مجله سیاست دفاعی
سال بیست و هشتم، شماره ۱۱۱، تابستان ۱۳۹۹: ۹۱ ـ ۷۱

شاخص‌های دفاعی ـ امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران مبتنی‌بر رویکردهای پدافند غیرعامل

سعید کافی[۱]

دریافت مقاله: ۱۳۹۹/۰۲/۰۳ **تأیید مقاله: ۱۳۹۹/۰۶/۰۶**

چکیده

حیات اجتماعی کشورها بر پایه تداوم عملکرد زیرساخت‌های حیاتی و حساس آنها استوار است. ازهمین‌روست که کشورهای متخاصم تلاش می‌کنند تا مانع تداوم این کارکرد در کشورهای هدف شوند. امروزه، توسعه فناوری اطلاعات و فضای سایبری موجب شده است تا بخش‌های مهمی از کارکرد زیرساخت‌های حیاتی و حساس وابسته به این فضا شوند. در نتیجه وجود چنین وابستگی‌ای، امنیت زیرساخت‌ها به فضای سایبری گره خورده است. پژوهش حاضر به‌عنوان دغدغه خود (هدف مقاله) درصدد است تا به شاخص‌های دفاعی ـ امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس کشور باتوجه‌به رویکردهای پدافند غیرعامل بپردازد؛ چراکه درصورت بی‌توجهی به عنوان این تحقیق هر آن باید در انتظار حملات سایبری به زیرساخت‌های حیاتی و حساس کشور بود. فراموش نشود که به گفته «کلاوزویتس» هر عصری جنگ و محدویت‌های خود را دارد و هم‌اکنون کشور در عصر فناوری اطلاعات، بیش‌ازپیش به تعیین شاخص‌های دفاعی ـ امنیتی فضای سایبری خود نیاز دارد و پرداختن به این تحقیق موجب تقویت تاب‌آوری زیرساخت‌ها در برابر چنین تهدیدهایی می‌شود. درهمین‌راستا، این شاخص‌ها در سه حوزه: نیروی انسانی، فرایندها و فناوری با استفاده از روش توصیفی ـ تحلیلی و با رویکرد پیمایشی و استفاده حداکثری از نظرات خبرگان تدوین شده است. برای این پژوهش نمونه آماری به تعداد ۵۰ نفر به روش تمام‌شمار درنظر گرفته شده است. روش نمونه‌گیری، غیرتصادفی هدف‌مند است و محقق به‌صورت هدف‌مند به افراد خاص و مشخص مراجعه مستقیم داشته است. نتیجه تحقیق مؤید آن است که هریک از رویکردهای پدافند غیرعامل در حوزه‌های سه‌گانه در شاخص‌های دفاعی ـ امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران شامل موارد زیر است: حوزه منابع انسانی: "آموزش و آگاه‌سازی و استفاده از نیروهای بومی" با میزان موافقت ۸۸ درصد؛ حوزه فرایندها: "تدوین پروتکل سیاست دفاعی ـ امنیتی، محدودسازی حیطه عملکرد و وابستگی متقابل" با میزان موافقت ۹۲ درصد و حوزه فناوری: "بهره‌گیری از اینترانت، بومی‌سازی سخت‌افزاری و نرم‌افزاری، راه‌اندازی آزمایشگاه‌های تشخیص بدافزارها، رمزنگاری داده‌ها و استفاده از «فایروال» و «هانی پات» و سامانه کشف و جلوگیری از رخنه"، با میزان موافقت ۹۸ درصد.

کلید واژه‌ها

شاخص‌های دفاعی امنیتی؛ زیرساخت‌های حیاتی و حساس؛ فضای سایبری؛ رویکردهای پدافند غیرعامل

۱. استادیار گروه آموزش هوافضای دانشگاه جامع امام حسین(ع) dr.saeedkafi@gmail.com

مقدمه

زیرساخت‌های حیاتی و حساس کشورها نقش بسزایی در تداوم کارکرد اجتماعی آنها ایفا می‌نماید. امروزه، به‌دلیل توسعه فناوری اطلاعات و اهمیت آن در سهولت انجام امور محوله، تلاش‌های وافری درراستای به‌کارگیری امکانات سخت‌افزاری و نرم‌افزای در زیرساخت‌ها صورت گرفته است. هرچند این اتفاق می‌تواند نوید از سهولت و سرعت در انجام امور دهد، اما نباید فراموش کرد که فضای سایبری[1] به‌عنوان فضای تبادل ارتباطات و اطلاعات، ضمن برخورداری از مواهب خود دارای مخاطراتی نیز می‌باشد. فضای سایبری به‌عنوان قلمرو پنجم پس از زمین، آسمان، دریا و فضا، نقش تعیین‌کننده‌ای در اجرای وظایف معمول زیرساخت‌های حیاتی و حساس ازجمله تداوم خدمات مانند تأمین آب، برق و گاز و یا بهداشت و درمان دارد. این فضا امکان تبادل ارتباطات و اطلاعات را در طیف ملی در درون زیرساخت‌ها با حفظ محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات فراهم می‌آورد. در پژوهش حاضر تلاش شده است تا ملاحظات پدافند غیرعامل[2] که یکی از رایج‌ترین و کم‌هزینه‌ترین رویکردها در جهان امروز است، به‌منظور توسعه زیرساخت‌های حیاتی و حساس کشور ارائه شود. رشد سریع فناوری اطلاعات و ارتباطات در جهان موجب تشدید تهدیدهای متوجه زیرساخت‌های حیاتی و حساس کشورها ازجمله میهن اسلامی عزیزمان شده است. در بسیاری از مواقع، مدیران تنها به مزایای توسعه این فناوری می‌اندیشند و کم‌تر توجهی به ابعاد مخاطره‌آمیز آن دارند. ازآنجاکه مخاطرات سایبری تا زمان وقوع آن در حالت خاموش و نهفته است، امکان تشخیص و شناسایی مخاطرات به‌آسانی ممکن نیست.

اما با همین شرایط و در حالت حاکمیت عدم‌قطعیت می‌توان اقداماتی را اتخاذ کرد که به‌موجب آن آثار تهدید کاهش یافته و قطعیت بیشتر شود. درهمین‌راستا، پدافند غیرعامل به مفهوم کلی دارای مزایایی است که با استفاده از آن امکان مهار تهدیدها با صرف هزینه اندک فراهم می‌شود. این شاخص‌ها در تحقیق حاضر مورد بررسی قرار گرفته و به آنها پرداخته می‌شود.

