فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره۳، تابستان ۱۴۰۱
مقاله چهارم، از صفحات ۸۹-۱۲۰

مقاله پژوهشی:

ارائه الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی جمهوری اسلامی ایران

مهدی رحمتی لارهنگ[۱]، محمدمهدی نژادنوری[۲]، مرتضی طالبی[۳]، حسین اسکندی[۴]

تاریخ دریافت: ۱۴۰۰/۰۸/۱۰ **تاریخ پذیرش:** ۱۴۰۱/۰۲/۱۶

چکیده

امروزه زیرساخت‌ها بسترهای مهم حیات، رشد و پویایی جوامع به شمار می‌روند. پایداری اقتصادی، کیفیت زندگی جامعه و ثبات امنیت ملی، به میزان قابل‌توجهی به در دسترس‌بودن، تداوم و پایداری عملکرد زیرساخت‌های حیاتی کشور وابسته است. با توجه به اتکا روزافزون این زیرساخت‌ها به فضای سایبر و هوشمند شدن تهدیدات سایبری، رویکرد دفاع از آن‌ها نیز باید رویکردی هوشمندانه باشد؛ ازاین‌رو این مقاله با هدف دستیابی به الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی جمهوری اسلامی ایران تهیه شده است. در پژوهش حاضر، ادبیات و مبانی نظری، شامل مفاهیم، طبقه‌بندی و انواع زیرساخت‌های حیاتی، اتکا زیرساخت‌ها به فضای سایبر، آگاهی وضعیتی سایبری، دفاع هوشمند، تهدیدات و آسیب‌پذیری‌های زیرساخت‌های حیاتی، دفاع سایبری و چالش‌های فناوری‌های نوظهور در زیرساخت‌های حیاتی مطالعه و بررسی گردید. سپس با تدقیق و تحلیل اسناد بالادستی و انجام مطالعه تطبیقی مدل‌ها، الگوها، چارچوب‌ها، طرح‌ها و روش‌های دفاع سایبری ملی و بین‌المللی، ابعاد، مؤلفه‌ها و شاخص‌ها احصاء و مدل مفهومی پژوهش ترسیم گردید. جهت ارزیابی مدل مفهومی احصاء شده، پرسشنامه‌ای بر اساس طیف لیکرت پنج گزینه‌ای تنظیم و طی پنل خبرگی، ضمن اصلاح پرسشنامه، روایی و پایایی پرسشنامه تأیید شد. سپس پرسشنامه نهایی در اختیار ۸۰ نفر از متخصصین و فعالان حوزه مورد مطالعه قرار گرفت و نظر تخصصی ۷۲ نفر اخذ گردید. برای تجزیه‌وتحلیل داده‌های پژوهش و تأیید عاملی مدل مفهومی پژوهش از نرم‌افزار اسمارت پی. ال. اس به روش حداقل مربعات جزئی بهره‌گیری گردید. بر اساس محاسبات انجام‌شده توسط این ابزار، برازش کلی مدل معادل ۰,۴۳۹ حاصل شد که نشان‌دهنده برازش قوی مدل است. درنهایت مطابق ابعاد، مؤلفه‌ها و شاخص‌های تأییدشده توسط ابزار تحلیل، مدل مفهومی پژوهش اصلاح و نهایی گردید.

کلیدواژه‌ها: دفاع سایبری، زیرساخت‌های حیاتی، دفاع هوشمند، دفاع هوشمند سایبری

۱. دانشجوی دکتری مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی (نویسندهٔ مسئول)، larhang78@yahoo.cim
۲. عضو هیئت علمی دانشگاه و پژوهشگاه عالی دفاع ملی m.noori@razavi.ir
۳. دانشجوی دکتری مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی m.talebi98@sndu.ac.ir
۴. دانشجوی دکتری مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی

مقدمه و بیان مسئله

امروزه داشتن اقتصادی پایدار و برخورداری از جامعه‌ای توسعه‌یافته، بدون برنامه‌ریزی راهبردی برای حفاظت، تأمین امنیت و پایداری زیرساخت‌های حیاتی امکان‌پذیر نیست. زیرساخت‌های حیاتی، ارائه‌دهنده خدمات اساسی و بنیادی هستند و حفاظت از زیرساخت‌های حیاتی و دارایی‌های کلیدی از مهم‌ترین وظایف و مأموریت‌های هر حاکمیتی محسوب می‌شود؛ چرا که تخریب یا وارد آمدن آسیب به آن‌ها، می‌تواند تداوم حیات کشور را با مشکل مواجه سازد و امنیت کشور را به لحاظ سیاسی، اقتصادی و دفاعی به شکل جدی به خطر اندازد. در سال‌های اخیر، به‌واسطه صدمات ناشی از تشدید حملات عامدانه، فجایع طبیعی و حوادث شدید آب‌وهوایی، مسئله حفاظت از زیرساخت‌های حیاتی (CIP)[۱] اهمیت دوچندان یافته است (Petit, ۲۰۱۸).

با رشد و گسترش نفوذ فضای سایبر در زیرساخت‌های حیاتی و شبکه‌ای شدن این زیرساخت‌ها به‌منظور افزایش کارایی و ارائه خدمات با ارزش‌افزوده بالاتر، وابستگی زیادی بین زیرساخت‌های حیاتی و فضای سایبر ایجاد شده و علی‌رغم مزایای بی‌شمار این وابستگی، باعث افزایش فزاینده آسیب‌پذیری‌ها و مخاطرات سایبری زیرساخت‌های حیاتی گردیده است. از طرفی علی‌رغم رعایت پروتکل‌های امنیت سایبری در اکثر زیرساخت‌های حیاتی، به علت ویژگی‌های خاص تهدیدات و حملات سایبری ازجمله تنوع، پویایی، حجم و سرعت بالا و از همه مهم‌تر هوشمندی، همچنان شاهد حوادثی در زیرساخت‌های حیاتی کشور با منشأ سایبری هستیم. بررسی سوابق گذشته نشان می‌دهد که تهدیدهای سایبری و اقدام‌های خصمانه برخی دولت‌های خارجی در قبال ایران، در مقاطع زمانی مختلف، حوزه‌های گوناگونی ازجمله زیرساخت‌های هسته‌ای، صنایع نفتی، حمل‌ونقل هوایی، بنادر و کشتیرانی، فناوری اطلاعات و ارتباطات، بانکداری و غیره، عرصه‌های تجاوز به زیرساخت‌های مهم کشورمان بوده‌اند. انجام حملات

۱. Critical Infrastructure Protection

سایبری مخرب، ازجمله حمله به سایت هسته‌ای نطنز با استفاده از بدافزار استاکس‌نت و استفاده از بدافزار فلیم در زیرساخت‌های صنعت نفت کشور نمونه‌های مشهوری از این اقدامات است.

باتوجه به گستردگی و پیچیدگی حملات به زیرساخت‌های حیاتی کشور، قطعاً پایش، تحلیل و اقدام متناسب در مدت‌زمانی محدود و با تکنیک‌های موجود برای مقابله با این حملات ممکن نخواهد بود و نیاز به نگاه و رویکردی جدید به موضوع دفاع از زیرساخت‌های حیاتی و توسعه و بهره‌گیری از فناوری‌های نو را روزافزون می‌نماید. سامانه‌های دفاع سایبری آینده در کنار امکانات امروزی قطعاً باید از امکانات هوشمند در درک، فهم، پیش‌بینی (آگاهی وضعیتی) و پیش‌گیری از انواع حملات سایبری پیچیده و در صورت وقوع حمله دارای قابلیت هوشمندی و خودمختاری[۱] در پاسخ به حملات سایبری در شبکه‌ها متناسب با سطح و تنوع تهدیدات برخوردار باشند.

از سوی دیگر به دلیل درهم‌تنیدگی و وابستگی اکثر زیرساخت‌های حیاتی به یکدیگر و وابستگی همه آن‌ها به فضای سایبر به‌عنوان زیرساخت همه زیرساخت‌ها، امکان تأمین امنیت و دفاع به‌صورت مستقل و بدون توجه به شرایط و وضعیت سایر حوزه‌ها مقدور نمی‌باشد و نیازمند مدیریت یکپارچه و هوشمند که با اشتراک منابع، اطلاعات و تجربیات همه ذی‌نفعان این عرصه و با بهره‌گیری از فرایندها و فناوری‌های نوین سایبری محقق خواهد شد.

در خصوص ضرورت تدوین الگوی دفاع هوشمند سایبری زیرساخت‌های حیاتی کشور می‌تواند به راه‌اندازی محیط‌های ایمن، آگاهی از وضعیت محیطی هوشمند، واکنش کاملاً خودکار هنگام حملات سایبری به زیرساخت‌های حیاتی و درنهایت حفاظت و تاب‌آوری بیشتر زیرساخت‌های حیاتی ج.ا.ا در برابر حملات مداوم پیشرفته اشاره نمود.

بنابراین به‌منظور ایجاد حرکتی منسجم و هم‌افزا برای مصون‌سازی حداکثری زیرساخت‌های حیاتی ج.ا.ا در مقابل تهدیدات روزافزون و پیشرفته فضای سایبر که ممکن است توسط دشمنان خارجی یا عوامل داخلی آن‌ها صورت پذیرد در این پژوهش به‌دنبال تدوین «الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی جمهوری اسلامی ایران» هستیم و به همین‌منظور سؤال اصلی تحقیق این‌گونه مطرح شده است: «الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی

۱. Autonomy

جمهوری اسلامی ایران کدام است؟» همچنین در سؤالات فرعی مفهوم، ماهیت، ویژگی‌ها و چالش‌های دفاع هوشمند سایبری، ابعاد و مؤلفه‌ها و شاخص‌های دفاع هوشمند و ارتباط بین ابعاد و مؤلفه‌ها مورد پرسش قرار گرفته است.
است.

۱- مبانی نظری تحقیق

پیشینه تحقیق

در خصوص اهمیت زیرساخت‌های حیاتی، تهدیدات مختلف این زیرساخت‌ها، چگونگی حفاظت از زیرساخت‌های حیاتی در برابر حملات مختلف از جمله حملات سایبری، تحقیقات زیادی صورت گرفته و اسناد و دستورالعمل‌هایی نیز در کشورهای مختلف در این خصوص صادر شده است. در جمهوری اسلامی ایران نیز سازمان پدافند غیرعامل چند دستورالعمل برای بخش‌های مختلف زیرساخت‌های حیاتی به‌صورت کلی و تخصصی صادر نموده است. از جمله این اسناد می‌توان به طرح پاسخ اضطراری سایبری در حوزه انرژی، سطح‌بندی زیرساخت‌های سایبری و وابسته به سایبر مبتنی بر متدولوژی CARVER+ Shock+Interdependency و سند راهبردی پدافند سایبری کشور اشاره نمود. ایالات متحده امریکا نیز دستورالعمل سیاست‌های ریاست جمهوری- امنیت و تاب‌آوری زیرساخت‌های حیاتی را در سال ۲۰۱۳ صادر نموده و در سال ۲۰۱۵ بازنشر داده است؛ همچنین راهنما امنیت و تاب‌آوری زیرساخت‌های حیاتی را در نوامبر ۲۰۱۹ صادر نموده است که به دسته‌بندی زیرساخت‌های حیاتی، تهدیدات این زیرساخت-ها و نقش و وظایف بخش‌های مختلف در جهت حفاظت از این زیرساخت‌ها پرداخته است.کشورهای دیگری چون استرالیا، کانادا، بلغارستان، اسکاتلند و اتحادیه اروپا نیز اسناد مهمی در خصوص حفاظت از زیرساخت‌های حیاتی صادر نموده‌اند؛ همچنین رساله‌ها و مقالات مختلفی در خصوص چگونگی حفاظت از زیرساخت‌های حیاتی در برابر تهدیدات گوناگون از جمله تهدیدات سایبری منتشر شده است؛ که از جمله این تحقیقات می‌توان به ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی که توسط محسن آقایی و همکاران در سال ۱۳۹۸ انجام شده است اشاره نمود که در نتایج این تحقیق مدل مفهومی منطقی طبقه‌بندی

تهدیدات سایبری زیرساخت‌های حیاتی با ابعاد شش‌گانه: تهدیدات، عوامل تهدید، مشخصات تهدید، نگاه از دیدگاه نفوذگر، توصیف سامانه و منابع شناسایی تهدیدات، ارائه شده است و یا تحقیق با عنوان امنیت ملی و حفاظت از زیرساخت‌های حیاتی در سال ۲۰۱۹ توسط آدریانا الکساندر و همکاران در کشور رومانی انجام شده است که در نتایج این تحقیق به ارتباط بین امنیت ملی و امنیت زیرساخت‌های حیاتی پرداخته شده و خواستار بازنگری در قوانین کشور رومانی برای حفاظت بیشتر از این زیرساخت‌ها شده است.

