تاریخ دریافت: ۱۴۰۰/۱۱/۱۲
تاریخ پذیرش: ۱۴۰۱/۳/۱۷

فصلنامه علوم و فنون نظامی
سال هجدهم، شماره ۶۰، تابستان ۱۴۰۱
صص ۱۲۳- ۱۰۳

عوامل موثر بر امنیت سایبری ارتش جمهوری اسلامی ایران (مطالعه موردی: ستاد ارتش جمهوری اسلامی ایران)

مهدی مهدوی پور*[۱]
داود آذر[۲]

نوع مقاله: پژوهشی

چکیده

گسترش تهدیدات نوظهور و فناورپایه از طرف دشمنان و بهره‌گیری از فضای سایبر برای انجام عملیات‌های مختلف علیه کشور و به خصوص نیروهای مسلح به گونه‌ای است که عدم توجه به آن می‌تولند موجب غافلگیری راهبردی شود. همچنین با توجه به وجود اطلاعات با ارزش در شبکه‌های ارتش جمهوری اسلامی ایران و امکان دستیابی، خرابکاری، افشاء و سرقت این اطلاعات ضرورت امنیت سایبری جهت مقابله با اینگونه فعالیت‌ها بیش از پیش روشن گردیده است. سرمایه گذاری گسترده دشمنان برای بهره‌گیری از فرصت‌های فضای سایبر به حدی است که انجام پژوهش‌های مختلف در این زمینه را طلب می‌کند. هدف پژوهش "شناسایی عوامل موثر بر امنیت سایبری ستاد ارتش جمهوری اسلامی ایران" و جامعه مورد مطالعه کلیه افراد و اسناد و مدارک، کتب، آئین نامه‌ها با موضوعات مرتبط با امنیت سایبری است. جامعه آماری، کارکنان ستاد ارتش ج.ا.ایران با مدرک تحصیلی مرتبط با حوزه سایبری بوده که تعداد آنها با احتساب ضریبی به علت طبقه بندی آماری برابر ۳۴ نفر است. روش جمع‌آوری اطلاعات، میدانی و کتابخانه‌ای بوده و گردآوری آن‌ها، به وسیله مصاحبه، پرسش‌نامه، اسناد و مدارک و سایت‌های اینترنتی بوده و برای تجزیه و تحلیل داده‌ها، از روش آمیخته استفاده شده است. نتایج حاصل بیانگر آن است که عوامل درون سازمانی شامل امن سازی تجهیزات، شبکه‌ها، نرم‌افزارها، رصد و پایش رخدادهای سایبری و واکنش به موقع به آن‌ها و ارتقاء دانش سایبری کارکنان و عوامل برون سازمانی شامل تهدیدات سایبری انسان ساز و طبیعی، عوامل موثر بر امنیت سایبری ارتش جمهوری اسلامی ایران را تشکیل می‌دهند.

واژگان کلیدی:
فضای سایبر، امنیت سایبری، عملیات سایبری، زیرساخت سایبری.

---

[۱] کارشناسی ارشد مدیریت دفاعی، دانشگاه فرماندهی و ستاد ارتش، تهران، ایران.
[۲] عضو هیئت علمی دانشگاه فرماندهی و ستاد ارتش، تهران، ایران.
* نویسنده مسئول: mahdi.mahdavi@chmail.ir

DOI: 10.22034/QJMST.2022.531717.1546

مقدمه

در حال حاضر، فناوری‌های نوین به صورت گسترده در ساختارها و سازمان‌های لشکری و کشوری استفاده می‌شود و باعث افزایش بهره‌وری و تاثیر مثبت بر ماموریت‌های محوله شده است. از سوی دیگر هزینه کم جنگ‌های سایبری نسبت به جنگ‌های سنتی، تغییر آرایش نظامی دشمنان، تأکید اسناد بالادستی کشور بر حوزه سایبری و تبدیل آن به زیرساختی برای دیگر زیرساخت‌های کشور باعث آشکار شدن یک حقیقت می‌شود: "تهدید اصلی نظامی دشمنان نظام مقدس جمهوری اسلامی ایران، از جنگ‌های سنتی به جنگ‌های سایبری تغییر کرده است." بنابراین کشور با حوزه جدید نظامی به نام حوزه سایبری روبه‌روست و گریزی از آن ندارد. حوزه‌ای کاملا جدی و بسیار مبهم، خطرناک و فاجعه‌بار که دشمن توجه ویژه‌ای به آن دارد (صاافتا، ۱۳۹۴).

در دنیای امروز بدلیل سادگی، دسترس‌پذیری بالا و هزینه کم سیستم‌های اطلاعاتی و سایبری، راهکارهای قدیمی و سنتی (غیرسایبری) به سرعت ناپدید می‌شوند و بدون وجود سیستم‌های اطلاعاتی، ارتباطی و سایبری قابل اتکا، بهره‌برداری کارا از قابلیت‌های نظامی میسر نیست.

اقدام امنیت سایبری به فرماندهان این اطمینان را می‌دهد تا به طور موثر مدیریت و انتشار اطلاعات را انجام داده و دارایی‌های سایبری خود را از خطرات مختلف محفوظ دارند. از این رو شناسایی عوامل موثر بر امنیت سایبری ستاد ارتش جمهوری اسلامی ایران گامی مهم جهت ارتقاء امنیت سایبری بوده و توجه ننمودن به این مساله موجب خسارت به دارایی‌های سایبری ستاد ارتش جمهوری اسلامی ایران می‌شود.

از طرفی فضای سایبر، فضایی منحصر به فرد است که در آن نرم افزارها و سخت افزارهایی که توسط بشر ساخته شده‌اند حکمرانی می‌کنند. جغرافیای فضای سایبری بی ثبات تر از سایر محیط‌ها است. کوه‌ها و اقیانوس‌ها را نمی توان جابجا کرد ولی سهم شما از فضای سایبری می‌تواند با قطع و وصل شدن یک سوییچ یا تزریق یک کد به یک روتر از بین برود یا به وجود آید یا جابجا شود (D Bryant, 2013).

با پیشرفت فناوری و افزایش پیچیدگی فضای سایبری، پیچیدگی دفاع در برابر حملات آن افزایش یافته است. حملات سایبری می‌توانند در شبکه‌های نظامی و همچنین زیرساخت‌های شبکه‌ای غیرنظامی پیامدهای ناگواری ایجاد کنند. ماهیت جنگ‌ها از حوزه‌ی نظامی به سایبری تغییر

پیداکرده است. در این حملات از طریق فضای سایبر به زیرساخت های مهم کشورها از راه دور حمله می شود. آنچه یک مهاجم با نفوذ به مرزهای سایبری دیگران به دست می آورد، از خاک و اشغال سرزمین بسیار ارزشمندتر است (جبار رشیدی، ۱۳۹۶).

هدف از این پژوهش "شناسایی عوامل موثر بر امنیت سایبری ستاد ارتش جمهوری اسلامی ایران" بوده و سوال اصلی " عوامل موثر بر امنیت سایبری ستاد ارتش جمهوری اسلامی ایران کدامند؟" است.

