فصلنامه مطالعات جنگ
سال چهارم، شماره دوازدهم، بهار ۱۴۰۱
مقالهٔ پنجم از صفحه ۱۱۵ تا ۱۴۰

تعیین عوامل مؤثر بر ارزیابی قدرت پدافند سایبری ارتش جمهوری اسلامی ایران

محمد قاسمی[۱]
داود آذر[۲]
وحید سجادی[۳]

دریافت مقاله: ۱۴۰۱/۰۱/۲۵ پذیرش مقاله: ۱۴۰۱/۰۳/۱۴

چکیده

طیف فعالیت‌های پدافند سایبری بسیار گسترده و شیوه‌های آن متنوع است. متخصصان امنیت سایبری باید انواع حملات و راه‌های پیشگیری، تشخیص، تجزیه‌وتحلیل و کاهش آنها را درک کنند. آنها همچنین باید ساختار و وابستگی دارایی‌های فناوری اطلاعات و شبکه‌های سازمان و همچنین ارزش تجاری داده‌ها و نرم‌افزارهایی را که در این سیستم‌ها نگهداری می‌شوند، درک کنند. هم آنها باید یک دید کلی از ساختار سازمان، فرایندهای تجاری و افراد واقعی که در سازمان کار می‌کنند، داشته باشند. مراکز سایبری در ساختار نظامی ارتش جمهوری اسلامی ایران یک سازمان مهم به‌حساب می‌آیند و نتایج عملکرد آن نقش حیاتی در عملکرد و کارآمدی ارتش خواهد داشت. ازاین‌رو پایش عملکرد آن‌ها بر اساس الگوهای نوین ارزیابی، یکی از وظایف مهم فرماندهان عالی نیروهای مسلح به‌حساب می‌آید. این تحقیق با هدف ارائه عوامل مؤثر بر ارزیابی قدرت پدافند سایبری ارتش جمهوری اسلامی ایران انجام شده است. نوع پژوهش کاربردی، روش پژوهش توصیفی و رویکرد تحقیق کیفی و کمی است. نتایج حاصل از تجزیه‌وتحلیل کیفی و کمی این پژوهش، احصا هفت شاخص برای ارزیابی قدرت پدافند سایبری در دو حوزه پدافند غیرعامل و عامل و تعیین عوامل مؤثر بر ارزیابی قدرت پدافند سایبری ارتش جمهوری اسلامی ایران است.

واژگان کلیدی: فضای سایبر، قدرت سایبری، پدافند سایبری

---

[۱] - کارشناس ارشد
[۲] - عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا
[۳] - عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا

مقدمه

فضای سایبر برخلاف سایر حوزه‌های فیزیکی، محدود نیست. ابزارهای قدرت در این فضا به‌وسیله عوامل متعددی شکل‌گرفته است. تا زمانی که فضای سایبر به‌عنوان یک محیط‌زیست مطرح است، قدرت سایبر نیز سنجه‌ای برای توانایی استفاده از آن محیط قلمداد می‌شود. فناوری عامل اصلی محسوب می‌شود که بدون استفاده از آن، امکان بهره‌برداری از این فضای جدید وجود ندارد، اما نکته اساسی در این است که برخلاف سایر حوزه‌هایی که در انحصار بازیگران دولتی قرار داشت، فضای سایبر محدود به بازیگران صرفاً دولتی نیست. (زابلی‌زاده، ۱۳۹۷)

اطلاعات سایبری می‌توانند در فضای سایبر گردش کنند تا به‌وسیله جذب شهروندان کشورهای دیگر قدرت نرم به‌وجود بیاورند؛ یک برنامه تبلیغات سیاسی در اینترنت مثالی برای این موضوع است. همچنین اطلاعات سایبری می‌توانند به یک منبع قدرت سخت تبدیل شوند، که توانایی وارد کردن صدمه به اهداف فیزیکی در یک کشور دیگر را دارد؛ برای مثال بیشتر صنایع مدرن و خدمات دولتی فرایندهایی دارند که توسط رایانه‌های متصل به سیستم‌های کنترل نظارتی و جمع‌آوری داده پردازش می‌شود، نرم‌افزار مخربی که به این سیستم‌ها وارد می‌شود، می‌تواند برای خاموش کردن فرایندی که آثار کاملاً فیزیکی دارد برنامه‌ریزی شده باشد؛ برای مثال یک هکر یا یک حکومت، برق یک شهر مانند شیکاگو یا مسکو را قطع کند که این خاموشی گسترده می‌تواند خساراتی بیشتر از بمباران این شهرها وارد کند. (Nye, 2010)

پس طیف فعالیت‌های پدافند سایبری بسیار گسترده است. شیوه‌های بین سازمان‌های مختلف و مجموعه‌های فناوری اطلاعات بسیار متفاوت هستند. متخصصان امنیت سایبری باید انواع حملات و راه‌های پیشگیری، تشخیص، تجزیه‌وتحلیل و کاهش آنها را درک کنند. آنها همچنین باید ساختار و وابستگی دارایی‌های فناوری اطلاعات و شبکه‌های سازمان و همچنین ارزش تجاری داده‌ها و نرم‌افزارهایی را که در این سیستم‌ها نگهداری می‌شوند، درک کنند. آنها باید یک دید کلی از ساختار سازمان، فرایندهای تجاری و افراد واقعی که در سازمان کار می‌کنند داشته باشند. (Tammet, 2021)

ضعف سیستم‌های ارزیابی و نظام کسب بازخورد، امکان تبادل اطلاعات لازم را برای رشد، توسعه و بهبود فعالیت‌های یک سازمان غیرممکن کرده و زمینه‌های بروز بحران‌های مدیریتی را در آن‌ها افزایش می‌دهد و نتیجه تداوم آن ممکن است انحلال و شکست سازمان‌ها را به دنبال داشته باشد. مراکز سایبری در ساختار نظامی ارتش جمهوری اسلامی ایران یک سازمان مهم به‌حساب می‌آیند و

نتایج عملکرد آن نقش حیاتی در عملکرد و کارآمدی ارتش خواهد داشت. برای اطمینان از وجود قدرت پدافند سایبری مناسب در ارتش جمهوری اسلامی ایران برای مقابله با تهدیدات لازم است، نسبت به وضعیت کنونی آگاهی حاصل شود، این امر نیازمند داده‌ها و اطلاعات است، تا از میزان ابهام‌های موجود کاسته شود، همچنین باید رویدادهای کلیدی و تأثیرگذار شناسایی شوند تا وضعیت این عوامل مؤثر در زمان حال مشخص شود و مسیرهای متفاوت مورد انتظار از هر عامل در آینده و تشخیص احتمال توسعهٔ هر یک نیز در نظر گرفته شود.

هدف از این پژوهش ارائه عوامل مؤثر بر ارزیابی قدرت پدافند سایبری ارتش جمهوری اسلامی ایران و سوال پژوهش حاضر، این است که عوامل مؤثر برای ارزیابی قدرت پدافند سایبری ارتش جمهوری اسلامی ایران کدامند؟

مبانی نظری

پیشینه‌های پژوهش

جلالی فراهانی(۱۳۹۶) در پژوهشی با عنوان ارائه راهبردهای پدافند غیرعامل کشور در برابر تهدیدات سایبری، بیان می‌کند: یکی از انواع تهدیدات نوین، تهدیدات سایبری، علیه زیرساخت‌های حیاتی و حساس سایبری و متکی به سایبر است، جهت مقابله با این تهدیدات جدید و فناورانه و همچنین کاهش آسیب‌پذیری‌های کشور در برابر آن‌ها، نیاز به راهبردهای دفاع غیرعامل کشور در برابر تهدیدات سایبری است. در این پژوهش پس از بررسی اسناد بالادستی نظام در حوزه‌های پدافند غیرعامل، فضای سایبر و امنیت، نسبت به شناخت محیط داخل و خارج و تجزیه‌وتحلیل آن‌ها، راهبردهای مربوطه تدوین گردیده است.

