طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران

رضا تقی‌پور[1]

علی اسماعیلی[2]

تاریخ دریافت:۱۳۹۷/۰۵/۲۰ تاریخ پذیرش:۱۳۹۷/۰۹/۲۲

چکیده:

گذشته از دستاوردهای فضای سایبر، توجه به تهدیدات روزافزون این فضا، در اولویت بسیاری از بازیگران دولتی و غیردولتی قرار گرفته است. حملات سایبری به‌عنوان جدیدترین و پیچیده‌ترین نبردها ذیل عملیات‌های نظامی به شمار می‌آید. حملات سایبری به دلیل جدید بودن، درصد هزینه پایین و فایده بالا، عدم توانایی کشور هدف در مشخص و اثبات نمودن منشأ تهدید و عدم توانایی در تعیین میزان و دامنه خسارات وارد شده در مراحل اولیه شروع حمله، مورد توجه کشورهای متخاصم به‌ویژه در جنگ‌های ترکیبی قرار گرفته است. جایگاه خاص جمهوری اسلامی ایران در ترتیبات منطقه‌ای و نظام بین‌الملل سبب شده تا نظام سلطه از فضای سایبری برای تحدید قدرت ملی به شکل فزاینده‌ای بهره‌برداری نماید. در این میان، به‌منظور ایجاد سازوکار مناسب برای تضمین امنیت و منافع ملی در این فضا، شناخت ابعاد مختلف این مسئله به دغدغه بسیاری از صاحب‌نظران این حوزه تبدیل شده است.

در همین راستا، ایجاد هرگونه نظام کارآمد دفاع سایبری مستلزم طراحی مدل مفهومی دفاع سایبری است. این پژوهش با این پرسش که چارچوب مفهومی دفاع سایبری و مؤلفه‌های اساسی آن در جمهوری اسلامی ایران چیست؟ با به‌کارگیری فن خوشه‌بندی در تحلیل محتوا و تکنیک دلفی درصدد طراحی مدل مفهومی دفاع سایبری برآمده است. برای این منظور، سه مفهوم بازدارندگی، پدافند (دفع) و برگشت‌پذیری به‌مثابه ابعاد اساسی دفاع سایبری مورد شناسایی قرار گرفتند و سپس مؤلفه‌های هر یک از این ابعاد استخراج و شاخص‌های هر مؤلفه معین شدند. با مجموع ابعاد، مؤلفه‌ها و شاخص‌های دفاع سایبری، مدل مفهومی دفاع سایبری طراحی گردید.

کلیدواژه‌ها: تهدیدات سایبری، دفاع سایبری، مدل مفهومی، ابعاد دفاع سایبری

۱- **مدرس دانشگاه و** پژوهشگر ارشد حوزه امنیت فضای سایبر

۲- دانش‌آموخته دوره دکتری مدیریت راهبردی امنیت فضای سایبر دانشگاه عالی دفاع ملی (نویسنده مسئول)- a.esmaily@sndu.ac.ir

مقدمه:

امروزه حملات و تهدیدات سایبری به‌مراتب پیچیده و مخرب‌تر شده‌اند. جمهوری اسلامی ایران نیز با توجه به شرایط ویژه خود و تقابل دائمی آن با استکبار جهانی با یک محیط تهدید فزاینده سایبری مواجه شده است. بازیگران دولتی و غیردولتی در این محیطِ مرزگریز و با عبور از زمان و مکان، زمینه را برای انجام حملات سایبری ذیل عملیات‌های نظامی فراهم ساخته‌اند. قدرت‌های بین‌المللی بهره‌مند از فناوری‌های برتر نیز در فضای سایبر از این فناوری‌ها برای مهندسی شبکه‌های اجتماعی و تغییر نظام‌های سیاسی در قالب انقلاب‌های مخملی استفاده می‌نمایند. در وقایع اخیر منطقه غرب آسیا، حملات سایبری بخشی از جنگ‌های ترکیبی بوده‌اند... حال با توجه به این شرایط جمهوری اسلامی ایران نیز نیازمند یک نظام مقابله‌ای هوشمند و برگرفته از ویژگی‌های خاص خود می‌باشد. طراحی هرگونه مدل عملیاتی برای تحقق دفاع سایبری متضمن داشتن الگوی مفهومی مناسب و همچنین تبیین چارچوب‌های نظری آن می‌باشد. مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران با تبیین مبانی نظری و پارادایم‌های حاکم بر آن و همچنین بررسی و مطالعه تطبیقی الگوهای کشورهای پیشرو و بهینه‌سازی آن با تکیه بر مطالعات اسناد بالادستی کشور و همچنین قوانین و مقررات جاری کشور، امکان‌پذیر خواهد بود.

بیان مسئله: اگرچه بازماندن از دستاوردها و بهره‌گیری بهینه از ظرفیت‌های فضای مجازی در حکمرانی منجر به ناکارآمدی خواهد شد، غفلت از آسیب‌پذیری‌ها و تهدیدهای فضای سایبر نیز می‌تواند لطمات و خسارت‌های جبران‌ناپذیری بر پیکره زیرساخت‌های حیاتی کشور و نرم‌افزار هویتی جامعه وارد آورد. بر همین اساس در سیاست‌های کلی ابلاغ شده توسط مقام معظم رهبری (مدظله‌العالی) برای بخش افتا[1]، به مواردی همچون ایجاد نظام جامع و فراگیر در سطح ملی و سازوکار مناسب برای امن‌سازی ساختارهای حیاتی، حساس و مهم در حوزه فناوری اطلاعات و ارتباطات و ارتقای مداوم امنیت شبکه‌های الکترونیکی و سامانه‌های اطلاعاتی و ارتباطی در کشور اشاره شده است (سند افتا، ۱۳۸۷).

اهمیت حملات سایبری به حدی است که پس از انتشار ویروس استاکس‌نت در ایران، برخی کشورهای پیشرو، به فکر بازسازی ساختار دفاع سایبری خود برآمدند (Herrington & Aldrich,2013). این کشورها از قبل نیز در راستای کاهش آسیب‌پذیری‌ها و استمرار خدمات در

۱- امنیت فضای تولید و تبادل اطلاعات

سطح ملی و همچنین بین‌المللی نسبت به ایجاد نظام دفاع سایبری و همچنین تعریف راهبردها و اقدامات اساسی ذیل آن اقدام کرده بودند. به‌عنوان مثال می‌توان به ساختار دفاع سایبری آمریکا و مرکز تعالی ناتو اشاره نمود. افراد بسیاری جنگ سایبری را یکی از ارکان جنگ‌ها در امروز و آینده می‌دانند؛ بنابراین باید سازوکاری را برای مقابله با تهاجمات پیش رو دنبال کرد.

در همین راستا جمهوری اسلامی ایران نیز با توجه به تقابل دائمی آن با نظام سلطه و ضرورت حفاظت از ارزش‌های اساسی و زیرساخت‌های خود نیازمند یک الگوی بومی برای دفاع سایبری خود متناسب با این مقتضیات می‌باشد. نظر به این‌که ساختار منسجم دفاع سایبری در کشور طراحی نگردیده و از سویی چیستی و ارتباط میان ابعاد و مؤلفه‌های تشکیل دهنده آن مشخص نیست؛ می‌بایست نسبت به تعریف و طراحی این ساختار اقدام لازم صورت پذیرد. الگوی مفهومی موصوف از بایسته‌های سازمان معنایی نظام دفاع سایبری کشور خواهد بود که با بهره‌گیری از چارچوب‌های معماری می‌توان به نظام دفاع سایبری دست یافت. فرآیندها، نهادها و ارتباطات میان عناصر تشکیل دهنده این نظام همگی مبتنی بر هندسه این الگو می‌باشند.

مسئله اصلی این است که عدم کارایی و اثربخشی اقدامات حوزه دفاع سایبری در جمهوری اسلامی ایران امکان حملات سایبری علیه کشور را به حداکثر رسانده و دائماً دشمن را متوجه نقاط ضعف ساختاری این حوزه می‌نماید. لذا چه الگویی می‌تواند برای مقابله با تهدیدات این حوزه مؤثر باشد و امر دفاع در فضای سایبر را روشمند و هدفمند نماید تا در برخورد با حملات سایبری علاوه بر کنترل تهدیدات، آسیب‌پذیری‌ها را نیز به حداقل برساند؛ بنابراین مسئله تحقیق ارائه الگوی مفهومی است که بتواند فرآیندها و ارتباطات نظام دفاع سایبری را ارائه نماید.

