبرج هانی که در بخش مبانی نظری پژوهش به آن‌ها پرداخته شد به‌عمل آمد. مهم‌ترین محورهایی که می‌توان از نتایج این پژوهش برشمرد عبارتند از:

- شناسایی و تبیین ابعاد و مؤلفه‌ها و ذی‌نفعان مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران؛
- تولید ادبیات در حوزهٔ ارزیابی امنیت سایبری؛
- ایجاد و فراهم نمودن وفاق در فرایند تصمیم‌سازی و تصمیم‌گیری مابین دستگاه-های مسئول در حوزهٔ امنیت سایبری؛
- تقویت و ارتقاء تفکر راهبردی در حوزهٔ امنیت سایبری در جمهوری اسلامی ایران؛
- فراهم آوردن زمینهٔ لازم برای مواجههٔ هوشمندانه و مقتدرانه با تهدیدات روزافزون فضای سایبر؛
- بی‌نیاز نمودن دستگاه‌های مسئول امنیت سایبری از مراجعه به الگوهای ارزیابی امنیت سایبری غیر بومی.

ب. پیشنهادها

با توجه به ارایهٔ مدل ارزیابی امنیت سایبری جمهوری اسلامی ایران در این تحقیق، شایسته است:

۱. با مقایسهٔ وضعیت موجود امنیت سایبری جمهوری اسلامی ایران با مدل ارائه شده، پیشنهاد می‌گردد با ایجاد مراکز اشتراک و تحلیل اطلاعات نسبت به افزایش امنیت سایبری جمهوری اسلامی ایران اقدام لازم صورت پذیرد؛

۲. با توجه به وضعیت نظام جمهوری اسلامی ایران و تقابل دایمی آن با استکبار جهانی و نظام سلطه، تسریع در ارتقاء امنیت سایبری جمهوری اسلامی ایران که منجر به ارتقاء امنیت ملی می‌شود، پیشنهاد می‌گردد؛

۳. دستگاه‌ها و نهادهایی که در حوزهٔ امنیت سایبری جمهوری اسلامی ایران دارای مسئولیت هستند از نتایج این تحقیق به‌منظور ارزیابی و ارتقای امنیت سایبری کشور استفاده نمایند؛

۴. با ایجاد مراکز علمی و فناوری با مشارکت ذی‌نفعان مختلف و انجام تحقیقات در حوزهٔ امنیت سایبری و تحلیل نتایج ارزیابی آن و استفاده از فناوری‌های نوظهور فضای سایبر، نسبت به ارتقاء تاب‌آوری سایبری جمهوری اسلامی ایران اقدام لازم صورت پذیرد؛

۵. در تحقیقات آتی مرتبط با موضوع این پژوهش، پرداختن به شاخص‌های ارزیابی امنیت سایبری حوزهٔ دفاعی می‌تواند افق وسیع‌تری در ادامهٔ این پژوهش بگشاید.

فهرست منابع ومآخذ

الف. منابع فارسی

- انتظامی، حسین (۱۳۹۲)، افق فناوری اطلاعات و ارتباطات در نگاه امنیت ملی، دانشگاه عالی دفاع ملی، تهران.
- اهداف و سیاست‌های مرکز ملی فضای مجازی،۱۰ تیر (۱۳۹۵).
- تقی‌پور، رضا؛ اسماعیلی، علی(۱۳۹۷)، طراحی مدل مفهومی الگوی دفاع سایبری ج ا ا ، فصلنامهٔ امنیت ملی، دانشگاه عالی دفاع ملی، تهران.
- حکم انتصاب اعضای جدید شورای عالی فضای مجازی،۱۴شهریور (۱۳۹۴).
- خلیلی‌پور رکن‌آبادی، علی؛ نورعلی وند، یاسر (۱۳۹۱)، تهدیدات سایبری و تأثیر آن بر امنیت ملی، فصلنامهٔ مطالعات راهبردی ش ۵۶.
- سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور (۱۳۸۷).
- سیاست‌های کلی برنامهٔ ششم توسعهٔ کشور (۱۳۹۴).
- شهیر، احسان (۱۳۹۶)، طراحی الگوی راهبردی بومی امنیت فضای مجازی کشور، رسالهٔ دکتری دانشگاه عالی دفاع ملی.
- عالی‌پور، حسن(۱۳۹۳)، امنیت سایبری در افق۱۴۰۴(چالش‌ها و راهکارهای حقوقی رویارویی با بزه‌های امنیتی سایبری)، تهران، همایش ملی دفاع سایبری.
- کمیتهٔ دایمی پدافند غیرعامل کشور، سند راهبردی پدافند سایبری کشور (۱۳۹۴).
- مؤسسهٔ آموزشی و تحقیقاتی صنایع دفاعی، راهنمای تدوین راهبرد ملی امنیت سایبری، ۱۳۹۵.
- محمودزاده، ابراهیم؛ اسماعیلی، کیوان (۱۳۹۷)، الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح، فصلنامهٔ امنیت ملی، س هشتم، ش سی‌ام، زمستان، تهران: دانشگاه عالی دفاع ملی.
- ملائی، علی؛ کارگری، مهرداد؛ خراشادی‌زاده، محمدرضا (۱۳۹۷)، الگوی بازدارندگی در فضای سایبر بر اساس نظریه بازی‌ها، فصلنامهٔ امنیت ملی، س هشتم، ش ۲۹.
- نصرت‌آبادی، جمشید؛ لشکریان، حمیدرضا؛ مردانی شهربابک، محمد؛ موحدی‌صفت، محمدرضا (۱۳۹۷)، ارائهٔ الگوی راهبردی ارزیابی قدرت سایبری نیروهای مسلح ج ا ا، فصلنامهٔ امنیت ملی، س نهم، ش سی و یکم، بهار.

- نصرت‌آبادی، جمشید؛ مؤمنه، محسن؛ یاقوت‌پور، محمدحسین؛ مهدی نژاد نوری، محمد (۱۳۹۸)، ارائهٔ الگوی راهبردی ارزیابی شبکهٔ ملی اطلاعات، فصلنامهٔ امنیت ملی، س نهم، ش سی و سوم، پاییز.
- نوبخت، محمدباقر (۱۳۹۳)، روش تحقیق پیشرفته برای دانشجویان کارشناسی ارشد و دکتری، سازمان انتشارات جهاد دانشگاهی، تهران

ب. منابع انگلیسی

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