دفاع هوشمند و دفاع از فضای سایبری از دیدگاه مقام معظم رهبری

عباراتی چون «مواجهه هوشمندانه و مقتدرانه با تحولات پرشتاب» فضای سایبر از سوی بالاترین مقام نظام مقدس جمهوری اسلامی (حکم انتصاب اعضای شورای عالی فضای مجازی، ۱۳۹۴)، نشان از نقش مهّم فضای سایبر در اداره امور جامعه دارد و «اهتمام ویژه به سالم‌سازی و حفظ امنیت همه‌جانبه فضای مجازی کشور» و «مقابله مؤثر بانفوذ و دست‌اندازی بیگانگان» (حکم انتصاب اعضای شورای عالی فضای مجازی، ۱۳۹۴) هیچ شکی در ضرورت دفاع از دارایی‌های سایبری و غیرسایبری موجود در این فضا باقی نگذاشته است. دفاع هوشمند در اندیشه فرمانده معظم کل قوا (مدظله‌العالی) علم، هنر و تدبیر به‌کارگیری همه ظرفیت‌ها، منابع قدرت (مادی و معنوی) آمادگی دائمی و همه‌جانبه به‌منظور مقابله با تهدیدات پیش‌روی نظام، همراه با هوش، بصیرت و اشراف به محیط پیرامونی بیان شده است؛ به‌طوری‌که نادیده‌گرفتن هریک از این موارد موجب کاستی در شاکله دفاع هوشمند خواهد شد؛ وی شرایط تحقق دفاع هوشمند را در سه حوزه ضرورت، تناسب و فوریت به شرح زیر تبیین نموده است:

- ضرورت: ارتقای سطح امنیت و دفع تهدید باتوجه به ماهیت تغییرپذیر تهدیدات و ظهور تهدیدات جدید؛
- تناسب: تناسب اقدام دفاعی با نوع و جنس تهاجم و تهدید؛
- فوریت: اقدام به دفاع فوری، به عبارتی دفاع قبل از تهاجم و پیش‌بینی حرکت‌های دشمن (لطفی مرزناکی، ۱۳۹۴).

دفاع از زیرساخت‌های حیاتی دراسناد بالادستی

در سند راهبردی پدافند غیرعامل کشور، ارزش‌های حاکم بر دفاع از زیرساخت‌های حیاتی کشور، معنویت و قداست دفاع، تفکر و عمل بسیجی، نفی سلطه استکبار، حفظ نظام جمهوری اسلامی، صلح‌آمیز بودن ذکرشده و از نفوذناپذیری، پویایی، خلاقیت و نوآوری، انسجام و هم‌افزایی، چندمنظوره و صرفه اقتصادی، دفاع همه‌جانبه، پیش‌دستی در درک تهدیدات، هوشمندی و ابتکار، تفکر راهبردی، دانش بومی‌سازی، صیانت از مردم و سرمایه‌های انسانی، حفظ آرامش روانی جامعه، پیوستگی مردم و جامعه، ارتقای آمادگی و مقاومت ملی به‌عنوان اصول راهبردی حاکم در این ساحت نام برده شده است. در بخشی از جهت‌گیری‌های کلان این سند، لزوم برآورد تهدیدات و احصای آسیب‌پذیری‌های سایبری زیرساخت‌های حیاتی کشور و کاهش آسیب‌پذیری‌های سایبری و افزایش ایمنی زیرساخت‌های ملی و مراکز حیاتی و استمرار خدمات ضروری دستگاه‌ها در برابر حملات سایبری تبیین گردیده است (سند راهبردی پدافند غیرعامل کشور، ۱۳۸۸).

در اصل چهارم سند قرارگاه پدافند سایبری کشور نیز به هوشمندی دفاع اشاره شده است. باتوجه‌به محیط پیچیده و ناشناخته سایبری و تحولات و پیشرفت‌های روزبه‌روز دانش و فناوری این عرصه، پدافند سایبری باید از عنصر هوشمندی و کیاست به خوبی بهره ببرد تا کشور دچار غافل‌گیری نشده و بالعکس دشمن در موضع انفعال و سردرگمی قرار گیرد. در ذیل اهداف کلان در افق چشم‌انداز قرارگاه پدافند سایبری کشور، اجرای نظام جامع فرماندهی و کنترل یکپارچه و هوشمند پدافند سایبری به‌منظور پایداری خدمات سایبری زیرساخت‌های حیاتی و حساس کشور تصریح شده است (قرارگاه پدافند سایبری کشور، ۱۳۹۴).

مفهوم‌شناسی فضای سایبری

یک قلمرو جهانی در داخل محیط اطلاعاتی است که شاخصه و کاراکتر منحصربه‌فرد آن از طریق بهره‌گیری از الکترونیک و الکترومغناطیس برای ایجاد، ذخیره‌سازی، اصلاح، مبادله و بهره برداری از اطلاعات از طریق شبکه‌های مرتبط و متصل‌به‌هم با بهره‌گیری از فناوری‌های ارتباطی طراحی‌شده است (Almeida, Virgilio, 2016).

روسیه و آمریکا به‌صورت مشترک فضای سایبر را یک رسانه الکترونیکی که از طریق آن اطلاعات تولید، منتقل، دریافت، ذخیره، پردازش یا حذف می‌شوند معرفی نموده‌اند (K.F. Rauscher and V. Yaschenko, 2011)؛ همچنین اسکندری فضای سایبر را شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده (جاگذاری شده)، کنترلرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات می‌داند که این فضا ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی باشد و یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه‌شده باشد (اسکندری، ۱۳۹۳: ۸۳).

در مدل ارائه شده شورای‌عالی فضای مجازی، فضای سایبر دارای چهار مؤلفه کلیدی شامل، مؤلفه سیستمی، مؤلفه کاربردی و محتوایی، مؤلفه انسانی و اجتماعی، مؤلفه مدیریتی- حاکمیتی. برای فضای سایبری است که آن را یکتا می‌سازد و برای پاسخ‌گویی به بسیاری از پرسش‌های مرتبط با آن مهّم هستند.

زیرساخت‌های حیاتی[1]

به مجموعه‌ای از مراکز و بخش‌های فعال اعم از تجهیزات، امکانات و خدمات در فرایند تولید، تبادل، انتقال، توزیع و انتشار در حوزه‌های مختلف از قبیل «برق»، «مخابرات و ارتباطات راه دور»، «مواد و انرژی هسته‌ای»، «سیستم اطلاعات دولتی و خصوصی»، «حمل‌ونقل اعم از راه آهن، بزرگراه، بنادر و راه‌های آبی، فرودگاه‌ها»، «شبکه‌های بهداشت، درمان و سلامت انسان، دام و محیط زیست»، «سامانه‌های کشاورزی» و موارد مشابه، زیرساخت گفته می‌شود که به‌صورت ویژه، حیاتی، حساس، مهم و قابل حفاظت دسته‌بندی می‌شوند (نظام عملیاتی پدافند سایبری کشور، ۱۳۹۸). نکته مهّم در مورد این زیرساخت‌ها این است که زیرساخت‌های حیاتی، ارائه‌دهنده خدمات اساسی و بنیادی است و ازاین‌رو چارچوب اصلی برای پشتیبانی از ساختارهای کلان امنیت ملی کشور و آحاد ملت هست. به همین جهت است که حفاظت از

[1] Critical Infrastructures

زیرساخت‌های حیاتی و دارایی‌های کلیدی از مهّم‌ترین وظایف و مأموریت‌های هر دولتی محسوب می‌شود؛ چراکه تخریب یا واردآمدن آسیب به آن‌ها، به‌راحتی می‌تواند تداوم حیاتی کشور را با مشکل مواجه سازد و امنیت آن را به لحاظ سیاسی، اقتصادی و دفاعی به شکل جدی به خطر اندازد. در سند راهبردی پدافند غیرعامل جمهوری اسلامی ایران، مراکز حیاتی، مراکزی هستند که انهدام کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات جدی و مخاطره‌آمیز در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی در سطح تأثیرگذاری ملی شود (سند راهبردی پدافند غیرعامل جمهوری اسلامی ایران،۱۳۹۱).

حفاظت از زیرساخت‌های حیاتی(CIP)

منظور از حفاظت از زیرساخت‌های حیاتی کلیه فعالیت‌هایی است که هدف آن‌ها تأیید عملکرد، تداوم و یکپارچگی زیرساخت‌های حیاتی برای کاهش یا کاهش تهدیدها، خطرات و آسیب‌پذیری‌ها است (۱۱۴/۲۰۰۸ / EC،۲۰۰۸، ماده ۲). به‌منظور حفاظت و دفاع از زیرساخت-های حیاتی جمهوری اسلامی ایران، مصوبات و دستورالعمل‌های مختلفی از سوی سازمان پدافند غیرعامل کشور صادر گردیده است که در ذیل به پنج دستورالعمل مرتبط با موضوع یاد شده اشاره شده است.

- دستورالعمل عملیاتی پدافند سایبری زیرساخت‌های صنعتی کشور (قرارگاه پدافند سایبری کشور فروردین ۱۴۰۰)؛
- اقدامات امن‌سازی اضطراری زیرساخت‌های سایبری و وابسته به سایبر کشور (قرارگاه پدافند سایبری تیرماه ۱۳۹۸)؛
- طرح پاسخ اضطراری به تهدیدات سایبری در حوزه انرژی CERP (قرارگاه پدافند سایبری کشور مردادماه ۱۳۹۷)؛
- دستورالعمل عملیات پیشگیرانه (اقدامات اساسی) در زمان هشدار (قرارگاه پدافند سایبری کشور مردادماه ۱۴۰۰)؛

۱. Critical Infrastructure Protection

- نظام عملیاتی پدافند سایبری کشور (قرارگاه پدافند سایبری کشور اردیبهشت‌ماه ۱۴۰۰)؛
- سطح‌بندی زیرساخت‌های سایبری و وابسته به سایبر مبتنی بر متدولوژی CARVER+Shock (قرارگاه پدافند سایبری کشور خردادماه ۱۳۹۹).