اهمیت و ضرورت: برای اهمیت این تحقیق از نگاه ایجابی و بر اساس فواید انجام پژوهش می‌توان موارد ذیل را برشمرد:

کاهش آسیب‌پذیری‌ها، ایجاد نظام مقابله با تهدیدات، ایجاد بازدارندگی، ایجاد نگاه کل‌گرایانه و سیستمی در مقابل نگاه واکنشی

از سوی دیگر از نگاه سلبی و بر اساس مضرات عدم انجام پژوهش می‌توان به موارد ضرورت این تحقیق اشاره نمود:

لطمات جبران‌ناپذیر به زیرساخت‌های حیاتی کشور، ناهماهنگی متولیان مقابله با تهدیدات سایبری،

هدف اصلی تحقیق، طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران و هدف فرعی، شناخت ابعاد، مؤلفه‌ها و شاخص‌های مدل مفهومی الگوی دفاع سایبری است.

متناظر با اهداف؛ سؤال اصلی مقاله نیز مدل مفهومی دفاع سایبری جمهوری اسلامی ایران چیست؟ و سؤال فرعی؛ ابعاد، مؤلفه‌ها و شاخص‌های مدل مفهومی دفاع سایبری کدام است؟ می‌باشد.

روش تحقیق:

این پژوهش از نوع مطالعات بنیادین برای رسیدن به مدل مفهومی الگوی دفاع سایبری است. برای این منظور، سه گام اصلی صورت گرفته است:

تحلیل محتوای کیفی: در این پژوهش به تحلیل محتوای کیفی اسناد بالادستی، تعاریف دفاع سایبری در ادبیات پژوهش و نیز بیانات امام خمینی (ره) و مقام معظم رهبری (مدظله‌العالی) و همچنین مطالعات تطبیقی پرداخته شد و با تکنیک خوشه‌بندی، کلیدواژه‌های مؤثر در دفاع سایبری استخراج شدند و بر اساس فراوانی کلیدواژه‌ها؛ ابعاد، مؤلفه‌های اصلی و شاخص‌های مؤلفه‌های دفاع سایبری مورد بازشناسی قرار گرفتند.

تکنیک دلفی: با استفاده از تکنیک دلفی، ابعاد بازشناسی شده در گام اول برای طراحی مدل مفهومی دفاع سایبری با اجماع نظر خبرگان اصلاح گردیدند. جمعیت نمونه تکنیک دلفی در این پژوهش، پانزده نفر از جامعه آماری اساتید و اعضای گروه مطالعاتی، متخصصین حوزه امنیت فضای سایبر، پژوهش‌گران، مدیران و متصدیان اجرایی در حوزه فناوری اطلاعات و فضای سایبری کشور هستند که با استفاده از روش نمونه‌گیری قضاوتی انتخاب گردیدند.

پرسشنامه باز: در گام سوم، پرسشنامه‌ای شامل سؤالات باز به‌منظور ارزیابی مدل مفهومی ارائه شده تهیه گردید و با توجه به جامعه آماری دوم که به‌صورت تمام شمار ۳۵ نفر از متخصصین فضای سایبر در دو حوزه اجرایی و دانشگاهی بودند برازش مدل مورد تأیید قرار گرفت.

مبانی نظری:

پیشینه پژوهش: پژوهش‌های مستقل درباره فضای سایبر را می‌توان به چند دسته تقسیم کرد: تعدادی از پژوهش‌های صورت گرفته در رابطه با فضای سایبر به مزیت‌ها، کارکردها و دستاوردهای این فضا پرداخته‌اند. تعداد قابل توجهی از پژوهش‌ها درباره فضای سایبری معطوف به آسیب‌پذیری‌ها و تهدیدات متصور از این ناحیه است. این آثار در زمینه‌های جنگ سایبری، امنیت، هویت، مرز، سایبر تروریسم و رویکردهای حقوقی و جرم‌انگاری به نگارش درآمده‌اند. در

رابطه با دفاع سایبری برخی آثار به راهبردها و رویکردهای قدرت‌های بین‌المللی پرداخته‌اند که در این میان می‌توان به مقاله «فضای سایبر و شیوه‌های نوین درگیری ایالات‌متحده آمریکا با جمهوری اسلامی ایران» اشاره نمود. این اثر به بررسی مشخصات اصلی جنگ سایبر به‌عنوان یک محیط استراتژیک پرداخته و از طریق بررسی ماهیت، اهداف، ابزار و روش‌های حملات در فضای مجازی و نیز واکنش‌های دفاعی مناسب در برابر این حملات را مورد تحلیل قرار داده است (ماه‌پیشانی، ۱۳۹۱: ۱۰۶).

مقاله «رویکرد دفاعی- تهاجمی جمهوری خلق چین در چارچوب فضای سایبر» نیز جنگ‌های آتی را جنگ‌های سایبری توصیف نموده و با روش توصیفی- تحلیلی رویکرد دفاعی- تهاجمی چین را در جهت طراحی نوعی جنگ جدید برای حفاظت از زیرساخت‌ها و شبکه‌های حیاتی خود و تخریب زیرساخت‌های حیاتی دشمنان ارزیابی نموده است (ابراهیمی و همکاران، ۱۳۹۱: ۲۴-۹).

در رابطه با الگوی دفاع سایبری نیز پژوهش‌هایی انجام شده است. مقاله «ارائه الگویی برای دفاع سایبری در آستانه حمله مبتنی بر پردازش رویدادهای پیچیده» به دنبال ارائه الگویی برای دفاع سایبری در آستانه حمله، با تکیه بر تئوری‌هایی چون پردازش رویدادهای پیچیده و کسب و کارهای پیش‌گویانه است. الگوی پیشنهادی این مقاله، برای مقابله با تهدیدات و دفاع در آستانه حمله‌های احتمالی است (رشیدی و نقیان، ۱۳۹۲). در مقاله‌ای دیگر با عنوان «چارچوب و اصول دفاع سایبری فعال» نوشته دوثی ای.دنینگ، تلاش شده ضمن مرور مفاهیم دفاع هوایی و موشکی فعال و غیرفعال و تسری این مفاهیم به فضای سایبری، اصول اخلاقی و قانونی برای راهبری دفاع سایبری فعال ارائه شود. این نویسنده دفاع سایبری فعال را با چهار مشخصه طیف تأثیرات (داخلی و خارجی)، درجه همکاری، نوع تأثیرات (اشتراک‌گذاری اطلاعات، جمع‌آوری، مسدودسازی فعالیت‌های خصمانه) و درجه مکانیزه بودن (در ارتباط با میزان اثرگذاری عامل انسانی) مورد ارزیابی قرار می‌دهند (E. Denning,2014:109).

رساله با عنوان «بازدارندگی و مسئله نسبت حملات سایبری» با تأکید بر مفهوم بازدارندگی به دنبال تبیین مشکلات اجرای دکترین بازدارندگی سایبری از طریق تحلیل پرونده‌های مختلف حملات سایبری مانند استونی و برزیل است. نویسنده در این رساله به این نتیجه رسیده است که به استناد تحلیل‌های مطرح شده، عمل نسبت دادن یک حمله سایبری از نظر فنی بسیار دشوار

است و پروتکل‌های شبکه، اجازه انواع حملات به منبع، مقصد و کانال عبور اطلاعات را می‌دهند و نسبت دادن حمله، همان‌طور که در این پرونده‌ها نشان داده شده در بهترین حالت با شک و عدم قطعیت همراه است. علاوه بر این، تصمیم به شروع جنگ یا اقدامات محکم تلافی‌جویانه به درجات بالاتری از اطمینان نیاز دارد و رسیدن به این درجات اطمینان‌پذیری به منابع فراوان، تعداد زیادی از کارشناسان خبره و زمان طولانی نیازمند است و گاهی با وجود تمامی این فاکتورها نیز غیرعملی است (Gelinas, 2010).