مبانی نظری و پیشینه‌های پژوهش

فضای سایبر

واژه‌ی فضای سایبری برای اولین بار در رمان علمی تخیلی «کرم سوزان» نوشته ویلیام گیبسون استفاده شد. گیبسون واژه فضای سایبری را از واژه سایبرنتیک الهام گرفته است که نوربرت وینر در دهه چهل میلادی بعنوان علم مناسبات انسان و ماشین، و مناسبات ماشین ها با یکدیگر اولین بار آن را تبیین نمود. گیبسون در باره استفاده از این واژه گفت: «من می خواستم این حس از حوزه‌ی دیگر را که یک حس گماشتگی در زندگی روزمره ام بود برانگیزم، حس جستجو به دنبال بیت های اطلاعات و قطعه ای از واقعیت که می‌تواند در عرصه‌ای که مورد نیاز بود (داستان های علمی، تخیلی)، قرار گیرد.»

سایبرنتیک از ریشه واژه‌ای یونانی به معنای هدایت، راهبری و سکان داری مشتق شده است. این واژه بعداً در جامعه پزشکی در رابطه با یکپارچه‌سازی انسان یا حیوان با ماشین آلات استفاده می شود. با این حال از زمان معرفی سایبر، این کلمه معانی مختلفی به خود گرفته است. این اصطلاح به طور موثری در تجارت، قانون و سیاست استفاده می‌شود. در حال حاضر این اصطلاح به دنیای ایجاد شده توسط اینترنت و سایر ارتباطات الکترونیکی اشاره کند.

درج کلمه "فضا" به این معنی است که سایبر باید دارای ابعادی است. یعنی فضای سایبری باید گستره‌ای را اشغال کند. بعلاوه، فضای سایبری به عنوان یک قلمرو جدید علاوه بر زمین، دریا، هوا و فضا در نظر گرفته شده با این تفاوت که آن‌ها طبیعی هستند ولی سایبر توسط انسان ایجاد شده است.

به طور کلی فضای سایبر یک دامنه جهانی در محیط اطلاعات متشکل از شبکه وابسته زیرساخت-های فناوری اطلاعات و داده‌های مقیم، از جمله اینترنت، شبکه‌های ارتباطی، سیستم‌های رایانه‌ای و پردازنده‌ها و کنترلرها است.

دامنه فضای سایبر

فضای سایبری یک دامنه فراگیر در محیط اطلاعاتی متشکل از شبکه‌های وابسته به زیرساخت-های فناوری اطلاعات و داده‌های مقیم است که در بر گیرنده اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و پردازنده‌ها و کنترل کننده‌های تعبیه شده است. نیروهای نظامی عملیات فضای سایبری را در قالب عملیات مستقل و یا مشرک انجام می‌دهند (DoD, 2016).

اگرچه فضای سابیر ارتش ج.ا.ایران یک دامنه مستقل در کنار دیگر دامنه‌ها است، اما قلمروهای فیزیکی را از طریق طیف الکترومغناطیس و شبکه‌های بی‌سیم و باسیم، فراگرفته و با حرکت داده‌ها در طول مسیرهای انتقال، از طریق لینک‌ها و گره‌ها در فضای سایبری و طیف الکترومغناطیس، سایر دامنه‌ها را به هم پیوند می‌دهد.

تاثیر فضای سایبر بر عملیات

فضای سایبر به نیروهای نظامی کمک می‌کند تا در صحنه عملیات مزیت کسب کنند. دسترسی گسترده به فضای سایبر به دیگران این امکان را می‌دهد که به طور مستقیم و غیرمستقیم و بدون حضور فیزیکی، یکپارچگی زیرساخت‌های حیاتی را به خطر بیندازند. اگرچه انجام عملیات سایبری به صورت مستقل در سطح تاکتیکی، عملیاتی یا استراتژیک امکان‌پذیر است، اما فرماندهان بیشتر آن را با سایر عملیات‌ها ادغام می کنند تا برای انجام مأموریت هم‌افزایی ایجاد کنند (DoD, 2018).

عملیات سایبری

در نیروهای نظامی از جمله ارتش ج.ا.ایران عملیات دنباله‌ای از اقدامات تاکتیکی با یک هدف مشترک یا یک موضوع متحد کننده است. بنا بر تعریف ستاد کل نیروهای مسلح ج.ا.ایران "عملیات سایبری به مجموعه اقدامات سایبری بر موجودیت‌های سایبری کشورهای بیگانه، سرویس‌های اطلاعاتی و گروه‌های معاند و جریانات برانداز و مرتبطین آن‌ها به منظور ایجاد دسترسی، سرقت، تخریب، تغییر اطلاعات یا فریب و مشغول سازی دشمن که با هدف اقدام

پیش‌دستانه و تهاجمی یا شناسایی و خنثی سازی اقدامات تهاجمی دشمن صورت می‌پذیرد"، است.

مأموریت سایبری

تمامی اقدامات در فضای سایبر ارتش ج.ا.ایران به غیر از فعالیت‌هایی که از فناوری اطلاعات برای رسیدن به اهداف غیر سایبری استفاده می‌کنند بخشی از ماموریت‌های آفند سایبری، پدافند سایبری و ایجاد، امن‌سازی، حفظ و نگهداری فضای سایبر سازمان است. این سه نوع مأموریت به طور کامل فعالیت‌های نیروهای نظامی در فضای سایبر را پوشش می‌دهد. یک عملیات موفقیت آمیز سایبری مستلزم یکپارچه سازی و هماهنگ نمودن این سه ماموریت است.

امنیت سایبری:

امنیت سایبری به کلیه اقداماتی که در فضای سایبر به منظور ممانعت از دسترسی غیرمجاز، استخراج یا صدمه به رایانه‌ها، تجهیزات الکترونیکی و اطلاعات جهت اطمینان از دسترس پذیری، یکپارچگی، احراز هویت، محرمانگی و انکارناپذیری است، گفته می‌شود (DoD, 2018). امنیت سایبری یک اقدام در راستای انجام ماموریت ایجاد، امن‌سازی، حفظ و نگهداری فضای سایبر ارتش ج.ا.ایران است. امنیت سایبری مبتنی بر شبکه و زیرساخت سایبری بوده و تهدید محور است.

تاریخچه امنیت سایبری البته نه به شکل امروزی به دهه ۶۰ میلادی و از زمانی که رایانه‌ها از شروع به انتقال داده‌ها به همدیگر کردند برمی‌گردد. تقریبا از همان زمان افرادی با نیت‌های متفاوت راه‌هایی برای اعمال مجرمانه و جاسوسی در این فضا ابداع کردند. اولین مورد گزارش شده مربوط به دستگیری یک جاسوس آلمان شرقی در یکی از شرکت‌های فرعی آی.بی.ام در آلمان غربی سال ۱۹۶۷ بوده است.