1. Cyber Space
2. Passive Defense

زیرساخت‌های حیاتی و حساس در کشور در حکم ستون‌های سقف جامعه محسوب می‌شوند. این زیرساخت‌ها باید امن، پایدار و غیرقابل تزلزل باشند؛ چراکه تزلزل آنها به‌معنای فروریختن سقف جامعه است. برای‌مثال، قطع شریان گاز در برخی از کشورهای دنیا می‌تواند به‌موجب وابستگی متقابل زیرساخت‌ها به یکدیگر منجر به قطع و یا اختلال در برقراری جریان برق در بخش‌هایی از کشور شود. مواردی مانند قطع جریان برق ۲۱ استان در ونزوئلا ازطریق حملات سایبری که مانع چرخش توربین‌ها و تولید برق شد و یا حمله سایبری به کوره فولاد آلمان که مانع قطع به‌موقع جریان تولید حرارت در کوره و درنتیجه انفجار کوره و کشته‌شدن چند تن از کارگران شد و یا حمله سایبری امریکا با استفاده از «بمب‌های منطقی»[1] به خطوط اصلی انتقال گاز روسیه و درنهایت حمله سایبری با ویروس «استاکس‌نت»[2] به تأسیسات غنی‌سازی نطنز همگی مواردی است که در دوره‌های اخیر روی داده و حاکی از قدرت عرصه پنجم درگیری‌های بشری بعد از عرصه‌های زمینی، هوایی، دریایی و فضایی است. ایجاد هرگونه اختلال و یا توقف در کارکرد هریک از زیرساخت‌های حیاتی و حساس جامعه باتوجه‌به وابستگی متقابل زیرساخت‌ها به یکدیگر به‌سرعت به سایر زیرساخت‌ها سرایت کرده و در مدت کوتاهی کارکردهای جامعه را مانند وابستگی به انرژی گاز، برق و خدمات وابسته به آن مانند بهداشت، درمان، آموزش، مالی و بانکی، ارتباطات و حمل‌ونقل تحت تأثیر مستقیم قرار می‌هد، تاجایی‌که تداوم ارائه خدمات اجتماعی غیرممکن می‌شود و هرآن باید انتظار وقوع بحران‌های شدید اجتماعی با ابعاد امنیتی را داشت. پدافند غیرعامل همواره راهکارهای ارزان و احتیاط‌آمیز را برای کاهش تهدیدهای متوجه کشور ارائه می‌دهد. نگارنده در این پژوهش بر آن است تا با طرح شاخص‌های دفاعی ـ امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس[3] جمهوری اسلامی ایران مبتنی‌بر رویکردهای پدافند غیرعامل زمینه صیانت از زیرساخت‌های حیاتی و حساس را با کم‌ترین بار مالی برای کشور فراهم سازد.

1. Logic Bombs
2. Stuxnet Malware
3. Critical & Vital Infrastructures

سؤال اصلی

شاخص‌های دفاعی ـ امنیتی زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران در فضای سایبری مبتنی‌بر رویکردهای پدافند غیرعامل چیست؟

سؤالات فرعی

شاخص‌های دفاعی امنیتی حوزه انسانی زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران در فضای سایبری مبتنی‌بر رویکردهای پدافند غیرعامل چیست؟

شاخص‌های دفاعی ـ امنیتی حوزه فرایندهای زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران در فضای سایبری مبتنی‌بر رویکردهای پدافند غیرعامل چیست؟

شاخص‌های دفاعی ـ امنیتی حوزه فناوری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران در فضای سایبری مبتنی‌بر رویکردهای پدافند غیرعامل چیست؟

اهمیت و ضرورت تحقیق

درصورت پرداختن به تحقیق حاضر، دستاوردهای زیر حاصل می‌شود:

ـ امکان پیاده‌سازی سیاست‌های پدافند غبرعامل در فضای سایبری زیرساخت‌ها مانند کاهش وابستگی متقابل زیرساخت‌ها به یکدیگر به‌منظور ممانعت از سرایت قطع کارکرد یک زیرساخت بر سایر زیرساخت‌ها؛

ـ افزایش قدرت تاب‌آوری زیرساخت‌های حیاتی و حساس کشور با کشف آسیب‌پذیری‌های نهفته و روز صفر و رفع آنها به‌موجب اجرای تست نفوذ و ارزیابی امنیتی و شاخص‌های مختلف پدافندی؛

ـ کاهش هزینه‌های مترتب ناشی از تهدیدهای خارجی با رفع آسیب‌پذیری‌ها (تهدیدها متوجه آسیب‌پدیری‌ها هستند و درصورت کاهش آسیب‌پذیری‌ها به همان نسبت تهدیدها نیز کاهش می‌یابد).

درصورت بی‌توجهی به تحقیق حاضر پیامدهای زیر متصور است:

ـ افزایش تهدیدهای متوجه زیرساخت‌های حیاتی و حساس به‌موجب وجود آسیب‌پذیری‌های نهفته در آنها (جذابیت هدف برای حمله بر مبنای جذابیت آن تعیین می‌شود)؛

ـ افزایش هزینه‌های اقتصادی و اجتماعی ناشی از تهدیدهای متوجه زیرساخت‌های حیاتی و حساس (قطع کارکرد یک یا چند زیرساخت نه‌تنها هزینه‌های اقتصادی بر جامعه تحمیل می‌کند، بلکه می‌تواند پیامدهای امنیتی نیز داشته باشد).

روش پژوهش

نوع تحقیق، کاربردی و روش آن توصیفی ـ تحلیلی است.

جامعه آماری، حجم نمونه و روش نمونه‌گیری

جامعه آماری شامل دو دسته مجریان و دانشگاهیان[1] متخصص در حوزه پدافند غیرعامل در فضای سایبری می‌شود.. حجم نمونه شامل ۵۰ نفر است که به‌دلیل محدودیت دسترسی به جامعه نمونه با مشخصات موردنظر نمونه‌گیری به روش غیرتصادفی هدف‌مند صورت گرفته است.

روش گردآوری داده و ابزار آن

گردآوری داده‌ها به دو روش کتابخانه‌ای مبتنی‌بر فیش‌برداری و پیمایشی با استفاده از پرسشنامه صورت گرفته است.

روایی و پایایی ابزار گردآوری داده‌ها

روایی‌سنجی پرسش‌ها با استفاده از جمع ۹ نفره از جامعه نمونه به‌عنوان خبرگان صورت گرفته است و پایایی آن نیز مبتنی‌بر آلفای کرونباخ عدد ۰,۷۸ بوده است.

روش تجزیه‌وتحلیل داده‌ها

تجزیه‌وتحلیل داده‌ها با استفاده از نرم‌افزار اس.پی.اس. اس انجام شده است.

مبانی نظری و ادبیات

واژه «سایبر»[2] ریشه یونانی دارد و در اصل به‌معنای سکاندار یا راهنما[3] است. نخستین‌بار اصطلاح «سایبرنتیک» توسط ریاضیدانی به نام نوربرت وینر[4] در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین»[5] در سال ۱۹۴۸ به‌کار برده شده است. «سایبرنتیک» علم

1. Academist
2. Cyber
3. Kybernetes
4. Norbert Wiener
5. Cybernetics and Control in Relation between Human and Machine

مطالعه و کنترل سازوکارها در سامانه‌های انسانی، ماشینی (و رایانه‌ها) است (Cotton, Oliver , 2015: 34).