در پژوهشی دیگر با عنوان «مدل کارگزار محور تیم تحلیل دفاع امنیت سایبری» راجیوان، ا.جیسون و جی.کوک از مدلی کارگزارپایه از تعامل و تکالیف تحلیل‌گر دفاع سایبری استفاده کرده‌اند. این مدل اثرات اندازه‌های تیمی و راهبردهای همکاری متفاوت در سنجش عملکردی مانند شمار هشدارهای نفوذ را گسترش می‌دهد که به درستی توسط تحلیل‌گران تحلیل می‌شوند و پاسخ‌ها که آن‌ها از دقت پردازش هشدارها به دست می‌آورند. (Janssen,2013).

مفهوم شناسی متغیرها:

فضای سایبر جمهوری اسلامی ایران: فضای سایبری نظام جمهوری اسلامی ایران شامل مجموعه‌ای از ارزش‌ها، منافع و دارایی‌های ملی در فضای سایبر بوده و جهت ارائه خدمات در راستای اهداف نظام جمهوری اسلامی ایران هست. این فضا محدود به مرزهای جغرافیایی نیست (تصویب‌نامه کمیسیون موضوع اصل ۱۲۷ و ۱۳۸ قانون مورخ ۹۱/۶/۶).

تهدیدات سایبری: هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر یا اشتهار دستگاه متولی، سرمایه ملی سایبری یا کارکنان دستگاه به‌واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام، افشاء، تغییر اطلاعات و یا ممانعت از ایجاد اختلال در ارائه خدمت (سند راهبردی پدافند سایبری کشور،۱۳۹۰).

دفاع سایبری: مجموعه اقدامات بازدارنده، رفع کننده، دفع‌کننده و بازیابی کننده که به‌منظور پیش‌گیری، حفظ، حمایت از ارزش‌ها، منافع و دارایی‌های ملی در مقابل تهدیدات و حملات سایبری انجام می‌گیرد (جمعی از محققین: ۱۳۹۵: ۳۱).

ساختار دفاع سایبری: زیرمجموعه‌ای از نظام دفاعی کشور شامل نهادهای دولتی همچنین سازمان مردم‌نهاد و زیر نظام‌های دیگر در سطح ملی به همراه روابط میان آن‌ها و فرایندهای مرتبط

به‌منظور پیش‌گیری، حفظ دارایی‌های زیرساختی، حمایت از ارزش‌ها، منافع و دارایی‌های ملی در مقابل تهدیدات و حملات سایبری (همان: ۳۲).

مدل‌سازی مفهومی دفاع سایبری: مدل‌سازی مفهومی، فعالیت توصیف‌گری رسمی برخی جنبه‌های جهان فیزیکی و اجتماعی پیرامون ما برای تحقق فهم و ارتباط است. عموماً این توصیف‌گری فعالیتی بنیادین در مهندسی سیستم‌های اطلاعاتی است که در آن، دامنه موضوع مفروض به‌صورت مستقل از گزینش‌های اجرایی ویژه توصیف می‌شود. محصول اصلی این فعالیت مدل نظری است (A. Carvalho, A. Almeida, M. Fonseca & Guizzardi,2017:4). چنین مدلی، همان‌طور که حاوی مفاهیمِ دارای تعریف اسمی است، حاوی یک منطق بنیادی و یک مکانیسم نیز هست. منطق بنیادی، دیدگاهی است درباره یک پدیده، راهی برای نگریستن به جهان اجتماعی، تصوری سازمان‌دهنده که از تخیل پژوهشگر و نه از داده‌ها حاصل می‌شود. ساختار روابط بین مفاهیم که توسط مفاهیم مورد استفاده تعیین می‌شود، مکانیسم مدل را شکل می‌دهد (بلیکی، ۱۳۹۳: ۲۲۱).

دفاع سایبری به‌مثابه مفهومی پیچیده، دارای بسترها و موضوعات به شدت دگرگون شونده است که فهم آن مستلزم درک ابعاد و رابطه آن با انسان به لحاظ هستی‌شناختی است. در حالی که منطق جدید امنیت سیستمی، نیازمند تنوع و حتی شاید انفکاک جدی است، گرایش وسیع در فناوری اطلاعات به سمت همگرایی موجودیت انسانی و رایانه‌ها است (Herrington & Aldrich,2013:306) . این هم‌آمیختگی هستی‌شناسانه ناشی از گره خوردن همه ابعاد زندگی انسانی با اینترنت و شبکه است. با گسترش روزافزون عمق و دامنه فضای سایبر، جنگ قدرت بین ذینفعان نیز با شدت بیشتر و خشونت، طرد و حذف سنگین‌تر در جریان است.

پنج قلمرو قدرت یعنی سرزمین، آب، هوا، فضا و فضای سایبر تولید و کسب منابع و نفوذ را میسر می‌سازند که امروزه فضای سایبر پیشگام گسترش قدرت دیپلماسی، اطلاعاتی[1]، نظامی و اقتصادی است. تمام انواع واحدها (دولت‌ها، شرکت‌ها، تروریست‌ها، سازمان‌های جنایی و گروه‌های غیرانتفاعی) همگی فعالیت‌های خود را در بستر فضای سایبر به پیش می‌برند (Rowland, Rice & Shenoi,2014:4).

در چنین فضایی سامان دفاع سایبری یکی از مهم‌ترین اولویت‌های زندگی نه فقط در بعد سیاسی، بلکه در کلیه ابعاد زندگی بشری است. این موضوع سبب شده تا تهاجم سایبری به‌مثابه

1- Information

تهدید ردیف اول در انگلیس در نظر گرفته شود و شورای امنیت ملی این کشور این پدیده را به‌عنوان خطری با بالاترین اولویت ارزیابی نماید (Herrington &Aldrich,2013:299).

بی‌تردید مفهوم دفاع سایبری در جمهوری اسلامی ایران به دلیل هدف تهاجم قرار گرفتن کشور ایران توسط برخی قدرت‌های بین‌المللی، منطقه‌ای و برخی عوامل غیردولتی فروملی و فراملی مانند گروه‌های تروریستی از اهمیت و اولویت فوق‌العاده‌ای حتی نسبت به کشورهایی مانند انگلیس برخوردار است. اگرچه بهره‌گیری از تجربه کشورهای پیش‌رو در دفاع سایبری موضوعی بسیار پراهمیت 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.

مدل مفهومی دفاع سایبری: افزایش جمعیت و پیچیدگی ساختارهای روابط اجتماعی سبب گردیده که کارآمدی دولت‌ها فقط در سایه فضای سایبری تأمین نگردد. عجین شدن زندگی انسانی با فضای مجازی، تهدیدات ناشی از رقیبان و دشمنان و عوامل اخلال‌گر در این فضا را تشدید کرده است. به‌طوری که فضای سایبر توسط دولت آمریکا به‌مثابه حوزه جنگی در نظر گرفته شده است. دولت‌ها و شرکت‌های خصوصی پیرامون جهان نیز در درک تهاجمات سایبری به‌مثابه یکی از بزرگ‌ترین تهدیدات اجماع نظر دارند. علاوه بر این، نیرو و هزینه‌های بسیاری صرف ساخت دفاع فعال علیه تهاجمات سایبری می‌شود (Rajivan, A. Janssen & J Cooke, 2013: 314). ایجاد هرگونه الگوی دفاع سایبری فعال و کارآمد، مستلزم زیرساخت مفهومی همه‌جانبه‌نگری است که ابعاد، مؤلفه‌های اصلی و شاخص‌های این مؤلفه‌ها را در دفاع سایبری احصاء نماید.