تهدیدات و آسیب‌پذیری سایبری زیرساخت‌های حیاتی

همچنین در سند راهبردی پدافند سایبری جمهوری اسلامی ایران، تهدید سایبری» عامل خارجی با قابلیت وارد نمودن ضربه فاجعه‌بار به امنیت، منافع و اقتصاد ملی، وجهه و روابط بین‌المللی، سلامت، ایمنی و اطمینان عمومی، باورهای دینی و ملی یا اداره امور کشور، از طریق تخریب یا ایجاد اختلال گسترده در عملکرد سرمایه‌های ملی سایبری کشور» تعریف‌شده است (محسن آقایی و دیگران،۱۳۹۸).

تعداد تهدیداتی که در حوزه سایبر وجود دارد دقیقاً قابل‌شناسایی نیست؛ زیرا به دلیل ماهیت فضای سایبر و پویا بودن این فضا، هر روز تهدیدات جدیدتری، با روش‌های کاملاً جدید و ابتکاری و با ابزارهای مختلفی و برای اهداف متفاوتی ارائه می‌گردند؛ همچنین می‌توانند این تهدیدات را با دیدگاه‌های مختلفی دسته‌بندی نمود (محسن آقایی و دیگران،۱۳۹۸).

بالاترین تهدیدات سایبری از جمله تهدیدات علیه زیرساخت‌های حیاتی عبارتند از؛ بدافزارها، حملات وب پایه، فیشینگ، منع خدمات، اسپم، بات نت، نقص اطلاعات، تهدیدات داخلی، سرقت و تخریب داده، نشت اطلاعات، سرقت هویت، رمزکاوی، باج افزار، جاسوسی سایبری. در این بین تهدیدات بدافزار در صدر قرار دارد و اولین هدف‌گذاری بد افزارها به خطر انداختن زیر ساخت‌های اطلاعاتی حیاتی است که به‌عنوان نمونه می‌توان به استاکس نت اشاره کرد (تقی‌پور و همکاران،۱۳۹۷).

به‌طورکلی آسیب‌پذیری‌های زیرساخت‌ها در سه حوزه منابع انسانی، فرایندها و فناوری مورد بررسی قرار می‌گیرد.

درحوزه 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 به معنای آن است کـه افـراد مجـاز در هر زمان قادر به دسترسی به سامانه و اطلاعات مرتبط باشند و از سـوی دیگـر افـراد غیرمجـاز، این امکان را نداشته باشند (کافی،۱۳۹۹).

دفاع سایبری

وابستگی روزافزون زیرساخت‌های حیاتی کشور بـه فضـای سـایبری، زمینـه‌سـاز افـزایش آسیب‌پذیری ناخواسته کشور در برابر حملات و تهدیدهای سایبری شده است. محـور قرارگـرفتن فضای اطلاعاتی و سایبری در ساختارهای قدرت ملی اگرچه باعـث افـزایش چشـم‌گیـر کـارایی، انعطاف‌پذیری، نوآوری و تحول می‌شود؛ امّا می‌تواند به نقطه ضعف عمده کشور مبدل گـردد؛ لـذا تقویت دفاع سایبری کشور اجتناب‌ناپذیر است (رامک و محمـدی، ۱۳۹۸). دفـاع فضـای سـایبری (دفاع سایبری) اقداماتی که برای شکست تهدیدهای خاصی در فضای سـایبر محافظـت شـده کـه امنیت فضای سایبر را نقض یا تهدید به نقض آن می‌کنند انجام مـی‌شـود و شـامل اقـداماتی بـرای شناسایی، توصیف، مقابله و کاهش تهدیدات، از جمله بدافزار یا فعالیـت‌هـای غیرمجـاز کـاربران و بازگرداندن سامانه به حالت پیکربنـدی امـن اسـت (سـتاد مشـترک ایـالات متحـده، ۲۰۱۸). دفـاع سایبری بر جلوگیری، شناسایی و ارائه به‌موقع پاسخ به حملات یا تهدیدها متمرکز اسـت تـا هـیچ زیرساخت یا اطلاعاتی تغییر نکند؛ به‌عبارتی دیگر دفاع سایبری، قابلیـت‌هـای سـازمان‌یافتـه بـرای محافظت در مقابل، یا کاهش و بازیـابی سـریع اثـرات حملـه سـایبری اسـت. رویکردهـای دفـاع سایبری به سه دسته کلی، واکنشی[۱] فعال[۲] و پیش‌کنش‌گرایانه[۳](یا پـیش‌دسـتانه[۴]) قابـل تقسـیم اسـت. رویکردهای واکنشی بعد از وقوع حمله سایبری عملیاتی می‌شوند؛ رویکردهـای فعـال بـه محـض وقوع حمله سایبری اجرا می‌گردند و رویکردهای پیش‌کنش‌گرایانه، قبـل از وقـوع حملـه سـایبری اجرایی می‌گردند (عزیزی، امیر، ۱۳۹۹).

۱. Reactive
۲. Active
۳. Proactive
۴. Preemptive

آقای تقی‌پور و اسماعیلی ابعاد دفاع سایبری را بازدارندگی در دفاع سایبری (ارتباط، توانایی، اعتبار، ثبات.)، پدافند در دفاع سایبری (پدافندعامل، پدافند غیرعامل) و تاب‌آوری در دفاع سایبری (مقاومت، قابلیت اطمینان، افزونگی، پاسخ و بازیابی) و مؤلفه‌های هر بعد را بیان نموده‌اند (آقای تقی‌پور و اسماعیلی، ۱۳۹۷).

مدل‌های دفاع سایبری

اگرچه بهره‌گیری از تجربه کشورهای پیشرو در دفاع سایبری موضوعی بسیار پراهمّیت است که تردیدی در ضرورت آن وجود ندارد، حساسیت‌های موجود در خصوص کشور ایران و تقابل دائمی نظام سلطه با جمهوری اسلامی ایران، ضرورت طراحی مدلی مفهومی بومی برای الگوی دفاع سایبری با رویکرد هستی‌شناسانه و بنیادین را مضاعف ساخته است (تقی‌پور و اسماعیلی، ۱۳۹۷) بنابراین در زیر به بررسی چند مدل دفاع سایبری خواهیم پرداخت.

الف- مدل دفاع در عمق سایبری: یک رویکرد امنیت اطلاعات است که از یک استراتژی دفاع نظامی اقتباس شده است، روشی که یک مهاجم مجبور می‌شود برای نفوذ از موانع زیادی عبور کند که در نهایت منابع مهاجم را خرج می‌کند. یک دفاع کاملاً دقیق در معماری عمیق، از اکثریت قریب به اتفاق حملات جلوگیری می‌کند و مدیر شبکه را از نفوذهایی که از آن عبور می‌کنند آگاه می‌کند (National Security Agency, 2012).

ب) **مدل مفهومی سامانه آگاهی وضعیتی دفاع سایبری:** این روش توسعه مبانی نظری، روش‌ها و توصیه‌ها و همچنین ابزارهای نرم‌افزاری برای آگاهی از وضعیت[1] است که در یک حالت تقریباً آنلاین، نیروهای امنیتی خودی را قادر می‌سازد تا بر فضای سایبر برای تشخیص تزریق اطلاعات مخرب و اطلاع‌رسانی به‌موقع در مورد حمله اطلاعاتی نظارت داشته باشند و شرایط لازم برای تصمیم‌گیری در مورد پیشگیری یا پاسخ به‌موقع به تزریق اطلاعات دشمن ایجاد نمایند (Stoianov.N & Bozhilova.M, 2020).

---

1. SA

ج) **مدل مرجع دفاع سایبری**:[۱] آزمایشگاه تحقیقاتی نیروی هوایی ایالات متحده، یک مدل مرجع سایبری ارائه کرده است که می‌تواند در طول حملات سایبری مورد استفاده قرار گیرد. مدل پیشنهادی می‌تواند تعامل بین قابلیت‌های دفاع سایبری و فرایندهای آماده‌سازی را که برای محافظت از دارایی‌های مورد نیاز است، توصیف کند؛ این مدل می‌تواند؛ اولاً حملات سایبری را که به لایه فیزیکی ختم می‌گردد، کاهش دهد. ثانیاً به‌عنوان ابزاری در طول برنامه‌ریزی راهبردی دفاع سایبری نیز مورد استفاده قرار گیرد؛ ثالثاً امنیت سایبری با تعامل و هم‌افزایی بین قابلیت‌های سایبری، فرایندهای سایبری و دارایی‌های حیاتی به دست می‌آید که برای محافظت در برابر حملات ترکیبی پیچیده ضروری است (Kolini & Janczewski, 2015: 05).

د) **مدل دفاع از قابلیت‌های سایبری و طبقه‌بندی**[۲]: هدف اصلی در این مدل ارائه مدلی است که بتواند بین انواع مختلف مکانیزم‌های دفاعی که در کاهش یا پاسخ به حملات سایبری استفاده می‌شوند، تمایز قائل شود؛ این مدل برخلاف مطالعات قبلی، طبقه‌بندی را پیشنهاد می‌دهد که سعی در شناسایی تمامی بازیگران صحنه درگیری در فضای سایبری را دارد به سه بعد مجزای دارایی (سخت‌افزار، نرم‌افزار، اطلاعات، نیروی انسانی)، قابلیت‌ها (پدافند عامل، غیرعامل، دفاع مشارکتی و همکاری با سایر بازیگران)و فرایندهای آماده‌سازی (طرح‌ریزی، ارتباط و تعامل، اجرا و ارزیابی) تقسیم‌بندی می‌شود (Kolini & Janczewski, 2015: 05).

منابع توانمندساز دفاع سایبری

موفقیت هر سازمانی از جمله سازمان‌های نظامی، وابسته به وجود سطح مطلوبی از مؤلفه‌های توانمندساز در آن سازمان است. منابع و توانمندسازها مهم‌ترین عوامل برای حفظ و ارتقای آمادگی دفاع سایبری در سطح ملی و سازمانی محسوب می‌گردد؛ که بدون آن‌ها آمادگی دفاعی سایبری معنا و مفهوم پیدا نمی‌کند. بر اساس تعریفی که اولین‌بار توسط مرکز آموزش و دکترین ارتش امریکا[۳]صورت گرفت؛ ولی بعداً توسعه یافت، مؤلفه‌های توانمندساز، شامل هفت عنصر کلیدی از قبیل: دکترین، سازمان‌دهی، آموزش، تجهیزات، نیروی انسانی، رهبری و منابع و امکانات

۱. Cyber Defense Reference Model
۲. Cyber Capability Defense Model and Taxonomy
۳. TRADOC

است که به مدل مرجع «سیستم توسعهٔ یکپارچه توانمندی‌ها» یا به‌اختصار به[1](DOTMPLF) مشهور هستند. بعداً مؤلفه‌های توانمندساز دیگری مانند سیاست‌ها و ... به آن‌ها اضافه گردید (مهدی‌نژاد نوری،۱۳۹۸).