امروزه، گستره فضای سایبری تمام شئون و ابعاد زندگی بشری را دربر گرفته است و به‌عنوان قلمرو پنجم زندگی بشری بعد از زمین، دریا، آسمان و فضا شناخته می‌شود. این ابعاد در حوزه زیرساخت‌های حیاتی و حساس نیز گسترش یافته است. بنا به تعریف زیرساخت‌های حیاتی و حساس عبارت است از مجموعه‌ای از زیرساخت‌ها که حیات اجتماعی کشور منوط به کارکرد صحیح آنها است و درصورت ایجاد وقفه و یا اختلال در این کارکرد احتمال به‌مخاطره افتادن امنیت ملی کشور وجود دارد (Doytsher, Jack, .2016: 11).

درهمین‌راستا، اقدامات پدافند غیرعامل به‌عنوان اقدامات احتیاطی و غیرمسلحانه که پیش از وقوع تهدید در حوزه‌های موردنظر با رویکرد پیش‌کنش‌گرانه به‌کار می‌رود، می‌تواند با کم‌ترین میزان صرف هزینه، آثار و پیامدهای تهدید را مهار و تا حدودی بی‌اثر نماید. مجمع تشخیص مصلحت نظام، پدافند غیرعامل را مجموعه اقدامات غیرمسلحانه‌ای می‌داند که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدها و اقدام‌های نظامی دشمن می‌شود (کانون اندیشه راهبردی سازمان پدافند غیرعامل، ۱۳۹۵: ٤١).

مقام معظم رهبری در همین خصوص در هفتم آبان ماه سال ۱۳۹۱ می‌فرمایند: "پدافند غیرعامل مثل مصونیت‌سازی بدن انسان است. از درون ما را مصون می‌کند. معنایش این است که ولو دشمن تهاجمی هم بکند و زحمتی هم بکشد و ضرب و زوری هم بزند، اثری نخواهد کرد. این پدافند غیرعامل نتیجه‌اش این است. ببینید چقدر مهم است که ما این حالت را در کل پیکره کشور و جامعه در دستگاه‌های مختلف به‌وجود بیاوریم. کاری کنیم که همت ما فقط مصروف به این نباشد که دشمن را منصرف کنیم یا برای مقابله خودمان را آماده بکنیم. نه، کاری کنیم که ما مصونیت در خودمان به‌وجود بیاوریم. این با پدافند غیرعامل تحقق پیدا می‌کند. بنابراین، این مسئله، مسئله بسیار مهمی است که بایستی راه بیفتد" (سازمان پدافند غیرعامل کشور، ۱۳۹۳: ٤).

با مروری بر رویدادهای گذشته پیرامون تهدیدهای مهم سایبری متوجه کشورهای منطقه غرب آسیا می‌توان به ضرورت تحقق سخنان مقام معظم رهبری درخصوص پیاده‌سازی شاخص‌های پدافند غیرعامل در زیرساخت‌های حیاتی و حساس کشور پی برد.

در سال ۱۳۸۹ شمسی معادل سال ۲۰۱۰ میلادی حمله سایبری مبتنی‌بر بدافزار «استاکس‌نت» به تأسیسات غنی‌سازی نطنز صورت گرفت. بدافزار «استاکس‌نت» نخستین بدافزار در رده نظامی بود که به‌صورت فیزیکی منجر به خرابی و ازکارافتادگی «سانتریفیوژها» می‌شد. این بدافزار با هدف به‌تأخیرانداختن برنامه هسته‌ای ایران بدون نیاز به حمله نظامی به‌کارگرفته شد، اما درعمل موجب بیداری کشور درخصوص اهمیت پرداختن به تهدیدهای سایبری شد.

حمله مبتنی‌بر بدافزار «دوکو»[1] در سال ۱۳۹۰ شمسی معادل سال ۲۰۱۱ میلادی در سطح غرب آسیا ازجمله ایران گسترش یافت. تصور می‌شد که این ویروس مرتبط با ویروس استاکس‌نت باشد و ازسوی یگان ۸۲۰۰ رژیم صهیونیستی تولید و منتشر شده باشد. این بدافزار نیز برای سرقت اطلاعات مورد استفاده قرار گرفت.

حمله بدافزار «شعله»[2] در سال ۱۳۹۱ شمسی معادل سال ۲۰۱۲ میلادی در سطح غرب آسیا و برخی دیگر از نقاط جهان به‌کار رفت. طبق گزارش مراکزی مانند «اسکای وایپر»[3] و «کسپرسکی»[4] این بدافزار با هدف جاسوسی و تخریب اطلاعات در کشورهای جهان ازجمله ایران به‌کار رفته است (Knight, 2012 :21).

حملات سایبری به‌صورت یک جریان مستمر بین کشورها درحال وقوع است که برخی از آنها به‌صورت شاخص مطرح می‌شوند. امروزه، سرقت مستمر اطلاعات از این راه یکی از روش‌های مرسوم بین کشورها شده است که بدون شک حاوی نکات بسیاری است. اما ازآنجاکه بیان تمام این وقایع خارج از حوصله نوشتار حاضر است، تنها به ذکر چند مورد بسنده شده است.

1. Duqu Malware
2. Flame Malware
3. Sky viper
4. Kaspersky

زیرساخت‌های حیاتی و حساس در یک طبقه‌بندی به ۱۶ مورد تقسیم می‌شوند. این ۱۶ مورد عبارتند از: زیرساخت‌های شیمیایی، تجاری، ارتباطات، صنایع تولیدات حساس، سدها، صنایع نظامی، انرژی، خدمات ضروری، مالی، صنایع غذایی و کشاورزی، تأسیسات دولتی، بهداشتی، رآکتورهای هسته‌ای و زباله‌های هسته‌ای، فناوری اطلاعات، شبکه حمل‌ونقل و شبکه آبرسانی و فاضلاب.

«شبکه جهانی اینترنت»[1] هر روز بیش از گذشته تمامی ابعاد و شئون زندگی بشر را به خود وابسته می‌کند. این وابستگی تنها برای کسانی که با رایانه شخصی خود به اینترنت متصل می‌شوند، نیست. بلکه این وابستگی گستره‌ای به وسعت یک کشور دارد. مهم‌ترین بخش وابستگی در هر کشوری به فضای سایبری وابستگی زیرساختی است. درحال‌حاضر، ۱۶ زیرساختی که نام برده شد، هریک تاحدی به فضای سایبری وابسته‌اند. این وابستگی ضمن آنکه می‌تواند عاملی برای تسهیل فعالیت زیرساخت‌ها در ارائه خدمات به مشتریان خود باشد، می‌تواند بستری برای شکل‌گیری تهدیدهای متنوع نیز باشد (Gabriel, 2017: 43).

اما نباید فراموش کرد که عملکرد زیرساخت‌های حیاتی و حساس در فضای سایبری به‌گونه‌ای است که بین آنها وابستگی متقابل وجود دارد. به‌عبارتی، درصورت تهدید یک زیرساخت، احتمال سرایت تهدید به سایر زیرساخت‌ها نیز وجود دارد. تهدیدهای سایبری طیف وسیعی دارند. تاب‌آوری زیرساخت‌ها در برابر طیف تهدیدها از اهمیت بسزایی برخوردار است. ازطرف‌دیگر، شناخت مخاطرات زیرساخت‌ها ناشی از فضای سایبری مهم است؛ چراکه این شناخت کمک می‌کند تا مدیریت ریسک مبتنی‌بر سطح تهدیدها در زیرساخت‌ها اعمال شود و اولویت‌بندی اقدامات براساس سطح آسیب‌پذیری‌ها صورت گیرد. حفاظت کل زیرساخت‌ها امری غیرممکن است، اما با شناخت نقاط حساس و سطح تأثیر آسیب‌ها می‌توان اولویت‌بندی لازم را صورت داد (Bashan, A, 2013: 11).

تهدیدهای زیرساخت‌های حیاتی و حساس در حوزه‌های زیر قابل بررسی است: تهدید در ایجاد اختلال، بهره‌برداری و یا قطع ارتباطات، تهدید در منع ارائه خدمات زیرساخت‌ها، افشای و یا سرقت اطلاعات حساس و مهم زیرساخت‌ها (Poovendran. R., 2014: 21).

1. World wide Internet

زیرساخت‌های حیاتی و حساس برای تسهیل ارائه خدمات خود از فضای سایبری بهره می‌گیرند. این اقدام ضمن‌آنکه می‌تواند تسهیل‌کننده باشد، مخاطراتی را نیز متوجه این زیرساخت‌ها می‌کند. آسیب‌پذیری‌های زیرساخت‌ها در سه حوزه منابع انسانی، فرایندها و فناوری مورد بررسی قرار خواهد گرفت (Chess, A. 2017: 12).

آسیب‌پذیری‌های زیرساخت‌های حیاتی و حساس در حوزه منابع انسانی

در حوزه منابع انسانی نخستین نکته‌ای که مطرح می‌شود حفظ محرمانگی اطلاعات است. محرمانگی به این معناست که تنها اشخاص مجاز قادر به دریافت، تغییر و یا مدیریت اطلاعات هستند. نکته دیگر یکپارچگی است که به‌معنای آن است که تنها افراد مجاز قادر به اعمال هرگونه تغییر در اطلاعات هستند. نکته دیگر، دسترسی است. دسترسی به‌معنای آن است که افراد مجاز در هر زمان قادر به دسترسی به سامانه و اطلاعات مرتبط باشند و ازسوی‌دیگر افراد غیرمجاز، این امکان را نداشته باشند. ملاحظه دیگر در حوزه منابع انسانی بهره‌گیری از نیروی انسانی متعهد داخلی است. واگذاری پروژه‌ها به شرکت‌های خارجی و غیربومی موجب افشای اطلاعات زیرساخت‌ها، تشخیص نقاط ضعف ذاتی، ایجاد آسیب‌پذیری‌های عمدی در آنها و درنهایت بهره‌گیری مستقیم این شرکت‌ها از آسیب‌پذیری‌ها و یا افشای آنها درازای مبالغی به رقبای کشور می‌شود. بنابراین، بین امنیت و دفاع از زیرساخت در برابر تهدیدها و فناوری پیشرفته و هزینه‌های احداث، راه‌اندزای و به‌کارگیری این زیرساخت‌ها باید انتخاب صحیح صورت گیرد (Baheti, R. .2015: 17)

آسیب‌پذیری‌های زیرساخت‌های حیاتی و حساس در حوزه فرایندها

در حوزه فرایندها یکی از اشتباهات ادغام سامانه‌های کوچک در سامانه‌های بزرگ است. به‌عبارتی، «وابستگی متقابل زیرساختی»[1] می‌تواند موجب گسترش تهدیدها از یک حوزه محدود به سایر حوزه‌های با سطح تأثیر نامحدود شود و درنتیجه یک اتفاق ساده به یکباره به یک بحران ملی تبدیل شود. برخی مواقع، تمرکز مدیران در زیرساخت‌ها بر افزایش میزان بهره‌وری است. مدیران به‌دلیل عدم اطلاع از تهدیدهای سایبری و یا ملاحظات دفاعی ـ امنیتی نسبت به تأمین امنیت زیرساخت‌ها غفلت می‌ورزند. نکته دیگر در فرایندها مربوط به سیاست

1. Infrastructure Interdependency

دفاعی ـ امنیتی می‌شود. هر زیرساخت باید متناسب با سطح تهدیدها، درجه حساسیت خود در زیرساخت‌های کشور و میزان وابستگی متقابل خود به سایر زیرساخت‌ها دارای یک پروتکل امنیتی دفاعی ـ امنیتی باشد. آخرین نکته نیز خلأ وجود پروتکل احراز هویت، مجوز اختیارات و حسابرسی[1] است. به‌این‌معناکه چه کسی به چه چیزی و تا چه میزان می‌تواند دسترسی داشته باشد (Shafi, Q., 2017: 7).

در حوزه فرایندها نوع روابط بازیگران داخلی برای مقابله با تهدیدهای فضای سایبری نیز حائز اهمیت است. برای‌مثال، در جمهوری اسلامی ایران بازیگران فضای سایبری در ستاد کل نیروهای مسلح ازجمله سازمان پدافند غیرعامل و موارد دیگر در این فضا ایفای نقش می‌کنند. این در حالی است که سازمان فناوری اطلاعات ایران براساس اسناد و راهبردهای ملی، ازجمله سند راهبردی امنیت فضای تولید و تبادل اطلاعات (سند افتا) و قوانین مصوب درقالب برنامه‌های پنج‌ساله توسعه، به‌منظور حمایت و گسترش خدمات امنیت فضای تولید و تبادل اطلاعات (افتا) درکشور و برنامه‌ریزی درزمینه به‌کارگیری بهینه ظرفیت‌های ملی و ساماندهی شرکت‌های توانمند در ارائه خدمات افتا، اقدام به ارزیابی و صدور پروانه فعالیت در حوزه افتا می‌نماید. وزارت ارتباطات و اطلاعات، بازیگر دیگری است که در حوزه زیرساخت و با تشکیل مرکز ماهر به‌عنوان مرکز پاسخگویی به رخدادهای امنیت رایانه‌ای فعالیت می‌کند. پلیس فتا نیز در رابطه با جرایم کیفری در فضای سایبری فعال است. علاوه‌براین، شورای عالی فضای مجازی نیز مسئولیت سیاست‌گذاری‌های کلان را برعهده دارد. حال چنانچه تمامی این ارکان با یکدیگر تعامل مثبت داشته باشند و به تبادل اطلاعات بپردازند، امکان دستیابی به یک فرایند سازنده به‌منظور دفع تهدیدها و هدایت و راهبری زیرساخت‌ها در شرایط عدم قطعیت میسر خواهد بود. وجود فرایندهای کاری تعامل‌پذیر به تحقق چنین مهمی کمک شایانی خواهد کرد. برای اینکه یک قدرت سایبری به انعطاف‌پذیری برسد، باید تمام مؤلفه‌های تشکیل‌دهنده آن انعطاف‌پذیر باشند (حکمرانی فضای مجازی، ۱۳۹۸).