ابعاد دفاع سایبری: تحلیل محتوای تعاریف مفهوم دفاع و نیز دفاع سایبری و همچنین بررسی اسناد بالادستی، ادبیات تحقیق و مطالعات تطبیقی با استخراج کلیدواژه‌های مهم این تعاریف مبتنی بر تکنیک خوشه‌بندی و دریافت اجماع نظر نخبگان درباره این کلیدواژه‌ها از طریق تکنیک دلفی، منتج به ترسیم سه کلیدواژه **بازدارندگی، پدافند و برگشت‌پذیری**[1] به‌عنوان ابعاد دفاع سایبری گردید. عبارت دیگر این تعریف از دفاع سایبری منطبق با توصیف مذکور و پس از تأیید خبرگان دارای جامعیت و مانعیت می‌باشد. نمونه‌ای از استخر کلیدواژه‌ها در تبیین ابعاد مدل مفهومی در جدول شماره ۱ ذکر گردیده است.

1- resilience

جدول (۱): استنتاج ابعاد دفاع سایبری

عنوان	عبارت دقیق	مرجع
بازدارندگی دفع و رفع	وَأَعِدّوا لَهُم مَا استَطَعتُم مِن قُوَّةٍ وَمِن رِباطِ الخَيلِ تُرهِبونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُم	قرآن کریم سوره انفال آیه ۶۰
دفع و رفع	برحسب تجربه‌های تاریخی آنچه بیش از همه برای ملت‌ها مایه افتخار است، عبارت است از قدرت دفاع و قدرت سازندگی در معیار تقدیر و ارزش‌گذاری بر روی ملت‌ها. آنچه در بالای صفحه قرار می‌گیرد این دو توانایی است. هرگز در تاریخ کشوری را به خاطر مثلاً وسعت بازرگانی‌اش یا تجملات زندگی یا مصرف زیاد و ازاین‌گونه چیزها ستایش نمی‌کنند، مگر زبان‌های سطحی جو و مغزهای سطحی‌نگر؛ اما ملت‌هایی را که توانسته‌اند در مواقع حساس از خود دفاع کنند، تاریخ ستایش می‌کند و قشرهای ژرف‌نگر به چشم تجلیل بر آن‌ها می‌نگرند. تاریخ همچنین ملت‌هایی را که توانسته‌اند، پس از ضربه‌های هولناک و ویرانی‌های وسیع با سازندگی و قدرت نوآوری دوباره خود را به حال اول بلکه بهتر برگردانند ستایش می‌کند.	سخنرانی مقام معظم رهبری (مدظله‌العالی) در مراسم صبحگاه نظامی پایگاه منطقه دوم دریایی نیروی دریایی ارتش در بوشهر ۱۲ دی ۱۳۷۰
	هماهنگی به‌منظور صیانت از آسیب‌های ناشی از آن	حکم تشکیل شورای عالی فضای مجازی کشور در تاریخ ۱۷ اسفند ۱۳۹۰
بازدارندگی دفع و رفع برگشت‌پذیری	ما باید پیش از آنکه تهدیدها بتوانند به سیستم‌های تبادل اطلاعاتی که زیرساخت حیاتی محسوب می‌شوند آسیب وارد کنند، نقاط ضعف و آسیب‌پذیری‌های خودمان را کاهش دهیم. این اقدامات پیشگیرانه باید به‌گونه‌ای باشد که اختلالات به حداقل برسد. همچنین در صورت بروز، کم‌دوام و قابل‌کنترل بوده و کمترین آسیب ممکن را به سیستم‌ها وارد سازند.	استراتژی ملی ایالات‌متحده آمریکا برای فضای تبادل اطلاعات امن (مقدمه جورج دبلیو بوش: ۱۷)
بازدارندگی دفع و رفع برگشت‌پذیری	بازدارندگی در مقابل حمله‌های سایبری علیه زیرساخت‌های حیاتی آمریکا، کاهش آسیب‌پذیری ملی در برابر حمله‌های سایبری، به حداقل رساندن خسارت و زمان ترمیم در حملات سایبری	استراتژی ملی ایالات‌متحده آمریکا برای فضای تبادل اطلاعات امن
دفع و رفع برگشت‌پذیری	دفاع بومی، همه‌جانبه و بازدارنده؛ هوشمندی در دفاع؛ کاهش آسیب‌پذیری‌ها؛ حفظ تداوم کارکرد سامانه‌ها؛ آمادگی و پایداری؛ حفظ و صیانت از سرمایه‌های سایبری؛ پیش‌دستی در شناخت تهدیدات اشراف اطلاعاتی در فضای سایبری کشور	سند راهبردی پدافند سایبری کشور

عنوان	عبارت دقیق	مرجع
دفع و رفع برگشت‌پذیری	کسب آمادگی دفاع سایبری، کاهش آسیب‌پذیری‌های موجود در سامانه‌های مبتنی بر فناوری اطلاعات در دستگاه‌ها/ استان‌ها/ مناطق ویژه، حفظ و مراقبت از زیرساخت‌های سایبری حیاتی، حساس و مهم، افزایش پایداری و تداوم چرخه خدمات فناوری اطلاعات و ارتباطات کشور در برابر تهاجم احتمالی سایبری دشمن	دستورالعمل ارتقاء آمادگی پدافند سایبری
دفع و رفع	عملیات صورت گرفته با استفاده از شبکه‌های کامپیوتری جهت محافظت کردن، نظارت، تحلیل، یافتن و پاسخ دادن به فعالیت غیرمجاز در داخل سیستم‌های اطلاعاتی و شبکه‌های کامپیوتری وزارت دفاع است.	سند وزارت دفاع آمریکا (تعریف دفاع سایبری)

از دیدگاه نظریه‌پردازان بازدارندگی، نظم سیستمی زمانی حفظ خواهد شد که رهبران دریابند، حریفان بالقوه آن‌ها در صورت رخداد رفتار نامطلوب، توان و اراده تلافی را خواهند داشت. برخی دیگر بازدارندگی را به‌منزله بهره‌گیری از تهدیدات توسط یکی از طرفین، به‌منظور اقناع طرف مقابل، برای خودداری از شروع برخی از اقدامات یا اقدام مورد نظر تعریف می‌کنند (قاسمی،۱۳۸۸: ۱۵۷). *پدافند* در مفهوم کلی، دفع، خنثی‌سازی یا کاهش تأثیرات اقدامات آفندی دشمن و ممانعت از دستیابی به اهداف خودی است. *برگشت‌پذیری* نیز، ظرفیت یا توانایی یک عامل برای سازگاری و بازگشت به وضعیت ثبات پس از اختلال است (Penadés, G. Núñez & H. Canós,2016: 83).

مؤلفه‌های ابعاد دفاع سایبری: به‌منظور استخراج مؤلفه‌ها و شاخصه‌های ابعاد سه‌گانه دفاع سایبری، کلیدواژه‌های مختلف مرتبط با این ابعاد با مطالعه ادبیات پژوهش مطابق با جدول شماره ۲ و ۳ و با تحلیل کیفی بیانات امام خمینی (ره) و مقام معظم رهبری (مدظله‌العالی) و اسناد زیر گردآوری شدند:

- حکم تشکیل شورای عالی فضای مجازی
- قانون اساسی جمهوری اسلامی ایران (اصول ۱۷۶، ۱۵۱، ۱۵۲)
- سند راهبردی پدافند سایبری کشور
- قوانین بین‌المللی منشور سازمان ملل متحد
- استراتژی امنیت و دفاع سایبری اتحادیه اروپا، ایالت متحده آمریکا، انگلیس، کره-جنوبی، ترکیه و اردن

سپس با تکنیک خوشه‌بندی و بر اساس فراوانی تکرار واژه‌ها مؤلفه‌های اصلی ابعاد سه‌گانه و شاخص‌های این مؤلفه‌ها مورد بازشناسی اولیه قرار گرفتند و این مؤلفه‌ها از طریق تکنیک دلفی با اجماع نظر خبرگان اصلاح گردیدند.

مؤلفه‌های بعد بازدارندگی در دفاع سایبری: مدل بازدارندگی معطوف به جلوگیری از تحقق تهدیدات علیه خود است؛ بنابراین طراحی این بعد مستلزم به‌کارگیری پارامترهای مختلفی است که تحقق چنین موضوعی را سبب می‌شوند. در این راستا اولین جزء مدل، طراحی حوزه‌های راهبردی است که کشور در آن منافع متعددی داشته و تهدیدات علیه آن نیز از چنین محیطی سرچشمه خواهد گرفت. دومین جزء این بعد معطوف به ایجاد شرایط مقدماتی و منطقی بازدارندگی است که در آن پارامترهای زیر مبتنی بر تعاریف بازدارندگی در نظر گرفته خواهد شد.