کافی (۱۳۹۹) در پژوهشی با عنوان شاخص‌های دفاعی – امنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی ایران مبتنی بر رویکردهای پدافند غیر عامل، بیان می‌کند: حیات اجتماعی کشورها بر پایه تداوم عملکرد زیرساخت‌های حیاتی و حساس آن‌ها استوار است از همین روست که کشورهای متخاصم تلاش می‌کنند تا مانع تداوم این کارکرد در کشورهای هدف شوند. امروزه، توسعه فناوری اطلاعات و فضای سایبری موجب شده است تا بخش‌های مهمی از کارکرد زیرساخت‌های حیاتی و حساس وابسته به این فضا شوند. در نتیجه وجود چنین وابستگی، امنیت

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

مفهوم شناسی متغیرهای پژوهش

فضای سایبر: فضای سایبر یک شبکه گسترده و پیچیده جهانی از ارتباطات باسیم و بی‌سیم است که نقاطی را در هر حوزه (زمین، هوا، دریا و فضا) به یکدیگر متصل می‌کنند. هسته اصلی این شبکه‌ها، زیرساخت‌های فناورانه متشکل از چندین شبکه محصور مجزا که به یک شبکه منطقی متصل هستند است که امکان انتقال داده را فراهم می‌کند. شناسایی این زیرساخت‌ها و عملیات آنها با تحلیل لایه‌های فضای سایبری، ابعاد محیط اطلاعات، متغیرهای محیط عملیاتی و سایر جنبه‌های فنی شبکه‌های باسیم و بی‌سیم انجام می‌شود. شبکه‌ها می‌توانند مرزهای جغرافیایی و سیاسی بین افراد، سازمان‌ها و سامانه‌ها را از بین برده و آنها را در سراسر جهان به یکدیگر متصل کنند. (Department of Army, 2017)

قدرت سایبری: قدرت سایبری، در چارچوب شاخص‌های قدرت سایبری ملی هنگامی است که یک کشور به طور مؤثر توانایی‌های سایبری را برای دستیابی به اهداف ملی خود، ایجاد می‌کند. برای تمایز بین قصد و توانایی کشورها در دستیابی به اهداف، اصطلاح جامعیت برای توصیف استفاده یک کشور از سایبر اختصاص داده می‌شود؛ برای دستیابی به اهداف متعدد جامع‌ترین قدرت سایبری

دارای بالاترین قصد و بالاترین توانایی برای دستیابی به بیشترین اهداف با استفاده از ابزارهای سایبری است. (Voo, 2020)

پدافند سایبری: مأموریت‌هایی برای حفظ توانایی استفاده از قابلیت‌های فضای مجازی آبی و محافظت از داده‌ها، شبکه‌ها، دستگاه‌های دارای فضای مجازی و سایر سیستم‌های تعیین شده با شکست فعالیت‌های مخرب در حال انجام یا قریب‌الوقوع فضای مجازی. (DOD Dictionary, 2021:60)

چارچوب نظری پژوهش

پدافند سایبری

پدافند سایبری توانایی‌های سازماندهی شده برای محافظت در برابر حمله‌ها، کاستن خسارت‌های ناشی از آنها و بازگشت سریع به وضعیت عادی در مقابل حمله سایبری است. یا دفاع سایبری به فعالیت‌هایی اشاره دارد که از سوی یک طرف برای محافظت از منافعش در برابر یک حمله، صورت می‌گیرد. دفاع مؤثر در سامانه‌های الکترونیکی اغلب بر مبنای تشخیص، جداسازی، گزارش‌دهی، بازگشت به وضعیت عادی و خنثی‌سازی قرار دارد. توانایی دفع یک حمله، می‌تواند راهبرد دفاعی مؤثری باشد. یک حمله تنها هنگامی مؤثر است که یک ضعف واقعی را مورد هدف قرار دهد. برای داشتن دفاع سایبری همه‌جانبه و یکپارچه در سراسر کشور، بایستی چهار دسته توانمندی‌ها را در کشور تولید و با تقویت نماییم:

۱. توانمندی‌های راهبردی: این بخش شامل تدوین سیاست‌ها، برنامه‌های راهبردی
۲. دستورالعمل‌های اجرایی: ایجاد وحدت فرماندهی در بخش سایبری، ایجاد ساختار سازمانی، توسعه بخش آموزشی و تخصیص بودجه به تمام قسمت‌های یادشده.
۳. توانمندی‌های علمی: لازمه دستیابی به دانش علمی، مطالعات بنیادی و نظریه‌پردازی در این زمینه است. هم چنین ایجاد ساختارهای لازم و زیرساخت‌های آموزشی و پژوهشی می‌تواند دستیابی به چنین توانمندی مهمی را تسهیل نماید.
۴. توانمندی عملیاتی: در این بخش بایستی توان دستگاه‌های کارفرما و نیز سایر دستگاه‌ها را به میزان کافی بالا برد تا بتوان توانمندی‌های عملیاتی را ارتقا داد. (اسدالله زاده، ۱۳۹۴: ۱۴۸)

اصول اساسی حاکم بر حوزه پدافند سایبری در جمهوری اسلامی ایران:

بر اساس اسناد بالادستی، اصول اساسی حاکم بر حوزه پدافند سایبری کشور به این شرح استخراج گردید:

- مصون‌سازی و پایداری فضای سایبر کشور
- یکپارچگی و وحدت فرماندهی پدافند سایبری کشور
- دفاع بومی همه‌جانبه و بازدارنده
- هوشمندی در دفاع
- روزآمدی و آینده‌نگری
- کاهش آسیب‌پذیری سایبری
- حفظ تداوم کارکرد سامانه‌های سایبری
- آمادگی و پایداری، نفوذناپذیری
- حفظ و صیانت از سرمایه‌های سایبری
- پیش‌دستی در شناخت تهدیدات
- اقتصادی سازی
- اشراف اطلاعاتی در فضای سایبری کشور
- دانش و فناوری بومی و مدیریت آن
- نفوذناپذیری و اقتدار
- بهداشت سایبری
- رعایت قوانین بین‌المللی
- بی اعتمادی به محصولات خارجی. (جلالی فراهانی، ۱۳۹۸)

اقدامات سایبری احتمالی علیه نیروهای مسلح، کارکنان، خانواده‌ها و وابستگان آن‌ها

- تخریب، انهدام، اختلال، فریب، جمع‌آوری اطلاعات، ازکارانداختن تجهیزات، ادوات و تسلیحات رزمی، پشتیبانی رزمی، پشتیبانی خدمات رزمی و سامانه‌های فرماندهی و کنترل نیروهای مسلح که متکی به سایبر است.
- نفوذ، جمع‌آوری و شنود اطلاعات از شبکه‌های فناوری اطلاعات نیروهای مسلح
- اختلال، فریب و نفوذ به حوزه شناختی (ادراک، باورها)، وابستگان نیرو مسلح و گروه‌های مقاومت
- دستیابی به بخش اطلاعات و داده‌های نیروهای مسلح به‌منظور جریان‌سازی علیه نیروهای مسلح
- جمع‌آوری اطلاعات فردی، تخلیه تلفنی، تهدید و ارعاب کارکنان و مرتبطین سایبری نیروهای مسلح
- القاء انواع دروغ، شایعه، اخبار جعلی به کارکنان و وابستگان از طریق فضای سایبر
- ذائقه‌سنجی، مهندسی اجتماعی و شکل‌دهی به ذائقهٔ کارکنان نیروهای مسلح
- دستیابی و پخش اطلاعات و داده‌های نیروهای مسلح به‌منظور جریان‌سازی علیه نیروهای مسلح
- القای ترس، ناامیدی و ناکارآمد نشان‌دادن نیروهای مسلح.

اقدامات احتمالی سایبری علیه کشور، که تهدیدات آن بر نیروهای مسلح اثرگذار است

- اختلالات در تبادلات و کارکردن تجهیزات و توانمندی‌های وابسته به سایر سازمان‌های کشوری
- اختلال در قابلیت‌ها، کارکرد و بهره‌برداری از اینترنت کشور
- جلوگیری و ممانعت از بهره‌برداری از سخت‌افزارها و نرم‌افزارهای متکی به سایبر
- جاسوسی، نفوذ و جمع‌آوری اطلاعات از دستگاه‌ها سازمان‌ها و نهادهای کشور وابسته به اینترنت و فضای سایبر

- تحریم و جلوگیری از دستیابی به اطلاعات موجود در فضای سایبر در حوزه علوم و فناوری‌های مختلف
- انجام پروژه‌های پیچیده بلندمدت سایبری و متکی به هوش مصنوعی برای کشور
- انجام عملیات روانی و جنگ شناختی بر علیه مردم کشور و نیروهای مسلح
- حمله به زیرساخت‌های دارای اتصال به اینترنت کشور.