در دهه ۷۰ میلادی اولین تلاش‌ها برای ایجاد امنیت در فضای تبادل اطلاعات بین رایانه‌ها آغاز شد و آی.بی.ام توانست اولین الگوریتم رمز کردن داده‌ها برای تراکنش‌های مالی بانک‌ها را در سال ۱۹۷۴ ابداع کند. در دهه ۸۰ میلادی با جهانی شدن شبکه‌های کامپیوتری، هک و ویروس نیز فراگیر شدند که باعث شد مباحث ایجاد امنیت در شبکه‌های کامپیوتری به عنوان اولویت مطرح شوند. در سال ۱۹۹۷ میلادی وزارت دفاع آمریکا و پنتاگون با تعریف عملیات سایبری،

واژه امنیت سایبری را استفاده و اولین استراتژی‌های امنیت سایبری را تدوین نمودند (Warner, 2012).

عملیات سایبری بکارگیری قابلیت‌های فضای سایبر در جایی که منظور اصلی دستیابی به اهداف درون فضای سایبر و یا از طریق آن باشد. فرماندهان و نیروهای رزمی، عملیات سایبری را برای تاثیرگذاری در فضای سایبری یا از طریق آن به منظور پشتیبانی است از اهداف نظامی، بکار می‌گیرند. عملیات نظامی در فضای سایبری در قالب ماموریت‌های اجرایی از طریق ترکیبی از اقدامات ویژه به منظور نیل به هدف‌های تایید شده انجام می‌شود (DoD, 2018).

همزمان کردن و پشتیبانی از تلاش‌ها ماموریت‌های سایبری برای حفظ آزادی عمل و فعالیت در فضای سایبری، ضروری است. اقدامات سایبری، پشتیبان و حمایت کننده ماموریت‌های سایبری هستند. اقدامات سایبری از عملیات سایبری داخلی و خارجی یا هر ترکیبی از آن‌ها پشتیبانی می‌کنند (سجادی، ۱۳۹۹).

همانطور که در بالا اشاره شد امنیت سایبری مبتنی بر شبکه و زیرساخت سایبری بوده و تهدید محور است. زیرساخت سایبری، مجموعه‌ی نرم‌افزارها، سخت‌افزارها، افراد، فرایندها و قوانین، و ترکیب این موارد در قالب شبکه‌ها که باهم فضای سایبر را تشکیل داده و امکان ذخیره، پردازش و انتقال داده و اطلاعات و همچنین ارائه خدمات را فراهم می‌آورند، است (صاافتا، ۱۳۹۴).

همچنین تهدید سایبری به احتمال هر گونه رویدادی که قابلیت وارد نمودن ضربه به ماموریت‌ها، وظایف و دارایی‌های سایبری به واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام، افشاء، تغییر اطلاعات و ایجاد اختلال یا ممانعت از ارائه خدمات را داشته باشد، اطلاق می‌شود (صاافتا، ۱۳۹۴).

در ادامه به بررسی عواملی می‌پردازیم که موثر بر امنیت سایبری ارتش ج.ا.ایران می‌پردازیم. در حوزه امنیت سایبری ارتش ج.ا.ایران تمامی عوامل زنجیروار به هم متصل هستند. اگر هر کدام از این عوامل دچار نقصان شود، ایجاد آسیب از همان نقطه محتمل است. از این رو در بایستی سعی نمود در همه زمینه‌های امنیت سایبری اقدامات لازم را انجام داد تا در سازمان رخنه ایجاد نشود.

۱- امنیت برنامه‌های کاربردی

امنیت برنامه‌های کاربردی استفاده از نرم‌افزار، سخت‌افزار و رویکردهای فنی برای دفاع از برنامه-های کاربردی در برابر تهدیدات است. امنیت برنامه‌های کاربردی اقدامات متنوعی دارد که ابتدایی‌ترین اقدام دیوارآتش برنامه کاربردی نام دارد. امنیت برنامه‌های کاربردی را می توان با تعریف دقیق دارایی‌های بهبود بخشید (Srinivasan, 2017). امنیت برنامه‌های کاربردی ویژگی-های مختلفی مانند احراز هویت کاربران، رمزنگاری داده‌ها و واقعه نگاری دارد.

احراز هویت، عملی برای شناسایی هویت کاربران یا فرآیندها است (Oxford Languages, 2021). توسعه دهندگان برنامه‌های کاربردی از طریق احراز هویت کاربران اطمینان حاصل می‌کنند که تنها کاربران مجاز می‌توانند به برنامه دسترسی پیدا کنند. ساده‌ترین اقدام درخواست نام کاربری و رمز عبور هنگام ورود به برنامه است.

رمزنگاری، فرآیندی برای کدگذاری داده‌ها و اطلاعات به منظور جلوگیری از دسترسی غیرمجاز است (Oxford Languages, 2021). پس از اینکه کاربر وارد برنامه کاربردی شد اقدام دیگری با عنوان رمزنگاری داده‌های در حال انتقال اتفاق می‌افتد.

واقعه نگاری، یک روش نظام‌مند برای ثبت وقایع و رخدادها است (Oxford Languages, 2021). اگر رخنه امنیتی در یک برنامه کاربردی اتفاق بیفتد، به کمک واقعه‌نگاری می‌توان دریافت که چه کسی، چگونه و در چه زمانی به برنامه دسترسی پیدا کرده است.

۲- امنیت اطلاعات

امنیت اطلاعات، حفاظت از اطلاعات و عناصر حیاتی آن که شامل محرمانگی، یکپارچگی و دسترس‌پذیری است در فرآیند ذخیره سازی، انتقال و استفاده از طریق سیاست‌گذاری، آموزش، فناوری، مهارت آموزی و هوشیاری است (Whitman, 2012).

محرمانگی، وضعیت نگه داشتن یا نگه داشته شدن به صورت خصوصی یا مخفی است(Oxford Languages, 2021). در امنیت اطلاعات، محرمانگی ویژگی است که در آن، اطلاعات برای اشخاص، هویت‌ها و فرآیندهای غیرمجاز در دسترس یا آشکار نیست.

یکپارچگی، ثبات درونی یا نبود خرابی در داده‌های الکترونیکی است (Oxford Languages, 2021). در امنیت اطلاعات، یکپارچگی داده اطمینان حاصل کردن از صحت و تمامیت داده در طول عمر آن است.

دسترس‌پذیری، ویژگی قابل استفاده بودن یا فراهم بودن است (Oxford Languages, 2021). هر سامانه اطلاعاتی برای اینکه به اهداف خود برسد نیاز است که همیشه در دسترس باشد. این بدان معنی است که سامانه‌هایی که برای ذخیره و پردازش اطلاعات، حفاظت از اطلاعات و ارسال و دریافت اطلاعات استفاده می‌شوند باید همواره درست عمل کنند. همچنین در دسترس‌پذیر بودن شامل جلوگیری کردن از حملات منع سرویس است.

انکار ناپذیری، اطمینان حاصل می‌کند که فرستنده و گیرنده اطلاعات نتوانند تولید، ارسال، قبول و دریافت کردن اطلاعات را انکار کنند.

۳- امنیت شبکه

امنیت شبکه کنترل موارد ناخواسته‌ای همچون نفوذ به داخل، استفاده از یا صدمه زدن به ارتباطات در یک شبکه بوده و شامل مانیتورینگ سوءاستفاده‌ها، جستجو برای خطای پروتکل‌ها، مسدودسازی ارسال‌های تایید نشده و پاسخ بی‌درنگ و دقیق به اشکالات پیش‌آمده است(Stewart, 2021).