– فراهم ساختن توانایی‌هایی فیزیکی به‌منظور تحمیل خسارت بر حریف بر اساس اصل عقلانیت؛

– برقرار ساختن ارتباط با حریف و آگاه ساختن آن از اعمال ممنوعه؛

– اعتبار بخشیدن به تهدیدات علیه رقیب و بیان این موضوع که در صورت اقدام ممنوعه اجرای تهدیدات حتمی خواهد بود. از همین‌رو، مؤلفه‌های بعد بازدارندگی عبارتند از:

۱– ارتباط به معنای برقراری رابطه با حریف و آگاه ساختن وی از قصد و نیت و حدود اعمال ممنوعه است (قاسمی، ۱۳۸۶: ۱۰۲). در نظریه بازدارندگی، جلوگیری از برخورد میان طرفین، به تبادل‌نظر صریح و ضمنی طرفین بستگی دارد؛ بنابراین لازم است دولت‌ها از طریق انتشار اعلامیه رسمی، ارسال پیام و اعلام برنامه‌های خود، نیات واقعی خود را در این زمینه آشکار کنند. بازدارندگی هنگامی مؤثر است که نیروی بازدارنده منظور خود را صریح و شفاف به اطلاع طرف مقابل برساند و معین کند در صورت موردحمله قرار گرفتن دقیقاً چه عواقبی در انتظار مهاجم خواهد بود. ارتباط می‌تواند به‌صورت صریح یا ضمنی باشد (ازغندی و روشندل، ۱۳۸۴).

۲– ***توانایی یا قابلیت*** به علاوه عقلانیت به معنای توانایی تحمیل خسارت غیرقابل تحمل بر دشمن و عقلانیت طرفین در محاسبه سود و هزینه احتمال رفتارهای خود است (قاسمی،۱۳۸۸: ۵۹). این ویژگی به جنبه توانایی دولت‌ها در نظریه بازدارندگی مربوط می‌شود. این به معنای توانایی وارد آوردن ضربه به مهاجم احتمالی به‌وسیله تجهیزات متعارف و غیرمتعارف است. نیروی

بازدارنده به‌جز مواردی که بلوف می‌زند، باید قادر باشد در صورت لزوم مجازات متناسب را برای طرف مهاجم به مرحله عمل درآورد (امیدوارنیا، ۱۳۸۲).

۳- ***اعتبار*** یعنی تهدید واقعی و باور حریف به این‌که طرف مقابل از چنین توانایی برخوردار است. به عبارتی عقلانی بودن تهدید شرط اعتبار تهدید به‌حساب می‌آید (قاسمی،۱۳۸۸: ۵۹).

۴- ***ثبات‌نظر*** به معنای ثابت ماندن در دیدگاه‌ها و استحکام در مواضع است. اگر برخورد به‌اندازه کافی شدید باشد، طرف‌های منازعه نه‌تنها باید بتوانند تصمیم به اجرای تهدید را به یکدیگر بفهمانند، بلکه باید رهبران دشمن را در مورد نیت خود، تحت تأثیر قرار دهند، یک نظام بازدارندگی مؤثر صرفاً به داشتن نیروی نظامی قدرتمند نیاز ندارد، بلکه یک قدرت بازدارنده مؤثر علاوه بر معتبر بودن، باید باثبات هم باشد (امیدوارنیا،۱۳۸۲).

مؤلفه‌های بعد پدافند در دفاع سایبری: پدافند به معنای دفاع در مقابل حمله خواهد بود. پدافند به دو نوع عامل و غیرعامل دسته‌بندی می‌شود. پدافند عامل به بهره‌گیری از تمامی ابزارها و جنگ‌افزارهای نظامی برای مقابله با دشمن گفته می‌شود. پدافند غیرعامل نیز به‌کارگیری روش‌هایی است که با بهره‌گیری از آن بتوان آثار بحران و حمله را به حداقل رساند. در این نوع از پدافند برخلاف نوع اول از هیچ‌گونه جنگ‌افزار نظامی استفاده نمی‌شود (جوزی‌خمسلویی،۱۳۹۲: ۸۸).

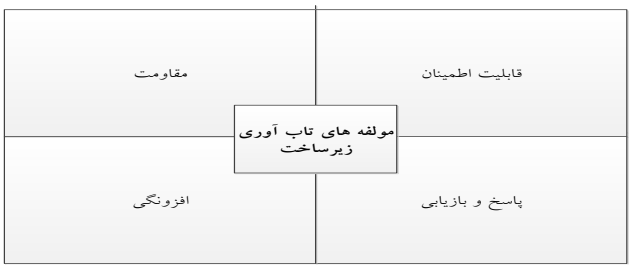
در این روش، باید شیوه‌ها، ابعاد گوناگون، گستره وسیع تهدیدات، تهاجم و حمله دشمن مورد بررسی قرار گرفته و برای تک‌تک آن‌ها با ارائه بهترین راهکارها چه قبل از وقوع و چه در حین وقوع، تدبیر نمود. سازمان پدافند غیرعامل، ابعاد پدافند غیرعامل را پوشش، اختفاء، استتار، پراکندگی، فریب، موانع، جابجایی، محکم‌سازی و حسگرها تعریف نموده است. پوشش، اختفاء، استتار، پراکندگی، فریب، موانع، جابجایی، مستحکم‌سازی و حسگر شاخص‌های مؤلفه پدافند غیرعامل را تشکیل می‌دهند (Beggs, 2010).

جدول (۲): مؤلفه‌ها و شاخص‌های پدافند غیرعامل و بازدارندگی در دفاع سایبری

مؤلفه	شاخص	منابع
پدافند غیرعامل	۱- .....پوشش ۲- .....اختفاء ۳- .....استتار ۴- .....پراکندگی ۵- .....فریب ۶- .....موانع ۷- .....جابجایی ۸- .....مستحکم‌سازی ۹- .....حسگر	سیاست‌های کلی نظام در بخش پدافند غیرعامل Securing the Nation's Critical Cyber Infrastructure (Beggs, 2010) تدوین راهبردهای پدافند غیرعامل نزاجا در مقابل تهدیدات ناهمطراز
پدافند عامل	۱- .....سلاح سایبری	
ثبات نظر	ثبات دیدگاه	امنیت در قرن بیست و یکم، نشر دفتر مطالعات سیاسی و بین‌المللی، تهران (امیدوارنیا، ۱۳۸۲)
اعتبار	۱- .....اثبات توانمندی ۲- .....اراده اقدام سایبری	امنیت در قرن بیست و یکم، نشر دفتر مطالعات سیاسی و بین‌المللی، تهران (امیدوارنیا، ۱۳۸۲) Cyberdeterrence and cyberwar (Libicki, 2009) Cyber Deterrence. Tougher in Theory than in Practice? (Goodman, 2010)
قابلیت	۱- .....تضعیف توانمندی دشمن ۲- .....ارتقای توانمندی خودی	امنیت در قرن بیست و یکم، نشر دفتر مطالعات سیاسی و بین‌المللی، تهران (امیدوارنیا، ۱۳۸۲)
ارتباط	۱- .....ضمنی ۲- .....صریح	مسائل نظامی و استراتژی معاصر، تهران: انتشارات سمت (ازغندی و روشندل، ۱۳۸۴)

مؤلفه‌های بعد برگشت‌پذیری در دفاع سایبری (تاب‌آوری سایبری): تاب‌آوری سایبری عبارت است از توانایی یک سازمان برای مقاومت، واکنش و بازیابی از تهدیداتی که بر روی اطلاعات تأثیر خواهد داشت که به آن اطلاعات در انجام کسب‌وکار نیاز است. تاب‌آوری سایبری عبارت از توانایی آمادگی و سازگاری برای تغییر شرایط و تحمل و بازیابی سریع پس از اختلال‌ها است. بازیابی شامل توانایی تحمل و بازیابی از حملات عمدی، رویدادها یا تهدیدات طبیعی یا حوادث است. تاب‌آوری سایبری، به‌عنوان توانایی سیستم‌ها و سازمان‌ها برای مقاومت در برابر حوادث سایبری تعریف می‌شود. تاب‌آوری سایبری، قابلیت سازمانی برای مقاومت در برابر تأثیرات منفی، با توجه به تهدیدات شناخته‌شده، قابل پیش‌بینی، ناشناخته، غیرقابل‌پیش‌بینی،

نامشخص و غیرمنتظره از فعالیت‌ها در فضای سایبری است. تاب‌آوری، توانایی دارایی‌ها، شبکه‌ها و سیستم‌ها برای پیش‌بینی، جذب و انطباق و یا بازیابی سریع از رویداد مخرب است. تاب‌آوری، از طریق ترکیب فعالیت‌ها یا مؤلفه‌ها امن گردیده است. چهار مؤلفه اصلی در شکل شماره (۱) نمایش داده شده است.