پدافند غیرعامل

اهمیت پدافند غیرعامل

اهمیت پدافند غیرعامل در بیانات مقام معظم رهبری نمایان است که در هفتم آبان‌ماه سال ۱۳۹۱ می‌فرمایند: "پدافند غیرعامل مثل مصونیت‌سازی بدن انسان است. از درون ما را مصون می‌کند. معنایش این است که ولو دشمن تهاجمی هم بکند و زحمتی هم بکشد و ضرب و زوری هم بزند، اثری نخواهد کرد. این پدافند غیرعامل نتیجه‌اش این است. ببینید چقدر مهم است که ما این حالت را در کل پیکره کشور و جامعه در دستگاه‌های مختلف به وجود بیاوریم. کاری کنیم که همت ما فقط مصروف به این نباشد که دشمن را منصرف کنیم یا برای مقابله خودمان را آماده بکنیم. نه، کاری کنیم که ما مصونیت در خودمان به وجود بیاوریم. این با پدافند غیرعامل تحقق پیدا می‌کند؛ بنابراین، این مسئله، مسئله بسیار مهمی است که بایستی راه بیفتد". (کافی، ۱۳۹۹)

حوزه‌های آسیب‌پذیر دارایی‌های متکی به سایبری نیروهای مسلح

امروزه، گستره فضای سایبری تمام شئون و ابعاد زندگی بشری را دربرگرفته است و به‌عنوان قلمرو پنجم زندگی بشری بعد از زمین، دریا، آسمان و فضا شناخته می‌شود. فضای سایبر با سایر حوزه‌ها ارتباط دارد و در حوزه زیرساخت‌های حیاتی و حساس گسترش یافته است. همه فضاها در برابر تهدیدات آسیب‌پذیر هستند که اهم آسیب‌پذیری‌هایی فضای سایبر نیروهای مسلح به شرح زیر است:

- شبکه‌های ارتباطی و اطلاعاتی
- بانک‌های اطلاعاتی و مخازن ذخیره‌سازی داده‌ها
- زیرساخت‌های حیاتی و حساس
- سامانه‌های متکی به رایانه نرم‌افزار و سامانه‌های سخت‌افزاری
- تجهیزات و ابزارهای متکی به شبکه ارتباطات و داده
- سیستم‌عامل و نرم‌افزارهای پایه و کاربردی

- شبکه سراسری آرمان و شبکه داخلی نیروهای مسلح
- سرورها، سوئیچ‌ها، راه‌یاب‌ها و تأسیسات زیرساختی شبکه‌ها
- مرکز داده و پردازش اطلاعات
- نرم‌افزارهای مختلف کاربردی و ذخیره‌سازی
- سامانه‌های فرماندهی و کنترل
- نیروها، خانواده‌ها و همکاران نیروهای مسلح
- تأسیسات و تجهیزات مهندسی نیروهای مسلح متصل به اینترنت و شبکه‌های رایانه‌ای
- خودروها و تجهیزات رزمی هوایی، دریایی، زمینی و پدافند هوایی متکی به نرم‌افزار
- رادارها، سامانه‌های جمع‌آوری اطلاعات، ردیاب‌ها.

تمهیدات پدافند غیرعامل سایبری

باتوجه‌به انواع حمله‌های سایبری، مدیران هر سازمان که قصد استفاده از سامانه رایانه‌ای را داشته باشند در وهله اول نگران امنیت داده‌ها و اطلاعات سازمان می‌باشند که این نگرانی برای سازمان‌های نظامی به‌مراتب بیشتر است. مجموعه‌ای از افراد، دستورالعمل‌ها، داده‌ها، سخت‌افزار و نرم‌افزار سامانه را تشکیل می‌دهند. حال اگر از هر قسمت سامانه اطمینان کافی وجود داشته باشد. در واقع به امنیت دلخواه سامانه نیز حاصل می‌گردد. تضمین ایمنی مستلزم تغییر در قوانین، سیاست‌ها، فرهنگ و نقطه‌نظر کلی دررابطه‌با ایمنی سایبری است. در این راستا مشارکت بخش‌های خصوصی و دولتی جهت حمایت نظام از تهدیدها و به‌کارگیری مدل‌های جدید یکی از راه‌حل‌های ممکن به شمار می‌آید. ازآنجاکه بخش عمده تبادلات اطلاعاتی از طریق اینترنت صورت می‌پذیرد، تمهیداتی در سطوح مختلف برای حفظ ایمنی اطلاعات باید صورت گیرد. جهت تضمین ایمنی اطلاعات در سازمان‌ها مدل‌های تضمین ایمنی اطلاعاتی که امروزه در اکثر سازمان‌ها متداول هستند، راه‌حل‌هایی مطابق با لحظه وقوع مشکل ارائه می‌کنند.

تمهیدات مدیریتی و انسانی

تکنیک‌ها و ابزارهای مدرن، همه‌وهمه زائده تفکر و مغز نوپرداز انسانی است. ازاین‌رو لازم است تمهیدات انسانی زیر در برابر جمع‌آوری سایبری مدنظر قرار گیرد.

۱. استخدام و به‌کارگیری افراد متخصص و متعهد

در عرصه جنگ رایانه‌ای، افراد متفکر هستند و البته متعهد به اصول اخلاقی و شرافت انسانی می‌توانند مانند یک سپر حفاظتی عمل کنند. این سازمان‌های اطلاعاتی – نظامی با استخدام و به‌کارگیری هکرها و متخصصین امر رایانه دست به هجوم رایانه‌ای و جمع‌آوری سایبری اطلاعات می‌زنند. ازاین‌رو تا در برابر مغزهای متفکر دشمن، مغزهایی متفکر آرایش داد تا بتوانند در برابر حمله‌های و هجمه‌ها و یا جمع‌آوری اطلاعات دشمن مقابله‌به‌مثل کند و یا تهدیدات دشمن را خنثی کند.

۲. آموزش صحیح و اصولی نیروی انسانی

سازمان‌های نظامی باید به‌روز بوده و تمامی تکنیک‌ها و شیوه‌های جدید جمع‌آوری اطلاعات سایبری را به کارکنان خود آموزش داده و آنها را در این مورد مطلع سازند. این آموزش خود می‌تواند به‌عنوان یک عامل بازدارنده از بسیاری از نشت اطلاعاتی جلوگیری کند چراکه تجربه ثابت کرده که بسیاری از نشت‌های اطلاعاتی به طور مستقیم یا غیرمستقیم با عامل انسانی ارتباط دارد.

۳. کنترل بهینه و مؤثر نیروی انسانی

انسان‌ها به دلیل عدم پایداری خصوصیات و روحیات مربوطه همواره در معرض آسیب‌پذیری هستند و از سوی دیگر در اثر وسوسه‌های ناشی از پیشنهادهای دل‌فریب، بسیار آسیب پذیرند. ازاین‌رو کنترل مؤثر کارکنان یکی از مهم‌ترین کار ویژهٔ سازمان‌های نظامی است. این کنترل باید به نحوی نامحسوس و مؤثر باشد و درعین‌حال چنان سایه‌ای بر زندگی فرد بیفکند که شخص فکر کند هر آن و درهرحال تحت مراقبت و کنترل به شیوه‌های نامرئی و نامحسوس است.

۴. دور از دسترس قراردادن وسایل چون رایانه و به‌ویژه اینترنت در زمان جنگ و بحران

ابزار ارتباطی چون اینترنت وسیله‌ای است که هر ارتباطی با کمترین ردپایی در آن ممکن و مقدور است. تجربه جنگ‌های اخیر در سطح منطقه نشان داد که دشمن می‌تواند از طریق ارسال پیام‌های الکترونیکی، به افراد و کارکنان و افسران ارشد و رده میانی، آنها را جهت همکاری، اغوا کند. حتی اگرچند نفر و یا حتی یک نفر نیز تحت تأثیر فریب پیام ارسالی گردد، می‌تواند خسارت جبران‌ناپذیری به نیروهای خودی وارد سازد. از این حتی‌الامکان باید سعی کرد در زمان بحران و یا جنگ ارتباط کارکنان را با دنیای خارج به حداقل رسانید و بیشتر ارتباط را با ساختار فرماندهی برقرار کرد. (اسدالله‌زاده، ۱۳۹۴: ۱۴۵)

تمهیدات فنی

فناوری‌های تدافعی و محوری که اکنون توسط حوزه‌های تجاری و نظامی به کار گرفته می‌شوند لایه‌هایی از امنیت را به‌منظور ازبین‌بردن شکاف بین دو رویکرد زیر ایجاد می‌کنند.