تهدیدات و حملات علیه امنیت شبکه از جنبه‌های مختلف قابل بررسی هستند. از یک نگاه حملات به دو دسته فعال و غیر فعال تقسیم می‌شوند و از دیدگاه دیگر مخرب و غیر مخرب و از جنبه دیگر می‌توان بر اساس عامل این حملات، آن‌ها را تقسیم بندی کرد. به هر حال حملات رایـج در شبکه‌ها بصورت ذیل است:

• حمله جلوگیری از سرویس: در این حمله، کاربر دیگر نمی‌تواند از منابع و اطلاعات و ارتباطات استفاده کند. این حمله از نوع فعال است و می تواند توسط کاربر داخلی و یا خارجی صورت گیرد.

• استراق سمع: در این نوع حمله، مهاجم بدون اطلاع طرفین تبادل داده اطلاعات و پیام‌ها را شنود می‌کند. این حمله غیر فعال است و می‌تواند توسط کاربر داخلی و یـا خـارجی صـورت گیرد.

• تحلیل ترافیک: در این نوع حمله مهاجم بر اساس یکسری بسته‌های اطلاعاتی ترافیک شبکه را تحلیل کرده و اطلاعات ارزشمندی را کسب می‌کند. این حمله یک نوع حمله غیر فعال است و اکثراً توسط کاربران خارجی صورت می‌گیرد.

• دستکاری پیام‌ها و داده‌ها: این حمله فعال است که در آن مهاجم جامعیت و صحت اطلاعات را با تغییرات غیر مجاز به هم می‌زند و معمولا توسط کاربر خارجی صورت می گیرد.

• جعل هویت: یک نوع حمله فعال است که در آن مهاجم هویت یک فرد مجاز شبکه را جعل می‌کند و توسط کاربران خارجی صورت می‌گیرد (مدیری، ۱۳۸۹).

مقابله با آسیب پذیری‌های امنیت شبکه در سازمان به شرح زیر است:

• برنامه‌ای برای حفاظت از فضای امنیت سازمانی: برای جلوگیری از مخاطرات و یا تشخیص آن‌ها سازمان باید برنامه مشخصی داشته باشد که در این برنامه چگونگی واکنش به موقع و بازیابی به هنگام در صورت موفقیت تهاجمات، مشخص شده باشد.

• پیشگیری: به منظور پیشگیری از مخاطرات، طبقه بندی اطلاعات، تجزیه و تحلیل مخاطرات، راهبردهای مقابله، حساس کردن و آموزش دادن پرسنل و تحقق بخشیدن به ممیزی‌های امنیت داخلی باید مورد توجه قرار گیرد. پیشگیری تمام سیاست‌هایی را شامل می‌شود که به منظور محدود کردن دامنه حوادث امنیتی و تهدیدات و مخاطرات به کار می‌رود. با تجزیه و تحلیل ریسک هم می‌توان اثر تهدید و هم احتمال آن را تقلیل داد.

• تشخیص: نصب ابزارهای تشخیصی، ردگیری و رهگیری اطلاعات و معماری هشدارهای نظارتی در این بخش حایز اهمیت است. نصب و راه‌اندازی ابزارهای تشخیص حملات و نفوذ برای یک سازمان بسیار حایز اهمیت است. همچنین نظارت و کنترل بر رفتارهای کاربران از طریق بررسی واقعه نگاری و دریافت هشدارهای لازم و به موقع هنگام آسیب‌های امنیتی باید مورد توجه قرار گیرد.

• واکنش: واکنش به موقع در صورت دریافت یک حمله و حادثه امنیتی و مسدود کردن حفره‌های امنیتی باید مورد توجه فراوان قرار گیرد.

• بازیابی: داشتن برنامه‌ای برای بازیابی و بازسازی اطلاعات و موجودیت‌ها در صورت تخاصم و حمله نیازمند طراحی سیاست‌های کارآمدی توسط مدیران ارشد سازمان است. (مدیری، ۱۳۸۹).

۴- طرح بازیابی از فاجعه

طرح بازیابی از فاجعه به دنبال معطوف ساختن تمامی منابع در دسترس برای بازگرداندن داده‌ها و اطلاعات سامانه‌ها بعد از رخ دادن فاجعه است. یک فاجعه را می توان به عنوان یک رویداد یا اتفاق ناگهانی یا یک حادثه طبیعی طبقه‌بندی کرد که باعث ایجاد آسیب‌های گسترده و زنجیروار می‌شود. طرح بازیابی از فاجعه به طور خاص بر روی فناوری تمرکز کرده و دستورالعمل‌هایی برای پاسخگویی به رخدادهای سایبر و حوادث طبیعی ارایه می‌دهد. وقتی طرح بازیابی از فاجعه به درستی طراحی و اجرا شود، بازیابی سامانه‌های حیاتی امکان پذیر شده و عملیات در سازمان ادامه می‌یابد.

بازیابی، توسعه و بکارگیری فعالیت‌ها و اقدامات مناسب بمنظور ایجاد ویژگی تاب‌آوری و بازیابی هر قابلیت یا خدمتی که بخاطر رویدادهای امنیت سایبری تضعیف یا مختل شده‌اند، است (صافتا، ۱۳۹۴).

۵- امنیت عملیات

امنیت عملیات جایگزینی برای برنامه‌های امنیتی مانند امنیت فیزیکی، امنیت اطلاعات و امنیت کارکنان نیست. امنیت عملیات در ارتش ج.ا.ایران برای بهبود اثربخشی عملیات به وسیله منع دشمن از دستیابی به شاخص‌های آشکار فعالیت‌های طبقه‌بندی شده یا حساس، قابلیت‌ها یا نیات عملیات است.

یکی از موارد مهم امنیت عملیات استفاده از مدیریت ریسک برای کشف تهدیدات و آسیب-پذیری‌های احتمالی در فرایندهای سازمان، نحوه فعالیت آنها و نیز نرم‌افزار و سخت‌افزاری مورد استفاده کارکنان است. نگاه به فرآیندها و عملکردها از زاویه دید سوم شخص، تیم های امنیت عملیات را قادر می سازد تا موارد نادیده گرفته شده را کشف کنند که این امر به اجرای اقدامات مناسب برای حفظ داده‌ها کمک شایانی می‌کند.

آنالیز تهدیدات، تعیین توانایی دشمن برای جمع‌آوری، پردازش، آنالیز و استفاده از اطلاعات است. از طرفی آنالیز آسیب پذیری‌ها ، شناسایی نقاط ضعفی است که احتمال می‌رود دشمن از طریق آن‌ها بتواند با استفاده از قابلیت جمع‌آوری خود رخنه ایجاد کند.

۶- آموزش کاربر نهایی

هر کاربری که سیاست‌های امنیت سایبری را اجرا یا دنبال نمی‌کند یک تهدید درون سازمانی است. گاهی اوقات سرعت عملیات و افزایش تقاضای فرماندهان برای دستیابی به اطلاعات، کاربر نهایی را وادار به استفاده از شیوه-های ضعیف امنیتی می‌کند (DoD, 2018).