شکل (۱) چهار مؤلفه اصلی تاب‌آوری زیرساخت

۱- مقاومت[1]: به‌صورت سنتی حالت جلوگیری و ایجاد مقاومت در برابر خطر یا تأثیر اولیه آن است. مؤلفه مقاومت تاب‌آوری بر تأمین حفاظت، متمرکز شده است. این مؤلفه به‌منظور جلوگیری از آسیب و اختلال از طریق تأمین قدرت یا حفاظت برای ایستادگی در برابر خطرات یا برخورد اولیه با آن است. راهبردهای مقاومت، نقاط ضعف عمده‌ای دارند، به‌طوری‌که غالباً حفاظت در برابر انواع رویدادهایی انجام می‌پذیرد که قبلاً تجربه شده‌اند، یا آن‌ها بر اساس سابقه تاریخی که پیش‌بینی‌شده‌اند، توسعه یافته‌اند، صورت می‌گیرد. اقدامات حفاظتی و امنیتی در جهت کاهش تأثیر تهدیدات مخرب ممکن است به کاهش تأثیر خطرات طبیعی کمک نکند. حوادث مخرب می‌توانند از استانداردهای ارائه شده برای حفاظت، درنتیجه از دست دادن یا آسیب و اثرات قابل توجه تخطی کنند، مخصوصاً که مقاومت، تنها مؤلفه یک راهبرد تاب‌آوری است.

۲- قابلیت اطمینان[2]: شامل حصول اطمینان از اجزای زیرساخت که تحت دامنه‌ای از شرایط کار می‌کنند. مؤلفه قابلیت اطمینان با تضمین اینکه مؤلفه‌های زیرساخت ذاتاً برای کار تحت طیف وسیعی از شرایط که با کاهش آسیب یا از دست دادن در یک رویداد، درگیر است؛ طراحی شده‌اند. تمایل یک راهبرد قابلیت اطمینان، تنها در حوادثی در محدوده مشخص است و نه حوادثی که بیش از محدوده، تمرکز می‌کند. این موضوع می‌تواند به آگاهی ناکافی و یا آماده‌سازی برای رویدادهای خارج از محدوده منجر شود و ازاین‌رو اثرات گسترده‌تر و طولانی‌مدت قابل‌توجهی می‌تواند رخ

1-Resistance
2-Reliability

دهد. درنتیجه قابلیت اطمینان نمی‌تواند تضمین شده باشد، اما خرابی گاهی اوقات می‌تواند در یک سطح قابل تحملی مدیریت شود تا اینکه خدمات کامل بتوانند پس از این رویداد دوباره بازسازی شوند. از همین‌رو، بازدید دوره‌ای، تجهیزات بومی، تست نفوذ و آستانه پذیرش ریسک شاخص‌های اصلی مؤلفه قابلیت اطمینان را تشکیل می‌دهند.

۳- افزونگی[1]: اعمال افزونگی به سطح شبکه و سیستم است. مؤلفه افزونگی با طراحی و ظرفیت شبکه یا سیستم درگیر است. در دسترس بودن تجهیزات[2] پشتیبان‌گیری و یا ظرفیت یدکی[3] عملیات را قادر به سوئیچ[4] یا انتقال[5] به قطعات جایگزین شبکه در صورت اختلال برای اطمینان از تداوم خدمات می‌کند. در برخی از بخش‌های زیرساخت‌های ملی، راهبرد افزونگی به از دست دادن اولیه کارایی منجر می‌شود تا اینکه زیرساخت‌های جایگزین بتوانند کار کنند. بخش مخابرات[6] راهبرد افزونگی را برای ارائه ظرفیت و انعطاف‌پذیری برای اوج تقاضای ملاقات[7] برای خدمات و فعال کردن مسیریابی دوباره ارتباطات «ترافیک» در صورت شکست و یا از دست دادن قطعات[8] به‌کار می‌برد. در این بخش، سوئیچ بر روی خدمات حفظ آنی است. تاب‌آوری شبکه‌ها، در حال اجرا یا در نزدیک ظرفیت کاهش می‌یابد، اگرچه در برخی از بخش‌ها یا سازمان مشخص‌شده، اما ممکن است همیشه برای کار با ظرفیت یدکی قابل‌توجه درون شبکه امکان‌پذیر نباشد؛ بنابراین، مهم‌ترین شاخص‌های مؤلفه افزونگی، سخت‌افزار، نرم‌افزار و نیروی انسانی هستند (Moteff,2012).

۴- پاسخ و بازیابی[9]: به‌طور بالقوه به‌عنوان انعطاف‌پذیری سازمانی[10] و بالعکس تعریف می‌شود. اهداف مؤلفه واکنش و بازیابی، توانایی واکنش و بازیابی مؤثر و سریع در برابر حوادث مخرب است. کارایی این مؤلفه با تکمیل تلاش‌ها برای طراحی، آماده‌سازی و مانور[11] در پیشرفت حوادث مشخص می‌شود. ممکن است راهبرد بین واکنش و بازیابی متفاوت باشد. بازیابی در طراحی، قبل از حوادث برای کشف فرصت‌ها در نظر گرفته می‌شود تا ریسک‌های بعدی کاهش

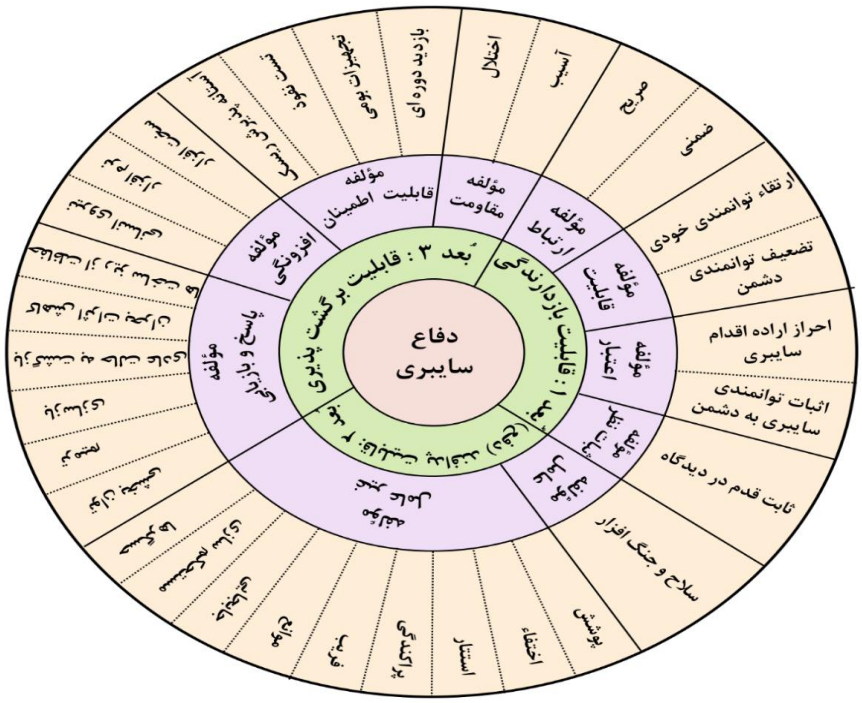
1-Redundancy
2-installations
3-spare capacity
4-Switched
5-diverted to
6-telecommunications
7-flexibility to meet peak demand
8-components
9-Response and Recovery
10-organisational resilience
11-exercise

یابد و یا تاب‌آوری در زیرساخت، طی مرحله بازیابی، ایجاد گردد. مهم‌ترین شاخص‌های این مؤلفه را حفاظت از زیرساخت‌ها، کاهش اثرات بحران، بازگشت به حالت عادی، بازسازی، ترمیم و توان‌بخشی تشکیل می‌دهند (Ibid,2012).