۱. رایانه‌های قابل‌اعتماد نظامی مبتنی بر آزمون تحلیل رایج شبکه‌های امن اختصاصی با رمزنگاری قدرتمند

۲. فناوری‌های اطلاعاتی تجاری رایانه‌ها، سیستم‌عامل ویندوز یا لینوکس و شبکه‌ها (با مؤلفه‌های تکمیل‌کننده مانند دیوارهای آتش، پوشه‌های نرم‌افزاری، صدور مجوز کارت‌های هوشمند) به‌منظور مدیریت خطرپذیری و دستیابی به درجه معینی از امنیت برای فعالت در محیط غیر امن

فناوری‌های توانمند، امنیت موردنیاز را برای شبکه‌های ناهمگن پیچیده با مکمل‌های سامانه باز (که لایه‌هایی از حفاظت را برای محیط‌های بسته و امن و شبکه‌هایی که در آن باهم ارتباط دارند برقرار می‌کنند ایجاد می‌نمایند این لایه‌های مطمئن) پوشه‌های نرم‌افزاری، دیوارهای سخت‌افزاری یا حصارها برای پایگاه‌های داده سامانه‌های عامل و دیگر مؤلفه‌های نامطمئن تحت کنترلشان، امنیت ایجاد می‌کنند. فناوری‌های نوظهور، امنیت و بقا را در محیط شبکه‌های بزرگ به‌وسیله سازوکارهای شناسایی، عکس‌العمل و بازیابی حتی خود اصطلاحی خودکار افزایش می‌دهند. عوامل مطمئن انتظارات امنیتی را تأمین می‌کنند. (اسدالله‌زاده، ۱۳۹۴: ۱۴۶)

در این چارچوب باید اصول زیر را موردتوجه قرارداد:

۱. امنیت رایانه‌ای: یکی از مهم‌ترین نقاط ضربه‌پذیر سامانه‌های رایانه‌ای مهم، نرم‌افزارهای مدیریت داخلی رایانه‌ها است. در اکثر مواقع نرم‌افزارهای موردنیاز جهت کشف و خنثی‌کردن عوامل رخنه یا نفوذ رایانه‌ای به‌گونه‌ای مؤثر و کارآمد مورداستفاده قرار نمی‌گیرد. نکته اصلی اینجاست که مهم‌ترین روش حمله و سرقت رایانه‌ای، روش رخنه رایانه‌ای توسط هکرها و یا سارقین اینترنتی است. سامانه‌های رایانه‌ای، سازمان‌های اطلاعاتی همواره مورد هجوم هکرهای حریف قرار می‌گیرند. هکرها به دو شیوه عمل می‌کنند یا اطلاعات موجود در سامانه را به سرقت می‌برند و یا به عبارتی تخلیه اطلاعاتی می‌کنند و یا اینکه با دست‌کاری در اطلاعات سامانه و یا نفوذ دادن ویروس‌ها و یا کرم‌های مخرب، سامانه را مختل کرده و آن را آلوده می‌کنند. نرم‌افزارهایی وجود دارند که همچون یک دیوار آتشین مانع این دست‌اندازی می‌گردند و یا

لااقل از تبعات تخریبی آن می‌کاهند. لازم به ذکر است که هیچ‌گاه نمی‌توان با تعبیه نرم‌افزارهای مختلف امنیت مطلق را برای سامانه به وجود آورد. بلکه می‌توان آن را کاهش داد و یا به حداقل خود رسانید.

۲. تهدیدات خارجی: یک تهدید نسبت به امنیت رایانه‌ای، ناشی از افراد خارجی است که سعی در تجاوز به سامانه رایانه‌ای دارند؛ یعنی دسترسی الکترونیکی به سامانه برای دستیابی غیرقانونی به اطلاعات از راه دور و «سرقت اطلاعات» است. برخی از سارقان اطلاعات، جوانانی هستند که علاقه شدیدی به رایانه دارند و در پی ماجراجویی هستند و برخی عوامل دیگر هستند که تحت کنترل سازمان‌های اطلاعاتی دولتی قرار دارند.

۳. تهدیدات داخلی: خودی‌ها یعنی کسانی که دسترسی قانونی و مجاز به سامانه دارند، می‌توانند تهدیداتی جدی برای امنیت اطلاعات فراهم کنند؛ خودی‌ها، چه به‌وسیله سامانه اطلاعاتی دشمن به خدمت گرفته شده باشند، چه کارکنان ناراضی باشند و چه صرفاً بی‌دقت و اشتباه کار باشند، می‌توانند داده‌های حساس را تغییر داده و یا از بین ببرند و یا آنها را به دشمن نظامی یا رقیب اقتصادی، انتقال دهند.

۴. تهدیدات نرم‌افزاری: نرم‌افزارهایی که حاوی داده‌های «مغرضانه» هستند به لحاظ تشخیص می‌توانند بسیار مشکل‌آفرین باشند و خسارات تقریباً نامحدودی را برای فایل‌های حاوی برنامه و دیسک‌های ذخیره‌ای اطلاعات یک سامانه رایانه‌ای وارد آورند. این داده‌ها ممکن است ناشی از منابع گوناگون باشند، اما اغلب اوقات، ناشی از نرم‌افزارهایی هستند که به‌وسیله کاربری وارد سامانه می‌شوند که از وجود بخش‌های مستندسازی نشده داده‌ها، ناآگاه است. (اسدالله‌زاده، ۱۳۹۴: ۱۴۷)

در حوزه پدافند غیرعامل سایبری، برای همگرایی و هم‌راستایی با سایر حوزه‌های پدافند غیرعامل باید در ابتدا شاخص‌های سنتی پدافند غیرعامل در فضای سایبر معادل‌سازی شود و به سند راهبردی پدافند سایبری کشور توجه گردد.

معادل‌سازی شاخص‌های سنتی پدافند غیرعامل در فضای سایبر

به‌منظور استفاده صحیح از فواید فضای سایبری و پرهیز از مخاطرات آن لازم است از رویکردی استفاده شود که ضمن تسهیل در ارائه خدمات زیرساخت‌های حیاتی و حساس، مانع مخاطرات

ناشی از فضای سایبری شود. یکی از این رویکردها بهره‌گیری از شاخص‌های پدافند غیرعامل است. شاخص‌های پدافند غیرعامل در برابر تهدیدهای سایبری در سه حوزه منابع انسانی، فرایندها و فناوری قابل بررسی است. اما پیش از طرح شاخص‌ها لازم است تهدیدها متناسب با هر یک از حوزه‌های منابع انسانی، فرایندها و فناوری استخراج شود.

پدافند غیرعامل رویکردی است که ضمن تسهیل در ارائه خدمات زیرساخت‌های حیاتی و حساس با استفاده از اقدامات احتیاطی بدون تحمیل هزینه چندان موجب کاهش مخاطرات متوجه زیرساخت‌ها می‌شود. اما شاخص‌های سنتی پدافند غیرعامل در فضای سایبری چندان کاربردی ندارد و لازم است تا این شاخص‌ها با معادل‌سازی تبدیل به شاخص‌های متناسب با فضای سایبری شود. در نتیجه، نوعی معادل‌سازی نیاز است. شاخص‌های سنتی استتار، اختفا، پوشش، فریب، تفرقه، پراکندگی، مقاوم‌سازی، استحکامات و اعلام خبر طبق جدول ۱ تبدیل به شاخص‌های متناسب با فضای سایبر می‌شوند. (کافی، ۱۳۹۹)

جدول ۱ انطباق شاخص‌های پدافند غیرعامل با پدافند سایبری (کافی، ۱۳۹۹)

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

شاخص‌های متناسب با فضای سایبری شامل موارد زیر است: رمزنگاری داده‌ها (مخفی‌سازی اطلاعات)، محدودسازی حیطه عملکرد و کاهش وابستگی متقابل زیرساختی (تفرقه و پراکندگی)، چندلایه سازی، بومی‌سازی نرم‌افزاری و سخت‌افزاری و نیز منابع انسانی مجرب و متعهد و بهره‌گیری از فایروال (مقاوم‌سازی و استحکامات) و سامانه کشف و جلوگیری از رخنه (اعلام خبر). حال این شاخص‌ها در سه حوزه‌ای که کارکرد صحیح زیرساخت‌های حیاتی و حساس منوط به کارکرد مطمئن آنهاست، ارائه می‌شود. این سه حوزه عبارتند از: منابع انسانی، فرایندها و فناوری. متناسب با هر یک از این حوزه‌ها شاخص‌های پدافند سایبری ارائه شده است. در منابع انسانی ارائه آموزش،

آگاه‌سازی و استفاده از منابع انسانی بومی و متعهد اهمیت بسزایی در حفظ و تداوم کارکرد زیرساخت‌ها دارد. بسیاری از تهدیدها ناشی از عدم آگاهی و یا خیانت نیروهای غیربومی و یا غیر متعهد است. در فرایندها خلا تدوین سیاست دفاعی امنیتی و متولی اجرای آن، حیطه گسترده وسیع و سطح زیرپوشش قابل‌توجه خدمات هر زیرساخت و وابستگی متقابل آنها به یکدیگر خود تبدیل به یکی از خطرات بالقوه خودساخته برای کشور شده است که با محدودسازی حیطه عملکرد هر زیرساخت و کاهش وابستگی متقابل آنها به یکدیگر این تهدید به میزان قابل‌توجهی تقلیل پیدا می‌کند. چندلایه سازی و فرایند دفاع در عمق نیز این امکان را می‌دهد تا برای کلیه مخاطرات که قابل‌پیش‌بینی نیستند، لایه‌های متعددی را پیش‌بینی کرد و در نتیجه هنگام وقوع حملات غیرمترقبه و فاقد شواهد و قرائن چندلایه در برابر این حملات قرار داده می‌شود تا در نهایت یکی از لایه‌ها مانع از موفقیت حمله شود.

در فناوری مهم‌ترین چالش کشور وابستگی نرم‌افزاری و سخت‌افزاری به شرکت‌های بیگانه و خارجی است. در نتیجه، بومی‌سازی تدریجی سخت‌افزارها و نرم‌افزارها به میزان قابل‌توجهی این خطر را رفع می‌کند. استفاده از شبکه اینترانت داخلی حجم بسیاری از حملات و تهدیدها را کم می‌کند. بهره‌گیری از آزمایشگاه‌های تشخیص بدافزار در تجهیزات سخت‌افزاری و نرم‌افزاری وارداتی مانع تکرار وقایع تلخی مانند بدافزار استاکس نت می‌شود. رمزنگاری داده‌ها نیز خود به امکان دسترسی عوامل غیرمجاز را به داده‌های حساس و مهم نمی‌دهد. بسیاری از تهدیدها در زیرساخت‌ها ناشی از دسترسی غیرمجاز گروه‌های ناراضی و یا متخاصم است. استفاده از هانی پات نیز موجب انحراف مهاجم از هدف اصلی به یک هدف کاذب می‌شود و به این شکل هدف اصلی در امان می‌ماند. علاوه بر این، رفتار و پروفایل مهاجم نیز در این حمله قابل‌بررسی و تحلیل است و امکان اتخاذ اقدامات متقابل برای حفظ امنیت و دفاع از زیرساخت اصلی بهتر فراهم می‌شود. در این میان، وجود سامانه‌های کشف و جلوگیری از رخنه و فایروال‌ها نیز می‌تواند عامل دیگری در اطلاع از وقوع حمله و ممانعت از رخنه و کاهش مخاطرات ناشی ازاین‌گونه حملات باشد. (کافی، ۱۳۹۹)

اهداف کلان پدافند غیرعامل سایبری در سند راهبردی پدافند سایبری کشور:

- طراحی، پیاده‌سازی و اجرای نظام پدافند سایبری هوشمندانه، انحصاری، ابتکاری، عمیق، لایه به لایه، بومی، پیشگیرانه، شبکه‌ای، گسترش‌یافته و سلسله‌مراتبی، چابک و منعطف.

- ارتقای آمادگی دفاعی و بازدارندگی کشور در مقابل تهدیدات و حملات سایبری کشورهای متخاصم.
- طراحی، پیاده‌سازی و اجرای سامانه جامع رصد، پایش، مراقبت، کنترل و تشخیص و هشدار تهدیدات سایبری.
- طراحی، پیاده سازی و اجرای نظام جامع فرماندهی و کنترل یکپارچه و هوشمند پدافند سایبری.
- حفاظت، صیانت و پایداری سرمایه‌های سایبری کشور در مقابل تهدیدات و حملات سایبری دشمنان.
- ارتقا توانمندی فرماندهی و کنترل و مدیریت بحران سایبری در راستای تضمین تداوم و خدمت‌رسانی. ضروری به مردم و دستگاه‌های حیاتی و بازیابی وضعیت عادی.
- آموزش، تربیت و توانمندسازی سرمایه انسانی کارآمد متناسب با اقتضائات حال و آینده پدافند سایبری.
- تولید، مدیریت و بومی‌سازی دانش پدافند سایبری با به‌کارگیری ظرفیت‌های ملی.
- ایجاد زیست بوم سایبری ملی، بومی، امن و پایدار با اولویت زیرساخت‌های حیاتی و حساس سایبری.
- مشارکت دستگاه‌های دولتی، بخش خصوصی و نهادهای مردمی در پدافند سایبری.
- ارتقا فرهنگ سایبری (نیازسنجی، طراحی، تدوین محتوا، اجرا، نظارت و راهبری، آیا تغییر رفتار).
- سازمان‌دهی، آموزش، هدایت، کنترل و ارزیابی مداوم دستگاه‌های کشور در راستای کارایی دفاعی و نیل به بازدارندگی پدافندی.
- آرامش بخشی و هدایت افکارعمومی در برابر تهدیدات و ارائه اقتدار پدافند ملی سایبری.
- تعامل بین‌المللی در حوزه پدافند سایبری در چارچوب سیاست‌ها، مقررات و قوانین ابلاغی.
- ایجاد، حمایت و ارتقا ظرفیت‌های خوداتکا و توسعه‌یافته صنعت بومی پدافند سایبری (دولتی و غیردولتی) در تولید سامانه‌های اساسی پدافند سایبری.

- طراحی پیاده‌سازی و راهبری نظام پدافند سایبری با ویژگی بومی‌سازی استانداردها، رویه‌ها و روال‌های پدافند سایبری کشور.
- ایجاد، استقرار، پیاده‌سازی و راهبری نظام دفاع حقوقی و قانونی از منافع ملی کشور در حوزه سایبری.
- فرهنگ‌سازی، آموزش عمومی، سازماندهی، تمرین رزمایش و تولید آمادگی پدافند سایبری در دستگاه‌های اجرایی.(سند راهبردی پدافند سایبری کشور، ۱۳۹۴)

پدافند عامل

اکثریت مطلق فعالیت‌های پدافند سایبری عامل، همان‌طور که از نامش مشخص است، تدافعی است، با تمرکز بر پیشگیری، تشخیص و پاسخ به حملات. ازآنجاکه طیف مهاجمان بالقوه بسیار گسترده است، حمله پیشگیرانه به مهاجمان احتمالی یا حتی "هک کردن" غیرعملی است: نه‌تنها نمی‌دانیم به چه کسی حمله کنیم بلکه این کار هزینه بالای هم دارد. بااین‌وجود، یک منطقه خاکستری برای موارد خاص وجود دارد که در آن حمله سایبری تهاجمی ممکن است بهترین دفاع باشد. رایج‌ترین عنصر در منطقه خاکستری، در اصطلاح هانی‌پت است که در آن داده‌ها و سیستم‌های بی‌فایده مهم به نظر می‌رسند، به طور خاص برای جذب مهاجمان احتمالی و در نتیجه شناسایی اقدامات آنها قبل از هدف قراردادن دارایی‌های واقعی، ایجاد شده‌اند.

بر خلاف فعالیت‌های منطقه خاکستری، انجام تهاجم سایبری پیشگیرانه واقعی ابتدا مستلزم این است که ما بدانیم به چه کسی حمله می‌کنیم، یعنی لیست مخالفان ما باید به‌شدت محدود باشد. این فرض به طور معمول برای دولت‌های ملی صادق است. چندین کشور، به‌ویژه ایالات متحده، چنین عملیات سایبری تهاجمی را تنظیم و قانونی کرده‌اند و توانایی انجام عملیات واقعی را ایجاد کرده‌اند. (Tammet, 2021)

در نشریه مشترک عملیات سایبری در سال ۲۰۱۸، پدافند عامل به‌عنوان مأموریت‌هایی که برای دفاع از شبکه اطلاعاتی وزارت دفاع یا سایر نیروهای سایبری وزارت دفاع که دستور دفاع از آنها صادر شده باشد، در برابر تهدیدات فعال در فضای سایبری انجام می‌شود، تعریف شده است. مأموریت‌های عملیات سایبری تدافعی، به طور خاص به حفظ توانمندی نیروهای خودی و محافظت از داده‌ها،

شبکه‌های تجهیزات مرتبط سایبری و سایر تجهیزات و توانمندی‌هایی که در معرض مواجهه با تهدیدات سایبری هستند، اختصاص‌داده‌شده‌اند. این اقدامات در واقع برای زمان‌هایی که تهدیدات جاری، موفق به شکستن یا دورزدن اقدامات امنیتی و ایمنی انجام شده در قالب عملیات شبکه اطلاعاتی وزارت دفاع شده و یا احتمال شکست یا دورزدن آنها توسط تهدیدات وجود دارد، طراحی و اجرا می‌گردند. عملیات سایبری تدافعی تهدید محور بوده و به طور مستمر از اهداف عملیاتی پشتیبانی می‌کنند. هدف اصلی عملیات سایبری تدافعی، دفع تهدید جاری و/ یا بازگرداندن یک شبکه در معرض خطر به شرایط امنیتی و کارکرد عادی است. کارکرد اصلی عملیات سایبری تدافعی، پاسخگویی به فعالیت‌های غیرمجاز، هشدارها و اطلاعات تهدید علیه شبکه اطلاعاتی وزارت دفاع و پیشنهاد اقدامات اطلاعاتی، ضد اطلاعاتی، اجرای قانون و سایر قابلیت‌های نظامی، در صورت نیاز، است. این عملیات همچنین دربرگیرنده اقدامات فعال برای به دام انداختن تهدیدات داخلی پیشرفته‌ای که اقدامات امنیتی جاری را نادیده گرفته یا از آنها عبور می‌کنند، نیز هست. در نهایت، عملیات سایبری تدافعی شامل اقداماتی است که برای محافظت از فضای سایبری خودی از اقدامات دشمنان و رقبا طراحی شده است. عملیات سایبری تدافعی می‌تواند به‌عنوان پاسخ به حملات، نفوذ، تجاوز یا اثرات بدافزار به شبکه اطلاعاتی وزارت دفاع یا سایر دارایی‌هایی باشد که وزارت دفاع مسئولیت اداره آن را برعهده دارد. اغلب، اقدامات عملیات سایبری تدافعی، در شبکه دفاع شده انجام می‌شود. مأموریت‌های عملیات سایبری تدافعی وزارت دفاع، با رویکرد دفاع در عمق، لایه به لایه و سازگار، به همراه عناصر پشتیبان محافظت فیزیکی و دیجیتال متقابل انجام می‌شود. یک ویژگی کلیدی فعالیت‌های عملیات سایبر تدافعی وزارت دفاع، دفاع سایبری فعال است. فعالیت عملیات سایبری تدافعی می‌تواند منجر به پیگیری فعالیت‌هایی نظیر اقدامات اضافی (تکمیلی) امنیتی سایبری، جمع‌آوری اطلاعات و یا توسعه اهداف عملیات سایبری تهاجمی شود. گزارش فعالیت‌های غیرمجاز شبکه و ناهنجاری‌ها، داده‌های موجود را برای شناسایی روند و اقدامات دفاعی مناسب افزایش می‌دهد. (DOD, 2018)

اغلب مأموریت‌های عملیات سایبری تدافعی، از نوع اقدامات داخلی هستند که شامل ردیابی تهدیدات جاری و پیشرفته فعال تهاجمی داخلی، در کنار اقدامات فعال و فعالیت‌های ضد تهدید داخلی و نیز واکنشی به‌کاررفته برای مقابله با این تهدیدات و نیز کاهش اثرات مخرب آنها می‌باشند. اقدامات دفاعی داخلی عملیات سایبری تدافعی، برای شناسایی تهدیدهای داخلی اجرا می‌شوند و می‌توانند در برگیرنده اقدامات شناسایی در داخل شبکه اطلاعاتی وزارت دفاع برای مکان‌یابی تهدیدات داخلی هستند و می‌تواند به فعالیت غیرمجاز، هشدارها و اطلاعات تهدید پاسخ دهد. این تهدیدات داخلی می‌توانند ناشی از ابزارهای امنیتی سایبری به‌کاررفته در شبکه باشد. اقدامات دفاعی داخلی عملیات سایبری تدافعی به‌منظور تضمین دسترسی سریع فرماندهان نیروهای رزمی مشترک به فضای سایبری، بر راه‌اندازی، مسیریابی و امن‌سازی مجدد، بازیابی و جداسازی شبکه‌های محلی تخریب شده و یا در معرض خطر متمرکز است.(DOD, 2018)

امروزه همگام با پیشرفت فناوری‌ها و گسترش بهره‌برداری از فضای سایبری، دفاع در برابر رخدادهای رایانه‌ای به یکی از دغدغه‌های اصلی همه دست‌اندرکاران فضای سایبری و حوزه فناوری اطلاعات و ارتباطات تبدیل شده است. در پاسخ به این دغدغه، گروه‌هایی به نام تیم پاسخگویی اضطراری رایانه‌ای[1] یا تیم پاسخگویی رخدادهای امنیتی رایانه‌ای[2] در دنیا تشکیل شده است. (Department of Army, 2017)

وزارت دفاع ایالات متحده مفهوم پدافند فعال سایبری را به‌عنوان قابلیت هماهنگ شده و زمان واقعی برای کشف، تشخیص، تجزیه‌وتحلیل و کاهش تهدیدها و آسیب‌پذیری‌ها تعریف کرده است. پدافند فعال سایبری طوری طراحی شده است که در دولت و همچنین زیرساخت‌های حیاتی قابل‌اجرا باشد. قابلیت پدافند فعال سایبری آگاهی وضعیتی را افزایش می‌دهد که معمولاً مستلزم سازماندهی جمع‌آوری داده‌ها، ادغام و اقدامات بین سیستم‌ها و سازمان‌های مختلف و مکان‌های جغرافیایی است؛ بنابراین، مسئله تفسیرپذیری خودکار داده‌های مبادله شده حیاتی می‌باشد که در

[1] - Computer Emergency Response Team (CERT)

[2] - Computer Security Incident Response Team (CSIRT)

محدوده هوش مصنوعی است. شش حوزه عملکردی پدافند فعال سایبری عبارت‌اند از: حس، تصمیم‌گیری، اقدام، پیام‌رسانی و کنترل و مدیریت مأموریت پدافند فعال سایبری.

طراحی پروتکل‌های بیان ساختاریافته تهدید اطلاعات[1] و مبادله الکترونیکی معتبر خودکار اخبار اطلاعاتی[2] گامی در همین راستا برای تبادل داده‌های ساختاریافته دقیق در مورد اطلاعات تهدید سایبری است. بیان ساختاریافته تهدید اطلاعات، سازمان‌ها را قادر می‌سازد تا اطلاعات تهدیدات سایبری را با یکدیگر به شیوه‌ای سازگار و قابل خواندن به‌وسیله ماشین به اشتراک بگذارند و به جوامع امنیتی این امکان را می‌دهد تا بهتر بفهمند که کدام حملات رایانه‌ای را بیشتر می‌بینند و آنها را سریع‌تر و بیشتر پیش‌بینی و یا به طور مؤثر پاسخ می‌دهند.

پس پدافند فعال سایبری را می‌توان با ویژگی‌های زیر توصیف کرد: یک راه‌حل جامع پدافند عامل دارای ویژگی‌هایی است که شامل: توانایی کار با سطوح قابل تصمیم‌گیری خودکار است که تشخیص و کاهش تهدیدهای مربوط به فضای سایبر را با سرعت امکان‌پذیر می‌کند. باید مقیاس‌پذیر باشد که بتوان در هر اندازه‌ای فعالیت کرد و در عین ایجاد و مصرف آگاهی وضعیتی مشترک، با سایر قابلیت‌های دفاع و قوی شدن شبکه به‌صورت یکپارچه کارکرد. سرانجام، این قابلیت‌ها باید به‌سرعت در دسترس باشند و به‌گونه‌ای طراحی شوند که به آنها اجازه دهد تا توسط بخش خصوصی و دولت ساخته و اداره شوند.

چارچوب پدافند فعال سایبری، مجموعه‌ای از قابلیت‌های سطح بالا را که برای انجام پدافند فعال سایبری، در هر مکانی در فضای سایبر لازم است را توصیف می‌کند. یک ساختار پیام‌رسانی اساسی باید وجود داشته باشد تا ارتباطات در زمان واقعی را با استفاده از پروتکل‌های استاندارد، رابط‌ها و طرح‌واره‌ها در بین سایر اجزاء فعال کند. سپس باید سنسورهایی وجود داشته باشند که داده‌ها را، در مورد وضعیت فعلی شبکه، تجزیه‌وتحلیل‌های منطقی برای درک وضعیت فعلی، تصمیم‌گیری

---

1 - STIX
2 - TAXII

خودکار برای تصمیم‌گیری در مورد نحوه واکنش به اطلاعات وضعیت فعلی، و قابلیت‌های عمل به آن تصمیمات برای دفاع از شبکه را گزارش دهند. (Tammet, 2021)

روش‌شناسی پژوهش

روش اجرای پژوهش توصیفی است، نوع این تحقیق کاربردی است و رویکرد این تحقیق آمیخته است.
صاحب‌نظران انتخاب شده همگی از فرماندهان و مسئولین و متخصصین آگاه در حوزه سایبری هستند که به موضوع تحقیق آشنایی کامل دارند؛ سؤال‌ها به‌گونه‌ای طراحی شده است که تمام ابعاد موضوع را پوشش دهد و محقق را در دستیابی به هدف تحقیق یاری دهد. سؤالات مصاحبه به گروهی از صاحب‌نظران در زمان‌های متفاوت ارائه شده و پاسخ‌های ارائه شده به‌منظور سنجش روایی سؤالات مصاحبه مقایسه شدند.
از اسناد و مدارک معتبر موجود در کتابخانه‌ها و مقاله‌های علمی از سایت‌های اینترنتی معتبر استفاده شده است و همچنین با استفاده از منابع متعدد پر ارجاع بر میزان اعتبار منابع افزوده شده و برای اطمینان از اعتبار منابع، از نظرات متخصصین موضوع و اساتید محترم استفاده شده است.
جامعه آماری این تحقیق، شامل کارکنان ارتش جمهوری اسلامی ایران در طیف درجات افسر ارشد و بالاتر هستند که دارای مدرک تحصیلی کارشناسی و بالاتر در رشته‌های مرتبط با علوم سایبری بوده و دارای حداقل ۱۰ سال سابقه خدمت در مشاغل فرماندهی، ستادی و فنی در حوزه فضای سایبر باشند. بر اساس برآوردهای انجام شده، تعداد اعضای جامعه آماری، ۷۹ نفر است. از طیف لیکرد برای کمی سازی نتایج پرسشنامه استفاده شده است و آلفای کرونباخ محاسبه شده برای پاسخ سؤالات جامعه آماری برابر ۸۴۴/. است که نشان دهنده پایایی سؤالات پرسشنامه است.