حتی حرفه‌ای‌ترین تیم‌های امنیت سایبری برای حفاظت از سازمانی که کارکنان آن از تهدیدات سایبری آگاهی کافی ندارند، دچار مشکل خواهند شد. اطمینان حاصل کردن از اینکه کارکنان آموزش‌های مقدماتی امنیت سایبری را دریافت کرده‌اند امری ضروری است. نیازی نیست که آموزش‌ها پیچیده باشد، بهتر است که ساده و به اندازه باشد (Kim, 2017).

۷- تهدیدات دولتی

تهدیدات دولتی خطرناک‌ترین تهدید هستند زیرا دولت‌ها به منابع، کارکنان و زمان دسترسی دارند که این امکانات برای بازیگران دیگر فراهم نیست. دشمنان ممکن است با بکارگیری قابلیت-های سایبری، حملات سایبری یا جاسوسی سایبری را علیه سازمان ترتیب دهند که در بحث جاسوسی سایبری حتی متحدان و دوستان هم ممکن است دست به این عمل بزنند. دولت‌ها می‌توانند به طور مستقیم یا با استفاده از بازیگر سومی مانند شرکت‌ها، هکرها و سایر جایگزین‌ها، حملات را انجام دهند (DoD, 2018).

یکی از راه‌های مقابله با تهدیدات دولتی، بازدارندگی سایبری است. بازدارندگی آنگونه که در طول جنگ سرد به کار می رفت اصولاً به عنوان قابلیت‌های یک کشور برای تحویل مجازات پاسخ به یک حمله تعریف می شود. گرچه با نگرانی فزاینده از پیشرفت فناوری‌های سایبری مفهوم

۸- تهدیدات غیر دولتی

تهدیدات غیر دولتی توسط سازمان‌های رسمی و غیر رسمی که در محدوده مرز کشور خاصی نیستند انجام می‌شوند. این سازمان‌ها از فضای سایبر برای درآمد زایی، ارتباط با جامعه هدف، ارتباط با یکدیگر، سازمان‌دهی، طراحی عملیات‌ها، فشار بر دولتمردان، جاسوسی و انجام عملیات تروریستی در فضای سایبری استفاده می‌کنند (DoD, 2018).

بازیگران غیردولتی شامل سازمان‌ها و اشخاصی هستند که وابسته یا سازمان دهی شده توسط دولت مشخصی نبوده و بودجه آنان نیز از طریق دولتی تامین نمی‌شود که شامل شرکت‌های چند ملیتی، موسسات مالی خصوصی و نیز گروه‌های مقاومت، شبه نظامی و مسلح است.

۹- تهدیدات اشخاص و گروه‌های کوچک

اشخاص و گروه‌های کوچک افراد می‌توانند با استفاده از تکنیک‌های موجود و نیز بدافزارها، به فضای سایبر سازمان حمله کرده و یا از آن بهره‌برداری کنند. افراد با نیات گوناگونی دست به این کارها می‌زنند که می‌تواند به ازای هر فردی متفاوت باشد. این افراد با استفاده از آسیب‌پذیری‌ها یا داده‌های حساس به اهداف خود دست پیدا می‌کنند. برخی اوقات فعالیت‌های این افراد بدون اینکه متوجه باشند با ورود بازیگران دولتی و غیر دولتی منجر به تهدیدات پیچیده و خطرناکی می‌شود. همچنین افراد ممکن است با پشتیبانی بازیگران دولتی و غیر دولتی دست به این اقدامات بزنند (DoD, 2018).

۱۰- حوادث و مخاطرات طبیعی

زیرساخت‌های سایبری می‌توانند بر اثر اشباهات اپراتورها، حوادث و بلایای طبیعی مختل شوند. این وقایع غیرقابل پیش‌بینی ممکن است اثرات مخرب‌تری از عملیات دشمن به جای بگذارند (DoD, 2018).

بلایای طبیعی به پنج دسته زمین شناختی، آب شناختی، آب و هوایی، جوی و زیست شناختی تقسیم می‌شوند.

و در نهایت برای مقابله با تهدیداتی که امنیت سایبری ارتش ج.ا.ایران را به خطر می‌اندازد باید به مفاهیم زیر نیز توجه شود.

بازدارندگی سایبری

بازدارندگی تکامل یافته است. هدف اصلی و رو به تکامل بازدارندگی تشویق خویشتنداری در تمامی طرفین است. ابزار اصلی این کار نیز ایجاد درک متقابل میان بازیگران است تا از اینکه یک بازیگر اقداماتی علیه سایر بازیگران انجام دهد یا رفتاری از خود بروز دهد که برای طرف دیگر قابل قبول نباشد و باعث شود آن طرف پاسخ دهد جلوگیری کند. در این زمینه بازدارندگی تنها برای اجرای مجازات اقدامات دشمن به کار نمی رود بلکه وسیله‌ای برای شناسایی منابع حیاتی دوستان و دشمنان، برقراری ارتباط با

دوستان و دشمنان، درک متقابل از خطوط قرمز و واپایش امکان دست بردن به آتش جنگ به کار می‌رود (جاجودیا، ۱۳۹۶).

نگهداشت و بروزرسانی تجهیزات سایبری

راه موثر دیگر نگهداشت و بروزرسانی تجهیزات سایبری است. نگهداشت و بروزرسانی، تمهیدات لجستیکی و فنی است که در ماموریت‌ها و نقل و انتقالات نیرو به کار گرفته می‌شود. پیشرفت سریع در فناوری سایبری نیاز به نگهداشت و بروزرسانی قابلیت‌ها و تجهیزات سایبری را دوچندان کرده است. همواره باید توجه داشت که بروزرسانی و ارتقاء تجهیزات نیازمند سیاست‌گذاری‌های سایبری است. طرح‌های نگهداشت و بروزرسانی بایستی تجهیزات قدیمی را نیز شامل شوند. بسیاری از سامانه‌های حساس ماموریتی به سادگی بروزرسانی نمی‌شوند که این مورد می‌تواند با اضافه کردن لایه‌های حفاظتی بیشتر تعدیل شود. تجهیزات و زیرساخت سایبری با گذشت زمان و کارکرد زیاد یا بر اثر فعالیت‌های دشمن دچار فرسودگی یا خرابی می‌شوند که باید به سرعت تعویض یا تعمیر و بروزرسانی شوند (DoD, 2018).

پدافند غیرعامل

دفاع یا پدافند، مجموعه اقداماتی است که در برابر تهاجم دشمن انجام می‌شود تا از نفوذ دشمن جلوگیری کند، نیروی دشمن را منهدم نماید، خسارت و تلفات را به حداقل برساند، در قوای یک منطقه صرفه‌جویی کند و شرایط لازم جهت تهاجم را فراهم نماید. در یک تقسیم بندی اولیه، دفاع را به دو بخش دسته‌بندی می‌کنند: دفاع غیرعامل و دفاع عامل(ولی‌وند زمانی، ۱۳۹۶).

ستاد کل نیروهای مسلح پدافند غیر عامل را اینگونه تعریف می‌کند: پدافند غیرعامل به مجموع اقداماتی اطلاق می‌گردد که مستلزم بکارگیری جنگ‌افزار نبوده و با اجرای آن می‌توان از وارد شدن خسارت مالی به تجهیزات و تاسیسات حیاتی و حساس و مهم نظامی و غیرنظامی و تلفات انسانی جلوگیری نمود و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد. اقدامات پدافند غیرعامل شامل استتار، اختفا، پوشش، فریب، تفرقه و پراکندگی، استحکامات و سازه‌های امن و سامانه‌های اعلام خبر و خطر است.

پیشینه‌های پژوهش

با کاوش در پژوهش‌های انجام گرفته در راستای مباحث امنیت سایبری با مقالاتی روبه رو می‌شویم که از جنبه‌های مختلف به شناخت و بررسی مفاهیم مورد نظر این پژوهش پرداخته‌اند.

جدول (۱) پیشینه تحقیقات انجام شده

محقق	موضوع	نتایج
حسن کاویانی ۱۳۹۹	الگوی توسعه راهبردی منابع انسانی در حوزه امنیت سایبری نیروهای مسلح ج.ا.ایران	تبیین ابعاد و مولفه‌های الگوی نهایی توسعه راهبردی منابع انسانی در حوزه امنیت سایبری نیروهای مسلح ج.ا.ایران که شامل ۱۴ بعد و ۴۵ مولفه است.
سعید کاویانی ۱۳۹۹	شاخص‌های دفاعی‌ـامنیتی فضای سایبری زیرساخت‌های حیاتی و حساس جمهوری اسلامی‌ایران مبتنی بر رویکردهای پدافند غیرعامل.	شاخص‌های پدافند غیرعامل در حوزه سایبر علاوه بر شاخص‌های ستتی مانند استتار، اختفا، پوشش و فریب، تفرقه و پراکندگی، مقاوم‌سازی و استحکامات و اعلام خبر، شاخص‌های رمزنگاری داده‌ها، استفاده از هانی پات، محدودسازی حیطه عملکرد زیرساخت‌ها، کاهش وابستگی متقابل زیرساختی، چند لایه سازی و بومی‌سازی، استفاده از فایروال و سامانه کشف و جلوگیری از رخنه هستند.
ابراهیم محمودزاده ۱۳۹۷	الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح.	الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح از سه بعد اصلی و ۱۹ مولفه تشکیل شده است. بعد عوامل اصلی فضای سایبر با ۴ مولفه، بعد اهداف امنیتی فضای سایبر نیروهای مسلح با ۶ مولفه و بعد اقدامات و راه‌کارهای صیانت امنیتی فضای سایبر نیروهای مسلح با ۹ مولفه و ۷۰ زیر مولفه.
بهمن ابراهیمیان ۱۳۹۴	راهکارهای مقابله با تهدیدهای سایبری علیه جمهوری اسلامی ایران با تاکید بر نقش فناوری و منابع انسانی.	ج.ا.ایران با دو دسته تهدید در فضای سایبری مواجه است. یک دسته شامل توزیع محتوای مغایر با ارزش‌های انقلاب اسلامی که از آن به عنوان جنگ نرم یاد می‌شود و دسته دوم تهدیدات مختلف علیه زیرساخت‌های ارتباطی کشور.

روش‌شناسی پژوهش

نوع تحقیق کاربردی و روش اجرای آن از نوع توصیفی کاربردی با رویکرد آمیخته است. جامعه مورد مطالعه کلیه افراد و اسناد و مدارک، کتب، آئین نامه‌ها با موضوعات مرتبط با امنیت سایبری است. جامعه آماری،کلیه کارکنان پایور که در جایگاه‌های ۱۶ و بالاتر با رشد کارشناسی ارشد و بالاتر در حوزه سایبر و سنوات خدمتی بالای۲۰ سال در ستاد ارتش ج.ا.ایران بوده که تعداد آنها با احتساب ضریبی به علت طبقه بندی آماری برابر ۳۴ نفر است و با توجه به محدود بودن حجم جامعه آماری از روش تمام شمار استفاده شده است.

در ابتدا پس از مطالعه کامل و استفاده از منابع و مدارک مستند و تجارب علمی فرم مصاحبه آماده و به نخبگان ستاد ارتش جمهوری اسلامی ایران ارایه شد. پس از انجام مصاحبه، پرسشنامه با ۳۰ سوال تهیه و توسط جامعه آماری تکمیل شد که ضریب آلفای کرونباخ برای پرسشنامه ۰/۸۳ به دست آمد.

تجزیه و تحلیل داده‌ها

هدف اول: شناسایی عوامل داخلی موثر بر امنیت سایبری ستاد ارتش جمهوری اسلامی ایران.

برای دستیابی به اهداف پژوهش، پس از انجام مصاحبه‌ها و مطالعه اسناد و مدارک، داده‌ها به صورت زیر پردازش شد:

۱- امنیت برنامه‌های کاربردی، بکارگیری تدابیری از سوی سازندگان برنامه‌های کاربردی است که جلوی دسترسی غیرمجاز به برنامه را می‌گیرد و باعث بالا رفتن امنیت سایبری می‌شود. برای امنیت برنامه‌های کاربردی می‌توان شاخصه‌های احراز هویت کاربران، رمز نگاری داده‌ها و واقعه نگاری را در نظر گرفت.

۲- امنیت اطلاعات، فرآیندی برای جلوگیری از دسترسی، استفاده، افشا و خواندن، نسخه برداری یا ضبط، خراب کردن، تغییر و دستکاری اطلاعات است که می‌توان برای آن شاخصه‌های محرمانه سازی، حفظ یکپارچگی، دسترس پذیر نمودن و انکار ناپذیر نمودن را تعریف نمود.

۳- امنیت در شبکه فرآیندی است که در آن به زیرساخت سایبری توجه ویژه‌ای شده است و می‌توان برای آن شاخصه‌های حفاظت، کشف تغییرات و پاسخ به رخدادهای شبکه را تعریف نمود.

۴- طرح بازیابی از فاجعه بر روی کم کردن تاثیرات یک فاجعه رخ داده بر فعالیت سامانه‌های سازمان و عملیات سایبری تاکید دارد و می‌توان برای آن شاخصه‌های بازیابی و پاسخ به رخدادها و وقایع سایبری را تعریف نمود.

۵- امنیت عملیات بر افزایش اثربخشی عملیات سایبری تاکید دارد و می‌توان برای آن شاخصه‌های آنالیز تهدیدات و آنالیز آسیب پذیری‌ها را تعریف نمود.

۶- آموزش کاربر نهایی منجر به طور مستقیم باعث بالا رفتن سطح امنیت سایبری در سازمان می‌شود می‌توان برای آن شاخصه‌های برگزاری دوره‌های آموزشی کاربری سامانه‌ها و قرار دادن سرفصل دروس مقدماتی سایبر در دانشگاه‌ها و مراکز آموزشی را تعریف نمود.

سپس، پس از توزیع پرسشنامه‌ها، نتایج با بهره‌گیری از نرم‌افزار تحلیل شد که نتایج آن به شرح جدول زیر است:

جدول (۲) شناسایی عوامل داخلی موثر بر امنیت سایبری ستاد ارتش جمهوری اسلامی ایران

ردیف	شاخص		جمع	جمع امتیاز	میانگین	واریانس
۱	احراز هویت کاربران استفاده کننده از برنامه‌های کاربردی	امنیت برنامه‌های کاربردی	۳۴	۱۵۹	۴/۶۸	۰/۲۲۵
۲	رمز نگاری داده‌های منتقل شده در برنامه‌های کاربردی		۳۴	۱۶۱	۴/۷۴	۰/۲۰۱
۳	واقعه نگاری فعالیت‌ها در برنامه‌های کاربردی		۳۴	۱۵۹	۴/۶۸	۰/۲۲۵
۴	محرمانه سازی اطلاعات	امنیت اطلاعات	۳۴	۱۶۲	۴/۷۶	۰/۱۸۵
۵	حفظ یکپارچگی اطلاعات		۳۴	۱۶۰	۴/۷۱	۰/۲۱۴
۶	دسترس‌پذیر بودن اطلاعات		۳۴	۱۶۱	۴/۷۴	۰/۲۰۱
۷	انکار ناپذیر نمودن اطلاعات		۳۴	۱۶۴	۴/۸۲	۰/۱۵۰
۸	حفاظت از تجهیزات شبکه	امنیت شبکه	۳۴	۱۶۰	۴/۷۱	۰/۲۱۴
۹	کشف رخدادهای سایبری در شبکه		۳۴	۱۵۵	۴/۵۶	۰/۳۱۵
۱۰	پاسخ به رخدادهای کشف شده در شبکه		۳۴	۱۵۴	۴/۵۳	۰/۲۵۷
۱۱	طرحریزی پاسخ به فاجعه رخ داده بر دارایی‌های سایبری	طرح بازیابی از فاجعه	۳۴	۱۵۷	۴/۶۲	۰/۲۴۳
۱۲	طرحریزی بازیابی از فاجعه		۳۴	۱۵۹	۴/۶۸	۰/۲۲۵
۱۳	آنالیز تهدیدات برای برقراری امنیت در عملیات	امنیت عملیات	۳۴	۱۵۶	۴/۵۹	۰/۲۵۰
۱۴	آنالیز آسیب پذیری‌ها برقراری امنیت در عملیات		۳۴	۱۵۷	۴/۶۲	۰/۲۴۳

ردیف	شاخص		جمع	جمع امتیاز	میانگین	واریانس
۱۵	برگزاری دوره‌های آموزشی کاربری سامانه‌ها برای اپراتورها.	آموزش کاربر نهایی	۳۴	۱۵۳	۴/۵۰	۰/۳۱۸
۱۶	قرار دادن سرفصل دروس مقدماتی سایبر در دانشگاه‌ها و نیز در مراکز آموزشی در قالب دوره‌های طولی و عرضی.		۳۴	۱۵۲	۴/۴۷	۰/۳۱۷
	میانگین		۳۴	۱۵۸/۰۶	۴/۶۵	

نتایج به دست آمده گویای این مطلب است که ۹۹٪ از جامعه آماری شاخص‌های ارایه شده در شناسایی عوامل داخلی موثر بر امنیت سایبری ستاد ارتش جمهوری اسلامی ایران را در سطح زیاد به بالا مورد تایید قرار دادند.

هدف دوم: شناسایی عوامل خارجی موثر بر امنیت سایبری ستاد ارتش جمهوری اسلامی ایران. برای دستیابی به اهداف پژوهش، پس از انجام مصاحبه‌ها و مطالعه اسناد و مدارک، داده‌ها به صورت زیر پردازش شد:

۱- مقابله با تهدیدات سایبری دولتی نیازمند سیاست‌ها، طرح‌ها و اقدامات مرتبط با امنیت سایبری در سازمان است.

۲- مقابله تهدیدات سایبری غیر دولتی نیازمند سیاست‌ها، طرح‌ها و اقدامات مرتبط با امنیت سایبری در سازمان است.

۳- مقابله تهدیدات سایبری اشخاص و گروه‌های کوچک نیازمند طرح‌ها و اقدامات مرتبط با امنیت سایبری در سازمان است.

۴- در نظر گرفتن حوادث و مخاطرات طبیعی و آمادگی در مقابل آن‌ها کلید بقای دارایی‌ها و زیرساخت سایبری است.

سپس، پس از توزیع پرسشنامه‌ها، نتایج با بهره‌گیری از نرم‌افزار تحلیل شد که نتایج آن به شرح جدول (۳) است:

جدول (۳) شناسایی عوامل خارجی موثر بر امنیت سایبری ستاد ارتش جمهوری اسلامی ایران

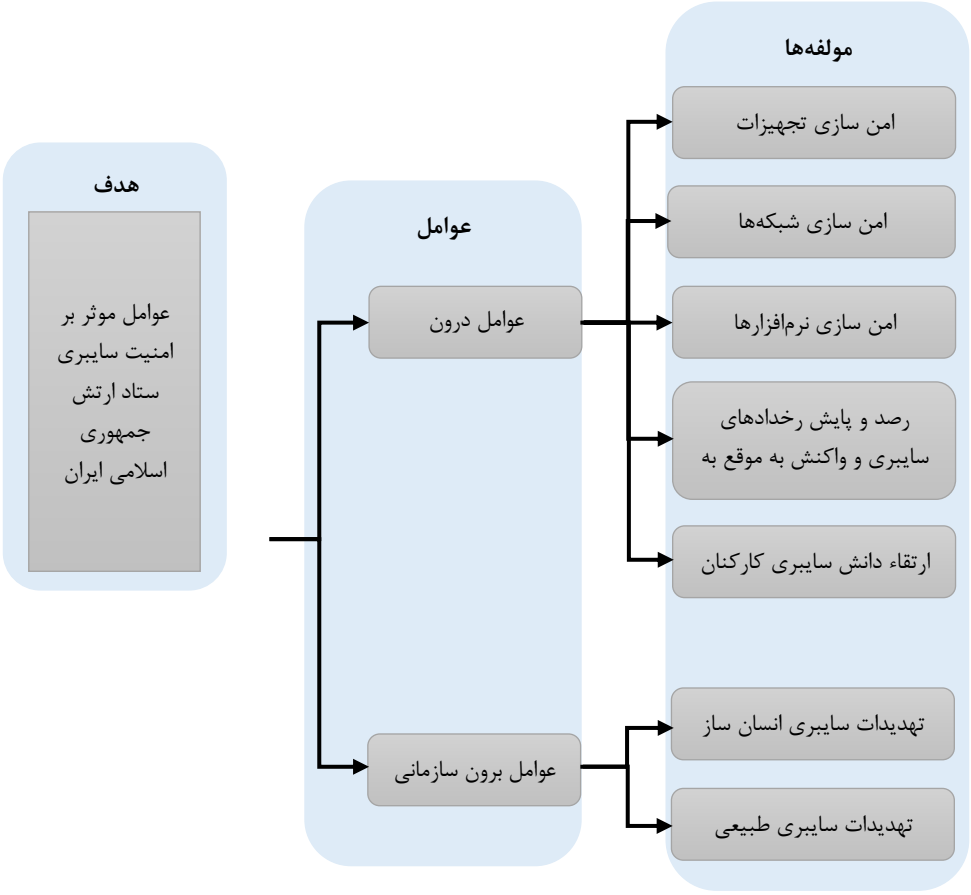
ردیف		شاخص	جمع	جمع امتیاز	میانگین	واریانس
۱	تهدیدات سایبری دولتی	ایجاد بازدارندگی سایبری برای مقابله با تهدیدات دولتی	۳۴	۱۵۳	۴/۵۰	۰/۳۱۸
۲		حفاظت از زیرساخت سایبری برای مقابله با تهدیدات دولتی	۳۴	۱۵۵	۴/۵۶	۰/۳۱۵
۳		نگهداشت و بروز رسانی تجهیزات برای مقابله با تهدیدات دولتی	۳۴	۱۵۲	۴/۴۷	۰/۲۵۷
۴		اجرای پدافند غیرعامل برای مقابله با تهدیدات دولتی	۳۴	۱۵۱	۴/۴۴	۰/۲۵۴
۵	تهدیدات سایبری غیر دولتی	ایجاد بازدارندگی سایبری برای مقابله با تهدیدات سازمان‌های غیر دولتی	۳۴	۱۵۱	۴/۴۴	۰/۳۷۵
۶		حفاظت از زیرساخت سایبری برای مقابله با تهدیدات سازمان‌های غیر دولتی	۳۴	۱۵۲	۴/۴۷	۰/۲۵۷
۷		نگهداشت و بروز رسانی تجهیزات برای مقابله با تهدیدات سازمان‌های غیر دولتی	۳۴	۱۵۲	۴/۴۷	۰/۲۵۷
۸	تهدیدات سایبری اشخاص	حفاظت از زیرساخت سایبری برای مقابله با تهدیدات اشخاص و گروه‌های کوچک.	۳۴	۱۵۲	۴/۴۷	۰/۲۵۷
۹		نگهداشت و بروز رسانی برای مقابله با تهدیدات اشخاص و گروه‌های کوچک.	۳۴	۱۵۱	۴/۴۴	۰/۲۵۴
۱۰	حوادث و مخاطرات طبیعی	در نظر گرفتن شرایط آب و هوایی منطقه در نصب تجهیزات و اجرای زیرساخت سایبری برای مقابله با حوادث و مخاطرات طبیعی.	۳۴	۱۵۴	۴/۵۳	۰/۲۵۷
۱۱		تدوین طرح‌های آمادگی مقابله با حوادث و بلایای طبیعی.	۳۴	۱۴۶	۴/۲۹	۰/۳۹۶
		میانگین	۳۴	۱۵۱/۷۲	۴/۵۸	

نتایج به دست آمده گویای این مطلب است که ۹۸٪ از جامعه آماری شاخص‌های ارایه شده در شناسایی عوامل خارجی موثر بر امنیت سایبری ستاد ارتش جمهوری اسلامی ایران را در سطح زیاد به بالا مورد تأیید قرار دادند.

در حوزه امنیت سایبری تمامی عوامل زنجیروار به هم متصل بوده و در برخی موارد هم‌پوشانی دارند. اگر هر کدام از این عوامل دچار نقصان شود، ایجاد آسیب از همان نقطه محتمل است. از این رو در بایستی سعی نمود در همه زمینه‌های امنیت سایبری اقدامات لازم را انجام داد تا در سازمان رخنه ایجاد نشود. از نتایج نیز اینگونه استنباط می‌شود که هیچکدام از عوامل بر هم برتری ندارند.

نتیجه‌گیری و پیشنهادها

از جمع‌بندی نتایج به دست آمده مشخص می‌گردد ۱۰ مولفه با ۲۷ شاخص بر امنیت سایبری ستاد ارتش ج.ا.ایران تأثیرگذار هستند که با در نظر گرفتن ادبیات پژوهش و مصاحبه با صاحب‌نظران قالب چارچوب نظری زیر از آن استنباط می‌شود.



نمودار (۱) چارچوب نظری عوامل موثر بر امنیت سایبری ستاد ارتش ج.ا.ایران

این تحقیق بر مبنای عملیات سایبر در ارتش ج.ا.ایران بوده است و می‌تواند پژوهش جدیدی از منظر سازمان‌های غیر نظامی مطرح گردد. با توجه به وسیع بودن دامنه این تحقیق پیشنهاد می‌گردد ارایه الگوی امنیت سایبری به طور جداگانه ارایه گردد.

قدردانی

در پایان از تمامی عزیزانی که ما را در راستای انجام این تحقیق یاری رساندند، کمال تشکر و امتنان بعمل می‌آید.

منابع

- آذر داود. (۱۳۹۳). *شناخت تهدیدات فضای سایبر و پدافند آن*. چاپ اول، تهران، دافوس.
- جاجودیا سوشیل. (۱۳۹۶). *جنگ سایبری*. چاپ اول تهران موسسه آموزشی و تحقیقاتی صنایع دفاع.
- جبار رشیدی علی. (۱۳۹۶). مدلسازی و شبیه‌سازی صحنه‌ی نبرد سایبری. *فصلنامه مدیریت فناوری*، ۹(۴): ۸۰۹-۸۲۸.
- سجادی وحید. آذر داود. (۱۳۹۹). *عملیات سایبری*. چاپ اول. تهران، دافوس.
- *سند معماری دفاع سایبری در بخش دفاعی کشور*. (۱۳۹۴). شرکت صنایع امنیت فضای تبادل اطلاعات صاایران.
- مدیری، ناصر. (۱۳۸۹). *مهندسی امنیت شبکه‌های کامپیوتری*. چاپ اول. تهران. مهرگان قلم.
- ولی‌وند زمانی حسین. شهلایی ناصر. (۱۳۹۸). *نظریه‌های راهبردی*. چاپ هفتم. تهران. دافوس۱۳۹۸.
- *Cyberspace Operations*. (2018). Department of Defense, JP 3-12.
- D. Bryant William. (2013). Cyberspace Superiority. *Air & Space Power Journal*. 1(1):25-44.
- *Dictionary of Military and Associated Terms*. - (2016). Department of Defense, JP 1-02.
- Kim Joe. (2017). Cyber-security in government: reducing the risk. *Computer Fraud & Security*. 1(1): 8-11.
- Srinivasan J. Simna, S. (2017). Disaster recovery an element of cybersecurity. *IJM*. 8(4): 125-133.
- Stewart. Micheal. Kinsey Denise. (2021) Network Security Firewalls and VPNs. *Jones & Bartlett Learning*.
- The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology. (2011). *EastWest Institute and the Information Security Institute of Moscow State University*.

- Warner Michael. (2012). Cybersecurity: A pre-history. *Intelligence and National Security*. 27(5): 781-799.
- Whitman Michael. Mattord Herbert. (2012). *Principles of Information Security*. Google books.