با در نظر گرفتن ابعاد بازدارندگی، پدافند و برگشت‌پذیری به‌عنوان ارکان اصلی دفاع سایبری و ترسیم مؤلفه‌ها و شاخص‌های هر مؤلفه، مدل شکل شماره (۲) به‌عنوان نقشه‌ای زیرساختی برای ترسیم هر نوع الگوی کارآمد دفاع سایبری به وجود می‌آید. متناسب و مقرون‌به‌صرفه بودن هر یک از مؤلفه‌های متفاوت در سراسر نه بخش از زیرساخت‌های ملی با توجه به انواع مختلف زیرساخت‌ها و فرصت‌های فنی است. هر یک از این مؤلفه‌ها می‌تواند مورد استفاده قرارگرفته یا برای سطوح مختلف در نظر گرفته شود. با توجه به طیف وسیعی از خطرات، سازمان‌ها باید ترکیبی از پاسخ تمام این چهار مؤلفه، به‌منظور توسعه راهبرد که می‌خواهد پیاده شود، مقرون به‌صرفه‌ترین و متناسب‌ترین پاسخ مدیریت ریسک به خطرات و تهدیدات را انتخاب کنند.

جدول (۳): مؤلفه‌های بعد برگشت‌پذیری در دفاع سایبری

مؤلفه	شاخص	منابع
مقاومت	۱- ..... آسیب ۲- ..... اختلال	Cyber Resilience – Implementing the Right Strategy,2013 : The components of Infrastructure Resilience - Crown Copyright 2011
قابلیت اطمینان	۱- ..... بازدید دوره‌ای ۲- ..... تجهیزات بومی ۳- ..... آزمون نفوذ ۴- ..... آستانه ریسک‌پذیری	Cyber Resilience – Implementing the Right Strategy,2013 : The components of Infrastructure Resilience - Crown Copyright 2011 Cyber resilience in financial market infrastructures, 2014 Cyber Resilience Malta Association of Risk Management, 2013
افزونگی	۱- ..... سخت‌افزار ۲- ..... نرم‌افزار ۳- ..... نیروی انسانی	Critical Infrastructure Resilience (Moteff ،2012) The components of Infrastructure Resilience - Crown Copyright 2011 CYBER RESILIENCE REVIEW, Homeland Security Office of Cybersecurity and Communications, 2014 Cyber Resilience Malta Association of Risk Management, 2013
پاسخ و بازیابی	۱- ..... حفاظت از زیرساخت‌ها ۲- ..... کاهش اثر بحران ۳- ..... بازگشت به حالت عادی ۴- ..... بازسازی ۵- ..... ترمیم ۶- ..... توان‌بخشی	Critical Infrastructure Resilience (Moteff ،2012) Cyber Resilience – Implementing the Right Strategy,2013 : The components of Infrastructure Resilience - Crown Copyright 2011 Cyber resilience in financial market infrastructures,2014



شکل (۲): مدل مفهومی الگوی دفاع سایبری

جمع‌بندی مدل مفهومی: برای دستیابی به این مدل، نخست مبانی نظری و اسناد بالادستی کشور در حوزه این پژوهش موردمطالعه قرار گرفت، بر اساس تعریف دفاع ابعاد اصلی الگو شامل قابلیت بازدارندگی، قابلیت پدافند و قابلیت برگشت‌پذیری احصا و مورد تأیید خبرگان پژوهش قرار گرفت. سپس با گزینش چند کشور و مطالعات تطبیقی اسناد راهبردی قابل‌دسترس آن‌ها، مؤلفه‌ها و شاخص‌های دفاع سایبری بر اساس تکنیک خوشه‌بندی در تحلیل محتوا احصاء و در نهایت مدل مفهومی دفاع سایبری در سه بعد، ده مؤلفه و سی‌ودو شاخص ارائه گردید.

نتیجه‌گیری:

روی دیگر سکه گسترش نفوذ فضای سایبر در لایه‌های مختلف زندگی انسانی برای ارتقاء سطح زیست بشری، آسیب‌پذیری‌ها و تهدیدات به‌شدت فزاینده‌ای است که می‌تواند مخاطرات سهمگینی را برای بشر به همراه داشته باشد. در این میان، اراده بهره‌گیری از این فضا از سوی دشمنانی که امنیت و بقای ایران را در عرصه بین‌المللی هدف قرار داده‌اند، ایجاد الگوی کارآمد دفاع سایبری را اجتناب‌ناپذیر ساخته است. دستیابی به چنین الگویی، مستلزم داشتن طرح‌واره و مدل جامع مفهومی به‌عنوان زیرساخت شناختی برای دفاع سایبری است.

بازدارندگی از ابعاد اساسی دفاع سایبری است که مانع ذهنی محکمی را برای حریفان ایجاد می‌نماید تا با افزایش هزینه‌های تهاجمات سایبری، در مرحله طرح‌ریزی و قبل از آن، عاملان عملیات تهاجم را با تشتت و تزلزل مواجه سازد. استحکام چنین مانعی بستگی به میزان قابلیت، توانمندی و ظرفیت‌های بالقوه پاسخگویی دارد که به نسبت بین قدرت سایبری در مقایسه با دشمن بستگی دارد. با توجه به وضعیت نظام جمهوری اسلامی ایران و تقابل دائمی استکبار جهانی و نظام سلطه با آن، تهیه و تأمین تجهیزات سایبری، از مشکلات اساسی در حوزه دفاع سایبری است و ضرورت دارد اقدامات لازم در زمینه بومی‌سازی تجهیزات سخت‌افزاری و نرم‌افزاری به‌ویژه در بخش دفاع و ایجاد زنجیره تأمین امن صورت پذیرد.

با توجه به اهمیت فضای سایبر و جدی بودن تهدیدات در این عرصه، لازم است بین نخبگان فکری و ابزاری کشور در خصوص ضرورت حفاظت از این فضا، اجماع ایجاد شود و حساسیت‌های ملی لازم به‌منظور افزایش مؤلفه اعتبار به‌مثابه ضرورت اثبات توانمندی سایبری و ضرورت پاسخگویی به هر حمله سایبری ایجاد شود. به علاوه، باید کانال‌های لازم انتقال پیام‌های ضمنی و صریح هشدار به حریفان برای ارتقاء سطح بازدارندگی ایجاد شوند.

به‌منظور کاهش حداکثری اثر هرگونه تهاجم یا تهاجمات سایبری، لازم است سامانه‌های پدافند غیرعامل سایبر در حوزه‌های مختلف زیرساخت‌های فناورانه، اقتصادی، اجتماعی، فرهنگی و نظامی مورد توجه قرار گیرد. گسترش پدافند عامل باید در امتداد اجماع نخبگان فکری و ابزاری در رابطه با دفاع سایبری در نظر گرفته شود که به لایه‌های اجتماعی تا کاربران اینترنت در جامعه شبکه‌ای تسری می‌یابد. تنها در این شرایط است که بخش‌های دولتی و خصوصی زیرساخت‌های پدافند غیرعامل را قبل از عملی شدن هر طرح و برنامه‌ای فراهم خواهند آورد. توجه به شاخص‌های پوشش، اختفاء، استتار، پراکندگی، فریب، موانع، جابجایی، مستحکم‌سازی و

حسگرها، آسیب‌های عملی شدن هر تهدید را به حداقل خواهند رسانید. در صورت بروز حمله سایبری، بنا به مقتضیات محیط‌های داخلی و خارجی و نیز محیط‌های روانی و عملیاتی لازم است سلاح و جنگ‌افزار لازم به‌منظور پاسخ‌های مؤثر به‌عنوان پدافند عامل فراهم گردد.