1. Authentication, Authorization and accounting

آسیب‌پذیری‌های زیرساخت‌های حیاتی و حساس در حوزه فناوری

دسترسی‌های غیرمجاز به شبکه‌های ارتباطی، فعالیت در بستر اینترنت، وجود سیستم عامل غیربومی، وابستگی نرم‌افزاری و سخت‌افزاری به سایر کشورها، خلأ وجود آزمایشگاه‌های تشخیص وجود بدافزارها در نرم‌افزارها و یا سخت‌افزارهای وارداتی، عدم بهره‌گیری از رمزنگاری و یا الگوریتم‌های مناسب رمزنگاری[1] در ارسال و دریافت اطلاعات. استفاده از «هانی‌پات» و «فایروال»[2] در این خصوص نقش بسزایی در پدافند سایبری ایفا می‌کند (Boyes, H. 2016: 32).

در همین خصوص، تأمین امنیت سایبری سامانه اسکادا[3] از چهار وجه قابل بررسی است: برقراری امنیت نظارت بر داده‌ها در زمان حقیقی، کشف به‌هنگام تهدیدها، تجزیه‌وتحلیل سطح تأثیر تهدیدها و راهبردهای مهار پیامدهای تهدید. مقابله با تهدیدها در حوزه فناوری به‌تنهایی کافی نبوده و نمی‌تواند امنیت کامل زیرساخت را فراهم آورد. درنتیجه، تأمین امنیت و دفاع در برابر تهدیدها مستلزم توجه به تمام ابعاد امنیت و دفاع است. به‌عبارتی، باید با یک نگاه چندوجهی در سه حوزه نیروی انسانی، فرایند و فناوری تهدیدها را مورد توجه قرار داد و اقدامات متقابل را به‌کار برد (Davis, P. 2016: 9).

شاخص‌های دفاعی ـ امنیتی پدافند غیرعامل در برابر تهدیدهای سایبری زیرساخت‌های حیاتی و حساس

شاخص‌های پدافند غیرعامل در برابر تهدیدهای سایبری زیرساخت‌های حیاتی و حساس در سه حوزه منابع انسانی، فرایندها و فناوری قابل بررسی است. اما پیش از طرح شاخص‌ها لازم است تهدیدها متناسب با هریک از حوزه‌های منابع انسانی، فرایندها و فناوری استخراج شود. این موارد که در پژوهش حاضر به تفصیل مورد بررسی قرار گرفته‌اند، در جدول زیر در یک نگاه درمقابل یکدیگر قرار می‌گیرند (Coleman, E. 2015: 19).

1. Suitable Algorithms of Cryptocurrency
2. Honey pot and Firewalls
3. Supervisory Control and Data Acquisition (SCADA)

جدول ۱. تهدیدهای سایبری، پیامدها و آسیب‌پذیری‌ها(Coleman, E. 2015: 19)

تهدید و پیامد	آسیب‌پذیری منابع انسانی	آسیب‌پذیری فرآیندها	آسیب‌پذیری فناوری
ـ اختلال در بهره‌برداری و یا قطع ارتباطات پیامد: نقض یکپارچگی و دسترسی	ـ ضعف آموزش و آگاه‌سازی ـ نیروی غیرمتعهد و یا غیربومی	خلأ سیاست دفاعی ـ امنیتی خلأ آیین‌نامه‌های مقابله با سناریوهای احتمالی تهدید ـ حیطه عملکرد وسیع و وابستگی متقابل زیرساخت‌ها ـ ضعف در چندلایه‌سازی و پدافند در عمق	ـ فعالیت در بستر اینترنت ـ وجود نرم‌افزار و سخت‌افزار غیربومی ـ خلأ آزمایشگاه تشخیص بدافزار ـ خلأ رمزنگاری داده‌ها و فایروال
منع ارائه خدمات پیامد: نقض دسترسی	ـ ضعف آموزش و آگاه‌سازی ـ نیروی غیرمتعهد و یا غیربومی	ـ سیاست امنیتی ـ دفاعی و وابستگی متقابل ـ حیطه عملکرد وسیع و وابستگی متقابل زیرساخت‌ها ـ ضعف در چندلایه‌سازی و پدافند در عمق	ـ وجود نرم‌افزار و سخت‌افزار غیربومی ـ خلأ آزمایشگاه تشخیص بدافزار ـ سیستم عامل غیربومی خلأ فایروال
افشا و یا سرقت اطلاعات حساس و مهم پیامد: نقض محرمانگی	ـ ضعف آموزش و آگاه‌سازی ـ نیروی غیرمتعهد و یا غیربومی	ـ سیاست امنیتی ـ دفاعی ـ حیطه عملکرد وسیع و وابستگی متقابل زیرساخت‌ها ـ ضعف در چندلایه‌سازی و پدافند در عمق	ـ فعالیت در بستر اینترنت ـ وجود نرم‌افزار و سخت‌افزار غیربومی ـ خلأ آزمایشگاه تشخیص بدافزار ـ خلأ رمزنگاری داده‌ها و فایروال

شاخص‌های سنتی پدافند غیرعامل

برخی از شاخص‌های رایج پدافند غیرعامل را می‌تون به قرار زیر خلاصه کرد: استتار، اختفا، پوشش، فریب، تفرقه و پراکندگی، مقاوم‌سازی و استحکامات و اعلام خبر[1]. نکته حائز اهمیت در این خصوص، تبدیل این شاخص‌ها به شاخص‌های متناسب با فعالیت زیرساخت‌های حیاتی و حساس در فضای سایبری است. درنتیجه، هریک از این شاخص‌ها با موارد مقتضی منطبق خواهند شد. شایان ذکر است شاخص‌های سنتی پدافند غیرعامل بیش از

1. Camouflage, Concealment, Cover, Deception, Desperation, Fortify and Fortification and Early Warning

موارد مورد اشاره در این پژوهش است و پژوهش حاضر به‌دلیل تحدید حدود و نیز لزوم تبدیل آنها به شاخص‌های معادل در پدافند سایبری تنها به موارد مندرج در جدول زیر بسنده کرده است: (Rinaldi, S. 2017: 23).

جدول ۲. انطباق شاخص‌های پدافند غیرعامل با شاخص‌های پدافند سایبری (Rinaldi, S. 2017: 23)

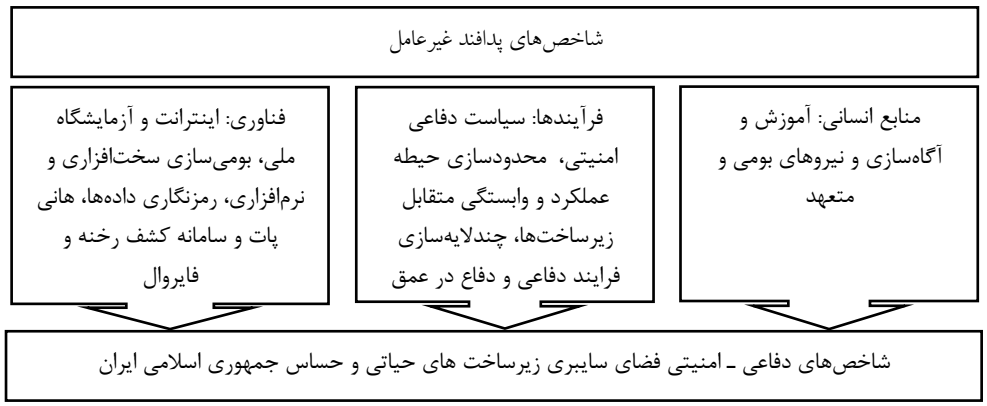
شاخص‌های پدافند غیرعامل	شاخص‌های معادل پدافند سایبری	
استتار، اختفا	رمزنگاری داده‌ها	آموزش و آگاهی بخشی
پوشش و فریب	هانی پات	
تفرقه و پراکندگی	محدودسازی حیطه عملکرد کاهش وابستگی متقابل زیرساختی	
مقاوم‌سازی و استحکامات	چندلایه‌سازی و پدافند در عمق، بومی‌سازی سخت‌افزاری و نرم‌افزاری، فایروال	
اعلام خبر	سامانه کشف و جلوگیری از رخنه	

جدول زیر به ارائه شاخص‌های پدافند سایبری به تفکیک برای هر یک از آسیب‌پذیری‌ها در سه حوزه منابع انسانی، فرایندها و فناوری می‌پردازد.

جدول ۳. شاخص‌های پدافند سایبری برای هر یک از آسیب‌پذیری‌های زیرساخت‌های حیاتی و حساس (Rinaldi, S. 2017: 23)

تهدید	آسیب‌پذیری منابع انسانی	آسیب‌پذیری فرایندها	آسیب‌پذیری فناوری
اختلال در بهره‌برداری و یا قطع ارتباطات پیامد: نقض یکپارچگی و دسترسی	ـ ضعف آموزش و آگاه‌سازی ـ نیروی غیرمتعهد و یا غیربومی	ـ خلأ سیاست دفاعی ـ امنیتی - خلأ آیین‌نامه‌های مقابله با سناریوهای احتمالی تهدید ـ حیطه عملکرد وسیع و وابستگی متقابل زیرساخت‌ها ـ ضعف در چندلایه‌سازی و پدافند در عمق	ـ فعالیت در بستر اینترنت ـ وجود نرم‌افزار و سخت‌افزار غیربومی ـ خلأ آزمایشگاه تشخیص بدافزار ـ خلأ رمزنگاری داده‌ها و فایروال ـ خلأ هانی پات و سامانه کشف رخنه
شاخص‌های پدافند سایبری	آموزش و آگاه‌سازی و بهره‌گیری از نیروهای بومی	ـ تدوین سیاست دفاعی ـ امنیتی و آیین‌نامه‌ها ـ کاهش حیطه عملکرد و وابستگی متقابل زیرساخت‌ها ـ چندلایه‌سازی و پدافند در عمق	راه‌اندازی اینترانت، بومی‌سازی سخت‌افزاری و نرم‌افزای، راه‌اندازی آزمایشگاه‌ها و رمزنگاری داده‌ها استفاده از هانی پات، سامانه کشف رخنه و فایروال

تهدید	آسیب‌پذیری منابع انسانی	آسیب‌پذیری فرایندها	آسیب‌پذیری فناوری
ـ منع ارائه خدمات پیامد: نقض دسترسی	ـ ضعف آموزش و آگاه‌سازی ـ نیروی غیرمتعهد و یا غیربومی	ـ سیاست دفاعی ـ امنیتی ـ حیطه عملکرد وسیع و وابستگی متقابل زیرساخت‌ها ـ ضعف در چندلایه‌سازی و پدافند در عمق	ـ وجود نرم‌افزار و سخت‌افزار غیربومی ـ خلأ آزمایشگاه تشخیص بدافزار ـ سامانه عامل غیربومی -خلأ هانی پات ، سامانه کشف رخنه و فایروال
شاخص‌های پدافند سایبری	آموزش و آگاه‌سازی و بهره‌گیری از نیروهای بومی	تدوین سیاست دفاعی ـ امنیتی - کاهش حیطه عملکرد و وابستگی متقابل زیرساخت‌ها ـ چندلایه‌سازی و پدافند در عمق	راه‌اندازی اینترانت، بومی‌سازی سخت‌افزاری و نرم‌افزای، راه‌اندازی آزمایشگاه‌ها و رمزنگاری داده‌ها و فایروال استفاده از هانی پات و سیامانه کشف رخنه
افشا و یا سرقت اطلاعات حساس و مهم پیامد: نقض محرمانگی	ـ ضعف آموزش و آگاه‌سازی ـ نیروی غیرمتعهد و یا غیربومی	خلأ سیاست دفاعی ـ امنیتی ـ حیطه عملکرد وسیع و وابستگی متقابل زیرساخت‌ها ـ ضعف در چندلایهسازی و پدافند در عمق	ـ فعالیت در بستر اینترنت ـ وجود نرم‌افزار و سخت‌افزار غیربومی ـ خلأ آزمایشگاه تشخیص بدافزار ـ خلأ رمزنگاری داده‌ها و فایروال
شاخص‌های پدافند سایبری	آموزش و آگاه‌سازی و بهره‌گیری از نیروهای بومی	ـ تدوین سیاست دفاعی ـ امنیتی و آیین‌نامه‌ها ـ حیطه عملکرد وسیع و وابستگی متقابل زیرساخت‌ها ـ چندلایه‌سازی و پدافند در عمق	راه‌اندازی اینترانت، بومی سازی سخت‌افزاری و نرم‌افزای، راه‌اندازی آزمایشگاه‌ها و رمزنگاری داده‌ها استفاده از هانی پات، سامانه کشف رخنه و فایروال



تصویر ۱. مدل مفهومی

تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق

تاکنون مطابق با مباحث مطرح شده، مشخص شد که زیرساخت‌های حیاتی و حساس در کشور نقش بسزایی در حفظ کارکرد اجتماعی ایفا می‌کنند و حیات جامعه بستگی به تداوم کارکرد امن آنها دارد. برهمین‌اساس ۱۶ زیرساخت تعریف شد. دامنه عملکرد این زیرساخت‌ها تا اندازه‌ای است که حفظ امنیت ملی کشور به شکلی به عملکرد آنها گره خورده است. زیرساخت‌های حیاتی و حساس در شرایط و عصر کنونی همانند بسیاری از ابعاد و شئون زندگی بشر به فضای سایبری متصل شده است و به‌منظور تسریع در روند ارائه خدمات از آن بهره می‌گیرد. این فضا ضمن آنکه می‌تواند برای ارائه خدمات بهتر در زیرساخت‌های حیاتی و حساس مفید باشد، خطرات و مخاطراتی را نیز می‌تواند متوجه آنها نماید.

به‌منظور استفاده صحیح از فواید فضای سایبری و پرهیز از مخاطرات آن لازم است از رویکردی استفاده شود که ضمن تسهیل در ارائه خدمات زیرساخت‌های حیاتی و حساس، مانع مخاطرات ناشی از فضای سایبری شود. یکی از این رویکردها بهره‌گیری از شاخص‌های پدافند غیرعامل است. پدافند غیرعامل رویکردی است که ضمن تسهیل در ارائه خدمات زیرساخت‌های حیاتی و حساس با استفاده از اقدامات احتیاطی بدون تحمیل هزینه چندان موجب کاهش مخاطرات متوجه زیرساخت‌ها می‌شود. اما شاخص‌های سنتی پدافند غیرعامل در فضای سایبری زیرساخت‌ها چندان کاربردی ندارد و لازم است تا این شاخص‌ها با

معادل‌سازی تبدیل به شاخص‌های متناسب با فضای سایبری شود. درنتیجه، نوعی معادل‌سازی نیاز است. شاخص‌های سنتی استتار، اختفا، پوشش، فریب، تفرقه، پراکندگی، مقاوم سازی، استحکامات و اعلام خبر تبدیل به شاخص‌های متناسب با فضای سایبر شدند. شاخص‌های متناسب با فضای سایبری شامل موارد زیر است: رمزنگاری داده‌ها (مخفی‌سازی اطلاعات)، هانی پات (فریب مهاجم)، محدودسازی حیطه عملکرد و کاهش وابستگی متقابل زیرساختی (تفرقه و پراکندگی)، چندلایه‌سازی، بومی‌سازی نرم‌افزاری و سخت‌افزاری و نیز منابع انسانی مجرب و متعهد و بهره‌گیری از فایروال (مقاوم سازی و استحکامات) و سامانه کشف و جلوگیری از رخنه (اعلام خبر)[1].

حال این شاخص‌ها در سه حوزه‌ای که کارکرد صحیح زیرساخت‌های حیاتی و حساس منوط به کارکرد مطمئن آنهاست، ارائه می‌شود. این سه حوزه عبارتند از: منابع انسانی، فرایندها و فناوری. متناسب با هریک از این حوزه‌ها شاخص‌های پدافند سایبری ارائه شده است.

در منابع انسانی ارائه آموزش، آگاه‌سازی و استفاده از منابع انسانی بومی و متعهد اهمیت بسزایی در حفظ و تداوم کارکرد زیرساخت‌ها دارد. بسیاری از تهدیدها ناشی از عدم آگاهی و یا خیانت نیروهای غیربومی و یا غیرمتعهد است.

در فرایندها خلأ تدوین سیاست دفاعی ـ امنیتی و متولی اجرای آن، حیطه گسترده وسیع و سطح زیرپوشش قابل توجه خدمات هر زیرساخت و وابستگی متقابل آنها به یکدیگر خود تبدیل به یکی از خطرات بالقوه خود ساخته برای کشور شده است که با محدودسازی حیطه عملکرد هر زیرساخت و کاهش وابستگی متقابل آنها به یکدیگر این تهدید به میزان قابل‌توجهی تقلیل پیدا می‌کند. چندلایه‌سازی و فرایند دفاع در عمق نیز این امکان را می‌دهد تا برای کلیه مخاطرات که قابل پیش‌بینی نیستند، لایه‌های متعددی را پیش‌بینی کرد و درنتیجه هنگام وقوع حملات غیرمترقبه و فاقد شواهد و قرائن چندلایه در برابر این حملات قرار داده می‌شود تا درنهایت یکی از لایه‌ها مانع از موفقیت حمله شود.

1.Data Cryptography (Data Hiding), Honey Pot (Deception of Invader), Limiting the Domain of Performance and Reduction of Infrastructure's Dependencies (Desperation), Multi layering, Software & Hardware Customizing, Experienced & Committed Human Resources, Using Firewalls (Fortifying & Fortification) and Intrusion Detection System (IDS)

در فناوری مهم‌ترین چالش کشور وابستگی نرم‌افزاری و سخت‌افزاری به شرکت‌های بیگانه و خارجی است. درنتیجه، بومی‌سازی تدریجی سخت‌افزارها و نرم‌افزارها به میزان قابل‌توجهی این خطر را رفع می‌کند. استفاده از شبکه اینترانت داخلی حجم بسیاری از حملات و تهدیدها را کم می‌کند. بهره‌گیری از آزمایشگاه‌های تشخیص بدافزار در تجهیزات سخت‌افزاری و نرم‌افزاری وارداتی مانع تکرار وقایع تلخی مانند بدافزار استاکس‌نت می‌شود. رمزنگاری داده‌ها نیز امکان دسترسی عوامل غیرمجاز را به داده‌های حساس و مهم نمی‌دهد. بسیاری از تهدیدها در زیرساخت‌ها ناشی از دسترسی غیرمجاز گروه‌های ناراضی و یا متخاصم است. استفاده از هانی پات نیز موجب انحراف مهاجم از هدف اصلی به یک هدف کاذب می‌شود و به این شکل هدف اصلی درامان می‌ماند. علاوه‌براین، رفتار و پروفایل مهاجم[1] نیز در این حمله قابل بررسی و تحلیل است و امکان اتخاذ اقدامات متقابل برای حفظ امنیت و دفاع از زیرساخت اصلی بهتر فراهم می‌شود. دراین‌میان، وجود سامانه‌های کشف و جلوگیری از رخنه و فایروال‌ها نیز می‌تواند عامل دیگری در اطلاع از وقوع حمله و ممانعت از رخنه و کاهش مخاطرات ناشی از این‌گونه حملات باشد.

میزان موافقت با گویه‌های مؤلفه «منابع انسانی»

پرسش اول: شاخص‌های دفاعی ـ امنیتی حوزه منابع انسانی زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران در فضای سایبری مبتنی‌بر رویکردهای پدافند غیرعامل چیست؟

جدول ۴. میزان موافقت با گویه‌های مؤلفه منابع انسانی

	فراوانی	درصد	درصد معتبر	درصد تجمعی
کاملاً مخالفم	۰	۰	۰	۰
مخالفم	۰	۰	۰	۰
نظری ندارم	۶	۱۲	۱۲	۱۲
موافقم	۳۲	۶۴	۶۴	۷۶
کاملاً موافقم	۱۲	۲۴	۲۴	۱۰۰
جمع	۵۰	۱۰۰	۱۰۰	۱۰۰

1. Attack Profile

جدول فوق بیانگر این است که ۸۸ درصد پاسخ‌دهندگان، با عبارت «آموزش و آگاه‌سازی و استفاده از نیروهای بومی در زیرساخت‌های حیاتی و حساس» موافق و کاملاً موافق هستند.

میزان موافقت با گویه‌های مؤلفه «فرایندها»

پرسش دوم: "شاخص‌های دفاعی ـ امنیتی حوزه فرایندهای زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران در فضای سایبری مبتنی‌بر رویکردهای پدافند غیرعامل چیست؟"

جدول ۵. میزان موافقت با گویه‌های مؤلفه فرایندها

	فراوانی	درصد	درصد معتبر	درصد تجمعی
کاملاً مخالفم	۰	۰	۰	۰
مخالفم	۰	۰	۰	۰
نظری ندارم	۴	۸	۸	۸
موافقم	۳۳	۶۶	۶۶	۷۴
کاملاً موافقم	۱۳	۲۶	۲۶	۱۰۰
جمع	۵۰	۱۰۰	۱۰۰	۱۰۰

جدول فوق بیانگر این است که ۹۲ درصد پاسخ‌دهندگان، با عبارت «تدوین پروتکل سیاست دفاعی ـ امنیتی و محدودسازی حیطه عملکرد و وابستگی متقابل در زیرساخت‌های حیاتی و حساس» موافق و کاملاً موافق هستند.

میزان موافقت با گویه‌های مؤلفه «فناوری»

پرسش سوم: شاخص‌های دفاعی ـ امنیتی حوزه فناوری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران در فضای سایبری مبتنی‌بر رویکردهای پدافند غیرعامل چیست؟

جدول ۶. میزان موافقت با گویه‌های مؤلفه فناوری

	فراوانی	درصد	درصد معتبر	درصد تجمعی
کاملاً مخالفم	۰	۰	۰	۰
مخالفم	۰	۰	۰	۰
نظری ندارم	۱	۲	۲	۲
موافقم	۳۵	۷۰	۷۰	۷۰
کاملاً موافقم	۱۴	۲۸	۲۸	۱۰۰
جمع	۵۰	۱۰۰	۱۰۰	۱۰۰

جدول فوق بیانگر این است که ۹۸ درصد پاسخ‌دهندگان، با عبارت "بهره‌گیری از اینترانت، بومی‌سازی سخت‌افزاری و نرم‌افزاری، راه‌اندازی آزمایشگاه‌های تشخیص بدافزارها، رمزنگاری داده‌ها، استفاده از فایروال و هانی پات و سامانه کشف و جلوگیری از رخنه در زیرساخت‌های حیاتی و حساس" موافق و کاملاً موافق هستند.

نتیجه‌گیری

تداوم عملکرد زیرساخت‌های حیاتی و حساس در کشور ضامن دوام حیات اجتماعی آن است. به‌عبارتی، هرگونه اختلال و یا توقف در عملکرد زیرساخت‌ها می‌تواند به‌معنای اختلال و توقف در حیات جامعه قلمداد شود و به‌تبع‌آن امنیت ملی کشور درمعرض مخاطرات جدی قرار گیرد. فضای سایبری که قلمرو پنجم جنگ‌های بشری را تشکیل می‌دهد تبدیل به یکی از حوزه‌های خطرناک برای ادامه بقای زیرساخت‌های حیاتی و حساس شده است. یکی از رویکردهای مقرون به صرفه و کارآمد در کاهش مخاطرات متوجه تداوم کارکرد زیرساخت‌های حیاتی و حساس در فضای سایبری استفاده از شاخص‌های پدافند غیرعامل است. این شاخص‌ها ضمن کارایی هزینه چندانی را دربرنداشته و در حکم اقدامات احتیاطی محسوب می‌شود که می‌تواند درصد قابل‌توجهی از مخاطرات را کاهش دهد.

درهمین‌راستا، شاخص‌های سنتی پدافند غیرعامل به شاخص‌های معادل و قابل‌استفاده در فضای سایبری تبدیل شده است. شاخص‌های رمزنگاری داده‌ها، استفاده از هانی پات، محدودسازی حیطه عملکرد زیرساخت‌ها، کاهش وابستگی متقابل زیرساختی، چندلایه‌سازی و بومی‌سازی، استفاده از فایروال و سامانه کشف و جلوگیری از رخنه مواردی بود که در برابر شاخص‌های سنتی پدافند غیرعامل مانند استتار، اختفا، پوشش و فریب، تفرقه و پراکندگی، مقاوم‌سازی و استحکامات و اعلام خبر مطرح شد.

برای تعیین شاخص‌های دفاعی ـ امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران مبتنی‌بر رویکردهای پدافند غیرعامل سه پرسش فرعی در حوزه‌های منابع انسانی، فرایندها و فناوری طرح شد. از جامعه نمونه آماری بالغ بر ۵۰ نفر به روش تمام‌شماری با نمونه‌گیری غیرتصادفی هدف‌مند سؤالات مطرح شد. درنهایت در سه حوزه

منابع انسانی، فرایندها و فناوری، شاخص‌ها احصا شد و متناسب با هر یک از حوزه‌ها موارد مرتبط به تفصیل بیان شد. هر یک از "شاخص‌های دفاعی ـ امنیتی حوزه منابع انسانی، فرایندها و فناوری فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران مبتنی‌بر رویکردهای پدافند غیرعامل" عبارتند از:

شاخص‌های حوزه منابع انسانی: آموزش و آگاه‌سازی و استفاده از نیروهای بومی در زیرساخت‌های حیاتی و حساس، با میزان موافقت ۸۸ درصد.

شاخص‌های حوزه فرایندها: تدوین پروتکل سیاست دفاعی ـ امنیتی، محدودسازی حیطه عملکرد و وابستگی متقابل در زیرساخت‌های حیاتی و حساس، با میزان موافقت ۹۲ درصد.

شاخص‌های حوزه فناوری: بهره‌گیری از اینترانت، بومی‌سازی سخت‌افزاری و نرم‌افزاری، راه‌اندازی آزمایشگاه‌های تشخیص بدافزارها، رمزنگاری داده‌ها و استفاده از «فایروال» و «هانی پات» و سامانه کشف و جلوگیری از رخنه در زیرساخت‌های حیاتی و حساس، با میزان موافقت ۹۸ درصد.

منابع

فارسی

۱. سازمان پدافند غیرعامل کشور (۱۳۹۳)، **اصول حاکم بر پدافند سایبری کشور**، تهران: انتشارات مؤسسه سایبربان.

۲. شورای عالی فضای مجازی (۱۳۹۸)، **حکمرانی فضای مجازی**، قابل دسترسی در: www.majazi.ir

۳. کانون اندیشه راهبردی سازمان پدافند غیرعامل (۱۳۹۵)، **مصون‌سازی و پایداری کشور در برابر تهدیدها با پدافند غیرعامل**، تهران: انتشارات روزنامه همشهری.

انگلیسی

1. Baheti, R. (2015), Cyber-physical systems: Netherland, Elsevier Publication.
2. Bashan, A. (2013), The extreme vulnerability of interdependent spatially: London, Taylor & Francis Publication.
3. Boyes, H. (2016), Trustworthy cyber-physical systems: Netherland, Wolters Kluwer Publication.
4. Chess, A. (2017), Hybrid and Embedded Software Systems: London, Pearson Publication.
5. Coleman, E.(2015), The City as a Platform - Stripping out complexity and Making Things Happen: London, Thomson Reuters.
6. Cotton, Oliver (2015) Cyberspace: The New World Game: London, Phaidon Publication.
7. Davis, P. (2016), How to Rebuild the City as a Platform: Netherland, Elsevier.
8. Doytsher, Jack, (2016) Rapid urbanization and mega cities: the need for spatial information management: London, Press Publication.
9. Gabriel, P. (2017), Global Health Observatory (GHO): London, Pearson Publication.
10. Knigh, Shawn, (2012), Duqu Trojan contains mystery programming language in Payload
11. Poovendran, R. (2014), Cyber-physical systems: close encounters between two parallel worlds: Washington, Pearson Publication.
12. Rinaldi, S. (2017), Identifying, understanding, and analyzing critical infrastructure interdependencies: London, Pearson Publication.
13. Shafi, Q. (2017), Cyber physical systems security: a brief survey: Netherland, Elsevier.