هوشمندی

یکی از دلایل ضرورت به‌کارگیری هوشمندی در دفاع سایبری این است که مهاجمان سایبری در حال توسعه حملات مبتنی بر هوش مصنوعی هستند که سرعت، مقیاس، پیچیدگی، دفعات و گستردگی حملات آن‌ها را افزایش می‌دهد (Talwar and Koury,2017). استفاده از هوش مصنوعی باعث شده است حملات مهندسی اجتماعی خودکارتر و پیچیده‌تر شده و نفوذ شبکه، سرقت داده‌های شخصی و سطح ویروس‌های رایانه‌ای افزایش یابد (Yampolskiy, 2017). یکی از کاربردهای هوش مصنوعی در دفاع سایبری، سیستم‌های اطلاعاتی هستند که با پیشرفت تکنولوژی و اتصال گسترده به‌طور مداوم در حال به‌روزرسانی، اصلاح و گسترش بوده تا در خدمت کاربران جدید و عملکردهای جدید تجاری باشند. ابزارهای هوش مصنوعی شامل منطق فازی[2]، سیستم‌های عامل هوشمند[3]، الگوریتم‌های ژنتیک و AIS در حل مشکلات پیچیده امنیت سایبری، تصمیم‌گیری، نظارت بر تهدیدات سایبری و شناسایی، پیشگیری و همچنین پیش‌بینی تهدیدات سایبری کلیدی بوده‌اند.

استفاده از هوش مصنوعی در دفاع سایبری به سازمان کمک می‌کند تا تهدیدات سایبری را در زمان واقعی و با دقت بسیار زیاد در مراحل اولیه حمله کشف و شناسایی کنند؛ علاوه براین، یک فناوری را در اختیار سازمان قرار می‌دهد که خودسازماندهی، تاب‌آوری، سازگاری و پویایی و توانایی یادگیری رفتارهای جدید، تهدیدات و روندهای سایبری را دارد.

هوشمندی در فضای سایبری

درحالی‌که انفجار اطلاعاتی با در دسترس‌بودن مجموعه‌های داده بزرگ و اتوماسیون برای کمک به انسان‌ها برای درک بهتر داده‌ها سروکار دارد، تقویت هوش به‌معنای افزایش هوش انسان

---

۱. Doctrine, Organization, Training, Materiel, Logistic, Personal, Facility
۲. Fuzzy Logic
۳. Intelligent Agent Systems

در اثر انفجار اطلاعات است؛ بنابراین انفجار اطلاعات منجر به تقویت هوش می‌شود. شاید بتوان گفت که ازآنجاکه فضای سایبری مفاهیم هوش مصنوعی، تقویت اطلاعات، اینترنت و دیجیتال گایا را پشتیبانی می‌کند، فضای سایبری نیز ممکن است یکی از حوزه‌هایی باشد که می‌تواند به زودی شاهد تکینگی (خودمختاری)[1] فناوری باشد (Vinge,2008).

از آنجا که هوشمندی مستقیماً با اطلاعات متناسب است (Soomro et al.2018)؛ اگر در شناسایی سیستم‌هایی که رفتار هوشمندانه در فضای سایبری از خود نشان می‌دهند موفق باشیم، ممکن است استنباط کنیم که تکینگی سایبری از طریق ویژگی‌های زیر امکان‌پذیر است.

(۱)- سیستم‌های خودآگاه- سیستم‌های سایبری-فیزیکی قادر به استخراج اطلاعات آگاهی و پردازش آن‌ها در دنیای سایبر هستند، درنتیجه خودآگاهی را در سیستم‌های سایبری فیزیکی که در فضای سایبری عملیاتی هستند، وارد می‌کنند (گورگن و همکاران، ۲۰۱۳)؛

(۲)- خودسازنده: جوامع هوش مصنوعی و یادگیری ماشینی مدت طولانی است که به فکر سیستم‌های خودسازنده هستند (Rowe، ۲۰۰۲). سیستم‌های فیزیکی سایبر خودسازنده و سیستم-های طبقه‌بندی خودسازنده (Soykan، ۲۰۱۱) وجود نهادهای هوشمند را در فضای سایبری تأیید می‌کنند؛

(۳) خودکنترلی: شناسایی ویژگی‌های مشترک هسته اصلی و استراتژی‌های مداخله‌ای که توسط ابزارهایی برای خود کنترلی دیجیتال ترویج می‌شوند، اساس سازوکار کنترل خود در فضای سایبری است؛ علاوه بر این، روند عملیاتی فرماندهی و کنترل در سیستم‌های فیزیکی سایبری شبکه‌های فیزیکی را به فضای سایبری متصل می‌کند (Z. Liu et al.، ۲۰۱۱)؛

(۴) خود بازیابی – ازآنجاکه فضای سایبری با امنیت سایبری سروکار دارد، حملات سایبری بسیار مکرر است. حملات سایبری ممکن است منجر به خرابکاری سامانه شود، به همین دلیل بازیابی سامانه ضروری است. دستگاه‌های خودترمیمی در فضای سایبری مجهز به مکانیسم محافظتی و انعطاف‌پذیری سایبری برای مقابله مستقل با حملات سایبری هستند. در گذشته

[1] singingularity

چارچوب‌های خودترمیمی نیز برای مقابله با حملات سایبری معرفی شده است (Seiger et al.، ۲۰۱۹)؛

(۵) خودآموزی- هوش مصنوعی آموزش و یادگیری را برای سیستم‌ها آسان می‌کند. یادگیری تقویت عمیق ربات‌های خودآموز را با موفقیت وارد فضای سایبری کرده است (آنانتو، ۲۰۱۷)؛ علاوه بر این سیستم‌های کنترل خودآموزی به دلیل شبکه‌های عصبی به وجود آمده‌اند (Nguyen and Widrow,1990a,)؛

(۶) خودسازماندهی- خودسازماندهی برای ارتقاء هماهنگی ضروری است؛ این نشان‌دهنده خود سازگاری است که منجر به تنظیم مجدد و پاسخ‌گویی بهتر می‌شود. فضای سایبری چندین سامانه خودسازماندهی شده را به‌صورت خودسازماندهی سیستم‌های فیزیکی سایبری در خود جای داده است (Heck et al.، ۲۰۱۶، Zhang et al.، ۲۰۱۶).

آگاهی وضعیتی سایبری

دفاع سایبری حوزه‌ای است که در آن یک یا چند تحلیل‌گر بر فضای سایبری نظارت دارند تا از آن‌ها در برابر استفاده غیر مجاز دفاع کنند. عدم آگاهی وضعیتی سایبری زمینه‌ساز از دست دادن اطلاعات محرمانه، سرقت پهنای باند و یا محرومیت از خدمات می‌شود. برای دفاع بهتر در فضای سایبری، مدافع سایبری ابتدا باید از وضعیت شبکه‌های سایبری خود آگاهی داشته باشد. همان‌گونه که اندسلی، آگاهی وضعیتی را شامل درک مؤلفه‌های محیط، فهم معنای آن‌ها و تجسم وضعیت آن‌ها در آینده نزدیک می‌داند، آگاهی وضعیتی، آگاهی از آنچه است که در فضای سایبری رخ می‌دهد و یک فرایند شناختی است که می‌تواند شرایط حال حاضر را درک کند و پس از فهم معنای آن‌ها، تصمیم‌گیری کند؛ بنابراین آگاهی وضعیتی به تصمیم‌ساز برای درک وضعیت به‌منظور تصمیم‌گیری درست کمک می‌کند (رشیدی و دیگران، ۱۳۹۳).

دفاع هوشمند سایبری

در شبکه اطلاعات جهانی آینده، سیستم‌های پیچیده به‌هم پیوسته، وسایل نقلیه دفاعی ایزوله شده، سنسورها و عوامل مؤثر و زیرساخت‌ها و سیستم‌هایی که میزان خرابی بسیار پایینی را می‌طلبند وجود دارند که اپراتورهای امنیت انسانی نمی‌توانند به راحتی به آن‌ها دسترسی داشته

باشند و نمی‌توانند واکنش‌های کافی و سریع به حملات سایبر داشته باشند؛ بنابراین در برابر این حملات، به یک دفاع سایبری فعال، خودمختار و هوشمند نیاز دارند (ترون و همکاران، ۲۰۱۸). اعتماد امروز ما به مدافعان سایبری انسانی در آینده قابل دفاع نخواهد بود. دلایل آن شامل موارد زیر هست:

تعداد زیاد عوامل خودی، پیچیدگی و تنوع شبکه‌ها (اشخاص و رویدادها)، سرعت و حجم بالای نبرد رباتیک، مشکلات دفاع متمرکز در یک محیط رقابتی ارتباطاتی و کمبود نسبی سربازان انسانی در عملیات پراکنده و بار شناختی زیادی که به دلیل فعالیت‌هایی غیر از دفاع سایبری بر آن‌ها تحمیل شده است (همان).

بنابراین می‌توان گفت دفاع هوشمند سایبری عبارت است از مجموعه اقدامات و تدابیر هدفمند، خودمختار و یادگیرنده مبتنی بر سنجش و آگاهی وضعیتی سایبری (درک، فهم، پیش-بینی) به‌منظور تصمیم‌گیری مناسب در جهت دفع مؤثر کلیه تهدیدات پیشرفته و مداوم در فضای سایبر (تکمیل شده در گروه مطالعات گروهی داعا).

ترون و همکاران معماری مرجع عامل دفاع سایبری هوشمند خودمختار(AICA[۱]) را ارائه داده‌اند که شامل پنج عملکرد اصلی؛ سنجش و شناسایی حالت محیطی؛ برنامه‌ریزی و انتخاب اقدام؛ تعاملات و ارتباطات؛ اجرای اقدام و یادگیری و بهبود دانش است (ترون و همکاران، ۲۰۲۰).

۲- روش‌شناسی تحقیق

روش تحقیق: روش تحقیق به‌کار گرفته شده در این پژوهش از نظر هدف کاربردی و از نظر اجراء روش آمیخته (کیفی و کمی) است. در بخش کیفی ابتدا با مراجعه به بیانات ارزشمند مقام معظم رهبری، اسناد بالادستی، مطالعات تطبیقی و خبرگان، ابعاد، مؤلفه‌ها و شاخص‌های الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی کشور استخراج و پرسشنامه طراحی گردید و در

۱. Autonomous Intelligent Cyber defense Agents

بخش کمی پس از انجام مراحل روایی و پایایی با مراجعه به جامعه آماری اقدام به نمونه‌گیری گردید و با به‌کارگیری روش‌های کمی نتایج نمونه‌گیری مورد تجزیه و تحلیل قرار گرفت.

جامعه آماری: تحقیق حاضر دارای دو جامعه آماری اسنادی و میدانی (پیمایشی) است. جامعه اسنادی که ادبیات پژوهش را تشکیل می‌دهد؛ عبارت است از کلیه اسناد بالادستی (سند چشم‌انداز ۱۴۰۴، تدابیر و رهنمودهای امامین انقلاب اسلامی، آئین‌نامه‌ها و دستورالعمل‌های ابلاغی) و کتب و مقالات علمی مرتبط با موضوع پژوهش که از اعتبار ملی و بین‌المللی برخوردار هستند.

جامعه میدانی (پیمایشی) شامل مشاهدات، پنل خبرگی و پرسشنامه‌ها است. خبرگان شامل مدیران و کارشناسان آشنا با مفاهیم دفاع هوشمند سایبری و زیرساخت‌های حیاتی می‌باشند که دارای حداقل ۵ سال سابقه مفید در حوزه پژوهش و مسئولیت در سطوح میانی یا عالی نظام هستند. برجستگان منتخب از این جامعه، جامعه آماری مصاحبه عمیق و پنل نخبگی را تشکیل می‌دهند که شامل مدیران راهبردی و کارشناسان خبره و متخصصان آشنا به دفاع سایبری می‌باشد و ویژگی مشترک آن‌ها تخصص و سابقه مفید و قابل توجه در سطح راهبردی و ملی است.

ابزارها و روش‌های جمع‌آوری داده‌ها: برای روش اسنادی (کتابخانه‌ای) از فیش‌برداری کلیه کتاب‌ها و مقالات علمی و اسناد و مدارک سازمان‌های رسمی و سایت‌های معتبر اینترنتی استفاده شده است. برای گردآوری داده‌های کمی از روش میدانی با تشکیل پنل‌های خبرگی و تهیه و توزیع پرسش‌نامه بین صاحب‌نظران (خبرگان) دفاع سایبری و زیرساخت‌های حیاتی استفاده شده است.

در تجزیه و تحلیل داده‌های کمی با بهره‌گیری از نرم‌افزار اسمارت‌پی.ال.اس از روش حداقل مربعات جزئی استفاده شده است. تأیید روایی پرسشنامه توسط نخبگان و خبرگان صاحب‌نظر و برای پایایی، مقدار الفای کرونباخ برای سؤالات پرسشنامه به‌صورت میانگین بدست آمده و تأیید شد.

۳- تجزیه و تحلیل یافته‌های تحقیق

تحلیل کیفی: در ابتدا با مطالعات کتابخانه‌ای به بررسی ابعاد، مؤلفه‌ها و عناصر اصلی تشکیل‌دهنده الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی پرداخته شد. به این منظور ابتدا مقالات مرتبط با دفاع هوشمند، دفاع سایبری و دفاع سایبری از زیرساخت‌های حیاتی در ایران و کشورهای پیشرو در جهان و مفاهیم مرتبط با آن مورد مطالعه و بررسی قرار گرفت و در جلسات مختلف با حضور گروه محققین روی نکات مهّم هر مقاله مباحثی مطرح گردید.

با توجه به توانایی و تأثیر مثبت رویکرد کیفی در شناسایی ابعاد، مؤلفه‌ها و شاخص‌های مربوط به تحقیق، به هر یک از اعضای تیم تحقیق مأموریت داده شد با توجه به مطالعات صورت گرفته بر روی مقالات و رساله‌های مختلف از منابع داخلی و خارجی و ادبیات تحقیق، شاخص-های اثرگذار بر روی دفاع هوشمند سایبری از زیرساخت‌های حیاتی را استخراج و ارائه نمایند. در طی چند جلسه خبرگی با حضور تیم راهنما و تیم تحقیق، شاخص‌های استخراج شده مورد بررسی قرار گرفت و نکات اشتراک و افتراق بین شاخص‌های استخراجی، مورد بررسی و تجزیه و تحلیل قرار گرفت و در نهایت حدود ۵۰ شاخص مهم و اثرگذار بر موضوع مورد مطالعه شناسایی گردید. شاخص‌های شناسایی شده بایستی کدگذاری و با توجه به نزدیکی و جنس شاخص‌ها در چندمحور دسته‌بندی می‌شدند که این اقدام نیز در جلسات خبرگی و به‌صورت گروهی مورد بحث و بررسی قرار گرفت. شاخص‌های کدگذاری شده، در چندمحور دسته‌بندی و مؤلفه‌های تحقیق با جلسات خبرگی تعیین و این مؤلفه‌ها نیز در چند بعد دسته‌بندی شدند و مدل اولیه تحقیق از ادبیات تحقیق و جلسات خبرگی و به روش طوفان فکری استخراج گردید.

بعد از مشخص شدن چهارچوب مدل تحقیق و با نظر اساتید محترم‌محور و مشاور با ارسال ادبیات تحقیق و همچنین مدل طراحی شده برای چند تن از خبرگان مرتبط با دفاع هوشمند سایبری، از تعدادی از خبرگان دعوت به‌عمل آمد تا با حضور در جمع گروه تحقیق نظرات تخصصی خود را در خصوص مدل طراحی شده اعلام نمایند. در دو جلسه خبرگی که با حضور اساتید محترم مدعو و تیم راهنما و گروه تحقیق برگزار گردید در ابتدا روند چگونگی استخراج

شاخص‌ها، مؤلفه‌ها و ابعاد دفاع هوشمند سایبری از زیرساخت‌های حیاتی توسط تیم تحقیق ارائه گردید و سپس هر یک از اساتید محترم نظرات تخصصی خود را در خصوص مدل طراحی شده و ادامه روند تحقیق مطرح نمودند. با توجه به مباحث مطرح شده در جلسات خبرگی با حضور اساتید محترم مدعو، در نهایت شاخص‌های استخراج شده در ۱۰ محور شامل مؤلفه‌های دفاع مشارکتی (شامل ۳ شاخص طرح‌ریزی مشترک، اشتراک‌گذاری منابع و اقدام مشترک)، دفاع غیرعامل (شامل ۴ شاخص محافظت، کشف و شناسایی، پاسخ و بازیابی)، دفاع عامل (شامل ۵ شاخص کشف و شناسایی، خنثی‌سازی، کاهش اثر، اختلال و تخریب یا انهدام)، آگاهی وضعیتی (شامل ۳ شاخص درک محیطی، فهم محیطی و تجسم وضعیت)، مؤلفه‌های خط‌مشی‌گذاری (شامل ۵ شاخص تدوین دکترین و سیاست و اهداف، شناسایی و ارزیابی عوامل داخلی و خارجی، نگاشت نهادی، تدوین برنامه اقدام و نظارت، ارزیابی و بازنگری)، فرماندهی و کنترل (شامل ۴ شاخص رصد و پایش محیط، تحلیل و ارزیابی اطلاعات، تصمیم‌گیری و اقدام) و دیپلماسی (شامل ۳ شاخص مشارکت فعال در مجامع بین المللی مرتبط، همکاری و ائتلاف منطقه‌ای و بین‌المللی و دفاع حقوقی در فضای سایبری)، مؤلفه‌های فرایندها (شامل ۴ شاخص طرح‌ریزی، برقراری ارتباط، فعال‌سازی و ارزیابی)، قوانین و مقررات (شامل ۳ شاخص جامع و مانع، هم راستا با قوانین داخلی و بین‌المللی و پویا و روزآمدی) و ارتباطات و تعاملات (شامل ۴ شاخص معماری مناسب، افزونگی، استفاده از ظرفیت همه ذی‌نفعان و انعطاف‌پذیری) دسته‌بندی گردیدند. در ادامه به چگونگی دسته‌بندی این ۱۰ مؤلفه و تعیین ابعاد موضوع تحقیق پرداخته شده و پیشنهادات مختلفی از جمله دسته‌بندی در سه، چهار و حتی پنج بعد مطرح شد که پس از بحث‌های کارشناسی و خبرگی تصمیم به دسته‌بندی ۱۰ مؤلفه اشاره شده در سه دسته کلی حکمرانی، ساختار و عملیات سایبری گرفته شد.

تحلیلی کمی: برای تجزیه وتحلیل اطلاعات حاصل از دریافت پرسشنامه‌ها در این تحقیق از روش «مدل‌سازی معادلات ساختاری»[1] با رویکرد حداقل مربعات جزئی استفاده شده است. برای این منظور اطلاعات گردآوری شده از طریق پرسشنامه‌های تکمیل شده در نرم‌افزار

[1] Structural Equation Modeling

اس‌پی‌اس‌اس[1] درج و پس از آن جهت تحلیل‌های لازم در نرم‌افزار اسمارت پی.ال.اس[2] بارگذاری گردید. سپس کلیه عوامل، اجزاء، ویژگی‌ها و الزامات ارائه الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی جمهوری اسلامی ایران به‌صورت انعکاسی[3] در محیط نرم‌افزار درج و در ادامه، اطلاعات گردآوری شده به آن تخصیص داده شد. آزمون مدل با اجرای سه مرحله و بررسی شاخص‌های آن صورت گرفت که عبارتند از:

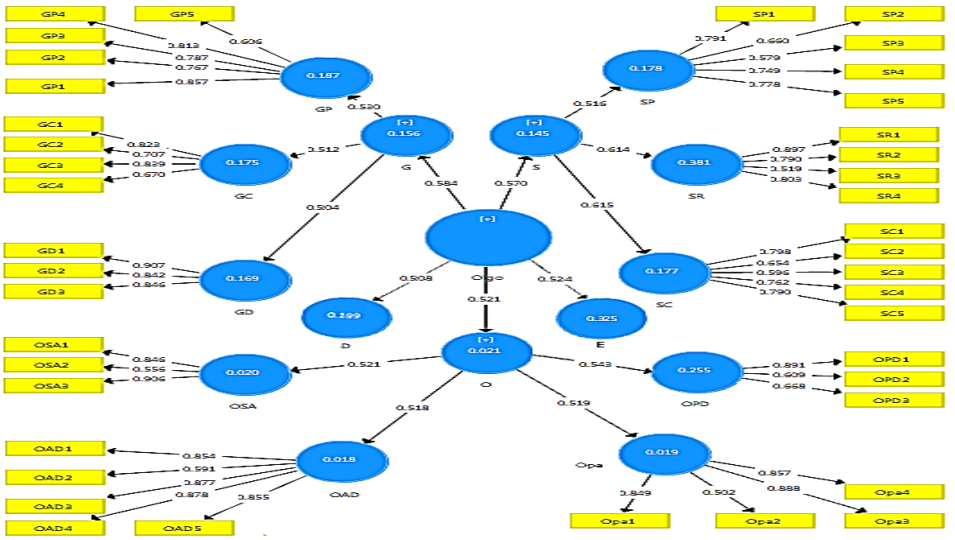
۱. ارزیابی مدل اندازه‌گیری (مدل بیرونی)؛
۲. ارزیابی مدل ساختاری (مدل درونی)؛
۳. ارزیابی مدل کلی انجام شده

برازش اندازه‌گیری الگو از طریق سنجش پایایی (آلفای کرونباخ، پایایی ترکیبی و بارهای عاملی) و روایی (روایی واگر و روایی همگرا) مورد ارزیابی قرار گرفت که از وضعیت مناسبی برخوردار بود.

الف- بارعاملی ابعاد، مؤلفه‌ها و شاخص‌های تحقیق

هریک از اعدادی که بر فلش‌های رسم شده از متغیرهای پنهان (متغیرهای آبی رنگ) به متغیرهای آشکار (متغیرهای زرد رنگ) بدست آمده؛ نشانگر **بارهای عاملی** می‌باشد. بارهای عاملی از طریق محاسبه مقدار همبستگی شاخص‌های یک سازه با آن سازه محاسبه می‌شوند که اگر این مقدار برابر و یا بیشتر از مقدار ۰/۴ شود، مؤید این مطلب است که واریانس بین سازه و شاخص‌های آن از واریانس خطای اندازه‌گیری آن سازه بیشتر بوده و پایایی در مورد آن مدل اندازه‌گیری قابل قبول است.

۱. Statistical Package for the Social Sciences
۲. Smart PLS
۳. Reflective



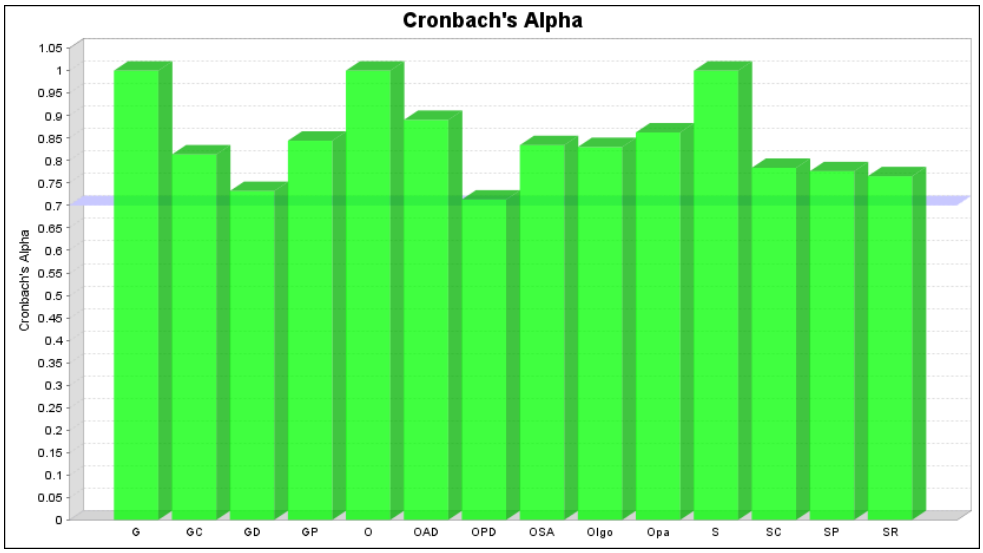
شکل (۱) ضرایب بارعاملی الگوی تحقیق

شکل(۱) بارعاملی ابعاد، مؤلفه و شاخص‌های الگوی نهایی را در یک نگاه نشان می‌دهد. همان‌گونه که در شکل دیده می‌شود همه ابعاد، مؤلفه‌ها و شاخص‌ها دارای بار عاملی بالای ۰/۴ می‌باشند؛ که این مؤید این مطلب است که واریانس بین سازه و شاخص‌های آن از واریانس خطای اندازه‌گیری آن سازه بیشتر بوده و پایایی در مورد این مدل اندازه‌گیری قابل قبول است.

ب- آلفای کرونباخ و پایایی ترکیبی

آلفای کرونباخ شاخص سنتی برای بررسی پایایی یا پایداری درونی[1] بین متغیرهای مشاهده‌پذیر در مدل اندازه‌گیری است. پایداری درونی نشانگر میزان همبستگی بین یک سازه و شاخص‌های مربوط به آن است. مقدار آلفای کرونباخ بالاتر از ۰/۷ نشانگر پایایی قابل قبول است. آلفای کرونباخ و پایایی ترکیبی ابعاد، مؤلفه‌ها، شاخص‌ها و گویه‌های الگو با استفاده از نرم‌افزار اسمارت پی.ال.اس محاسبه و در نمودارها زیر آمده است.

۱. Internal Consistency

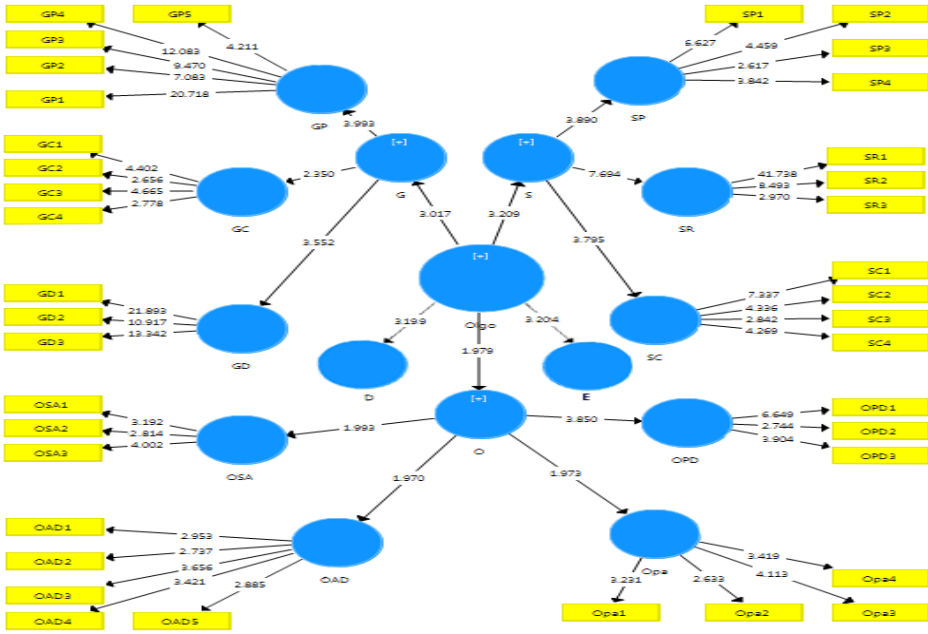


نمودار (۱) مؤلفه‌ها، شاخص‌ها و گویه‌های الگو محاسبه شده با استفاده از نرم افزار Smart PLS

با توجه به اعداد نمودار فوق ضریب آلفای کرونباخ و مقدار پایایی ترکیبی کلیه ابعاد، مؤلفه بالاتر از ۰/۷ بوده که نشان‌دهنده پایایی مناسب ابعاد و مؤلفه‌های الگو است.

برازش ساختاری الگو از طریق محاسبه ضرایب معناداری z (مقادیر t-values) و معیار R۲ (ضریب تعیین) مورد ارزیابی قرار گرفت که از وضعیت مناسبی برخوردار بود.

یکی از شاخص‌های تأیید روابط در مدل ساختاری معنادار بودن ضرایب مسیر است. منظور از ضرایب مسیر همان بتای استانداردشده در رگرسیون خطی می‌باشد. ضرایب مسیر باید از لحاظ بزرگی، علامت و معناداری مورد بررسی قرار بگیرند. ضریب معناداری یا همان مقادیر t-values باید از ۱/۹۶ بیشتر باشد تا بتوان در سطح اطمینان ۹۵ درصد معنادار بودن آن را تأیید نمود.

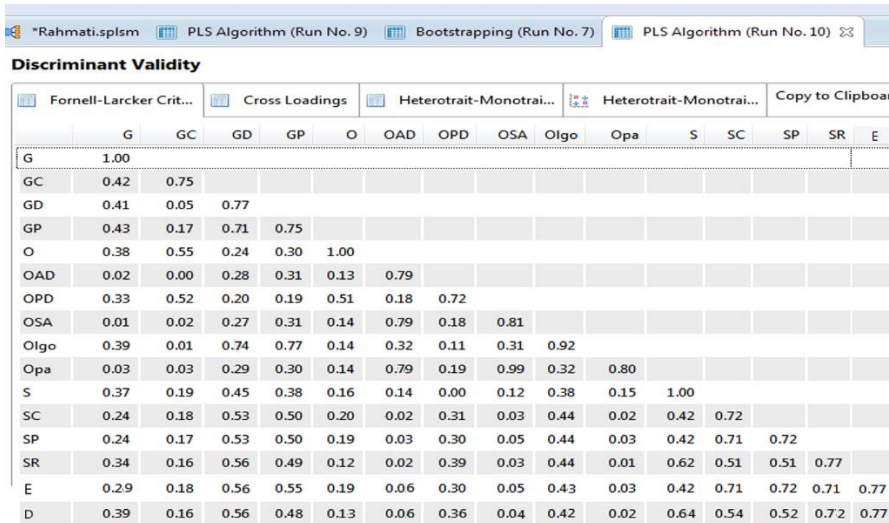


شکل (۲) ضرایب تعیین مسیر الگوی تحقیق

همان‌طور که در شکل (۲) ملاحظه می‌شود ضرایب کلیه مسیرها از ۱/۹۶ بیشتر بوده، فلذا ساختار ابعاد، مؤلفه‌ها و شاخص‌ها و روابط بین متغیرهای الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی جمهوری اسلامی ایران در سطح اطمینان بالای ۹۵ درصد مورد تأیید است.

به منظور بررسی ارتباط بین ابعاد با یکدیگر و یا ارتباط بین هر یک از ابعاد با مؤلفه‌ها و شاخص‌های سایر ابعاد، باید به مقادیر جدول «روایی واگرای ابعاد الگوی تحقیق» که در جدول (۱) آماده است؛ توجه کنیم این مقادیر به مقایسه میزان همبستگی یک‌سازه با شاخص‌هایش در مقابل همبستگی آن سازه با سایر سازه‌ها اشاره دارد که اگر مقادیر جدول فوق از مقادیر قطر اصلی مثلث پایین‌تر باشد نشان‌دهنده این موضوع خواهد بود که روابط بین ابعاد و مؤلفه‌ها و شاخص‌های الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی درست تعریف شده است و جدول زیر این موضوع را تأیید می‌کند.

جدول (۱) روایی واگرای ابعاد الگوی تحقیق



*Rahmati.splsm | PLS Algorithm (Run No. 9) | Bootstrapping (Run No. 7) | PLS Algorithm (Run No. 10)

Discriminant Validity

Fornell-Larcker Crit... | Cross Loadings | Heterotrait-Monotrai... | Heterotrait-Monotrai... | Copy to Clipboard

	G	GC	GD	GP	O	OAD	OPD	OSA	Olgo	Opa	S	SC	SP	SR	E	D
G	1.00															
GC	0.42	0.75														
GD	0.41	0.05	0.77													
GP	0.43	0.17	0.71	0.75												
O	0.38	0.55	0.24	0.30	1.00											
OAD	0.02	0.00	0.28	0.31	0.13	0.79										
OPD	0.33	0.52	0.20	0.19	0.51	0.18	0.72									
OSA	0.01	0.02	0.27	0.31	0.14	0.79	0.18	0.81								
Olgo	0.39	0.01	0.74	0.77	0.14	0.32	0.11	0.31	0.92							
Opa	0.03	0.03	0.29	0.30	0.14	0.79	0.19	0.99	0.32	0.80						
S	0.37	0.19	0.45	0.38	0.16	0.14	0.00	0.12	0.38	0.15	1.00					
SC	0.24	0.18	0.53	0.50	0.20	0.02	0.31	0.03	0.44	0.02	0.42	0.72				
SP	0.24	0.17	0.53	0.50	0.19	0.03	0.30	0.05	0.44	0.03	0.42	0.71	0.72			
SR	0.34	0.16	0.56	0.49	0.12	0.02	0.39	0.03	0.44	0.01	0.62	0.51	0.51	0.77		
E	0.29	0.18	0.56	0.55	0.19	0.06	0.30	0.05	0.43	0.03	0.42	0.71	0.72	0.71	0.77	
D	0.39	0.16	0.56	0.48	0.13	0.06	0.36	0.04	0.42	0.02	0.64	0.54	0.52	0.72	0.77	0.74

برازش مدل کلی

معیار GoF[۱] : این معیار برای برازش مدل کلی که هر دو بخش مدل اندازه‌گیری و ساختاری را کنترل می‌کند، به‌کار برده می‌شود. مقدار معیار از رابطه زیر محاسبه می‌شود که در آن $\overline{communalities}$ مقادیر اشتراکی یک سازه درون‌زا و $\overline{R^2}$ میانگین متغیرهای درون‌زای وابسته است.

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

برای محاسبه $\overline{R^2}$ یا همان میانگین R^2، مقادیر R^2 مربوط به تمامی متغیرهای پنهان درون‌زای مدل اعم از مرتبه اول، دوم و سوم به تعداد متغیر مدنظر قرار گرفته و مقادیر میانگین آن‌ها محاسبه گردید. برای مدل این پژوهش، میانگین R^2 برابر با ۰/۳۳۵ حاصل شد. در جدول زیر مقادیر Communality پس از اجرای فرمان PLS Algorithm آمده است. محاسبه میانگین این مقادیر برای تحصیل مقدار GoF ضرورت دارد.

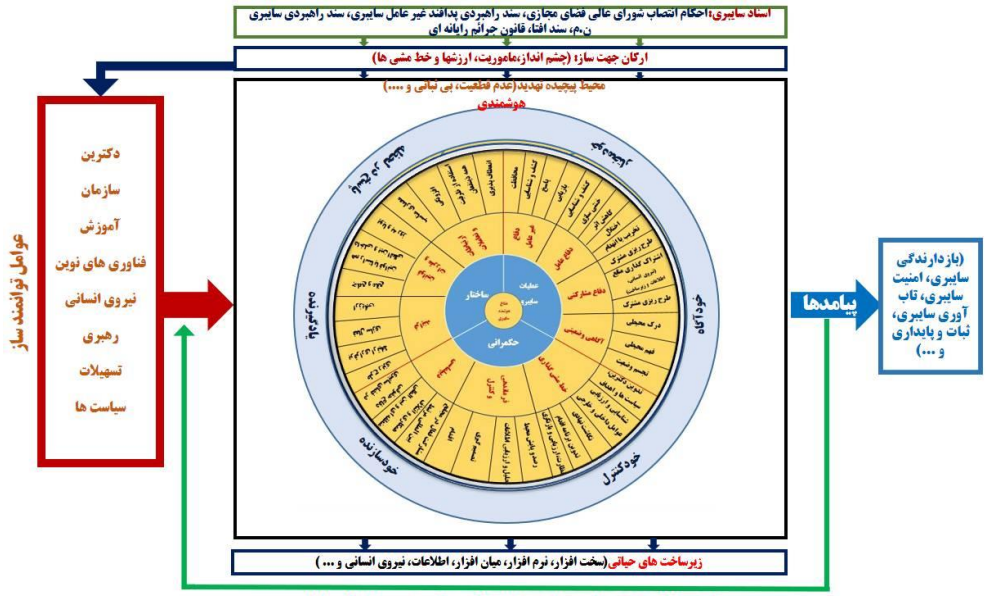
$$GoF = \sqrt{0.577 \times 0.335} = 0.439$$

۱) Goodness of Fit

با جای‌گذاری مقادیر در فرمول، مقدار GoF معادل 0.439 گردید؛ و چون بزرگتر از ۰,۳۶ بود، برازش کلی الگو قوی ارزیابی شد. در نهایت نیز بر اساس یافته‌ها، الگوی نهایی ترسیم گردید.

۴- نتایج و پیشنهادها

بررسی‌های انجام‌شده در این تحقیق نشان می‌دهد سه بعد الگوی دفاع هوشمند سایبری از زیرساخت‌های حیاتی جمهوری اسلامی ایران احصاء شده که (عملیات سایبری، حکمرانی و ساختار) به‌صورت مکمل بر الگو تأثیرگذار می‌باشند؛ ولی میزان تأثیرگذاری آن‌ها از نگاه جامعه آماری متفاوت است.



الگوی دفاع هوشمندسایبری از زیرساخت های حیاتی جمهوری اسلامی ایران

جامعه آماری این اعتقاد را داشتند که بعد حکمرانی از دو بعد دیگری بر دفاع هوشمند سایبری از زیرساخت‌های حیاتی کشور اثرگذارتر است. تجزیه و تحلیل داده نشان می‌دهد که بین بعد حکمرانی با الگوی دفاع هوشمند سایبری یک همبستگی مستقیم، مثبت و بالایی وجود دارد؛ یعنی به میزانی که بعد حکمرانی سایبری تقویت شود به‌طور نسبی به همان نسبت وزن دفاع هوشمند سایبری از زیرساخت‌های حیاتی کشور ارتقاء خواهد یافت؛ درواقع می‌توان گفت که این بعد نشان می‌دهد؛ به میزان بهره‌گیری از شاخص‌های حکمرانی سایبری مانند

خط‌مشی‌گذاری، فرماندهی و کنترل هوشمند سایبری و دیپلماسی سایبری به تقویت دفاع هوشمند سایبری از زیرساخت‌های حیاتی جمهوری اسلامی ایران کمک می‌شود.

یافته‌های این تحقیق دلالت بر این امر دارد که هر کدام از مؤلفه‌های خط‌مشی‌گذاری، فرماندهی و کنترل هوشمند سایبری و دیپلماسی سایبری بعد حکمرانی متناسب با شاخص‌های احصاء شده آن‌ها باید به‌طور مستمر مورد بهره‌گیری قرار گیرند تا چرخه تقویت دفاع هوشمند سایبری ادامه داشته باشد. قطعاً عدم توجه به شاخص‌های مؤلفه‌های بعد حکمرانی، باعث تضعیف دفاع هوشمند سایبری شده و این تضعیف نیز بر کاهش توانایی حفاظت از زیرساخت‌های حیاتی ج.ا.ایران مؤثر است. میزان بهره‌گیری از این شاخص‌ها، وزن حکمرانی سایبری را نشان می‌دهد و این وزن یکی از سه بعد دفاع هوشمند سایبری ج.ا.ایران، احصاء شده در این تحقیق است. پس می‌توان گفت؛ به میزان افزایش بهره‌گیری از این شاخص‌ها توانایی دفاع هوشمند سایبری افزایش‌یافته و برعکس به میزان کاهش بهره‌گیری از آن‌ها این توانایی کاهش خواهد یافت.

جامعه آماری دومین بعد تأثیرگذار بر دفاع هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران را بعد ساختار می‌داند. از دید جامعه آماری این بعد با سه مؤلفه (فرایندها، قوانین و مقررات و ارتباطات و تعاملات) و ۱۱ شاخص با الگو دفاع هوشمند سایبری از زیرساخت‌های حیاتی کشور همبستگی دارد؛ یعنی دارای یک همبستگی بسیار بالا، مستقیم و مثبتی با الگوی تحقیق است. نکته میزان بهره‌گیری از شاخص‌های سه مؤلفه این بعد است؛ که به میزان افزایش بهره‌گیری از شاخص‌های مؤلفه‌ها، میزان نقش‌آفرینی ساختار در دفاع هوشمند سایبری افزایش خواهد یافت و این ارتقاء نیز بر تقویت توانایی دفاع هوشمند سایبری از زیرساخت‌های حیاتی مؤثر است؛ البته در صورت کاهش میزان بهره‌گیری از شاخص‌ها برعکس مورد اشاره شده عمل خواهد شد.

سومین بعد تأثیرگذار از دید جامعه آماری بر دفاع هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران، بعد عملیات سایبری هوشمند می‌باشد؛ این بعد با چهار مؤلفه و ۱۵ شاخص در رتبه سوم این الگو قرار گرفته است؛ البته میزان همبستگی این بعد با دفاع هوشمند سایبری از

زیرساخت‌های حیاتی ج.ا.ایران همبستگی بسیار مطلوب، مثبت و مستقیمی دارد. مهم میزان بهره-گیری از شاخص‌های چهار مؤلفه این بعد است؛ که به میزان افزایش بهره‌گیری از شاخص‌های مؤلفه‌ها، میزان نقش‌آفرینی عملیات سایبری در دفاع هوشمند سایبری افزایش خواهد یافت و این ارتقاء نیز بر تقویت توانایی دفاع هوشمند سایبری از زیرساخت‌های حیاتی مؤثر است؛ البته در صورت کاهش میزان بهره‌گیری از شاخص‌ها برعکس مورد اشاره شده عمل خواهد شد.

در الگوی ارائه شده در ورودی الگو عوامل توانمندساز (دکترین، سازمان، آموزش، فناوری‌های نوین، نیروی انسانی، رهبری، تسهیلات و سیاست‌ها) قرار گرفته است. بر اساس نتایج تحقیق این عوامل اثر مطلوب، مثبت و مستقیمی بر دفاع هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران دارند به این مضمون که هر چقدر بر عوامل توانمندساز پرداخته شود، می‌تواند بر تقویت دفاع هوشمند سایبری کمک نماید. به‌عنوان مثل تدوین دکترین دفاع هوشمند سایبری می‌تواند، یک عامل اثرگذار مثبت بر تقویت دفاع هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران باشد. یا ایجاد ساختارهای مناسب و بهره‌برداری از فناوری‌های نوین مثل هوش مصنوعی و کلان داده‌ها می‌توانند به‌عنوان عوامل توانمندساز در ارتقای توانایی دفاع هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران بسیار مؤثر باشند.

در الگوی ارائه شده به اسناد بالادستی (احکام انتصاب شورای عالی فضای مجازی، سند راهبردی پدافند غیرعامل سایبری، سند راهبردی سایبری ن.م، سند افتا، قانون جرایم رایانه‌ای) نیز توجه خاص شده است و از صاحب‌نظران در خصوص میزان اثر این عوامل بر موضوع مورد مطالعه سؤال شده است. بر اساس نتایج تحقیق توجه و به‌کارگیری این اسناد اثر مطلوب، مثبت و مستقیمی بر دفاع هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران دارند. به‌عنوان‌مثال پیاده‌سازی و اجرایی شدن سند راهبردی پدافند غیرعامل سایبری می‌تواند باعث ارتقای پدافندغیرعامل سایبری زیرساخت‌های حیاتی کشور گردد که این خود به‌عنوان یکی از مؤلفه‌های اثرگذار بر موضوع مورد مطالعه می‌باشد.

مهّم‌ترین بخش در الگوی ارائه شده، بخش هوشمندی با ویژگی‌های خودمختاری، خودآگاهی، خودکنترلی، خودسازمانده، یادگیرنده و پاسخ درلحظه می‌باشد. از مجموعه جلسات

خبرگی و مطالعات انجام شده در خصوص ویژگی دفاع هوشمند سایبری چنین استنباط می‌شود که شش ویژگی اشاره شده جزء ذات دفاع هوشمند سایبری بوده و این ویژگی‌ها قابل تفکیک از مفهوم دفاع هوشمند سایبری نمی‌باشند؛ یعنی به‌طور مثال دفاع هوشمندی سایبری که خودمختار نباشد و یا از تجربیات قبلی نتواند درس بیاموزد و یادگیرنده نباشد و یا نتواند در لحظه به هر تهدیدی پاسخ دهد نمی‌توان آن را دفاع هوشمند سایبری نامید؛ بنابراین این موضوع به‌صورت یک حلقه‌ای محاط بر کل ابعاد، مؤلفه‌ها و شاخص‌های احصاء شده در الگو آورده شده است و این به این مفهوم است که منظور از بعد عملیات سایبری در این الگو، عملیات سایبری هوشمند است که شش ویژگی اشاره شده را دارد و یا منظور از بعد حکمرانی و ساختار در این الگو، حکمرانی و ساختار هوشمند است که شش ویژگی هوشمندی را باید داشته باشند.

پیشنهادها

پیشنهادهای اجرایی

- پیاده‌سازی الگوی دفاع هوشمند سایبری در زیرساخت‌های حیاتی ج.ا.ایران؛
- ایجاد زیرساخت‌ها و شرایط لازم برای پیاده‌سازی فرماندهی و کنترل هوشمند سایبری زیرساخت‌های حیاتی ج.ا.ایران؛
- فعال‌سازی دیپلماسی سایبری به‌منظور مشارکت در تدوین قوانین بین‌المللی، منطقه‌ای و ملی در جهت حفاظت از زیرساخت‌های حیاتی؛
- اصلاح یا ایجاد فرایندهای مورد نیاز در جهت پیاده‌سازی دفاع هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران؛
- به‌کارگیری همه ظرفیت‌های داخلی و خارجی کشور در جهت دفاع هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران؛
- اجرای دفاع مشارکتی از زیرساخت‌های حیاتی ج.ا.ایران (طرح‌ریزی مشترک، اشتراک‌گذاری منابع و اقدام مشترک)؛

- سرمایه‌گذاری و توجه ویژه به موضوع دفاع غیرعامل هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران؛
- اجرای برنامه‌های دفاع عامل هوشمند سایبری زیرساخت‌های حیاتی ج.ا.ایران.

پیشنهاد پژوهشی

- تدوین دکترین، سیاست‌ها و اهداف دفاع هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران؛
- تدوین قوانین و مقررات مورد نیاز جهت پیاده‌سازی دفاع هوشمند سایبری از زیرساخت‌های حیاتی ج.ا.ایران؛
- طراحی معماری فرماندهی و کنترل هوشمند سایبری زیرساخت‌های حیاتی ج.ا.ایران؛
- تدوین الگوی دفاع مشارکتی زیرساخت‌های حیاتی ج.ا.ایران.

فهرست منابع و مآخذ

الف- منابع فارسی

- اسکندری، حمید (۱۳۹۳)، دانستنی‌های پدافند غیرعامل، دوره عمومی مدیران و کارکنان دستگاه اجرایی، تهران: بوستان حمید.
- آقایی، محسن؛ معینی، علی؛ عرب سرخی، ابوذر؛ محمدیان، ایوب؛ زارعی، علی‌اصغر (۱۳۹۸)، ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی، فصلنامه مطالعات امنیتی.
- تقی‌پور، رضا؛ اسماعیلی، علی (۱۳۹۷)، " طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران"، س هشتم، ش سی ام، زمستان ۱۳۹۷، فصلنامه امنیت ملی.
- حکم انتصاب اعضای شورای‌عالی فضای مجازی (۱۳۹۴)، قابل دسترسی در: https://farsi.khamenei.ir/message-content?id=30658.
- جبار رشیدی، علی؛ داداش تبار، کوروش؛ نظرپور، بهزاد ۴۷ (۱۳۹۷)،" آگاهی وضعیتی سایبری ": انتشارات دانشگاه مالک اشتر.
- جباررشیدی، علی؛ داداش‌تبار، کوروش؛ بایرام‌زاده، مهدیه (۱۳۹۳)،"چارچوبی برای مدل‌سازی آگاهی وضعیتی سایبری مبتنی بر ادغام اطلاعات"،هشتمین کنفرانس ملی فرماندهی و کنترل ایران**(C4I)**، تهران: قابل دسترسی در: https://civilica.com/doc/412530.
- حسن‌لو، خسرو (۱۳۹۷)، دفاع هوشمند (در نظام دفاعی جمهوری اسلامی ایران)، تهران: دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی.
- رامک، مهراب؛ محمدی، علی (۱۳۹۸)، "مقاله پژوهشی: ارائه مدل مفهومی همکاری‌های بین‌المللی با رویکرد تقویت دفاع سایبری کشور (بر اساس نظریه‌پردازی داده بنیان)"، س دهم، پاییز ۱۳۹۹، ش ۳۷، ۷-۴۲، فصلنامه علمی امنیت ملی.
- سازمان پدافند غیرعامل کشور (۱۳۸۸)، سند راهبردی پدافند غیرعامل کشور، ویراست دوم.
- سازمان پدافند غیرعامل کشور، قرارگاه پدافند سایبری (۱۴۰۰)، دستورالعمل عملیاتی پدافند سایبری زیرساخت‌های صنعتی کشور.
- سازمان پدافند غیرعامل کشور، قرارگاه پدافند سایبری (۱۳۹۸)، اقدامات امن‌سازی اضطراری زیرساخت های سایبری و وابسته به سایبر کشور.
- سازمان پدافند غیرعامل کشور، قرارگاه پدافند سایبری (۱۳۹۷)، طرح پاسخ اضطراری به تهدیدات سایبری در حوزه انرژیCERP .
- سازمان پدافند غیرعامل کشور، قرارگاه پدافند سایبری (۱۴۰۰)، دستورالعمل عملیات پیش‌گیرانه (اقدامات اساسی) در زمان هشدار.
- سازمان پدافند غیرعامل کشور، قرارگاه پدافند سایبری (۱۴۰۰)، نظام عملیاتی پدافند سایبری کشور.

- سازمان پدافند غیرعامل کشور، قرارگاه پدافند سایبری (۱۳۹۹)، سطح‌بندی زیرساخت‌های سایبری و وابسته به سایبر مبتنی بر متدولوژی CARVER+ Shock+Interdependency.
- سازمان پدافند غیرعامل کشور، قرارگاه پدافند سایبری (۱۳۹۱)، سند راهبردی پدافند غیرعامل جمهوری اسلامی ایران.
- قرارگاه پدافند سایبری کشور (۱۳۹۴)، اهداف کلان در افق چشم‌انداز قرارگاه پدافند سایبری کشور، ش ۱۲، نشریه پاپسا.
- کافی، سعید (۱۳۹۹)، شاخص های دفاعی–امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران مبتنی بر رویکردهای پدافند غیرعامل، مجله سیاست دفاعی، ش ۱۱۱.
- کافی، سعید (۱۳۹۲)، تدوین راهبردهای پدافند غیرعامل در فضای سایبری زیرساخت‌های حیاتی ج.ا.ا، رساله دکترا، دانشکده دفاع، دانشگاه و پژوهشگاه عالی دفاع ملی.
- لطفی مرزناکی، رحمان (۱۳۹۴)، دفاع هوشمند در اندیشه امام خامنه‌ای‌مدظله‌العالی. تهران: آوای سبحان.
- محمدعلی‌زاده، اکبر؛ باقری، حسین (۱۳۹۷)، دفاع هوشمند، مفهوم جدید در راهبرد امنیتی ناتو تا سال ۲۰۲۰، ش ۳۰، فصلنامه دانش راهبردی.
- مهدی‌نژاد نوری، محمد (۱۳۹۸)، مدیریت راهبردی فضای سایبر، جزوه درسی مقطع دکتری، دانشگاه عالی دفاع ملی.

ب- منابع لاتین

- Endsley,M.R,"Toward a theory of situation awareness in dynamic systems," Hum. Factors J. Hum. Factors Ergon. Soc., vol. 37, no. 1, pp. 32– 64, (۲۰۱۲).
- European Union,(2008), COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protec-tion.Accessed March 29 2016 available at: http://eurlex.europa.eu/ LexUriServ/ LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF
- Gurgen, L., Gunalp, O., Benazzouz, Y., & Gallissot, M. (2013, March). Self-aware cyber-physical systems and applications in smart buildings and cities. In 2013 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp.1149–۱۱۵۴).
- Heck, H., Kieselmann, O., & Wacker, A. (2016, September). Evaluating connection resilience for self-organizing cyber-Physical systems. In 2016 IEEE 10th international conference on Self-Adaptive and Self-Organizing Systems.(SASO) (pp. ۱۴۰–۱۴۱).
- Joint Chiefs of Staff. (2018). Cyberspace Operations. Joint Chiefs of Staff
- Kolini, F., & Janczewski, L. (2015). Cyber Defense Capability Model: A Foundation Taxonomy. CONF-IRM.
- Liu, Z., Yang, D. S., Wen, D., Zhang, W. M., & Mao, W. (2011). Cyber-physical-social systems for command and control. IEEE Intelligent Systems, 26(4), 92–96. available at: https://doi.org/10.1109/MIS.2011.69

- National Security Agency, “Defense in Depth,” 2012. available at: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf
- Nguyen, D., & Widrow, B. (1990a). Neural networks for self-learning control systems. IEEE control systems magazine.
- Rauscher, K.F., Yashenko, V.: Russia-U.S. Bilaterial on Cyber Security: Critical Terminology Foundations, EastWest Institute (2011),available at: http://www.ewi.info/system/files/reports/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20%282%29.pdf
- Rowe, N. C. (2002). Marie-4: A high-recall, self-improving web crawler that finds images using captions. IEEE Intelligent Systems, 17(4), 8–14. available at: https://doi.org/10.1109/MIS.2002.1024745
- Petit, F., & Verner, D., & Phillips, J., & Lewis, L. P. (2018).Critical Infrastructure Protection and Resilience Integrating Interdependencies. In Security by Design, A. J. Masys, Ed., Cham., Switzerland: Springer.
- Seiger, R., Huber, S., Heisig, P., & Amann, U. (2019). A framework for self-adaptive workflows in cyber-physical systems. Software Engineering and Software Management, 2019. available at: https://dl.gi.de/handle/20.500.12116/ 20898
- Soomro, S., Miraz, M. H., Prasanth, A., & Abdullah, M. (2018). Artificial intelligence enabled IoT: Traffic congestion reduction in smart cities. doi: ۱۰.۱۰۴۹/□□.۲۰۱۸.۱۳۸۱.
- Soykan, O. (2011). U.S. Patent No. 8,027,791. U.S. Patent and Trademark Office.
- Stoianov.N & Bozhilova.M.(2020). A Model of a Cyber Defence Awareness Sys-tem of Campaigns with Malicious Information. available at: https://doi.org/10.11610/isij.4613
- Talwar, R. and Koury, A., 2017. Artificial intelligence–the next frontier in IT security?. Network Security, 2017(4), pp.14-17.
- Theron,P. Kott,A. Drašar, M.Mancini,L. Gaspari,F.Pihelgas, M and Rzadca,K. (2020). Reference Architecture of an Autonomous Agent for Cyber Defense of Complex Military Systems.Adaptive Autonomous Secure Cyber Systems, pp1-21. DOI : 10.1007/978-3-030-33432-1_1
- Theron,P. Kott,A. Drasar,M. LeBlanc,B. Rzadca, K. Pihelgas, M. Mancini, L and Panico, A. (2018).Towards an active, autonomous and intelligent cyber defense of military sysems.the International Conference on Military Communications and Information Systems Warsaw, Poland, 22nd - ۲۳□□.
- Vinge, V. (2008). Signs of Singularity. IEEE Spectrum, 45(6), 76–82. https://doi.org/10.1109/MSPEC.2008.4531467
- Virgilio Almeida,2016, Cyberwarfare and Digital Governance.
- Yampolskiy, R. (2017). The singularity may be near. MDPI.

Zhang, Y., Qian, C., Lv, J., & Liu, Y. (2016). Agent and cyber-physical system based self organizing and self-adaptive intelligent shopfloor. IEEE Transactions on Industrial In rmatics, 13(2), 737–747. available at: https://doi.org/10.1109/TII.2016.2618892