بعد برگشت‌پذیری در مرحله پس از حمله سایبری، ناظر بر حفظ خودآگاهی، حفاظت و بازیابی کارکردهای سیستم در کمترین بازه زمانی ممکن است. این بعد در ارتباط با مؤلفه مقاومت در برابر آسیب و اختلال و نیز مؤلفه قابلیت اطمینان است که موجب شناخت حد آستانه تحمل و کاهش هزینه‌های مقابله و افزایش حداکثر بهره‌وری در موقعیت بحران می‌شود. مؤلفه افزونگی نیز ناظر بر نیروهای انسانی، سخت‌افزار و نرم‌افزارها است که در طراحی الگوی سایبری باید مورد توجه جدی قرار گیرند. مؤلفه پاسخ و ارزیابی نیز برای حفاظت از زیرساخت‌ها، کاهش اثرات بحران، بازگشت به حالت عادی، بازسازی، ترمیم و توان‌بخشی است که ارتقاء این شاخص‌ها مستلزم هوشمندسازی کلیت و اجزای سیستم واحد سیاسی و نیز در نظر گرفتن تکثر و جایگزینی کارکردی برای اجزا است تا در صورت از کار افتادن یک جزء یا مرکزیت، کلیت سیستم به حیات خود ادامه دهد.

با توجه به نتایج پاسخ‌های پرسشنامه مدل مفهومی که حاکی از ارتباط خیلی خوب میان ابعاد، مؤلفه‌ها و شاخص‌ها می‌باشد، می‌تواند پیش‌زمینه طراحی نظام دفاع سایبری و معماری نهاد و فرایندهای کارآمد دفاع سایبری قرار گیرد. تدوین هرگونه راهبرد در عرصه دفاع سایبری پس از استحکام پایه‌های چنین نظام کارآمدی ممکن است که در آن وظایف کلیه نهادها مشخص شده باشد. تدوین راهبرد نیز مستلزم شناخت دقیق نقاط ضعف و قوت و نیز تهدیدات و فرصت‌ها در فضای سایبر است. مشخص شدن نقاط ضعف و قوت موجب تقویت سرمایه‌گذاری در توسعه دانش و فناوری در زمینه فضای سایبر می‌شود که این موضوع خود می‌تواند زمینه درنوردیده شدن مرزهای علمی و جهش در سایر ابعاد به‌ویژه در عرصه اقتصادی کشور گردد.

منابع:

- ***قرآن کریم***.
- کتب و بیانات ***امام خمینی (ره)*** قابل دسترس در صحیفه نور.
- کتب و بیانات ***امام خامنه‌ای (مدظله‌العالی)*** قابل دسترس در سایت www.khamenei.ir
- ازغندی، علیرضا و روشندل، جلیل، (۱۳۷۴)، ***مسائل نظامی و استراتژی معاصر***، تهران: انتشارات سمت.
- امیدوارنیا، محمدجواد، (۱۳۸۲)، ***امنیت در قرن بیست و یکم***، تهران: نشر مطالعات سیاسی و بین‌المللی.
- اصلانی‌مقدم، (۱۳۸۵)، ***جهانی‌شدن فناوری اطلاعات و ارتباطات و تأثیر آن بر امنیت ملی جمهوری اسلامی ایران***، دانشگاه عالی دفاع ملی.
- بلیکی، نورمن، (۱۳۹۳)، ***طراحی پژوهش‌های اجتماعی***، ترجمه حسن چاوشیان. تهران: نشرنی.
- جوزی‌خمسلویی، علی و جواهران، هدی، (۱۳۹۲)، ***تحلیلی بر نقش پدافند غیرعامل در امنیت راهبردی کلان‌شهرها***، تهران: مجله اطلاعات جغرافیایی (فضایی). شماره ۸۷.
- ماه‌پیشانیان، مهسا، (۱۳۹۰)، ***فضای سایبر و شیوه‌های نوین درگیری ایالات‌متحده آمریکا با جمهوری اسلامی ایران***، فصلنامه مطالعات فرهنگ – ارتباطات.
- قاسمی، فرهاد، (۱۳۸۶)، ***نگرشی بر طراحی مدل بازدارندگی سیاست خارجی ایران***، تهران: فصلنامه ژئوپلیتیک، سال سوم، شماره اول.
- قاسمی، فرهاد، (۱۳۸۸)، ***الزامات تئوریک بازدارندگی منطقه‌ای جمهوری اسلامی ایران***، تهران: فصلنامه روابط خارجی، سال اول، شماره سوم.
- قاسمی، فرهاد و کشاورزشکری، عباس، (۱۳۸۸)، ***نگرشی به سیستم بازدارندگی منطقه‌ای در روابط بین‌الملل: مطالعه موردی ایران و آمریکا***، تهران: رهیافت‌های سیاسی و بین‌المللی. شماره ۲۰.
- رشیدی، علی‌جبار؛ نقیان فشارکی، مهدی و داداش‌تبار احمدی، کوروش، (۱۳۹۲)، ***ارائه الگویی برای دفاع سایبری در آستانه حمله مبتنی بر پردازش رویدادهای پیچیده***، ششمین همایش فرامنطقه‌ای پیشرفت‌های نوین در علوم مهندسی، تنکابن: مؤسسه آموزش عالی آیندگان.
- ابراهیمی، شهروز؛ جالینوسی، احمد و قنواتی طیبه، (۱۳۹۳)، ***رویکرد دفاعی – تهاجمی جمهوری خلق چین در چارچوب فضای سایبر***، دوفصلنامه مطالعات قدرت نرم.
- عراقچی، سیدعباس، جوزانی‌کهن شاهین، (۱۳۹۶)، ***بهره‌برداری داعش از فضای مجازی***، فصلنامه

روابط خارجی، شماره ۳۳.

- نجات‌پور، مجید؛ محمدی، مصطفی؛ اصغری، امید و شهریاری، حیدر، (۱۳۹۱)، ***جنگ نرم و امنیت در فضای سایبر***، تهران: فصلنامه مطالعات راهبردی بسیج. سال پانزدهم. شماره ۵۴.

- Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE,Publication, Tallinn 2012
- Beggs, P. (2010). Securing the Nation's Critical Cyber Infrastructure. US Department Of Homeland Security.
- Retrieved from http://www.ocio.ca.gov/OIS/Government/events/documents/Patrick_Beggs.pdf
- Carvalho, V. A. Almeida, J. P. A. Fonseca, C. M. & Guizzardi, G. (2017). Multi-level ontology-based conceptual modeling. Data & Knowledge Engineering.
- Cyber Resilience – Implementing the Right Strategy,2013, The components of Infrastructure Resilience, Crown Copyright 2011
- Cyber resilience in financial market infrastructures, 2014, Bank for International Settlements
- Cyber Resilience Malta Association of Risk Management, 2013, The Federation of European Risk Management Associations
- Denning, D. E. (2014). Framework and principles for active cyber defense. Computers & Security, 40, 108-113.
- Gelinas, R. R. (2010). Cyberdeterrence and the problem of attribution.
- Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice DTIC Document. Retrieved from: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA 528033
- Herrington, L. & Aldrich, R. (2013). The future of cyber-resilience in an age of global complexity. Politics, 33(4), 299-310.
- Libicki, M. C. (2009). Cyberdeterrence and cyberwar. Santa Monica, Calif.: Rand.
- Moteff, John D. (2012). Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. Congressional Research Service US
- Penadés, M. C. Núñez, A. G. & Canós, J. H. (2016). From planning to resilience: The role (and value) of the emergency plan. Technological Forecasting and Social Change.
- Rajivan, P. Janssen, M. A. & Cooke, N. J. (2013, September). Agent-based model of a cyber security defense analyst team. In Proceedings of the Human Factors and Ergonomics Society
- Annual Meeting (Vol. 57, No. 1, pp. 314-318). Sage CA: Los Angeles, CA: SAGE Publications.
- Rowland, J. Rice, M. & Shenoi, S. (2014). The anatomy of a cyber power. International Journal of Critical Infrastructure Protection, 7(1), 3-11.

- The DOD cyber strategy, 2015, accessible: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf
- Uk national cyber sercurity strategy, 2016, accessible https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf