مقاله پژوهشی:
الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران

رضا تقی‌پور[1] و حمیدرضا لشکریان[2] و علی ناصری[3] و رحیم یزدانی چهاربرج[4]

تاریخ دریافت: ۱۳۹۷/۰۹/۱۲ **تاریخ پذیرش: ۱۳۹۷/۱۲/۱۵**

چکیده

در سال‌های اخیر، به موازات فضای واقعی، فضای سایبر[5] تمام ابعاد زندگی بشر را در برگرفته است. بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، فرهنگی، اجتماعی کشور در فضای سایبر انجام می‌گیرد. بخش بزرگی از اطلاعات حیاتی کشور در این فضا شکل می‌گیرد و زیرساخت‌های حیاتی کشور هم از طریق این فضا، مدیریت و بهره‌برداری می‌شوند.

بی‌توجهی به مقوله حفاظت در زیرساخت‌های اطلاعاتی حیاتی، علاوه بر مخاطرات و تهدیدات کلان، اقتدار و امنیت ملی را خدشه‌دار خواهد کرد. بر این اساس، ارائه الگوی راهبردی جهت محافظت، از ضرورت‌ها به شمار می‌آید و هدف از این پژوهش، دستیابی به الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی با شناسایی ابعاد، مؤلفه‌ها و روابط فی‌مابین آن‌ها است. محقق با استفاده از روش پژوهش آمیخته، ابتدا از روش تحلیل کیفی برای مستندسازی دانش حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی در سطوح راهبردی با مراجعه به بیانات ارزشمند امام خامنه‌ای (مدظله‌العالی)، اسناد بالادستی کشور، اسناد و اقدامات راهبردی امنیتی کشورهای مختلف، مدل‌ها و طرح‌های بین‌المللی، استفاده کرده و سپس با تحلیل خبرگی، چارچوب مدل مفهومی تحقیق و همچنین ابعاد و مؤلفه‌های الگوی راهبردی حفاظت از زیرساخت‌های اطلاعاتی حیاتی احصاء گردیدند و سپس برای

---

۱. دانشیار دانشگاه عالی دفاع ملی، **taghipour@sndu.ac.ir**

۲. استادیار دانشگاه امام حسین (ع)

۳. دانشیار دانشگاه جامع امام حسین(ع)

۴. دانشجوی دوره دکترای مدیریت راهبردی امنیت سایبر دانشگاه عالی دفاع ملی، نویسنده مسئول r.yazdani@sndu.ac.ir

۵Cyber Space

رسیدن به اهداف تحقیق از پرسشنامه محقق‌ساخته که مبتنی بر مصاحبه و بررسی اسناد بالادستی بود استفاده گردید.

نتایج این تحقیق نشان می‌دهد که الگوی راهبردی حفاظت سایبری، دارای ۴ بُعد، ۱۸ مؤلفه و ۱۳۱ زیرمؤلفه است که مهم‌ترین مؤلفه‌ها در بعد «حکمروایی» حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی به ترتیب، «سیاست‌گذاری»، «ظرفیت‌سازی»، «راهبری»، «دیپلماسی سایبری» و «نگاشت نهادی» هستند. همچنین مهم‌ترین مؤلفه‌ها در بعد «حقوقی» به ترتیب «قوانین»، «مقررات» و «نظامات» هستند. همچنین در بعد «مدیریت امنیت»، مهم‌ترین مؤلفه‌ها عبارت‌اند از «امنیت خدمات»، «سازمان‌دهی امنیت»، «امنیت زیرساخت»، «امنیت داده»، «امنیت کاربران» و در نهایت در بعد «عملیات»، مهم‌ترین مؤلفه‌ها، «اقدامات پیشگیرانه»، «اقدامات واکنشی»، «اقدامات تشخیصی» و «مدیریت حوادث» هستند.

کلیدواژه‌ها: زیرساخت‌های اطلاعاتی حیاتی، حفاظت، حفاظت سایبری، الگوی مفهومی

مقدمه

با توجه به فراگیرشدن فضای مجازی در تمام حوزه‌های زندگی با کارکردهای متنوع؛ مانند کسب‌وکارهای مجازی، ارتباط انسان با اشیاء، انجام فعالیت‌های حاکمیتی، تبادلات مالی و اقتصادی، تجارت الکترونیک، تعاملات اجتماعی، نشر و تبادل اطلاعات، ارتباطات سیاسی و افکارسنجی، فعالیت‌های فرهنگی و محتوایی، بخش عمده‌ای از تعاملات کشور در تمام سطوح، اعم از افراد، مؤسسات غیردولتی، نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد و این فضا یک قلمروی عملیاتی شده است. اهمیت این فضا آن‌چنان است که حضرت امام خامنه‌ای(مدظله‌العالی) در این خصوص فرموده‌اند: «فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد»[۱].

زیرساخت‌های اطلاعاتی حیاتی یا بخشی از فضای سایبری هستند و یا از طریق این فضا، مدیریت و بهره‌برداری می‌شوند. زیرساخت‌های اطلاعاتی حیاتی؛ شامل شبکه‌ها و سامانه‌های اطلاعاتی به‌هم‌پیوسته است که اختلال یا تخریب آن‌ها تأثیر جدی بر سلامت، ایمنی، امنیت، رفاه، اقتصاد و حاکمیت در سطح ملی دارد (Segura Serrano, 2015: 3).

زیرساخت‌های اطلاعاتی حیاتی علاوه بر آسیب‌پذیری‌های داخلی ناشی از ضعف

۱. http://farsi.khamenei.ir/others. dialog?id=19272

زیرساخت‌های فنی و نیز کمبودها و ضعف‌های آموزشی، در معرض طیف وسیعی از عوامل مهاجم قرار دارند. مهم‌ترین نگرانی دراین‌باره تهدید ناشی از حملات سایبری سازمان‌یافته است که قادر به تحمیل لطمه‌های جبران‌ناپذیر بر زیرساخت‌های حیاتی کشور است.

بدافزارها و سلاح‌های سایبری (مانند استاکس نت)، انواع هک‌ها با قابلیت جاسوسی و خرابکاری (غیر قابل دسترس کردن خدمات دولتی، سرقت اطلاعات)، تروریسم دولتی، نرم‌افزارهای مخرب، ویروس‌ها با قابلیت‌های مختلف، انواع تروجان‌ها و درهای پشتی، کرم‌ها، فروش تجهیزات با قابلیت مدیریت و کنترل از راه دور ازجمله تهدیداتی هستند که زیرساخت‌های اطلاعاتی کشور را تهدید کرده و می‌کنند. مصداق بارز این تجهیزات، سامانه‌های اسکادای غیربومی است که مدخل تهدیدات سایبری در حوزه زیرساخت تلقی شده و زیرساخت‌های پرخطر و عموماً صنعتی را با دقت بالا کنترل و مدیریت می‌کنند به‌طوری که با جاسازی ویروس‌های نرم‌افزاری و سخت‌افزاری و سپس آزادسازی آن‌ها با فرمان از راه دور و انجام تخریب، تسلط و کنترل را امکان‌پذیر می‌سازند. خرید سهام شرکت‌های تولیدکننده اسکادا توسط آمریکایی‌ها، طراحی یک پروتکل امنیتی که قابلیت‌های کنترل دسترسی و وارسی به زیرساخت‌ها را به آن‌ها بدهد[۱] همکاری شرکت زیمنس و مایکروسافت در استاکس نت با آمریکا مثالی از این تهدیدات است. علاوه بر استفاده از محصولات غیربومی که اشاره شد، از مشکلات حوزه حفاظت، می‌توان به عدم توانایی در از بین بردن تهدیداتی که متوجه نرم‌افزارها و سخت‌افزارهای نگهداری‌کننده از اطلاعات کلیدی هستند و همچنین می‌توان به نگاه سنتی به امنیت و حفاظت و معضل تأثیر نیروی انسانی بر حفاظت اشاره کرد.

حفاظت از زیرساخت‌های اطلاعاتی حیاتی در مقابل تهدیدات سایبری یک موضوع مرتبط با امنیت ملی است. به این معنا که شکست یا نابودی زیرساخت‌های اطلاعاتی حیاتی، تأثیر جدی بر امنیت، اقتصاد و رفاه شهروندان می‌گذارد. لذا حفاظت از

---

۱. به نقل از خبرگزاری ایسنا در ۲۵ دی ۱۳۹۳، کدخبر ۹۳۱۰۲۵۱۳۹۱۵ (https://isna.ir)

زیرساخت‌های اطلاعاتی حیاتی به دلیل منافع عمومی و امنیت ملی مبحث کلان و راهبردی است. با آنکه در سطح جهانی، رویکرد کشورها از حالت «دخالت حداکثری حاکمیت» تا «حداقل دخالت حاکمیتی» متغیر است، لکن حفاظت از زیرساخت‌های اطلاعاتی حیاتی به‌عنوان بخش مهمی از امنیت ملی در کشورهای مختلف مطرح است (ENISA,2015: 1). مهم‌تر از این‌ها، حفاظت از زیرساخت‌های حیاتی و ازجمله زیرساخت‌های اطلاعاتی حیاتی که در همه کشورها مورد تأکید است در کشور ما نیز در اسناد بالادستی، مانند امنیت فضای تولید و تبادل (سند افتا)، سند راهبردی پدافند غیرعامل در حوزه الکترونیک، سند پیوستی شورای عالی فضای مجازی و ... به این موضوع پرداخته شده است. لذا از پیامدهای حفاظت از زیرساخت‌های اطلاعاتی حیاتی، رسیدن به اهداف مذکور در اسناد بالادستی است.

حال به‌منظور حفاظت از زیرساخت‌های اطلاعاتی حیاتی، با در نظر گرفتن تهدیدات، مشکلات، تنگناها، ناکارآمدی‌ها و ضعف‌های مورد اشاره، مواردی مانند نگاه جامع و یکپارچه به همه ابعاد مؤثر در حفاظت توسط الگو و عملکرد مؤلفه‌ها به‌طور هم‌زمان، بررسی وضعیت‌های موجود و مطلوب در الگو و بررسی مسیر لازم برای رسیدن به وضعیت مطلوب، از دلایل عمده برای تدوین الگوی راهبردی و کلان در سطح زیرساخت‌های اطلاعاتی حیاتی کشور برای محافظت سایبری است که پاسخی کاربردی به دغدغه‌ها و تهدیدات است.

مسئله اصلی در این تحقیق آن است که با توجه به تنوع، تغییر ماهیت و جنس تهدیدات سایبری که هم از ناحیه منابع خصمانه، مانند دولت‌های متخاصم، گروه‌های تروریستی، جاسوسان، کارکنان ناراضی و هم از ناحیه آسیب‌های ناشی از آموزش و فرهنگ برای مشارکت در حفاظت و ... است، «ابعاد و مؤلفه‌های الگوی راهبردی حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی چیست»؟

اهمیت حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی از چند وجه قابل بررسی است. اولاً به دلیل عدم کار پژوهشی مشابه موجب شناسایی ابعاد و مؤلفه‌های حفاظت

سایبری، تولید ادبیات بومی، ارتقای دانش کارگزاران نظام و افزایش کارآمدی در این حوزه می‌گردد. ثانیاً موجب کارکردهای الگوی راهبردی حفاظت سایبری جهت توسعه و اعتلای روش‌های پدافندی و پیشگیرانه در فضای پرچالش و محیط بی‌ثبات سایبری می‌گردد و زمینه برقراری ارتباط بین جهت‌گیری راهبردی و تفکر اجرایی در فرآیندها، معماری‌ها، ظرفیت‌ها می‌شود. ثالثاً با تدوین الگوی راهبردی، تسهیل سیاست‌گذاری، ارتقای الگوهای حفاظتی از سطح تاکتیکی و غیربومی به سطح راهبردی و بومی، بروز هماهنگی در عملکرد متوازن تمامی عوامل مؤثر در حفاظت سایبری رخ می‌دهد. رابعاً داشتن رویکرد پیشگیرانه، جهت‌دهی هدفمند به فعالیت‌ها در راستای اهداف و مأموریت‌های کلان، قابل ردیابی کردن و قابل اندازه‌گیری کردن فرآیندها، تصمیم‌گیری مؤثر و منطقی، تداوم‌بخشی به کسب‌وکار، افزایش ثمربخشی اقدامات و ... همه این‌ها از مواردی است که به‌عنوان اهمیت تدوین الگوی راهبردی محسوب می‌گردد.

از ضرورت‌های این تحقیق می‌توان به سیاست‌های ابلاغی مقام معظم رهبری (مدظله‌العالی) در قالب اسناد بالادستی مبنی بر امن‌سازی زیرساخت‌های (اطلاعاتی) حیاتی در حوزه فناوری اطلاعات و ارتباطات و ارتقای مداوم امنیت شبکه‌ها و سامانه‌های اطلاعاتی و ارتباطی به‌منظور پایداری زیرساخت‌ها، صیانت از اسرار کشور، ایجاد آمادگی لازم در عالی‌ترین سطح به‌منظور صیانت از زیرساخت‌های حیاتی در برابر حملات اینترنتی و دفاع مناسب در برابر حملات اشاره کرد. همچنین می‌توان گفت که بی‌توجهی به مقوله حفاظت سایبری در زیرساخت‌های حیاتی، علاوه بر مخاطرات و تهدیداتی که در زندگی فردی و اجتماعی افراد جامعه ایجاد می‌کند، اقتدار و امنیت ملی را خدشه‌دار خواهد کرد و این امر کلان و راهبردی بودن حفاظت از زیرساخت‌های اطلاعاتی حیاتی و لزوم تدوین الگوی راهبری را نشان می‌دهد. همچنین در صورت فقدان الگوی راهبردی حفاظت سایبری، اتخاذ تصمیمات ناهمگن، نامنسجم، نگاه بخشی و محدودنگری، نداشتن رویکرد و اهداف راهبردی، عدم توجه به الزامات و نیازمندی‌های اهداف راهبردی در مباحث حفاظت سایبری از زیرساخت‌های اطلاعاتی

حیاتی اجتناب‌ناپذیر است.

نوآوری تحقیق در این است که با اینکه در برخی از تحقیقات، ارائه راهبردهای پدافند غیرعامل، پیشنهاد سامانه‌های حفاظتی و ارائه مدل امنیتی برای محافظت از برخی از زیرساخت‌های حیاتی صورت گرفته است؛ اما زیرساخت‌های اطلاعاتی حیاتی کشورمان دارای مؤلفه‌ها و شاخص‌های ویژه‌ای است که نیازمند پژوهش و بررسی عمیق برای نیل به محافظت از آن‌ها است و در این تحقیق مدنظر قرار گرفته است. لذا نوآوری این تحقیق را می‌توان در نگاه راهبردی، جامع‌نگری، نگاه ویژه به سوابق حملات و ارائه الگوی راهبردی برای حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی مبتنی بر ابعاد و مؤلفه‌های خاص ج.ا.ا، نوآوری دانست که با بهره‌گیری از اسناد بالادستی، مطالعه مدل‌های بین‌المللی، انجام مصاحبه خبرگی، مستندسازی نظرات خبرگان حوزه امنیت و دفاع سایبری صورت گرفته است.

مبانی نظری

اطلاعات راهبردی: اطلاعات راهبردی ناظر به همه اطلاعاتی است که در سطوح کلان تصمیم‌گیری در کشور مورد استفاده می‌باشد. این اطلاعات در حوزه‌های مختلف دفاعی، سیاسی – امنیتی، اقتصادی و فرهنگی- اجتماعی شکل می‌گیرد. اطلاعات راهبردی باعث شکل‌گیری سازوکارها، خط‌مشی‌ها و طرح‌های عملیات اطلاعاتی در همه سطوح ملی و بین‌المللی می‌گردد و لذا ضعف در اطلاعات راهبردی تأثیر مستقیم در مواجهه با حل مسائل راهبردی کشور در همه حوزه‌های راهبردی، عملیاتی و اجرایی خواهد داشت (Esmaeili,2014:2).

زیرساخت حیاتی: طبق تعریف دولت آمریکا، زیرساخت‌های حیاتی عبارت‌اند از (Poustourli et al.,2015:552): «دارایی‌ها، سامانه‌ها، شبکه‌های فیزیکی یا مجازی که برای ایالات متحده ضروری بوده و نابودی یا ناتوانی آن‌ها تأثیر مخربی بر امنیت، اقتصاد ملی، سلامت عمومی یا هر ترکیبی از این مسائل دارد. همچنین کمیسیون اروپا زیرساخت‌های حیاتی را چنین تعریف می‌کند» (Poustourli et al.,2015: 551): دارایی‌ها، سامانه‌ها یا بخشی از آن‌ها در کشورهای عضو که برای بقای عملکردهای اجتماعی اساسی، سلامت، بهداشت، امنیت، اقتصاد، رفاه مردم ضرورت دارند و تخریب یا ناتوانی آن‌ها تأثیر قابل توجهی

خواهد داشت.

سازمان پدافند غیرعامل زیرساخت‌های کشور را به‌صورت زیرساخت‌های حیاتی، حساس و مهم تقسیم‌بندی کرده است. زیرساخت‌های حیاتی، زیرساخت‌هایی هستند که مرتبط با امنیت ملی است و همچنین اگر در معرض تهدید قرار گیرند کشور دچار مخاطره[1]جدی خواهد شد.[2] در کشورمان، مراکز حیاتی مراکزی هستند که در صورت تخریب کامل یا بخشی از آن، موجب بروز بحران، آسیب و صدمات جدی در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با تأثیرگذاری در سطح ملی می‌گردد (مصطفایی، ۱۳۹۴: ۳۳).

زیرساخت اطلاعاتی حیاتی: سامانه‌های اطلاعاتی به‌هم‌پیوسته که اختلال یا تخریب آن‌ها تأثیر جدی بر سلامت، ایمنی، امنیت، رفاه، اقتصاد و حاکمیت در سطح ملی دارد (Segura Serrano,2015: 3). در این تحقیق، منظور از زیرساخت‌های اطلاعاتی حیاتی، مراکز داده، اطلاعات راهبردی در حوزه‌های اتوماسیون صنعتی، بانکی، مالی، حمل‌ونقل، سلامت، خدمات الکترونیکی دولت، سیاست خارجی، امنیتی، نظامی، ... و همچنین نرم‌افزارهای پردازشی اطلاعات راهبردی است که زیرساختی را برای تجمیع (ذخیره‌سازی، یکپارچه‌سازی،...)، تبادل و بهره‌برداری از اطلاعات راهبردی فراهم می‌کنند و همچنین بخشی از فناوری اطلاعات و ارتباطات که اطلاعات راهبردی در آن جریان دارد، به‌طوری که اختلال یا تخریب داده، منجر به وارد شدن خسارت جدی به امنیت ملی و منافع عمومی می‌شود.

ویژگی زیرساخت‌های اطلاعاتی حیاتی: با آنکه اختلاف نظرهایی در تعیین خدمات و دارایی‌های زیرساخت‌های اطلاعاتی حیاتی وجود دارد (ENISA, 2014: 22) به‌طوری که فهرست دقیقی از خدمات حیاتی در دسترس نیست و همچنین تعریف معیار حیاتی بودن برای تعیین دارایی‌های حیاتی خود یک فرآیند چالشی است و همچنین همکاری مؤثر بین بخش‌های مختلف دولتی و خصوصی برای تعیین و حفاظت از خدمات و دارایی‌ها،

---

۱ Risk

۲. به نقل از خبرگزاری مهر در ۳ آبان ۱۳۹۵، شناسه خبر ۳۸۰۴۸۹۳، (https://www.mehrnews.com)

ضرورت دارد، لکن ویژگی‌های مشترکی که در زیرساخت‌های اطلاعاتی حیاتی وجود دارند عبارت‌اند از (Koyabe,2015: 13): شبکه‌ای بودن، فرابخشی بودن، مجتمع با قابلیت دسترسی محدود، دارای اطلاعات با ارزش بسیار بالا، تصمیم‌ساز، محور بودن داده و اطلاعات، تسهیل‌کننده نظارت، کنترل و مدیریت کلان، تأثیرگذاری وسیع، اهمیت بالای محرمانگی و جامعیت، پشتیبان و ضروری برای عملکرد زیرساخت‌های حیاتی، مؤثر در اقتصاد و سلامت و امنیت ملی، نقطه هدف هکرها و بدافزارها و حملات سایبری، تمرکز عمده بر دارایی‌ها و سرمایه‌های فناوری پایه.

اجزای زیرساخت‌های اطلاعاتی حیاتی و تهدیدات مربوطه: جدول ۱، عناصر، تهدیدات و راه‌حل‌های راهبردی زیرساخت‌های اطلاعاتی حیاتی را نشان می‌دهد:

جدول ۱. عناصر، آسیب‌پذیری‌ها، تهدیدات و راه‌حل‌ها در زیرساخت‌های اطلاعاتی حیاتی

عناصر	آسیب‌پذیری‌ها و تهدیدات	راه‌حل‌ها
مراکز داده	حملات منع خدمات توزیع‌یافته، حملات ویروسی، آسیب‌پذیری‌های مدیریت دسترسی، آسیب‌پذیری‌های مدیریت پیکربندی، تهدیدات مخرب داخلی، حملات چندمرحله‌ای، مهندسی اجتماعی، داده‌های رمزنگاری‌نشده، حملات حرارتی و ... (Gao et al.,2018:1).	توسعه سیاست‌های امنیتی داده، شبکه و میزبان-توسعه عملیاتی امنیت شبکه و ارتباطات مرکز داده-تعیین طرح امنیت راهبردی شبکه و ارتباطات مرکز داده-تعیین سطح حفاظتی داده‌های ذخیره‌شده-تعیین حساسیت داده‌ها-ایجاد سیستم تأیید هویت و مجوز-کنترل‌های امنیتی-آزمون‌ها و ممیزی امنیتی در شبکه و ارتباطات مرکز داده-امنیت افراد-تهیه گزارش‌ها-آموزش امنیت فناوری اطلاعات-مدیریت مخاطره امنیتی-تداوم کسب‌وکار-استفاده از استانداردهای اختصاصی
اتوماسیون صنعتی	حملات علیه دسترس‌پذیری انکار دسترسی به دارایی سامانه‌های کنترل صنعتی، ایستگاه‌های مهندسی، سیستم ارتباطی و کنترلی، تجربه استاکس نت (حمله مخرب به سیستم‌عامل اسکادا) حملات علیه جامعیت، حملات علیه محرمانگی (دسترسی به گذرواژه‌ها، پیکربندی کنترل‌گرهای منطقی) (Drias et al., 2015: 6).	استفاده از کنترل خاص (تجربه استاکس نت)، اختصاصی کردن سامانه‌های تشخیص نفوذ برای سامانه‌های کنترل صنعتی که بر اساس ویژگی حملات، تشخیص ناهنجاری، مدل‌های آماری، مشخصات سیستم، مشخصات پروتکل‌ها، همچنین رفتار اجزای سامانه‌های کنترل صنعتی عمل کنند - استفاده از اقدامات رمزنگاری همراه با مدیریت کلید با حداقل کلید و حداقل تبادل بین گره‌های سیستم، استفاده از استانداردهای اختصاصی.
امور بانکی	ارزهای دیجیتال رمز پایه که غیرمتمرکز،	تعریف و ایجاد ارز دیجیتالی با کشورهای همسو.

عناصر	آسیب‌پذیری‌ها و تهدیدات	راه‌حل‌ها
	بدون واسطه، ناشناس بودن معامله‌گران، فاقد رصدپذیری از طرف نهادهای ملی.	
حمل‌ونقل	هک سامانه‌های حیاتی هوانوردی، حمله ناشی از ضعف کنترل دسترسی به سیستم مدیریت پرواز هواپیما، سرایت دادن بدافزار بر روی رابط‌های خارجی بی‌سیم، وجود آسیب‌پذیری جدی در سامانه‌های کنترل دریایی (Eichenhofer,2017:5)، حملات سایبری به زیرساخت ریلی ۲۰۱۶، تهدیدات سایبری شبکه خودرویی، نرم‌افزار «ویز».	پیاده‌سازی مکانیسم‌های امنیتی (احراز هویت داده و کنترل دسترسی)، امنیت نرم‌افزار، داده و ارتباطات در لینک‌های ارتباطی، ارزیابی و مدیریت مخاطره، لاگ‌گیری از رویدادهای امنیتی و تحلیل ترافیک شبکه و تشخیص نفوذ، ارزیابی کنترل‌های امنیتی و میزان کارآمدی آن‌ها- مدیریت دارایی‌های ثابت و سیار، آموزش (آگاهی‌بخشی، مسئولیت‌پذیری، نقش‌دهی)، حفظ حریم خصوصی افراد، شکل‌دهی سیاست پاسخ‌دهی به حوادث، استفاده از استانداردهای اختصاصی.
خدمات سلامت	هکرها، ویروس‌ها و کرم‌های تهدیدکننده امنیت و حریم خصوصی در پرونده الکترونیک سلامت، افشای پرونده سلامت، دسترسی‌های غیرمجاز به پرونده الکترونیک سلامت.	توجه به جامعیت، محرمانگی و دسترس‌پذیری، جلوگیری از افشای داده بیماران (با لحاظ کردن امنیت و کنترل دسترسی و محدودیت‌های دسترسی)، امنیت داده بیماران (از طریق مسئولیت‌ها، راه‌حل‌های فنی، پروتکل‌های امنیتی و توافقنامه‌ها)، اجازه به بیماران برای کنترل اطلاعاتشان، ایجاد بستر ارتباطی امن برای تجمیع، اشتراک‌گذاری و تبادل داده، انطباق با الزامات امنیتی پیاده‌سازی پرونده الکترونیک سلامت، حفظ حریم خصوصی، دقت و کیفیت، استفاده از استانداردهای ISO 29100 وISO/IEC27002
خدمات الکترونیکی دولت	آسیب‌پذیری‌های سیستم مدیریت احراز هویت، تصدیق اصالت مرجع، صحت‌سنجی.	تبادل امن اطلاعات، دسترسی امن به اطلاعات.
اطلاعات راهبردی	رانت‌های اطلاعاتی، دسترسی غیرمجاز، خدشه در جامعیت داده‌های تصمیم‌ساز، آسیب‌پذیری‌های شبکه ارتباطی حاکمیت،	کنترل دسترسی، استفاده از رمزنگاری و حاکم بودن محرمانگی و جامعیت، نقش نیروی انسانی در تمام مراحل تولید و انتقال و ذخیره و بهره‌برداری، امنیت ملی.
نظارت بین‌المللی بر خدمات مالی	اشراف اطلاعاتی بر سامانه‌های تبادل اطلاعات مالی و رصد جریان پولی، اعمال محدودیت و فشار مالی بر مؤلفه‌های قدرت ملی، محدودسازی مالی محور مقاومت.	بازدارندگی و امنیت‌افزایی قوانین و مقررات و تناسب آن‌ها با تهدیدات کارگروه ویژه اقدام مالی، اجرای قوانین داخلی مبارزه با پول‌شویی.

لایه‌های زیرساخت‌های اطلاعاتی حیاتی: می‌توان زیرساخت‌های اطلاعاتی حیاتی را از منظر عملیاتی، دارای چهار لایه زیرساخت، خدمات، محتوا و کاربر دانست. در زیرساخت‌های

اطلاعاتی حیاتی هر کدام از لایه‌ها دارای اجزایی هستند که در جدول ۲ آمده است:

جدول ۲. اجزای لایه‌های زیرساخت‌های اطلاعاتی حیاتی

لایه	اجزاء
زیرساخت	زیرساخت‌های داده / زیرساخت‌های اطلاعاتی و محتوایی / شبکه (ساختار، معماری و پیکربندی، عملیات و اجزاء، منابع و تجهیزات، حسابداری) / زیرساخت‌های نرم‌افزاری و پردازشی / زیرساخت‌های کاربردی و خدماتی / زیرساخت‌های رایانشی / زیرساخت‌های پایه / زیرساخت‌های ذخیره و پشتیبان‌گیری.
خدمات	نرم‌افزارهای پردازشی و برنامه‌های کاربردی، خدمات شبکه محوری، نرم‌افزارهای پایه.
محتوا	— داده‌ها و اطلاعات حساس مراکز داده — اطلاعات کنترل و پایش در دیسپاچینگ‌ها — اطلاعات حیاتی موجود در سامانه‌های بانکداری الکترونیکی — اطلاعات مدیریتی، فرماندهی و کنترلی حوزه حمل‌ونقل موجود در سامانه‌های ناوبری، سامانه‌های ارتباطی، سامانه‌های گزارشی، سامانه‌های اسکادا، لینک‌های ارتباطی — اطلاعات موجود در سامانه‌های حیاتی حوزه سلامت (سامانه پرونده الکترونیک سلامت، اطلاعات هویت ژنتیک) — داده‌های اشتراک‌گذاری‌شده، اطلاعات یکپارچه‌شده در تعامل بین دستگاه‌ها، تراکنش‌های خدمات یکپارچه دولت در خدمات الکترونیکی دولت — اطلاعات طبقه‌بندی‌شده در حوزه‌های سیاست خارجی (اسناد و مکاتبات وزارت امور خارجه در رابطه با کشورهای خاص، اسناد و گزارش‌های محرمانه گروه امنیت ملی و سیاست خارجی مجلس شورای اسلامی، اسناد شورای راهبردی روابط خارجی، اسناد مجمع تشخیص مصلحت نظام)، همچنین در حوزه نظامی و دفاعی (اسناد مربوط به دفاع در خارج از مرزها– اسناد مربوط به پیشرفت‌های نظامی، مانند پروژه‌های موشکی – اسناد سازمان‌های حفاظت اطلاعات سپاه و ارتش و ناجا در مباحث رصد و پیشگیری، کشف، شناسایی و خنثی کردن فعالیت‌های براندازی، جاسوسی، خرابکاری، موارد ایجاد نارضایتی، نفوذ جریانات سیاسی و ایجاد اختلال در انجام مأموریت‌ها)، امنیتی (اسناد طبقه‌بندی‌شده، سامانه‌های کلیدی، داده‌کاوی‌ها در وزارت اطلاعات، جامعه اطلاعاتی کشور) است.
کاربر	نیروی انسانی دارای دسترسی به اطلاعات حساس در مراکز داده، دسترسی به ساختار دیسپاچینگ‌های ملی، افراد کلیدی یا شرکت‌های رابط مؤثر در سامانه‌های بانکداری الکترونیکی، افراد دارای دسترسی به اطلاعات مدیریتی، فرماندهی و کنترلی در سامانه‌های ناوبری، ارتباطی، گزارشی، اسکادا، لینک‌های ارتباطی حوزه حمل‌ونقل، افراد کلیدی سامانه پرونده الکترونیک سلامت و اطلاعات هویت ژنتیک در سامانه‌های حیاتی حوزه سلامت، افراد کلیدی در تراکنش‌های خدمات

	یکپارچه در خدمات الکترونیکی دولت، نیروی انسانی دارای دسترسی به اطلاعات طبقه‌بندی‌شده در حوزه‌های سیاست خارجی و نظامی و دفاعی و امنیتی است.

مفهوم حفاظت از زیرساخت‌های اطلاعاتی حیاتی: در اسناد جهانی، برای حفاظت از زیرساخت‌های اطلاعاتی حیاتی، به‌جای تعریف، از عبارات مفهوم[1]، کارهای اساسی[2]، الزامات[3]، توصیه‌ها[4] و اصول[5] استفاده می‌شود. در آمریکا، مفهوم حفاظت از زیرساخت‌های اطلاعاتی حیاتی عبارت است از محافظت از مؤلفه‌های مجازی زیرساخت‌های اطلاعاتی حیاتی که جامعه به آن نیاز دارد. این محافظت بایستی در قبال آسیب‌پذیری‌هایی متعدد (مانند دسترسی‌های غیرمجاز به اطلاعات حساس و محرمانه، تخریب، دستکاری، محدودسازی دسترسی عوامل کاهنده عواقب حملات) باشد. از اهداف این محافظت، جلوگیری از حملات سایبری علیه زیرساخت‌های حیاتی و کاهش آسیب‌پذیری‌ها و همچنین حداقل‌سازی آسیب‌ها و در نهایت حداقل‌سازی زمان بازیابی از حملات سایبری می‌باشد. از «کارهای اساسی» برای حفاظت می‌توان به پیشگیری و هشدار اولیه، تشخیص، واکنش، مدیریت بحران اشاره کرد (paik et al., 2012:35). در کشور آلمان «کارهای اساسی» برای حفاظت سایبری به‌صورت «پیشگیری کافی، واکنش مؤثر، پایداری از طریق تقویت امنیت» بیان شده است (Kaska & Trinberg, 2015: 38). در کشور استرالیا «الزامات» حفاظت به‌صورت «تشخیص، ارزیابی و کاهش مخاطرات، ارزیابی خدمات و دارایی‌های فناوری اطلاعات و ارتباطات، شناسایی زیرساخت‌های اطلاعاتی حیاتی، ارزیابی سلامت دارایی‌ها، اتخاذ واکنش مناسب در راستای کاهش مخاطرات» تعیین شده است (Victorian Government CIO Council,2012). سازمان همکاری و توسعه اقتصادی[6] «توصیه‌هایی» مانند «سیاست‌گذاری شفاف، تعیین نهادهای راهبر، افزایش سطح امنیت، داشتن راهبرد ملی

1. Concept
2. Tasks
3. Requirements
4. Recommendations
5. Principles
6. The Organisation for Economic Co. operation and Development's OECD

مدیریت مخاطرات، ایجاد تیم‌های پاسخگو، راه‌اندازی سازوکار تبادل اطلاعات، همکاری‌ها» را عنوان کرده است (Segura Serrano,2015: 3) و همچنین کشورهای عضو G8، «اصول» حفاظت را به‌صورت «سیاست‌گذاری، قانون‌گذاری، داشتن شبکه‌های هشدار، شناخت وابستگی بین زیرساخت‌ها، سازوکار تبادل اطلاعات، شبکه ارتباطی شرایط بحران، همکاری‌ها، افزایش توانمندی پاسخ‌دهی، تحقیق و توسعه»، بیان کرده‌اند (Luiijf, 2016: 35). در این تحقیق تعریف عملیاتی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی عبارت است از: اعمال حکمروایی و ارتقای امنیت و کاهش مخاطرات سایبری در جهت پیشگیری، تشخیص، واکنش جهت مقابله با تهدیدات سایبری در زیرساخت‌های اطلاعاتی حیاتی که این تهدیدات ناشی از دولت‌های متخاصم، مزدوران سایبری، جاسوسان سایبری، تروریست‌های سایبری، مجرمین سازمان‌یافته سایبری و هکتویست هستند.

حملات سایبری: حملات سایبری عبارت‌اند از: بهره‌برداری عملیاتی مخرب از فضای سایبر (منع خدمات، جعل، سرقت، دست‌کاری، تخریب اطلاعات، کنترل جریان اطلاعات، تخریب ارتباط بین سامانه‌ها، ...) که باعث وارد شدن خدشه به دسترس‌پذیری، جامعیت، محرمانگی در سامانه‌ها و یا داده‌های آن‌ها می‌شود. در تعریف حملات سایبری گفته شده که عملیاتی با توانایی سرقت اطلاعات و آسیب رساندن به سامانه‌های رایانه‌ای و ارتباطی و شبکه‌های حیاتی (مانند انرژی، حمل‌ونقل، سامانه‌های فرماندهی و کنترل) است (Akyazi,2014:15). در تعریف دیگری حملاتی با قابلیت‌های: الف) دسترسی غیرمجاز به اطلاعات حیاتی ذخیره‌شده یا منتقل‌شده؛ ب) تخریب، اصلاح یا جایگزینی نرم‌افزارهای پردازشی مورد نیاز؛ پ) محدود کردن دسترسی به عوامل کاهش‌دهنده پیامد حملات ذکر شده است (Youm et al, 2015:25). همچنین تهدیدات علیه دسترس‌پذیری، جامعیت و محرمانگی اطلاعات حیاتی، منابع سخت‌افزاری و نرم‌افزاری و مجوزهای دسترسی را حملات سایبری گویند (Cazorla et al.,2016: 6). وزارت دفاع آمریکا حمله سایبری را چنین تعریف می‌کند (FFIEC, 2015: 5): تلاش برای آسیب‌رسانی، تخریب، مختل ساختن، غیرفعال‌سازی، به دست آوردن دسترسی غیرمجاز به رایانه، سامانه رایانه‌ای، محیط

محاسباتی، زیرساخت محاسباتی، شبکه ارتباطی الکترونیکی از طریق فضای سایبری به‌منظور از بین بردن جامعیت داده یا سرقت اطلاعات کنترل‌شده.

حفاظت از زیرساخت‌های اطلاعاتی حیاتی در اسناد بالادستی: حفاظت از زیرساخت‌های (اطلاعاتی) حیاتی و امنیت به‌عنوان بخشی از فرآیند حفاظت، در برنامه همه کشورها وجود دارد و در کشور ما نیز در اسناد بالادستی سیاست‌های کلی نظام در حوزه امنیت فضای تولید و تبادل اطلاعات کشور–افتا (منوط کردن توسعه فناوری اطلاعات و ارتباطات به رعایت ملاحظات امنیتی و همچنین با تأکید بر ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای امن‌سازی زیرساخت‌های حیاتی و حساس و مهم در حوزه فناوری اطلاعات و ارتباطات و ارتقای مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور به‌منظور استمرار خدمات عمومی، پایداری زیرساخت‌های ملی، صیانت از اسرار کشور)، سند راهبردی پدافند غیرعامل در حوزه الکترونیک (تأکید بر استفاده از محصولات سایبری امن بومی در زیرساخت‌های حیاتی و حساس کشور)، سند افتا، حکم تشکیل شورای عالی فضای مجازی و تمدید عضویت اعضای آن (با تأکید بر ایجاد آمادگی لازم در عالی‌ترین سطح به‌منظور صیانت از زیرساخت‌های حیاتی در برابر حملات اینترنتی و دفاع مناسب در برابر هرگونه حمله)، سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای، سیاست‌های کلی برنامه ششم توسعه (افزایش ظرفیت‌های قدرت نرم و دفاع سایبری و تأمین پدافند و امنیت سایبری برای زیرساخت‌های کشور)، سند راهبردی نظام جامع فناوری اطلاعات کشور (استقرار نظام امنیت فضای الکترونیکی تبادل اطلاعات کشور)، نظام ملی پیشگیری و مقابله با حوادث فضای مجازی (ایجاد ساختار مناسب، تقسیم کار ملی، هماهنگی و همکاری ملی)، سند حمایت از افراد موضوع داده (رعایت حقوق افراد موضوع داده، امنیت، حریم خصوصی، مسئولیت‌پذیری، ایجاد تعادل میان حقوق افراد و منافع ملی، نحوه حفاظت داده‌ها و مدیریت به‌کارگیری آن)، سند تبیین الزامات شبکه ملی اطلاعات، سند الزامات امنیتی عملیاتی زیرساخت‌های حیاتی (الزامات امنیت سایبری سامانه‌های کنترل صنعتی)، سند

الزامات اینترنت اشیاء بر بستر شبکه ملی اطلاعات (ملاحظه مخاطرات اینترنت اشیاء برای زیرساخت‌های حیاتی کشور، تحقق اینترنت اشیاء بر بستر شبکه ملی اطلاعات با اعضای شناسنامه‌دار، بومی‌سازی نظام‌مند اجزای زیست‌بوم اینترنت اشیاء، مشمول بودن کلان داده‌های تجمیع‌شده از کاربران به الزامات حمایت از داده افراد) مورد تأکید است.

منشأ حملات سایبری علیه زیرساخت‌های اطلاعاتی حیاتی: حملات سایبری عبارت‌اند از: نفوذ و بهره‌برداری غیرمجاز از شبکه دیجیتال و ممانعت کاربران از دسترسی به خدمات، تخریب ماشین‌های کنترل‌شونده با رایانه به‌طوری‌که بهره‌برداری سایبری منجر به نفوذ در شبکه رایانه‌ها و دریافت اطلاعات شود (Kiboi,2015:39). تهدیدکنندگان، انگیزه‌های مختلف سیاسی، امنیتی، اقتصادی یا رقابتی را دنبال می‌کنند. این تهدیدکنندگان نیمه‌سخت می‌توانند دولت‌های متخاصم، مزدوران سایبری یا گروه‌های تحت حمایت دولت‌ها، جاسوسان سایبری، تروریست‌های سایبری، مجرمین سازمان‌یافته سایبری، هکرها با انگیزه‌های سیاسی (هکتویست‌ها) باشند که از روش‌های شناسایی، مانند پویش، استراق سمع، جمع‌آوری بسته‌ها و ... استفاده می‌کنند (آندرس، ۱۳۹۶: ۷۹).

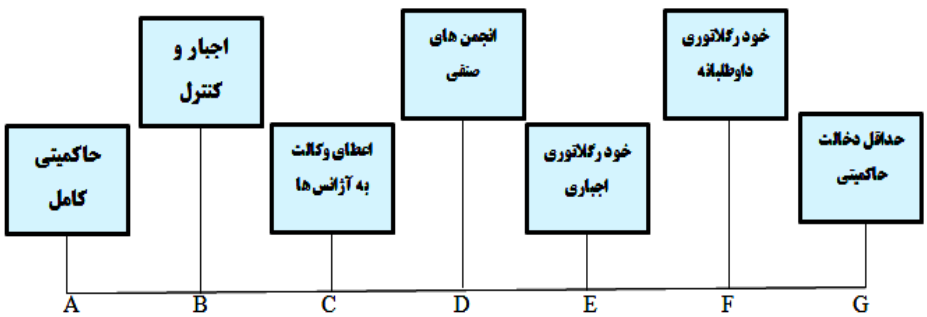
تنوع تهدیدات سایبری علیه زیرساخت‌های حیاتی: بالاترین تهدیدات سایبری ازجمله تهدیدات علیه زیرساخت‌های حیاتی عبارت‌اند از (ENISA,2018:29): بدافزارها، حملات وب پایه، فیشینگ، منع خدمات، اسپم، بات نت، نقض اطلاعات[1]، تهدیدات داخلی[2]، سرقت و تخریب داده[3]، نشت اطلاعات[4]، سرقت هویت، رمزکاوی[5]، باج‌افزار[6]، جاسوسی سایبری. در این بین تهدید «بدافزار» در صدر قرار دارد و اولین هدف‌گذاری بدافزارها به خطر انداختن زیرساخت‌های اطلاعاتی حیاتی است که به‌عنوان نمونه می‌توان به استاکس نت اشاره کرد.

---

1. Data Breaches
2. Insider Threat
3. Damage/Theft
4. Information Leakage
5. Cryptojacking. Cryptomining
6. Ransoware

رویکردهای حفاظت از زیرساخت‌های اطلاعاتی حیاتی: رویکرد دولت‌ها در زمینه حفاظت از زیرساخت‌های اطلاعاتی حیاتی متفاوت بوده و همچنان که در شکل ۱ نشان داده‌شده، می‌تواند یکی از حالت‌های زیر باشد (Min,2015: 15): کاملاً حاکمیتی (حفاظت کامل حاکمیت از دارایی زیرساخت‌ها)، اجباری کردن استانداردهای امنیت سایبری توسط دولت، استانداردسازی، نظارت و اجرای امنیت در زیرساخت‌های اطلاعاتی توسط آژانس‌های عمومی، حفاظت توسط انجمن‌های صنفی، اجرای حفاظت با بخش خصوصی و تصدیق با حاکمیت، ایجاد و اجرای استانداردها به‌طور خصوصی و پذیرش استانداردها به‌عنوان تجارب موفق، تشویق و روان‌سازی و ایجاد چارچوب قانونی توسط حاکمیت و حداقل دخالت.

آمریکا و رژیم صهیونیستی دارای درک مشترک از تهدیدات هستند ولی دارای سیاست‌گذاری متفاوتی هستند. در آمریکا، مکانیسم‌های حفاظت از زیرساخت‌های اطلاعاتی حیاتی، بر پایه بازار است (سمت راست نمودار). در حالی که در رژیم صهیونیستی، محوریت با حاکمیت است (سمت چپ نمودار) و مداخله آن بر پایه تدارک تجهیزات امنیتی برای رگلاتوری است.



شکل ۱. رویکردهای حفاظت (Min,2015: 15)

اقدامات بین‌المللی در زمینه حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی: جدول ۳

فعالیت نهادهای بین‌المللی را در موضوع حفاظت از زیرساخت‌های اطلاعاتی حیاتی نشان می‌دهد که هر کدام از آن‌ها، دارای موضوع و الزامات خاصی هستند:

جدول ۳. فعالیت‌های بین‌المللی در موضوع حفاظت از زیرساخت‌های اطلاعاتی حیاتی (Satola et al.,2017:318)

نهادها	موضوعات مرتبط با حفاظت از زیرساخت‌های اطلاعاتی حیاتی
اجلاس جهانی جامعه اطلاعاتی	تدوین مجموعه اصول و برنامه عملی در زمینه ایجاد تنظیم مقررات و محیط سیاست‌گذاری جهت حداکثرسازی مزایای جامعه اطلاعاتی، تصریح در ارتقای فرهنگ جهانی امنیت سایبری با هدف افزایش محرمانگی، حفاظت از جامعیت داده و شبکه و همچنین مورد توجه قرار دادن تهدیدات فناوری اطلاعات و ارتباطات و دیگر موضوعات امنیت شبکه و امنیت اطلاعات.
ITU	ارائه مدل چهار مرحله‌ای شامل مراحل پیشگیری و هشدار، تشخیص، واکنش و مدیریت بحران.
انجمن تیم‌های پاسخ به حوادث امنیتی[1]	نهاد بین‌المللی فنی فعال در تهیه استانداردهاست که با تعدادی از تیم‌های پاسخ به حوادث رایانه‌ای همکاری می‌کند و زمینه اشتراک‌گذاری اطلاعات بین تعدادی از تیم‌های پاسخ به حوادث رایانه‌ای و دیگر سازمان‌های پاسخ‌دهی به حوادث را آماده می‌کند و انباره‌ای از اطلاعات لازم برای حفاظت از زیرساخت‌های حیاتی را دارا است.
OECD	ارائه‌دهنده «خطوط راهنما برای امنیت سامانه‌ها و شبکه‌های اطلاعاتی» جهت فرهنگ‌سازی امنیت است.
کشورهای G8	اصول نه‌گانه‌ای را ارائه کرده است؛ شامل داشتن شبکه‌های هشدار، ارتقای سطح آگاهی، شناسایی وابستگی بین زیرساخت‌های اطلاعاتی حیاتی، ارتقای مشارکت بین سهامداران عمومی و خصوصی، داشتن شبکه‌های ارتباطی برای شرایط بحران، اطمینان داشتن از وجود سیاست‌های دسترسی به داده به‌عنوان الزام، وجود قوانین کافی در تعقیب حملات، تسهیل ردیابی حملات و تبادل تجربیات، انجام رزمایش‌ها و تمرینات، مشارکت در همکاری‌های بین‌المللی.
اتحادیه اروپا	طرح پنج مرحله‌ای شامل آمادگی و پیشگیری، تشخیص و واکنش، مقابله و بازیابی، تقویت همکاری بین‌المللی در زمینه اصول و دستورالعمل‌های تاب‌آوری، توسعه معیارهای شناختی را ارائه کرده است و همچنین چارچوبی را با هشت محور (امنیت جامع سیستمی، مدیریت مخاطرات و تحلیل آسیب‌پذیری، پیشگیری و تشخیص، پاسخ به حوادث و بازیابی، بقاپذیری سامانه‌ها، مباحث حقوقی و سیاست‌گذاری، تحقیق و توسعه بنیادی و مسائل غیر فنی) ارائه کرده است.

1. The Forum of Incident Response and Security Teams (FIRST)

نهادها	موضوعات مرتبط با حفاظت از زیرساخت‌های اطلاعاتی حیاتی
سازمان بین‌المللی استاندارد[1]	پوشش‌دهنده استانداردهایی است که مرتبط با زیرساخت اطلاعات و سامانه‌های ارتباطی و فناوری اطلاعات است.
انجمن حکمرانی اینترنت[2]	مدل جذابی برای مشاوره‌های حفاظتی و انجمن بین‌المللی برای دیالوگ‌های بسیار وسیع حول حفاظت از زیرساخت‌های حیاتی است.
کشورهای پیشرو	در آمریکا در طرح‌های NIPP[3]، Presidential Commission on Critical Infrastructure Protection، National Strategy for Physical Protection of Critical Infrastructure and Key Assets بر توجه به امنیت و تاب‌آوری در زیرساخت‌های حیاتی، اولویت‌بندی، هدایت سازمان‌یافته و هماهنگ کردن فعالیت‌ها، ارتقای آمادگی ملی، مدیریت مخاطرات، داشتن نقش مؤثر در نهادهای بین‌المللی مرتبط، همکاری بین‌المللی و تبادل اطلاعات تهدیدات، اجرای رزمایش‌های سایبری، آموزش، راه‌اندازی مراکز هشدار، مشارکت فعال محققان و مراکز تحقیقاتی و آزمایشگاهی تأکید شده است. در آلمان در قانون IT Security Act، طرح مشارکت برای حفاظت از زیرساخت‌های حیاتی، قانون فدرالی تقویت امنیت اطلاعات و ...بر پیاده‌سازی اقدامات فنی و سازمانی، انجام ممیزی امنیتی و اعمال استانداردها، تبادل و تحلیل اطلاعات امنیتی، هدایت سازمان‌یافته فعالیت‌ها و هماهنگ کردن فعالیت‌ها در راستای مدیریت امنیت، راه‌اندازی مدیریت مخاطرات، راه‌اندازی مراکز واکنش سریع و همکاری بین‌المللی تأکید شده است. در فرانسه آژانس ANSSI[4] به‌عنوان مسئول اصلی حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی، چهار وظیفه اصلی راهبری، بازرسی، اعمال مدیریت بحران، تعیین الزامات امنیتی را بر عهده دارد. در کره جنوبی قانون حفاظت از زیرساخت‌های اطلاعاتی کره جنوبی و در استرالیا شبکه TISN[5]، طرح ضد تروریسم ملی و راهبرد تاب‌آوری زیرساخت‌های حیاتی مورد استفاده قرار می‌گیرند.

در بین مراجع مذکور، OECD و G8 و طرح EU Action Plan، بیشتر از بقیه مراجع، به جزئیات حفاظت پرداخته‌اند. دستورالعمل‌های سازمان OECD در رابطه با حفاظت از زیرساخت‌های اطلاعاتی حیاتی برای کشورهای عضو عبارت‌اند از (OECD,2018:28):

۱) حفاظت از زیرساخت‌های اطلاعاتی حیاتی در سطح داخلی:

---

1. The International Organization for Standardization (ISO)
2. The Internet Governance Forum (IGF)
3. National Infrastructure Protection Plan (NIPP)
4. Agence nationale de la sécurité des systèmes d'information (ANSSI)
5. Trusted Information Sharing Network

۱-۱) اتخاذ سیاست با اهداف شفاف در بالاترین سطح دولتی همراه با تعیین نهادهای دولتی متولی

۱-۲) همکاری با بخش خصوصی و اپراتورهای زیرساخت‌های اطلاعاتی حیاتی برای نیل به اهداف

۱-۳) بررسی سامانمند سیاست‌ها و چارچوب‌ها و تنظیم طرح‌های زیرساخت‌های اطلاعاتی حیاتی

۱-۴) انجام اقداماتی برای افزایش سطح امنیت اجزای شبکه‌ها و سیستم اطلاعاتی

۱-۵) مدیریت مخاطرات از طریق: توسعه راهبرد ملی تعهدآور برای دولت و بخش خصوصی، ارزیابی مخاطره بر اساس تحلیل آسیب‌پذیری‌ها و تهدیدات زیرساخت‌های اطلاعاتی حیاتی، ارزیابی و بررسی دوره‌ای فرآیند مدیریت مخاطره جهت نظارت بر اجرای راهبرد مدیریت مخاطرات

۱-۶) ایجاد تیم پاسخ به حوادث با مسئولیت نظارت، هشداردهی، بازیابی، ارتقای همکاری

۱-۷) همکاری با بخش خصوصی در زمینه‌های مدیریت مخاطره، پاسخ به حوادث، تبادل اطلاعات، تحقیق و توسعه پروژه‌های بهبود امنیت زیرساخت‌های اطلاعاتی حیاتی

۲) حفاظت از زیرساخت‌های اطلاعاتی حیاتی در بین کشورهای عضو به‌صورت دو یا چندجانبه:

۲-۱) تبادل دانش و تجربه برای توسعه شیوه‌ها، سیاست‌های داخلی، نحوه مشارکت با اپراتورها

۲-۲) توسعه درک مشترک از مخاطرات، آسیب‌پذیری‌ها، تهدیدات و تأثیر آن‌ها بر زیرساخت‌های اطلاعاتی حیاتی

۲-۳) تسهیل در شناساندن همتایان از طریق دسترس‌پذیر کردن اطلاعات مربوط به نهادهای ملی درگیر در حفاظت از زیرساخت‌های اطلاعاتی حیاتی، نقش و مسئولیت آن‌ها

جهت بهبود اقدامات فرامرزی

۲-۴) پشتیبانی از همکاری بین‌المللی در تحقیق و توسعه مرتبط

همچنین هشت کشور صنعتی (آمریکا، بریتانیا، ایتالیا، فرانسه، آلمان، ژاپن، کانادا و روسیه) موسوم به گروه هشت G8 نیز اصولی را برای حفاظت از زیرساخت‌های اطلاعاتی حیاتی اعلام کرده‌اند (Luiijf, 2016: 35):

۱) کشورها بایستی شبکه‌های هشدار اضطراری را در برابر تهدیدات و آسیب‌پذیری‌های سایبری داشته باشند.
۲) کشورها بایستی سطح آگاهی را بالا ببرند تا حفاظت از زیرساخت‌های اطلاعاتی حیاتی بهبود یابد.
۳) کشورها بایستی زیرساخت‌های خود را بررسی کرده و وابستگی بین آن‌ها را شناسایی کنند تا حفاظت از زیرساخت‌های اطلاعاتی حیاتی بهبود یابد.
۴) کشورها بایستی مشارکت بین سهامداران عمومی و خصوصی را ارتقا دهند تا با تحلیل اطلاعات زیرساخت‌های حیاتی، پیشگیری و یا پاسخ‌دهی مناسب به حملات علیه این زیرساخت‌ها رخ دهد.
۵) کشورها بایستی شبکه‌های ارتباطی شرایط بحران را داشته باشند.
۶) کشورها بایستی از وجود سیاست‌های دسترسی به داده به‌عنوان الزام حفاظت از زیرساخت‌های اطلاعاتی حیاتی و همچنین از وجود قوانین کافی در تعقیب حملات اطمینان داشته باشند.
۷) کشورها بایستی ردیابی حملات علیه زیرساخت‌های اطلاعاتی حیاتی را تسهیل کنند.
۸) رزمایش‌ها و تمرینات جهت افزایش توانمندی‌های پاسخ‌دهی به حملات ضرورت دارد.
۹) کشورها در همکاری‌های بین‌المللی برای امن‌سازی زیرساخت‌های اطلاعاتی حیاتی مشارکت نمایند که شامل توسعه سامانه‌های هشدار اضطراری، اشتراک‌گذاری و تجزیه‌وتحلیل اطلاعات مرتبط با آسیب‌پذیری‌ها، تهدیدات و حوادث و هماهنگ‌سازی نتایج تحقیقات با قوانین داخلی کشورها است.

۱۰) کشورها بایستی تحقیقات ملی و بین‌المللی را ترویج نمایند. همچنین استفاده از فناوری‌های امنیتی استانداردشده را تشویق نمایند.

همچنین در اتحادیه اروپا، طرح اقدام حفاظت از زیرساخت‌های اطلاعاتی حیاتی اتحادیه اروپا[1] بر پنج مرحله استوار است (ENISA., 2015: 18):

– آمادگی و پیشگیری بر اساس دو چارچوب EFMS[2] (تبادل اطلاعات و تجارب موفق سیاست‌گذاری بین کشورهای عضو) و EP3R[3] (همکاری بین بخش خصوصی و عمومی حول موضوعات امنیت و تاب‌آوری، الزامات پایه، تجارب موفق سیاست‌گذاری).

– تشخیص و واکنش (توسعه و استقرار یک سیستم اطلاعاتی مشترک و آگاه‌سازی اروپا با نام EISAS[4] با جامعه هدف شهروندان و سازمان‌های کوچک و متوسط).

– مقابله و بازیابی از طریق برنامه‌های ملی کشورهای عضو و سازماندهی رزمایش‌های منظم برای پاسخ به حوادث امنیتی و بازیابی فاجعه (در این زمینه آژانس امنیت اطلاعات و شبکه اتحادیه اروپا[5] خطوط راهنما برای رزمایش‌های ملی ارائه کرده‌اند).

– تقویت همکاری بین‌المللی در زمینه اصول و دستورالعمل‌های تاب‌آوری

– توسعه معیارهای شناختی برای شناسایی زیرساخت‌های حیاتی اروپا در بخش فناوری اطلاعات و ارتباطات

در زمینه اجرایی کردن مراحل مذکور، آژانس امنیت اطلاعات و شبکه اتحادیه اروپا، نُه اقدام اساسی را مورد توجه قرار داده است (Mitnick., 2016: 23): تنظیم چشم‌انداز، دامنه، اهداف و اولویت‌ها در راستای افزایش امنیت و تاب‌آوری در دارایی‌های فناوری اطلاعات و ارتباطات / ایجاد و تبعیت از رویکرد ملی ارزیابی مخاطرات با تمرکز بر زیرساخت‌های اطلاعاتی حیاتی/ شناسایی و مشارکت ذینفعان / ایجاد سازوکارهای تبادل اطلاعات رخدادهای امنیتی/ سازماندهی رزمایش‌های سایبری برای آزمون طرح‌های اضطراری و

1. European Action Plan on Critical Information Infrastructure Protection
2. European Forum for Member States (EFMS)
3. European Public. Private Partnership for Resilience (EP3R)
4. European Information Sharing and Alert System (EISAS)
5. European Union Agency for Network and Information Security (ENISA)

شناسایی آسیب‌پذیری‌ها و افزایش همکاری‌ها/ ایجاد سازوکار گزارش‌دهی/ تحقیق و توسعه در فرآیندهای امنیتی / ایجاد سازوکار مشارکت عمومی و خصوصی / ارزیابی اقدامات.

در اسناد مورد مطالعه، کلیدواژه‌های استخراجی مرتبط با حفاظت از زیرساخت‌های اطلاعاتی حیاتی در جدول ۴ نشان داده شده است.

جدول ۴. کلیدواژه‌های مرتبط با حفاظت از زیرساخت‌های اطلاعاتی حیاتی در اسناد بین‌المللی

نهادها	گزاره‌های اصلی
OECD	سیاست‌گذاری، راهبری، داشتن ساختار، مقررات، ظرفیت‌سازی، نگاشت نهادی، همکاری‌های ملی و بین‌المللی، سازمان‌دهی امنیت، مدیریت حوادث امنیتی، امنیت لایه‌های دخیل در زیرساخت‌های اطلاعاتی حیاتی، ایجاد تیم‌های پاسخ به حوادث در راستای اقدامات پیشگیرانه، تشخیصی، واکنشی و بازیابی.
G8	سیاست‌گذاری، راهبری، قوانین و مقررات، همکاری، ظرفیت‌سازی، ارتقای آمادگی، ایجاد شبکه‌های هشدار، آزمون‌های امنیتی، ایجاد شبکه‌های ارتباطی شرایط بحران، تحلیل رخدادها، همکاری‌های ملی و بین‌المللی، تحقیق و توسعه.
EU	ایجاد تیم‌های پاسخ به حوادث، استقرار سیستم آگاهی‌بخشی و هشداردهی، داشتن طرح ملی مرتبط با حفاظت از زیرساخت‌های اطلاعاتی حیاتی، رزمایش‌های سایبری، داشتن طرح بازیابی از فاجعه، همکاری‌های ملی و بین‌المللی، توسعه معیارهای شناخت.
ITU	انتشار دستورالعمل‌ها، آموزش، رزمایش، اطلاع‌رسانی، شناخت تهدیدات، داشتن تیم‌ها، همکاری، داشتن آمادگی دائمی، داشتن زیرساخت‌های قانونی، پیگردهای قانونی، مدیریت لاگ، مدیریت بحران، هدایت اقدامات نهادها، تحلیل حوادث امنیتی.
مطالعه تطبیقی	اهمیت امنیت، سیاست‌گذاری، راهبری، نگاشت نهادی، مدیریت مخاطرات، همکاری‌ها، آموزش، هشداردهی، ارتقای آمادگی ملی و ظرفیت‌سازی، ممیزی‌های امنیتی، مراکز واکنش سریع، مدیریت بحران، مدیریت حوادث امنیتی، قانون‌گذاری، نظارت.
وضعیت موجود کشورمان	نقاط قوت (GCI-2017[1]): وجود نظامات، قوانین و اسناد متعدد در حوزه حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی، تقسیم کار ملی (نظام ملی پیشگیری و مقابله با حوادث فضای مجازی)، مشارکت بین‌المللی و همکاری ملی، تحقیق و توسعه، وجود نهادهای پاسخگو، تجارب مثبت امنیت سایبری، تیم‌های متعدد، وجود ابزارها، مراجع و تیم‌های دولتی و بخشی برای پیشگیری و تشخیص و واکنش. نقاط ضعف (GCI-2017): فقدان نقشه راه برای فناوری‌هایی نوین، مانند زنجیره بلوکی، رایانش ابری، ضعف در تعیین سنجه‌های امنیت سایبری، ضعف در دیپلماسی سایبری (فقدان قراردادهای دو

1. Global Cybersecurity Index(GCI)

	یا چندجانبه)، ضعف در ظرفیت‌سازی (مانند عدم استقرار زیست‌بوم فناوری‌های نوین در زیرساخت‌های ملی)، ضعف در آموزش، ضعف در عملیات پدافندی بهنگام، داشتن سطح متوسط امنیت سایبری، ضعف در استانداردهای سازمانی و صنفی.

مدل مفهومی ابعاد و مؤلفه‌های حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی: بعد از مباحث محیط‌شناسی و مطالعه مدل‌ها، اصول، دستورالعمل‌ها و مطالعه تطبیقی، مدل مفهومی تحقیق به‌صورت سه بعد حکمروایی، مدیریت امنیت و عملیات احصاء گردید. لکن برای تکمیل و اصلاح، با خبرگان در حوزه زیرساخت‌های اطلاعاتی حیاتی در حد اشباع نظری، مصاحبه عمیق در قالب پاسخ به سؤالات باز به عمل آمد. لذا پس از مصاحبه خبرگی، علاوه بر اینکه سه بعد مذکور مورد تأکید قرار گرفتند، با نظر خبرگی بعد «حقوقی» پیشنهاد داده شد که جدا دیده شود. همچنین مؤلفه‌های دیگری پیشنهاد و توسط اساتید راهنما و مشاور بررسی شدند. لذا ابعاد و مؤلفه‌های نهایی به‌صورت جدول ۵ و مدل مفهومی به‌صورت شکل ۲ پیشنهاد می‌گردد.

جدول ۵. ابعاد و مؤلفه‌های احصاشده برای حفاظت از زیرساخت‌های اطلاعاتی حیاتی

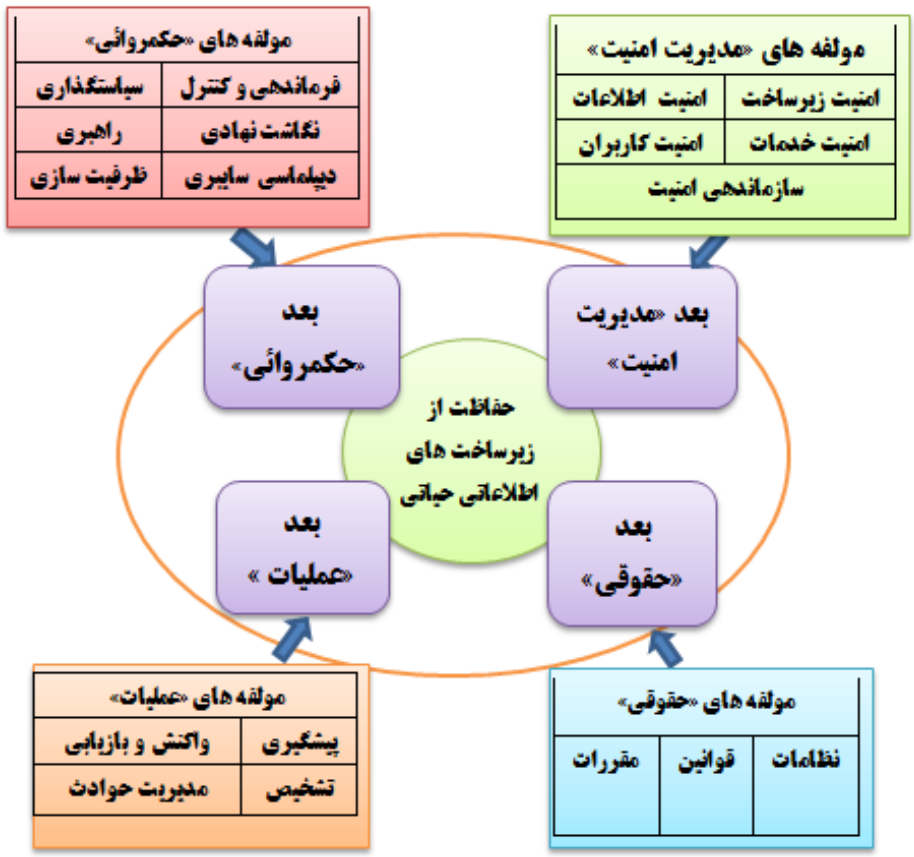
ابعاد	مؤلفه‌ها
حکمروائی	راهبری، سیاست‌گذاری، نگاشت نهادی، فرماندهی و کنترل، دیپلماسی سایبری، ظرفیت‌سازی
حقوقی	قوانین، مقررات، نظامات
مدیریت امنیت	سازمان‌دهی امنیت، امنیت کاربران، امنیت زیرساخت، امنیت داده و اطلاعات، امنیت خدمات
عملیات	اقدامات پیشگیرانه، اقدامات تشخیصی، اقدامات واکنشی و بازیابی، مدیریت حوادث

حکمروایی: حکمروایی زیرساخت‌های اطلاعاتی حیاتی در اتحادیه اروپا، بر پنج محور تعیین نهادهای راهبر[1] ارائه چارچوب‌ها[2] تعیین ساختارهای مدیریتی[3] تعیین نقش‌ها و مسئولیت‌ها[4] تعیین وظایف و الزامات اپراتور زیرساخت‌های اطلاعاتی حیاتی[5] متمرکز است (ENISA,2016:4). همچنین در اسناد کشورهای مختلف مباحثی با مفهوم

1. Leading Authorities
2. Relevants Framework
3. Management Structures
4. Roles and Responsibilites
5. Obligations and Requirements for Operators of CII

«سیاست‌گذاری»[۱]، مفهوم «راهبری»[۲] مفهوم «نگاشت نهادی»[۳]، مفهوم «همکاری‌های سایبری»[۴]، مفهوم «ظرفیت‌سازی»[۵]، مفهوم «مدیریت شرایط بحران»[۶]، دیده می‌شود. لکن بعد از انجام مصاحبه خبرگی، مؤلفه‌های بعد «حکمروایی» به‌صورت «راهبری، سیاست‌گذاری، نگاشت نهادی، فرماندهی و کنترل، دیپلماسی سایبری، ظرفیت‌سازی» مورد تأکید قرار گرفتند.

1. Policy
2. Leading Authorities
3. Identifying government agencies
4. Bilateral and Multilateral Co. operation at regional and global levels
5. Capability Building
6. Impose Measures in case of Major Crices



شکل ۲. مدل مفهومی پیشنهادی برای حفاظت از زیرساخت‌های اطلاعاتی حیاتی

حقوقی: نظامات (توافقنامه‌های جامع حقوقی مانند DURSA[1] در آمریکا و IGSoC[2] در انگلیس، طرح‌های حفاظت در سطح جهانی، مانند NIPP[3]، طرح KRCIIP[4] و ...) نقش مهمی در حفاظت و امنیت اطلاعات دارند. همچنین قوانین و مقررات از مؤلفه‌های حفاظت از زیرساخت‌ها در سطح جهانی می‌باشند که به عناوینی مانند Frameworks, Laws,

1. Data Use and Reciprocal Support Agreement (DURSA)
2. Information Governance Statement of Compliance (IGSoC)
3. National Infrastructure Protection Plan (NIPP)
4. Korean CIIP

Legal Responsibility and Penalty دلالت دارند.

مدیریت امنیت: در همه کشورها توجه به امنیت به‌عنوان محور اصلی حفاظت از زیرساخت‌های اطلاعاتی حیاتی مورد توجه قرارگرفته است که از آن جمله می‌توان به اقدامات فنی افزایش سطح امنیت شبکه‌ها و سامانه‌ها، راه‌اندازی مرکز عملیات امنیتی، تحلیل ترافیک، گزارش‌گیری از رخدادهای امنیتی و گزارش‌دهی به مراجع، مدیریت محرمانگی و جامعیت و دسترس‌پذیری داده، مدیریت وصله‌های امنیتی، استفاده از سخت‌افزارها و نرم‌افزارهای پیشگیری‌کننده از نفوذ، آزمون و رزمایش‌های امنیتی، فرهنگ‌سازی امنیت، آموزش امنیت، کاهش وابستگی‌های امنیتی از طریق بومی‌سازی فناوری‌های امنیتی، استفاده از نرم‌افزارها و سیستم‌عامل خاص، محافظت ویژه از نقاط حساس، احراز هویت، کنترل دسترسی و مجوزها، پیاده‌سازی کنترل‌های امنیتی، راه‌اندازی مدیریت مخاطرات، امنیت سامانه‌ها و شبکه و سیستم‌عامل، جلوگیری از افشای داده و ... اشاره کرد. به‌عنوان مثال در کشورهای عضو اتحادیه اروپا همانند فرانسه و آلمان، محوریت امنیت سامانه‌های اطلاعاتی حیاتی دستورالعمل «امنیت و اطلاعات شبکه»[1] است تأکید دارد(Chen et al., 2017:10). در طرح NIPP آمریکا، بر «ارائه طرح افزایش امنیت زیرساخت‌های حیاتی» تأکید شده است. همچنان که در OECD Recommendation، بر «انجام اقداماتی برای افزایش سطح امنیت اجزای شبکه‌ها و سیستم اطلاعاتی تشکیل‌دهنده زیرساخت اطلاعاتی حیاتی» تأکید شده است. در طرح NIIP آلمان بر «افزایش تلاش ملی در امنیت فناوری اطلاعات از طریق خدمات و محصولات امنیتی مورد اعتماد حرفه‌ای»[2]، در استرالیا بر اهمیت «مرکز عملیات امنیت سایبری»[3]، در ENISA بر لزوم اتخاذ «اقدامات الزام‌آور امنیتی»[4] تأکید شده است. بعد از انجام مصاحبه خبرگی، مؤلفه‌های این بعد به‌صورت «سازمان‌دهی امنیت، امنیت کاربر، امنیت زیرساخت، امنیت داده و اطلاعات،

1. Network and Information Security (NIS)
2. Enhancing national competence in IT security by experts and trusted IT services and security products(German NIIP)
3. Australian Cyber Security Operation Center
4. Mandatory Security Measures(ENISA2016)

امنیت خدمات» مورد تأکید قرار گرفت.

عملیات: در مدل اتحادیه اروپا، مدل ITU و اصول کشورهای گروه هشت، برای حفاظت از زیرساخت‌های اطلاعاتی حیاتی، فازهای «پیشگیری، تشخیص، واکنش، بازیابی» مورد تأکید قرار گرفته‌اند (Rehak et al.,2016:15). همچنین در ENISA، قانون فناوری اطلاعات آلمان[1]، وظایف آژانس امنیت اطلاعات فرانسه[2] به مؤلفه‌های مدیریت حوادث (استفاده از سامانه‌های مدیریت حوادث[3]، گزارش‌دهی حوادث عمده امنیت فناوری اطلاعات[4]، هندل کردن حوادث[5] ...) اشاره شده است. پس از مصاحبه خبرگی، مؤلفه‌های این بعد به‌صورت «اقدامات پیشگیرانه، اقدامات تشخیصی، اقدامات واکنشی و بازیابی، مدیریت حوادث» مورد تأکید قرار گرفتند.

روش تحقیق

نظر به اینکه پژوهش حاضر در پی رفع نیازها و حل مشکلات مطرح در حوزه زیرساخت‌های اطلاعاتی حیاتی و ارائه راه‌حل آن‌ها است، می‌توان آن را کاربردی محسوب نمود و با توجه به اینکه، الگوی راهبردی متناسب و مطابق با شاخص‌ها و متغیرهای بومی ارائه می‌گردد و نوآوری در فرآیندها و ابزارها مدنظر بوده است، لذا توسعه‌ای است. روش تحقیق در این پژوهش از نظر ماهیت و نحوه گردآوری داده‌های آن، توصیفی، تحلیلی است. رویکرد مورد استفاده در این پژوهش ترکیبی و یا آمیخته (کمی و کیفی) است. در بخش کیفی روش‌های تحلیل کیفی و بررسی خبرگی برای مستندسازی دانش حفاظت از زیرساخت‌های اطلاعاتی حیاتی در سطوح راهبردی استفاده گردیده و محورهای مستندسازی با مراجعه به بیانات ارزشمند مقام معظم رهبری، اسناد بالادستی نظام جمهوری اسلامی ایران، اسناد و اقدامات راهبردی امنیتی کشورهای مختلف و پژوهش‌های علمی

1. German IT Security ACT
2. ANSSI FR.
3. Incident Management Systems
4. Report Major IT Security Incidents
5. Incident handling and Incident Notification

مورد بررسی و مفاهیم استخراج شده است و سپس با بهره‌گیری از روش بررسی خبرگی (مصاحبه با ۱۵ خبره) چارچوب مدل مفهومی تحقیق ایجاد گردیده است. محقق برای رسیدن به اهداف تحقیق با استفاده از پرسشنامه محقق‌ساخته مبتنی بر مصاحبه با متخصصین و بررسی اسناد بالادستی اقدام کرده است. لذا در ابتدا ادبیات و چارچوب نظری و مدل‌های مربوط به متغیرهای تحقیق مورد مطالعه قرار گرفته و سپس موضوعات مهم و تأثیرگذار بر حفاظت از زیرساخت‌های اطلاعاتی حیاتی بررسی شده‌اند که در این رابطه اسناد بالادستی، مدل‌ها، رویکردهای بین‌المللی، فعالیت نهادهای بین‌المللی، طرح‌های عملی، اسناد راهبردی امنیت سایبری کشورها مطالعه شده و با تحلیل خبرگی ابعاد و مؤلفه‌های حفاظت از زیرساخت‌های اطلاعاتی حیاتی احصاء گردیده‌اند. با اطلاعات به‌دست‌آمده در بخش کیفی و مطالعات انجام‌شده، چارچوب مفهومی و مدل تحقیق طراحی شد. در این چارچوب، ابعاد و مؤلفه‌های حفاظت از زیرساخت‌های اطلاعاتی حیاتی مورد شناسایی قرار گرفتند.

در بخش کمی، پس از اینکه ابعاد و مؤلفه‌های حفاظت سایبری شناسایی شدند، پرسشنامه محقق‌ساخته‌ای که شامل ۴ بعد، ۱۸ مؤلفه و ۱۳۳ گویه اولیه بود (ولی در نهایت ۱۳۱ گویه تأیید شدند) به‌صورت طیف لیکرت پنج‌گزینه‌ای طراحی گردید و پس از انجام مراحل روایی و پایایی (تعیین اعتبار و پایایی سؤالات پرسشنامه با استفاده از ضریب آلفای کرونباخ)، با مراجعه به جامعه آماری اقدام به نمونه‌گیری شد که با توجه به جامعه آماری که در این تحقیق در نظر گرفته شده است، ۱۰۰ نفر بودند که به این افراد پرسشنامه ارسال و جمع‌آوری گردید. سپس نتایج نمونه‌گیری انجام‌شده به‌وسیله روش‌های کمی، آمار توصیفی و نرم‌افزار SPSS مورد تجزیه‌وتحلیل قرار گرفتند و در نهایت مدل مفهومی ترسیم‌شده توسط نرم‌افزار مدل‌یابی معادلات ساختاری SMART-PLS (تحلیل بار عاملی و آزمون معناداری و ...) مورد برازش و اعتبارسنجی قرار گرفت.

روایی و پایایی: مفهوم روایی به این سؤال پاسخ می‌دهد که ابزار اندازه‌گیری تا چه حد خصیصه مورد نظر را می‌سنجد. روش‌های متعددی برای تعیین روایی ابزار اندازه‌گیری

(اسناد، مصاحبه و پرسشنامه) وجود دارد که یکی از آن‌ها روش اعتبار محتوا است. در این تحقیق برای رسیدن به هدف روایی ابتدا با مطالعه متون، مقالات با ارجاعات بالا، رساله‌های دکتری، گزارش‌های تحقیقی، اسناد راهبردی، مدل‌های مرجع و پس از بهره‌گیری از نظرات اساتید محترم، اخذ نظریه کارشناسان و مصاحبه با خبرگان تا حد اشباع نظری، ابعاد و مؤلفه‌های الگوی تحقیق استخراج گردید و در تدوین پرسشنامه اولیه و تنظیم نهایی لحاظ گردیده و مورد تأیید قرار گرفت و در ادامه برای بالا بردن روایی پرسشنامه، ابتدا پرسشنامه در میان منتخب جامعه آماری توزیع شد و در طول تکمیل پرسشنامه نظرات اصلاحی از آنان اخذ و سپس سؤال‌هایی که اهداف تحقیق را برآورده نمی‌کردند اصلاح و یا حذف گردید تا سؤالات هیچ‌گونه ابهام و نارسایی نداشته باشند و در تنظیم پرسشنامه نهایی نظرات افراد مورد نظر لحاظ گردید.

برای مفهوم پایایی، پایایی اسناد و پایایی مصاحبه و پایایی پرسشنامه بررسی شدند. به‌منظور پایا بودن اسناد و مدارک، داده‌های حاصل از منابع گوناگون، با یکدیگر و با نظرات صاحب‌نظران مصاحبه‌شونده، مطابقت داده شد تا همگرایی آن‌ها با چارچوب نظری تطبیق داده شده و اعتبار منابع تأیید گردد. گرچه نشریه‌هایی که چاپ آن‌ها از سوی سازمان‌های معتبر است به‌خودی‌خود متضمن اعتبار منابع است. برای پایایی مصاحبه، سؤالات مصاحبه در زمان‌های مختلف ارائه شد تا با مقایسه پاسخ‌های دریافتی با پاسخ‌های پیشین به مشابهت و تکرارپذیری یا همان پایایی دست یافتیم. برای پایایی پرسشنامه، با استفاده از نرم‌افزار SPSS ضریب آلفای کرونباخ پرسشنامه طیف لیکرت محاسبه شد. نتایج این محاسبه در جدول ۷ آمده است که همگی بیشتر از ۰/۶ بوده و نشانگر پایداری گویه‌ها است.

جدول ۷ نتایج پایایی (ضریب آلفای کرونباخ) برای متغیرها

متغیر	ضریب کرونباخ
دیپلماسی سایبری	۰/۸۳
فرماندهی و کنترل	۰/۶۲
حکمروایی	۰/۹۲

راهبری	۰/۸۱
سیاست‌گذاری	۰/۸۲
ظرفیت‌سازی	۰/۷۸
قوانین	۰/۸۹
حقوقی	۰/۹۱
نظامات	۰/۷۴
مقررات	۰/۷۷
امنیت داده	۰/۷۲
امنیت کاربران	۰/۹
امنیت خدمات	۰/۸۴
امنیت زیرساخت	۰/۹۴
مدیریت امنیت	۰/۹۶
سازمان‌دهی امنیت	۰/۹۱
عملیات	۰/۹۴
اقدامات پیشگیرانه	۰/۹
اقدامات تشخیصی	۰/۸۴
اقدامات واکنشی	۰/۷۹
مدیریت حوادث	۰/۸۵

تجزیه‌وتحلیل داده‌ها

تحلیل عاملی ابعاد و مؤلفه‌های شناسایی‌شده حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی: برای آزمون مدل مفهومی از فن مدل‌سازی معادلات ساختاری مبتنی بر رویکرد حداقل مربعات جزئی با نرم‌افزار SMART-PLS استفاده شده است. با استفاده از این نرم‌افزار، هم برازش مدل اندازه‌گیری و هم برازش مدل ساختاری برای سنجش رابطه میان متغیرها با استفاده از ضرایب معناداری انجام می‌شود و می‌توان

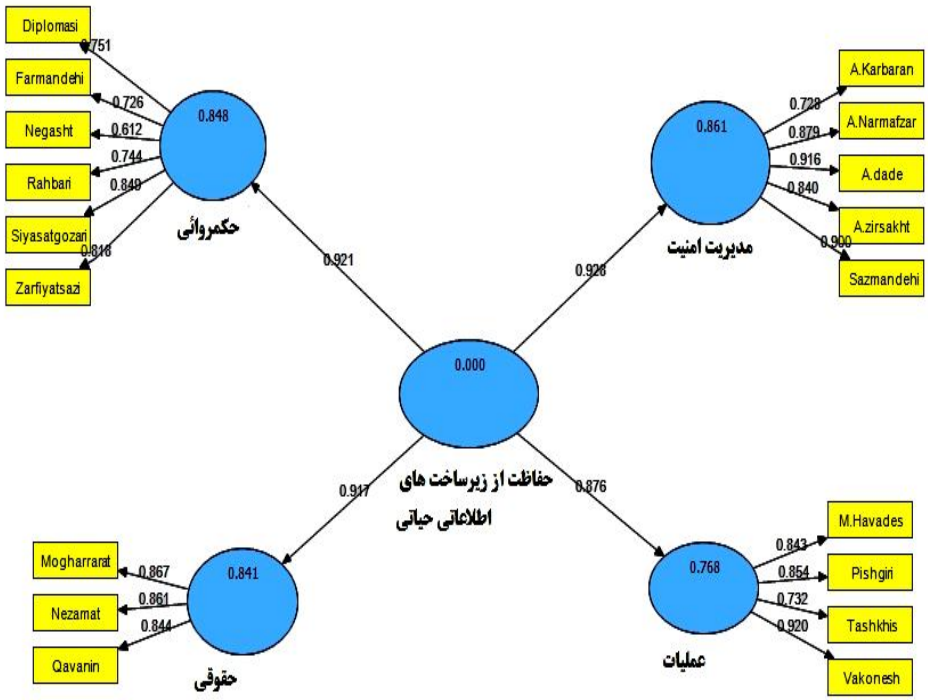
اولویت‌بندی مؤلفه‌ها و گویه‌ها را نیز از این طریق مشخص نمود. در این تحقیق میزان سهم هر گویه یا عامل در ایجاد متغیر مورد بررسی قرار می‌گیرد و برای این کار از تحلیل عاملی تأییدی استفاده شده است. در تحلیل عاملی، مقدار بار عاملی کمتر از ۰/۳ نشان‌دهنده مقیاس ضعیف بوده و باید از مدل حذف شود. بارهای عاملی بین ۰/۳ تا ۰/۶ نشان می‌دهند که متغیر مشاهده‌شده مقیاس متوسطی بوده و برای ادامه آنالیز کفایت می‌کند. مقادیر بزرگ‌تر از ۰/۶ نیز نشان می‌دهند که متغیر مشاهده‌پذیر مقیاس قابل اطمینان برای محاسبه متغیر پنهان است. در کل مقادیر بارهای عاملی بزرگ‌تر از ۰/۴ را می‌توان در مدل حفظ کرد (داوری و رضازاده، ۱۳۹۲: ۴۷).

برای هر یک از ابعاد حکمروایی، حقوقی، مدیریت امنیت و عملیات یک مدل تحلیل عاملی جداگانه محاسبه شده است و سهم هر یک از گویه‌های مربوط به مؤلفه‌ها مشخص شده‌اند. در نهایت با استفاده از مدل تحلیل عاملی مرتبه دوم، مدل نهایی بررسی شده است.

– **تحلیل بار عاملی:** نتایج تحلیل عاملی تأییدی مدل مفهومی در جدول ۶ و شکل ۳ ارائه شده است.

جدول ۶ نتایج تحلیل عاملی تأییدی مدل مفهومی

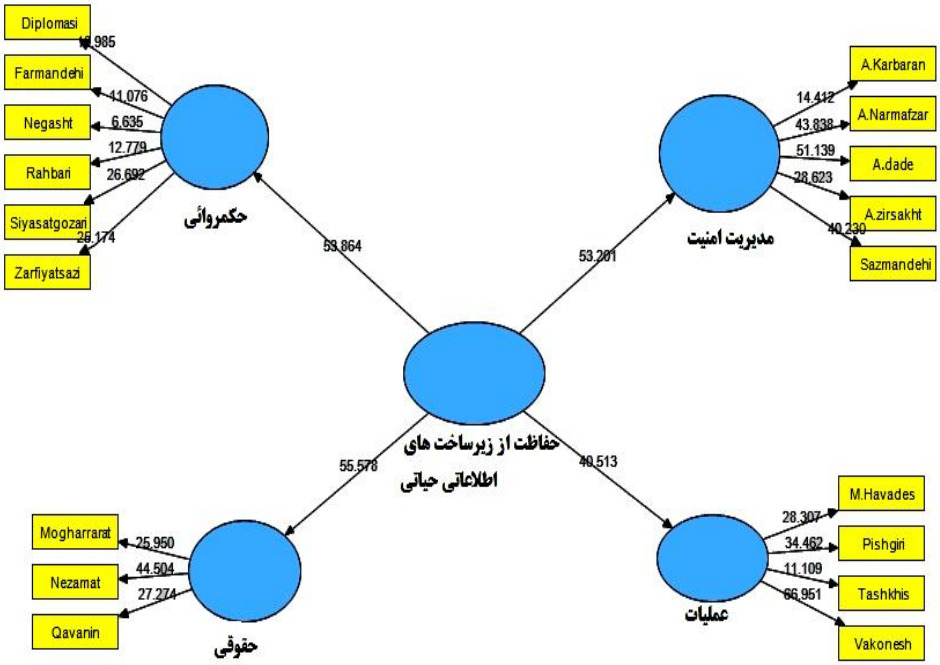
بعد	مؤلفه	بار عاملی	خطای معیار	مقدار t	سطح معناداری
حکمروایی	راهبری	۰/۷۴	۰/۰۱۷	۱۲/۷۷	<0.05
	سیاست‌گذاری	۰/۸۴	۰/۰۱۸	۲۶/۶۹	
	نگاشت نهادی	۰/۶۱	۰/۰۲۲	۶/۶۳	
	فرماندهی و کنترل	۰/۷۲	۰/۰۲	۱۱/۰۷	
	دیپلماسی سایبری	۰/۷۵	۰/۰۲۵	۹/۹۸	
	ظرفیت‌سازی	۰/۸۱	۰/۰۱۸	۲۶/۱۷	
حقوقی	قوانین	۰/۸۴	۰/۰۱۳	۲۷/۲۷	
	نظامات و ساختارها	۰/۸۶	۰/۰۲۱	۴۴/۵	
	مقررات	۰/۸۶	۰/۰۱۵	۲۵/۹۵	
مدیریت امنیت	سازمان‌دهی امنیت	۰/۹	۰/۰۰۷	۴۰/۲۳	
	مدیریت امنیت زیرساخت	۰/۸۴	۰/۰۰۸	۲۸/۶۲	
	مدیریت امنیت داده و اطلاعات	۰/۹۱	۰/۰۰۷	۵۱/۱۳	
	مدیریت امنیت نرم‌افزارها و خدمات	۰/۸۷	۰/۰۰۳	۴۳/۸۳	
	مدیریت امنیت کاربران	۰/۷۲	۰/۰۱	۱۴/۴۱	
عملیات	اقدامات پیشگیرانه	۰/۸۵	۰/۰۱۸	۳۴/۴۶	
	اقدامات تشخیصی	۰/۷۳	۰/۰۲۶	۱۱/۱	
	اقدامات واکنشی و بازیابی	۰/۹۲	۰/۰۱۳	۶۶/۹۵	
	مدیریت حوادث	۰/۸۴	۰/۰۱۴	۲۸/۳۰	
حفاظت زیرساخت اطلاعاتی	حکمروایی	۰/۹۲۱	۰/۰۱	۵۳/۸۶	
	حقوقی	۰/۹۱۷	۰/۰۱۳	۵۵/۵۷	
	مدیریت امنیت	۰/۹۲۶	۰/۰۱۸	۵۴/۶	
	عملیات	۰/۸۷۶	۰/۰۰۶	۵۳/۲	



شکل ۳ ضرایب تحلیل عاملی مدل مفهومی تحقیق

اطلاعات جدول نشان می‌دهد که تمام مؤلفه‌ها (گویه‌ها) مقادیر بارهای عاملی بزرگ‌تر از ۰/۴ داشته و از اعتبار لازم برخوردار هستند. در مدل فوق ضرایب مسیرها برای ۴ بعد مدیریت امنیت، حکمروایی، حقوقی، عملیات به ۰/۹۲۶، ۰/۹۲۱، ۰/۹۱۷، ۰/۸۷۶ است. لذا بعد مدیریت امنیت دارای بالاترین تأثیر در حفاظت است و تأثیر بعد حقوقی و بعد حکمروایی تقریباً یکسان است.

– آزمون معناداری: نتایج آزمون معناداری در شکل ۴ و جدول ۶ در ستون مقادیر t نشان داده شده است. به دلیل بیشتر از ۱/۹۶ بودن مقادیر t، در سطح احتمال ۹۵ درصد معنی‌دار وجود دارد و مدل از اعتبار لازم برخوردار است.



شکل ۴. آزمون معناداری مدل مفهومی تحقیق

-آزمون برازش مدل مفهومی تحقیق: به‌منظور بررسی برازندگی مدل، می‌توان از شاخص‌هایی با عنوان کیفیت مدل[1] استفاده کرد. نتایج آزمون در شکل ۵ نشان داده شده است.

-پارامتر پایایی مرکب[2]: به دلیل اینکه تمام اعداد از ۰/۶ بیشتر هستند، دارای سطح بالایی از پایداری است.

- پارامتر آلفای کرونباخ[3]: به دلیل بیشتر از ۰/۶ بودن، نشانگر پایداری گویه‌ها می‌باشد.

- پارامتر ضریب تعیین[4]: مقادیر استاندارد برای سطوح «قابل ملاحظه»، «متوسط»،

1. Model Quality
2. Composite Reliability
3. Cronbach Alpha
4. R. Square

«ضعیف» به ترتیب عبارت‌اند از: ۰/۶۷، ۰/۳۳ و ۰/۱۹ و در مدل ما، به دلیل بیشتر از ۰/۶۷ بودن مقادیر، دارای سطح قابل قبولی است.

	AVE	Composite Reliability	R Square	Cronbachs Alpha
Amaliyat	0.705537	0.904959	0.768150	0.858214
CIIP	0.557602	0.957155		0.951817
Hoghoghi	0.735292	0.892844	0.841356	0.820224
Hokmravaei	0.568128	0.886547	0.847504	0.846292
M.Amniyat	0.731599	0.931247	0.861187	0.906336

	Communality	Redundancy
Amaliyat	0.705537	0.541791
CIIP	0.557602	
Hoghoghi	0.735292	0.615565
Hokmravaei	0.568127	0.475026
M.Amniyat	0.731599	0.629344

شکل ۵. پارامترهای برازش مدل مفهومی تحقیق

همچنین برای برازش مدل، می‌توان از شاخص نیکویی برازش[1] استفاده کرد. این شاخص به‌عنوان معیاری برای سنجش عملکرد کلی مدل به کار می‌رود. این شاخص، مجذور ضرب دو مقدار متوسط مقادیر اشتراکی[2] و متوسط ضریب تعیین است. مقدار GOF بین صفر و یک در نوسان است. مقدار ۰/۰۱، ۰/۲۵ و ۰/۳۶ به ترتیب به‌عنوان مقادیر ضعیف، متوسط و قوی معرفی شده‌اند.

$$GOF = \sqrt{\overline{Communality} \times \overline{R^2}}$$

شاخص نیکویی برازش در چهار بعد مدیریت امنیت، حقوقی، حکمروایی، عملیات به ترتیب عبارت‌اند از: به ترتیب ۰/۷۹، ۰/۷۸، ۰/۶۸ و ۰/۷۲ هستند و چون همگی بیشتر از ۰/۳۶ هستند، لذا در حد قابل قبول و قوی می‌باشند.

1 .GOF
2. Communality

نتیجه‌گیری

ابعاد و مؤلفه‌های الگوی راهبردی حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی، پس از بررسی مدل‌های بین‌المللی، دستورالعمل‌ها، اصول منتج از تئوری‌ها و کارکردها همراه با بررسی تطبیقی اسناد بالادستی و اسناد راهبردی و ساختار نهادی و طرح‌ها و قوانین حداقل هفت کشور و همچنین از طریق مراجعه به آرای خبرگان در حوزه‌های راهبردی و دفاع و امنیت فضای سایبر، به‌طور منطقی و مفهومی استنباط گردید و در نهایت مفهوم حفاظت سایبری به‌صورت الگویی متشکل از ابعاد و مؤلفه‌ها بر اساس اسناد بالادستی، تطبیق با مدل و اسناد راهبردی کشورها با استفاده از روش پژوهش آمیخته با روش توصیفی استخراج گردید.

پس از تجزیه‌وتحلیل داده‌ها مشخص شد حفاظت از زیرساخت‌های اطلاعاتی حیاتی کشور دارای چهار وجه بوده که حفاظت از طریق آن‌ها، منجر به حفاظت از زیرساخت‌های اطلاعاتی حیاتی کشور در مقابل حملات سایبری خواهد شد. چهار وجه مذکور که تأمین‌کننده حفاظت هستند عبارت‌اند از:

- حفاظت از طریق عوامل حکمروایی با ۶ مؤلفه و ۳۹ زیرمؤلفه؛
- حفاظت از طریق عوامل حقوقی با ۳ مؤلفه و ۱۸ زیرمؤلفه؛
- حفاظت از طریق مدیریت امنیت با ۵ مؤلفه و ۴۸ زیرمؤلفه؛
- حفاظت از طریق عملیات با ۴ مؤلفه و ۲۶ زیرمؤلفه.

با توجه به نتایج به‌دست‌آمده از تحلیل داده‌های کمی تحقیق، رتبه‌بندی ابعاد و مؤلفه‌ها به شرح زیر است:

مثررترین بُعد، مدیریت امنیت و سپس به ترتیب ابعاد حکمروایی، حقوقی، عملیات هستند.

پس از محاسبه ضرایب بار عاملی بعد «حکمروایی» جمله ناقص در بعد «حکمروایی» با شش مؤلفه سیاست‌گذاری، ظرفیت‌سازی، راهبری، دیپلماسی سایبری، فرماندهی و کنترل، نگاشت نهادی میزان تأثیرگذاری به ترتیب عبارت‌اند از: ۰/۸۷۰، ۰/۸۶۹، ۰/۷۷۷، ۰/۷۵۸،

۰/۷۵۲، ۰/۶۵۵. لذا سیاست‌گذاری بالاترین تأثیر و نگاشت نهادی کمترین تأثیر را دارند و تأثیر دو مؤلفه دیپلماسی سایبری و فرماندهی کنترل تقریباً یکسان است.

در بعد «حقوقی» با سه مؤلفه قوانین، مقررات و نظامات به ترتیب عبارت‌اند از: ۰/۹۱۹، ۰/۸۶۸، ۰/۸۶۱ لذا قوانین بالاترین تأثیر را داشته و تأثیر دو مؤلفه تنظیم مقررات و نظامات تقریباً یکسان است.

در بعد «مدیریت امنیت» با پنج مؤلفه امنیت نرم‌افزار، امنیت داده، امنیت زیرساخت، سازمان‌دهی امنیت و امنیت کاربران، میزان تأثیرگذاری به ترتیب عبارت‌اند از: ۰/۹۴، ۰/۸۳، ۰/۹۱، ۰/۹۲، ۰/۶۳. دیده می‌شود که تأثیر گزینه‌های امنیت نرم‌افزار، امنیت زیرساخت و سازمان‌دهی امنیت تقریباً یکسان و در حفاظت تأثیر بسیار قوی دارند.

در بعد «عملیات» با چهار مؤلفه پیشگیرانه، واکنشی، تشخیصی، مدیریت حوادث، به ترتیب عبارت‌اند از: ۰/۹۲، ۰/۸۸، ۰/۵۶، ۰/۷۱. لذا اقدامات پیشگیرانه بالاترین تأثیر را در حفاظت دارد و تأثیر مؤلفه اقدامات واکنشی نیز قابل توجه است.

پس از محاسبه ضرایب تحلیل عاملی بعد «حکمروایی»، با شش مؤلفه، تأثیرگذاری مؤلفه‌ها به ترتیب سیاست‌گذاری، ظرفیت‌سازی، راهبری، دیپلماسی سایبری، فرماندهی و کنترل و نگاشت نهادی به دست آمدند. لذا سیاست‌گذاری بالاترین تأثیر و نگاشت نهادی کمترین تأثیر را دارند. همچنین پس از محاسبه ضرایب تحلیل عاملی بعد «حقوقی» با سه مؤلفه، تأثیرگذاری مؤلفه‌ها به ترتیب قوانین، مقررات و نظامات به دست آمدند. همچنین پس از محاسبه ضرایب تحلیل عاملی بعد «مدیریت امنیت» با پنج مؤلفه، تأثیرگذاری مؤلفه‌ها به ترتیب امنیت نرم‌افزار، سازمان‌دهی امنیت، امنیت زیرساخت، امنیت داده، امنیت کاربران به دست آمدند و در نهایت در بعد «عملیات» با چهار مؤلفه، تأثیرگذاری مؤلفه‌ها به ترتیب پیشگیرانه، واکنشی، مدیریت حوادث، تشخیصی به دست آمدند لذا اقدامات پیشگیرانه بالاترین تأثیر را در حفاظت دارند.

مهم‌ترین محورهای تحقیق عبارت‌اند از:

- شناسایی و تبیین ابعاد و مؤلفه‌های حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی؛

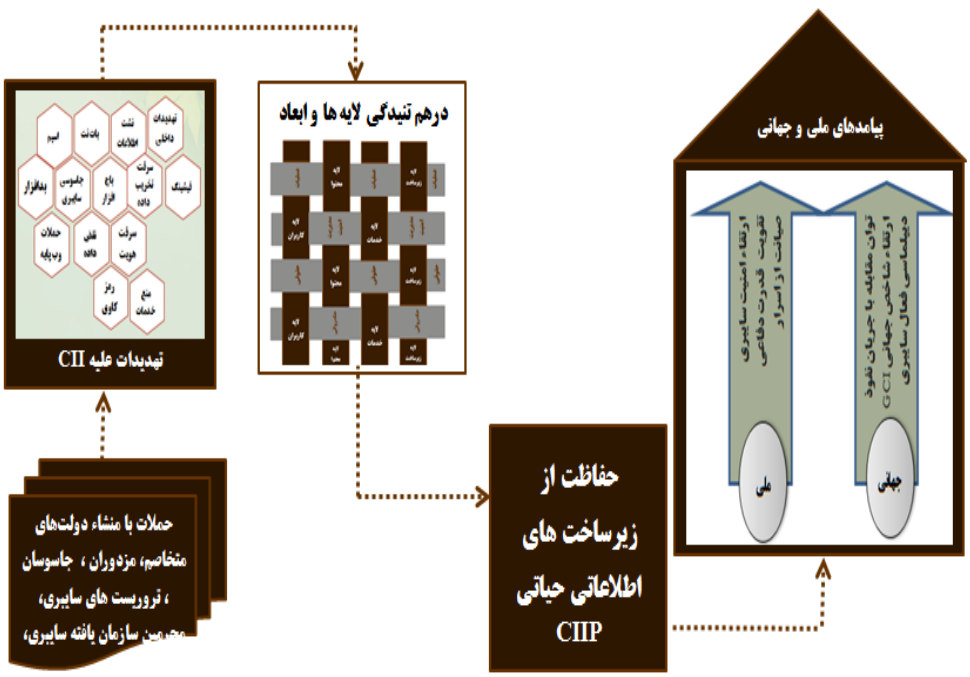
- تولید ادبیات در خصوص حفاظت سایبری؛
- برقراری ارتباط بین جهت‌گیری راهبردی و تفکر اجرایی در فرآیندها، معماری‌ها، ظرفیت‌ها؛
- ارتقای دانش کارگزاران نظام و افزایش کارآمدی در این حوزه؛
- ارتقای الگوهای حفاظتی از سطح تاکتیکی و غیربومی به سطح راهبردی و بومی؛
- فراهم نمودن زمینه برای مواجهه هوشمندانه و پیشگیرانه در فضای پرچالش و محیط بی‌ثبات سایبری؛
- زمینه‌سازی پایداری زیرساخت‌ها، صیانت از اسرار کشور، ایجاد آمادگی لازم در عالی‌ترین سطح به‌منظور صیانت از زیرساخت‌های حیاتی در برابر حملات.