تجزیه‌وتحلیل داده‌ها ویافته‌های تحقیق :

تجزیه‌وتحلیل کیفی داده‌های تحقیق:

برای تعیین عوامل مؤثر بر ارزیابی قدرت پدافند سایبری ارتش جمهوری اسلامی ایران در حوزه پدافند غیرعامل، فرهنگ‌سازی و ارتقاء فرهنگ سایبری باعث افزایش آگاهی عمومی و تولید آمادگی پدافند سایبری می‌گردد. استفاده از تجربیات، راهبردها و استانداردهای بین‌المللی و انجام اصلاحات لازم در قوانین و سیاست‌های داخلی و اطمینان از اجرای قوانین در به‌دست آوردن قدرت پدافند سایبری مؤثر است.
فرماندهی و کنترل متمرکز، یکپارچه و هوشمند و توسعه توان کنترل و مدیریت بحران سایبری، در راستای تضمین تداوم و خدمت‌رسانی ضروری به مردم و دستگاه‌های حیاتی و بازیابی وضعیت عادی از موارد مؤثر در پدافند غیرعامل سایبری است.

پدافند غیرعامل در سه حوزه تمهیدات انسانی، تمهیدات فنی و فرایندها اجرا می‌گردد که اقدامات هر حوزه به شرح زیر است:

- تمهیدات انسانی شامل ارائه آموزش، آگاه‌سازی، استفاده از منابع انسانی بومی و متعهد و مجرب، کنترل مؤثر و بهینه است.
- تمهیدات فنی شامل استفاده از نرم‌افزارها و سخت‌افزارهای بومی، بهره‌گیری از آزمایشگاه‌های تشخیص بدافزار، بومی‌سازی نرم‌افزارها و سخت‌افزارها، استفاده از شبکه اینترنت داخلی، شیلد بودن مراکز داده، رمزنگاری داده‌ها، بهره‌گیری از فایروال و سامانه کشف و جلوگیری از رخنه، به‌روز بودن اطلاعات از شگردهای سایبری مهاجمان است.
- فرآیندها شامل عدم نیاز به نیروی انسانی و خوداتکا بودن سامانه پدافندی، نهادینه کردن اصول و ملاحظات پدافند غیرعامل در طرح‌های توسعه شبکه‌های ارتباطی و الکترونیکی، مستحکم‌سازی زیرساخت‌های سایبری، پراکندگی در زیرساخت‌ها و بانک اطلاعاتی با محدودسازی حیطه عملکرد هر زیرساخت و کاهش وابستگی متقابل آنها به یکدیگر، چندلایه سازی و فرایند دفاع در عمق، برگزاری رزمایش سایبری است.

در حوزه پدافند عامل سایبری توانمندی، بستگی به میزان تجهیزات، آموزش و راهکارهای مقابله‌ای در این حوزه دارد. رصد و پایش زنده رویدادها و رخدادهای امنیتی و مهم‌تر از آن پاسخگویی به‌موقع در برابر حوادث امنیتی امری ضروری است لذا پیشگیری، تشخیص و پاسخ به حملات سه حوزه مهم پدافند عامل هستند.

- پیشگیری: در این تحقیق، این واژه در فضای سایبر معادل حمله پیش‌گیرانه در سایر فضاها (زمین، هوا، دریا و فضا) است و با طراحی و پیاده‌سازی اهداف جعلی و فریب، در اصطلاح هانی‌پت، با هدف جذب مهاجمان احتمالی و در نتیجه شناسایی اقدامات آنها قبل از هدف قراردادن دارایی‌های واقعی، استفاده می‌گردد.
- برای تشخیص مطلوب، طراحی پروتکل‌های بیان ساختاریافته تهدید اطلاعات و مبادله الکترونیکی معتبر خودکار اخبار اطلاعاتی باید انجام شود. استفاده از هوش مصنوعی در تفسیر خودکار داده‌های مبادله شده باعث افزایش کیفیت و کمیت تشخیص می‌گردد پس باید یک ساختار پیام‌رسانی اساسی وجود داشته باشد تا ارتباطات در زمان واقعی را با استفاده از پروتکل‌های استاندارد، رابط‌ها و طرح‌واره‌ها در بین سایر اجزاء فعال کند تا با

جمع‌آوری داده‌ها، ادغام و اقدامات بین سیستم‌ها و سازمان‌های مختلف و مکان‌های جغرافیایی تشخیص صحیح و به موقع انجام شود.

- در پاسخ به حملات، دفع تهدید جاری و/ یا بازگرداندن یک شبکه در معرض خطر به شرایط امنیتی و کارکرد عادی هدف اصلی است. در ادامه حفظ توانمندی نیروهای خودی و محافظت از داده‌ها، شبکه‌های تجهیزات مرتبط سایبری و سایر تجهیزات و توانمندی‌هایی که در معرض مواجهه با تهدیدات سایبری هستند، مورد نظر است؛ پس باید با به‌کارگیری ظرفیت نیروی سازمانی سایبری، ظرفیت نیروی ویژه سایبری و پدافند سلسله‌مراتبی همراه با استفاده از فناوری‌های نوین جهت کاهش زمان واکنش، با رویکرد دفاع در نقطه تهاجم، دفاع در عمق، دفاع لایه به لایه، پدافند شبکه‌ای، به ردیابی تهدیدات جاری و پیشرفته فعال تهاجمی داخلی، پرداخت و با پاسخگویی به فعالیت‌های غیرمجاز، تهدید را دفع نمود. پس از دفع تهدید در صورت امکان لازم است اقدامات تکمیلی امنیتی سایبری، جمع‌آوری اطلاعات و توسعه اهداف برای عملیات سایبری تهاجمی انجام شود.

تجزیه‌وتحلیل کمی داده‌های تحقیق:

از نتایج آماری به‌دست آماده از جامعه پرسش شوندگان در حوزه پدافند غیر عامل چهار شاخص استفاده از تجربیات، راهبردها و استانداردهای بین‌المللی در تدوین قوانین و سیاست‌ها، فرماندهی یکپارچهٔ هوشمند بحران، فرهنگ‌سازی سایبری، توسعه همزمان و متوازن در سه حوزه تمهیدات انسانی، فنی و فرایندها دارای میانگین پاسخ‌های بالاتر ۴ بودند و در سطح زیاد به بالا مورد تأیید جامعه آماری قرار گرفتند. در حوزه پدافند عامل نیز سه شاخص متناسب با تهدید بودن تجهیزات، استفاده از هوش مصنوعی در تفسیر خودکار داده‌های مبادله شده، طراحی و پیاده‌سازی اهداف جعلی و فریب با میانگین بالاتر از ۴، در سطح زیاد به بالا مورد تأیید قرار گرفتند.

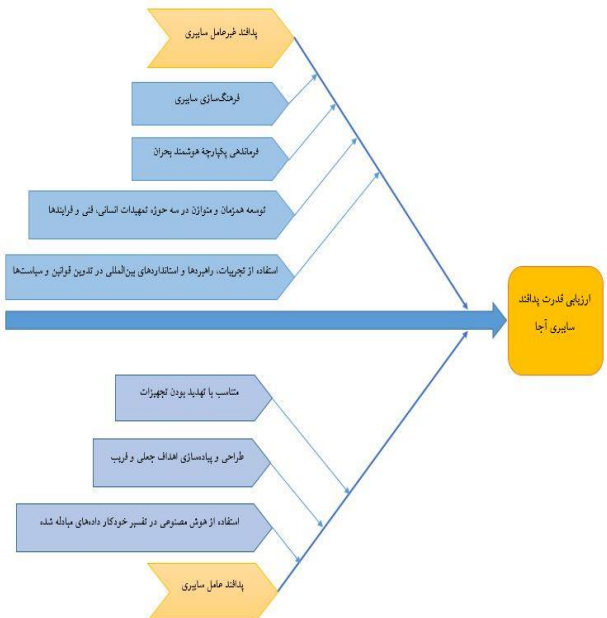
تجزیه‌وتحلیل آمیخته داده‌ها برای نیل به هدف پژوهش:

نتایجی که از تجزیه‌وتحلیل کیفی و کمی برای نیل به هدف تعیین عوامل مؤثر بر ارزیابی قدرت پدافند سایبری ارتش جمهوری اسلامی ایران حاصل شده است، حاکی از آن است که ۷ با میانگین بالاتر از ۴ برای ارزیابی حوزه پدافند سایبری در اولویت هستند و می‌توانند مدنظر قرار گیرند ترتیب اولویت این شاخص‌ها بر اساس نظر گروه پرسش‌شوندگان و میانگین شاخص‌ها به شرح جدول ۲ است:

جدول ۲ شاخص‌های مناسب برای ارزیابی پدافند سایبری

اولویت	شاخص	میانگین
۱	استفاده از هوش مصنوعی در تفسیر خودکار داده‌های مبادله شده	۴.۴۳
۲	فرماندهی پکپارچهٔ هوشمند بحران	۴.۴۱
۳	توسعه همزمان و متوازن در سه حوزه تمهیدات انسانی، فنی و فرایندها	۴.۲۹
۴	متناسب با تهدید بودن تجهیزات	۴.۲۴
۵	طراحی و پیاده‌سازی اهداف جعلی و فریب	۴.۲۰
۶	فرهنگ‌سازی سایبری	۴.۱۹
۷	استفاده از تجربیات، راهبردها و استانداردهای بین‌المللی در تدوین قوانین و سیاست‌ها	۴.۰۶

مدل مفهومی عوامل مؤثر بر ارزیابی قدرت پدافند سایبری آجا



نتیجه‌گیری و پیشنهادها

الف. نتیجه‌گیری

در پدافند غیرعامل، استفاده از تجربیات، راهبردها و استانداردهای بین‌المللی در تدوین قوانین و سیاست‌ها، فرماندهی پیکپارچهٔ هوشمند و توسعه همزمان و متوازن در سه حوزه منابع انسانی، فرایندها و فناوری مهم است. فرهنگ‌سازی در منابع انسانی و ارائه آموزش، آگاه‌سازی و استفاده از منابع انسانی بومی و متعهد اهمیت بسزایی در نیل به اهداف پدافند غیرعامل دارد. در فرایندها تدوین سیاست دفاعی امنیتی و متولی اجرای آن با استفاده از تجربیات، راهبردها و استانداردهای بین‌المللی، توجه به گسترده وسیع و سطح زیرپوشش قابل‌توجه خدمات هر زیرساخت و وابستگی متقابل آنها به یکدیگر که با محدودسازی حیطه عملکرد هر زیرساخت و کاهش وابستگی متقابل آنها به یکدیگر، تهدید به میزان قابل‌توجهی تقلیل پیدا می‌کند. چندلایه سازی و فرایند دفاع در عمق نیز این امکان را می‌دهد تا برای کلیه مخاطرات که قابل‌پیش‌بینی نیستند، لایه‌های متعددی را پیش‌بینی کرد تا در نهایت یکی از لایه‌ها مانع از موفقیت حمله شود. در فناوری بومی‌سازی تدریجی سخت‌افزارها و نرم‌افزارها به میزان قابل‌توجهی این خطر حمله را رفع می‌کند. بهره‌گیری از آزمایشگاه‌های تشخیص بدافزار در تجهیزات سخت‌افزاری و نرم‌افزاری وارداتی مانع موفقیت دشمن می‌گردد.

یک راه‌حل جامع پدافند عامل توانایی کار با سطوح قابل تصمیم‌گیری خودکار است که تشخیص و کاهش تهدیدهای مربوط به فضای سایبر را با سرعت امکان‌پذیر می‌کند. بنابراین، مسئله تفسیرپذیری خودکار داده‌های مبادله شده حیاتی می‌باشد که در محدوده هوش مصنوعی است. طراحی پروتکل‌های بیان ساختاریافته تهدید اطلاعات و مبادله الکترونیکی معتبر خودکار اخبار اطلاعاتی گامی در همین راستا برای تبادل داده‌های ساختاریافته دقیق در مورد اطلاعات تهدید سایبری است. بیان ساختاریافته تهدید اطلاعات، سازمان‌ها را قادر می‌سازد تا اطلاعات تهدیدات سایبری را با یکدیگر به شیوه‌ای سازگار و قابل خواندن به‌وسیله ماشین به اشتراک بگذارند و به جوامع امنیتی این امکان را می‌دهد تا بهتر بفهمند که کدام حملات رایانه‌ای را بیشتر می‌بینند و آنها را سریع‌تر و بیشتر پیش‌بینی و یا به طور مؤثر پاسخ می‌دهند.

ب. پیشنهادها

۱. پیشنهاد می‌گردد: معاونت طرح و برنامه آجا با همکاری سایر بخش‌های مرتبط از جمله معاونت فاوای آجا، معاونت اطلاعات آجا، معاونت عملیات، قرارگاه جنگ‌های نوپدید و مرکز پدافند غیرعامل، نسبت به تدوین و به‌روزرسانی قوانین و سیاست‌ها با توجه به تجربیات، راهبردها و استانداردهای بین‌المللی اقدام نماید.

۲. پیشنهاد می‌گردد: معاونت عملیات آجا با همکاری سایر بخش‌های مرتبط از جمله معاونت فاوای آجا، معاونت اطلاعات آجا، معاونت عملیات و قرارگاه جنگ‌های نوپدید، فرماندهی یکپارچه هوشمند برای بحران‌های سایبری طرح‌ریزی نماید و در رزمایش‌های سایبری به گونه‌ای طرح‌ریزی نماید تا این اقدام به صورت عملی تمرین شود.

۳. پیشنهاد می‌گردد: قرارگاه جنگ‌های نوپدید با همکاری سایر بخش‌های مرتبط از جمله معاونت فاوای آجا ، معاونت آموزش آجا، معاونت نیروی انسانی، ساحفاجا و مرکز پدافند غیرعامل، باید ضمن بازنگری فرهنگ سایبری (سازمانی و شخصی) اقدامات عملی برای ارتقاء آن را طرح‌ریزی و اجرا نماید.

۴. پیشنهاد می‌گردد: معاونت عملیات آجا با همکاری سایر بخش‌های مرتبط از جمله معاونت فاوای آجا، معاونت اطلاعات آجا و قرارگاه جنگ‌های نوپدید، تجهیزات سایبری آجا را از نظر تناسب با تهدیدات نوین بررسی نماید و کاستی‌ها را حتی‌الامکان با همکاری اداره تحقیقات و جهاد خودکفایی، مراکز دانشگاهی صنعتی به صورت بومی مرتفع نمایند.

۵. پیشنهاد می‌گردد: معاونت طرح و برنامه آجا با همکاری سایر بخش‌های مرتبط از جمله معاونت فاوای آجا و قرارگاه جنگ‌های نوپدید، در طرح‌ها و برنامه‌ها، توسعه همزمان و متوازن در سه حوزه تمهیدات انسانی، فنی و فرایندها را مد نظر داشته باشد.

منابع

منابع فارسی

- اسدالله زاده، محمد، خطیر، غلامرضا. (۱۳۹۴). پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات. چاپ اول. تهران. انتشارات دافوس آجا.
- جلالی فراهانی، غلامرضا، میررفیع، سیدعلی. (۱۳۹۸). ارائه راهبردهای پدافند غیرعامل کشور در برابر تهدیدات سایبری، فصلنامه مطالعات دفاعی استراتژیک. سال هفدهم. شماره ۷۵. ۲۵۹-۲۸۲
- زابلی‌زاده، اردشیر، وهاب‌پور، پیمان. (۱۳۹۷). قدرت بازدارندگی در فضای سایبر. فصلنامه علمی و پژوهشی رسانه و فرهنگ. پژوهشگاه علوم انسانی و مطالعات فرهنگی. سال هشتم. شماره اول.۴۷-۷۴
- سند راهبردی پدافند سایبری کشور. (۱۳۹۴). سازمان پدافند غیرعامل کشور و مرکز پدافند سایبری کشور.
- کافی، سعید. (۱۳۹۹). شاخص‌های دفاعی ـ امنیتی فضای سایبری زیرساخت حیاتی و حساس جمهوری اسلامی ایران مبتنی بر رویکرد پدافند غیر عامل. مجله سیاست دفاعی. سال ۲۸. شماره ۱۱۱. ۲۱-۱

منابع انگلیسی

- Department of Army. (2017). FM3-12. Cyberspace and Electronic Warfare Operations.
- Department of Defense. (2018). JP 3-12. cyberspace operations
- DOD. Dictionary of Military and Associated Terms. (2021)
- Nye, Joseph S. (2010) Cyber Power (The future of power in the 21th century). MIT-Harvard Minerva Project, Harvard Kennedy School.
- Tammet, Tanel. (2021). Autonomous Cyber Defence Capabilities. Autonomous Cyber Capabilities under International Law. NATO CCDCOE Publications. Chapter 3
- Voo, Julia. (2020). NATIONAL CYBER POWER INDEX 2020. Methodology and Analytical Considerations. BELFER CENTER.