الگوی راهبردی حفاظت سایبری زیرساخت‌های اطلاعاتی حیاتی، به‌منظور حفاظت، اقدامات پسیو (امن‌سازی، پدافند غیرعامل، ...) و اکتیو (حکمروایی، عملیات، ...) را در هر چهار لایه زیرساخت، کاربر، داده و محتوا جهت مقابله با تهدیدات سایبری شامل می‌شود. تمام مؤلفه‌ها با نگاه به اسناد بالادستی به‌روز گردیده و همواره در حال رصد، کشف و شناسایی تهدیدات و آسیب‌پذیری‌ها است و این فرآیند همواره پیامدهای ملی و جهانی داشته و علاوه بر ارتقای امنیت سایبری و تقویت قدرت دفاعی و افزایش توان مقابله با تهدیدات، تاب‌آوری زیرساخت را به‌عنوان پیامد حفاظت زیرساخت‌ها دنبال می‌کند. در همین راستا جایگاه حفاظت سایبری به‌صورت شکل ۶ و الگوی راهبردی که بتواند فرآیندهای اصلی حفاظت سایبری را تبیین کند به‌صورت شکل ۷ ارائه گردیده است.

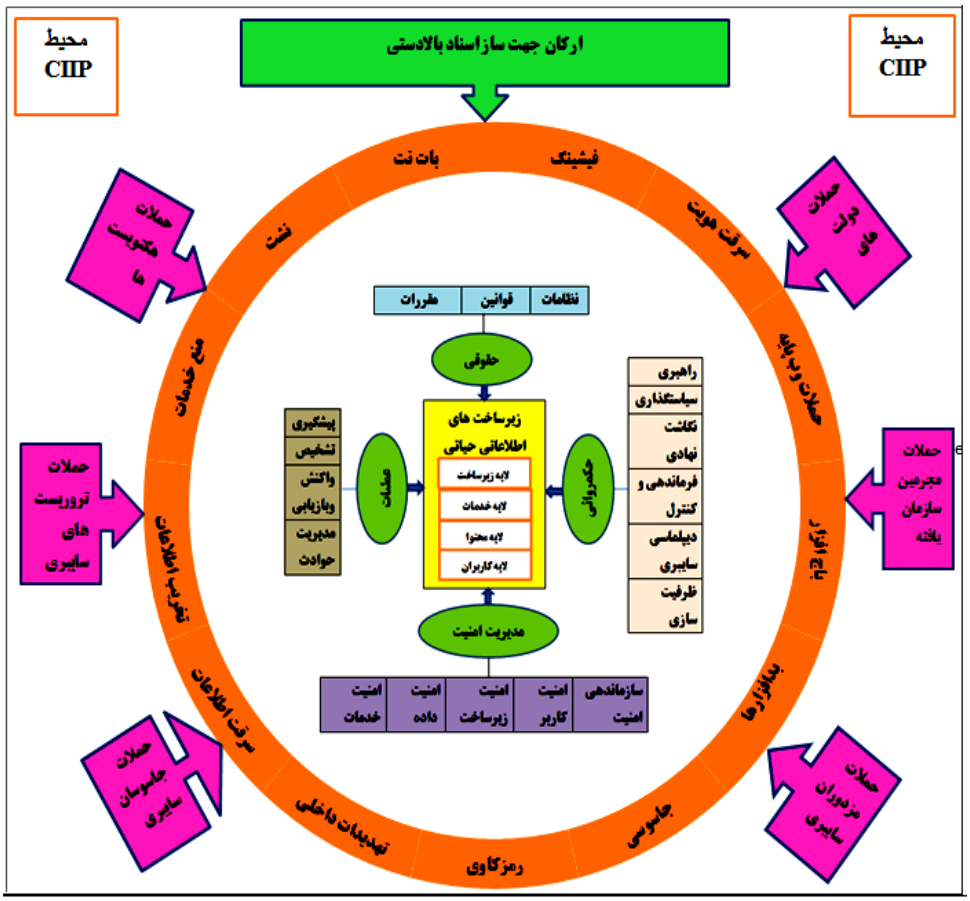
این الگو دارای این ویژگی است که با توجه به سوابق حملات متعدد علیه زیرساخت‌های حیاتی کشورمان، تهدیدات و چالش‌های نوین را شناسایی کرده (به‌خصوص سیاست‌گذاری‌ها، لزوم تدوین الزامات، لزوم تدوین نقشه راه، لزوم تدوین مقررات، لزوم تدوین پیوست‌های امنیتی، لزوم تعیین چارچوب‌ها، در فناوری‌های نوین مرتبط مانند زنجیره بلوکی، کلان‌داده، هوش مصنوعی، رایانش کوانتوم، رمزنگاری نوین و ...) و با پرداختن به اقدامات پیشگیرانه و مقابله‌ای و واکنشی درصدد پاسخگویی به

تهدیدات است. لذا نگاه به آینده و انجام پیش‌بینی و ارائه راهکارهـای پیشـگیرانه از دیگـر ویژگی‌های این الگوی راهبردی است.

در این الگو همواره مواردی مانند نقش نهادهای حاکمیتی، هماهنگی بین نهادهای کلان مدیریتی، داشتن رویکـرد یکپارچـه، داشـتن سـاختار اجرایـی و عملیـاتی، پدافنـد بهنگـام، حداقل‌سازی زمان بازیابی، همکاری‌های ملی و منطقه‌ای، استفاده از ظرفیت‌هـای بـومی، ... نقش پررنگی دارند.



شکل ۶. جایگاه حفاظت از زیرساخت‌های اطلاعاتی حیاتی



شکل ۷. الگوی راهبردی حفاظت از زیرساخت‌های اطلاعاتی حیاتی

پیشنهادات

۱- الگوی ارائه‌شده برای بهره‌برداری و به‌کارگیری در اختیار نهادهای پدافندی، حفاظتی، نظارتی و امنیتی که مشمول زیرساخت‌های اطلاعاتی حیاتی هستند ازجمله مرکز افتای ریاست جمهوری، سازمان پدافند غیرعامل، مرکز ملی فضای مجازی، وزارت امور خارجه، وزارت اطلاعات، وزارت ارتباطات و فناوری اطلاعات، وزارت نیرو، وزارت راه و شهرسازی، وزارت بهداشت، وزارت اقتصاد و دارایی، بانک مرکزی، وزارت دفاع، وزارت کشور و مجلس شورای اسلامی.

۲- به دلیل نقش بی‌بدیل استقرار زیست‌بوم فناوری‌های نوین (مرتبط با زیرساخت‌های اطلاعاتی حیاتی) بر بستر زیرساخت‌های ملی مانند شبکه ملی اطلاعات در بحث حفاظت، عملی کردن این استقرار، نقش مؤثری در حفاظت زیرساخت‌های اطلاعاتی حیاتی در مقابل حملات سایبری خواهد داشت.

۳-مؤلفه‌ها و زیرمؤلفه‌های «عملیات» که شامل اقدامات پیشگیرانه، اقدامات تشخیصی، اقدامات واکنشی و بازیابی، مدیریت حوادث می‌باشد، در سازمان پدافند غیر عامل می‌تواند در راستای اقدامات پدافندی مؤثر واقع شود.

۴-مؤلفه‌ها و زیرمؤلفه های «مدیریت امنیت» که دارای محتوای غنی بوده و بخش قابل توجهی از مباحث الگوی راهبردی را به خود اختصاص داده است در مرکز افتای ریاست جمهوری می‌تواند در راستای نظارت بر عملکرد متولیان زیرساخت‌های اطلاعاتی حیاتی و انجام ممیزی مؤثر واقع شود.

۵- نتایج مطالعه تطبیقی که حاوی چارچوب‌ها، طرح‌ها و برنامه‌ها، قوانین، نگاشت‌های نهادی، تقسیم کارها و تعیین مسئولیت‌ها، شبکه‌های تبادل اطلاعات، ساختارهای حکمروایی، ساختار نهادی متنوع کشورها در زمینه حفاظت از زیرساخت‌های اطلاعاتی حیاتی است، مورد توجه مسئولان و متولیان دستگاه‌های مشمول زیرساخت اطلاعاتی حیاتی قرار گیرد.

۶-حفاظت از زیرساخت‌های اطلاعاتی حیاتی به دنبال تاب‌آور کردن زیرساخت‌هاست. با توجه به اینکه در این تحقیق ابعاد، مؤلفه‌ها و شاخص‌های حفاظت احصاء شدند و فقط به عوامل مؤثر در تاب‌آوری پرداخته شد، لذا پیشنهاد می‌شود ابعاد، مؤلفه‌ها و شاخص‌های تاب‌آوری زیرساخت‌های اطلاعاتی حیاتی در یک رساله دکتری به‌طور مفصل مورد بحث قرار گیرد.

فهرست منابع ومآخذ

الف) منابع فارسی

۱. امام خامنه‌ای (مدظله‌العالی)، مجموعه بیانات قابل‌دسترسی در پایگاه www.khamenei.ir

۲. آندرس، جیسن (۱۳۹۶)، جنگ سایبری؛ تکنیک‌ها، تاکتیک‌ها و ابزارها برای فعالان حوزه امنیت، ترجمه حوزه نوآوری آرایه‌های دفاعی، تهران، مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

۳. عبداللهخانی، علی (۱۳۸۵)، حفاظت از زیرساخت‌های حیاتی اطلاعاتی، فصلنامه سیاست دفاعی، شماره ۵۴.

۴. کافی، سعید (۱۳۹۳)، تدوین راهبردهای پدافند غیرعامل در فضای سایبری زیرساخت‌های حیاتی ج.ا.ایران، تهران، دانشگاه عالی دفاع ملی، دانشکده امنیت.

۵. مصطفایی، محمد (۱۳۹۴)، زیرساخت‌ها و ضرورت حفاظت از آن‌ها، راهبرد پایدار، سال اول، شماره ۱، صص ۳۲ -۳۵.

۶. موحدی صفت، محمدرضا؛ ولوی، محمدرضا (۱۳۹۵)، ارائه الگوی امن استقرار زیرساخت‌های دفاعی کشور در محیط رایانش ابری، مجله دانش راهبردی، سال ۶، شماره ۲۳، صص ۱۸۹-۲۰۶.

ب-۱) منابع لاتین

7. David Rehak and Martin Hromada (2016), "Failures in a Critical Infrastructure System", repot intechopen, pp 76-97. (http://dx.doi.org/10.5772/intechopen.70446(
8. ENISA, (2016), "Strategies for Incident Response and Cyber Crisis Cooperation", PUBLISHED Version 1.1.
9. Euisun Paik, Heung Youl Youm, (2012), " Knowledge Sharing Series Cybersecurity", APCICT Publication, PP 1-108.
10. Kevin Mitnick, (2016), "Top 10 risk and compliance management related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next", International Association of Risk and Compliance Professionals (IARCP), pp 1-168.

ب-۲) مقالات

11. A.Poustourli and D. Ward and A.Zachariadis, (2015), "An Overview of European Union and United States Critical Infrastructure Protection Policies". Proceedings of the 12th International Conference "Standardization, Protypes and Quality: A means of Balkan Countries' Collaboration", pp 549-557.
12. Chen K. Hu C. Zhang X. Zheng K. Chen Y. and Vasilakos A. (2011), "Survey on routing in data centers: insights and future directions," IEEE Network, vol. 25, no. 4, pp. 6 –10.

13. David Satola, W.J. Luddy, (2017),” The Potential for an International Legal Approach to Critical Information Infrastructure Protection”, 47 JURIMETRICS, PP 315-334.
14. Drias, Z. Serhrouchni, A. Vogel, O. (2015) “Analysis of Cyber Security for Industrial Control Systems,” in Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on, vol. no. pp. 1–8.
15. FFIEC, (2015), FFIEC Cybersecurity Assessment Tool. Appendix C: Glossary, pp 1-38.
16. ENISA, (2018), " ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends, ENISA Report ETL 2018.
17. ENISA, (2015), “Critical Information Infrastructures Protection approaches in EU”, Final Document, TLP Green, Version 1.
18. ENISA, (2014), “ Methodologies for the identification of Critical Information Infrastructure assets and services Guidelines for charting electronic data communication networks ”, PP 1-39.
19. Esmaeili, mohammadreza, (2014) " A STUDY ON THE EFFECT OF THE STRATEGIC INTELLIGENCE ON DECISION MAKING AND STRATEGIC PLANNING",International Journal of Asian Social Science.
20. Eric Luiijf, (2016), “The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers”, Meridian Connecting and Protecting, pp 1-62.
21. Joseph O. Eichenhofer and Elisa Heymann and Barton P. Miller, (2017), “ In-Depth Software Vulnerability Assessment of Container Terminal Systems”, 2nd NATO Conference on Cyber Security in the Maritime Domain, Souda, Crete, Greece, pp 1-17.
22. Kadri Kaska and Lorena Trinberg, (2015),Regulating Cross-Border Dependencies of Critical Information Infrastructure,Nato Cooperation Cyber Defence Center of Excellence report, Tallinn Eslonia, 2015.
23. KS Min, (2015), “An International Comparative Study on Cyber Security Strategy”, International Journal of Security and Its Applications Vol.9, No.2 (2015), pp 13-20.
24. L. Cazorla, C. Alcaraz, and J. Lopez, (2016), “Cyber Stealth Attacks in Critical Information Infrastructures", IEEE Systems Journal, pp. 1-15.
25. Luiijf E, van Schie T, van Ruijven T, Huistra, A, (2016), good practice guide on critical information infrastructure protection for governmental policy-makers, The GFCE-MERIDIAN.
26. Martin Koyabe, (2015), “Critical Information Infrastructure Protection A Commonwealth Perspective”, ITU Workshop on “ICT Security Standardization for Developing Countries, pp 1-45.
27. OECD, (2018), “Recommendation of the Council on the Protection of Critical Information Infrastructures”, OECD/LEGAL/0361
28. Segura Serrano A. "Cybersecurity: towards a global standard in the protection of critical information infrastructures", in European Journal of Law and Technology, Vol 6, No 3.

29. Ugur Akyazi, (2014), “Possible Scenarios and Maneuvers for Cyber Operational Area”, 13th European Conference on Cyber Warfare and Security - Cryptome, PP 15-21.
30. Xing Gao, Zhang Xu, Haining Wang, Li Li, and Xiaorui Wang, (2018), "Reduced Cooling Redundancy: A New Security Vulnerability in a Hot Data Center", in NDSS 2018, San Diego, CA.