الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح

ابراهیم محمودزاده[۱]

کیوان اسماعیلی[۲]

تاریخ دریافت:۱۳۹/۰۳/۲۰ تاریخ پذیرش:۱۳۹۷/۰۸/۴

چکیده:

در طول سه دهه اخیر فضای سایبر نیروهای مسلح جمهوری اسلامی ایران همواره با تهدیدات متنوع و مستمری از سوی بیگانگان مواجه بوده، به‌طوری که فضای سایبر به‌عنوان ابزار اصلی سرویس‌های اطلاعاتی برای جاسوسی و خرابکاری قرار داشته است. عدم پیش‌بینی و اعمال راهکارهای پیشگیرانه برای صیانت امنیتی فضای سایبر نیروهای مسلح به‌منظور پیشگیری و مقابله با این تعرض‌ها با مدیریت نظام‌مند و یکپارچه تبعات جبران‌ناپذیری را به همراه خواهد داشت.

بر این اساس ارائه الگویی راهبردی جهت خنثی‌سازی این تهدیدات از ضرورت‌ها به شمار می‌آید و هدف از این پژوهش دستیابی به الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح با شناسایی ابعاد، مؤلفه‌ها، روابط فی‌مابین آن‌ها است.

محقق با استفاده از روش پژوهش آمیخته، ابتدا از روش کیفی با استفاده از روش تحلیل مضامین اقدام به مطالعه فرامین، تدابیر فرماندهی معظم کل قوا، اسناد بالادستی کشور و نیروهای مسلح در حوزه سایبر پرداخته است و پس از استخراج مدل مفهومی صیانت امنیتی فضای سایبر نیروهای مسلح، با تشکیل جلسات گروه خبرگی و مصاحبه با خبرگان به توصیف متغیرها به‌منظور شناسایی ابعاد، مؤلفه‌ها در الگو پرداخته شد و برای تأیید مدل مفهومی به دست آمده پرسشنامه‌ای محقق ساخته تدوین گردید و جمع‌آوری اطلاعات پرسشنامه‌ای و تجزیه و تحلیل داده‌ها انجام پذیرفت.

نتایج این تحقیق نشان می‌دهد که الگوی راهبردی صیانت امنیتی، دارای ۳ بُعد و ۱۹ مؤلفه است که مهم‌ترین مؤلفه‌ها در بُعد عوامل اصلی فضای سایبر نیروهای مسلح به ترتیب داده‌ها و اطلاعات، کاربران، شبکه و زیرساخت، خدمات و نرم‌افزار است. همچنین مهم‌ترین مؤلفه‌ها در بُعد اهداف امنیتی فضای سایبر نیروهای مسلح به ترتیب محرمانگی، احراز هویت، یکپارچگی و صحت، دسترسی پذیری، انکارناپذیری و در نهایت حفاظت از حریم خصوصی سازمان است. در بُعد اقدامات و راهکارهای صیانت امنیتی فضای سایبر نیروهای مسلح نیز مهم‌ترین مؤلفه‌ها عبارتند از شناسایی منابع و دارایی‌های سایبری، محافظت، تشخیص و کشف، تحلیل، پاسخ و واکنش، بازیابی، بازدارندگی، مقابله مؤثر، نوآوری و تحول است.

کلیدواژه‌ها: فضای سایبر، امنیت فضای سایبر، صیانت، صیانت امنیتی، تهدیدات سایبری، الگوی مفهومی

۱- دانشیار دانشگاه صنعتی مالک اشتر (نویسنده مسئول)- Maheb20 @gmail.com

۲- دانش‌آموخته دوره دکتری مدیریت راهبردی امنیت فضای سایبر، دانشگاه عالی دفاع ملی- esmaili@nict.ir

مقدمه:

یکی از موضوعات مهم و اساسی در عصر کنونی که آن را عصر دیجیتال می‌نامند، سرعت، پیچیدگی و نفوذ فضای سایبر و فناوری اطلاعات و ارتباطات است و این موضوع تمامی ابعاد زندگی بشر را تحت تأثیر قرار داده و به‌واسطه این تغییرات، موجودیت و عرصه کنشگری تمامی نهادها و سازمان‌ها به درک صحیح و به‌موقع از این دگرگونی و برنامه‌ریزی برای مواجه‌شدن با آن گره خورده است. فرماندهی نیروهای مسلح و حفاظت اطلاعات نیز مستثناء از شرایط این تغییرات نیست بلکه به عبارتی در نوک پیکان فضای چالش‌برانگیز عصر کنونی قرار دارد.

استفاده از فضای سایبر، با تمام چالش‌ها و پیچیدگی‌های موجود در آن مانند یک جریان آب شدیدی است که نمی‌توان برخلاف آن حرکت کرد، بلکه می‌بایست آن را مدیریت کرد. همان‌طور که مقام معظم رهبری (مدظله‌العالی) در دیدار با اعضای هیئت دولت در تاریخ ۱۳۹۵/۰۶/۰۳ با درک هوشمندانه این فضا را به‌صورت زیر تشریح نموده‌اند:

... فضای مجازی واقعاً یک دنیای رو به رشدِ غیرقابل توقّف است، یعنی واقعاً آخر ندارد؛ آدم هرچه نگاه می‌کند، آن چیزِ اوّل بلا آخر، فضای مجازی است. هرچه انسان پیش می‌رود در این فضا، این همین‌طور ادامه دارد. این‌یک فرصت‌های بزرگی در اختیار هر کشوری می‌گذارد، تهدیدهایی هم در کنارش دارد؛ ما بایستی کاری کنیم که از آن فرصت ها حداکثر استفاده را بکنیم، از این تهدیدها تا آنجایی که ممکن است خودمان را برکنار نگه بداریم.

با توجه به شرایط و محیط فضای سایبر، وجود الگوهای راهبردی برای شناخت و درک نقاط بحرانی، تهدیدات، عوامل اثرگذار خارجی و داخلی بسیار ضروری بوده و برنامه‌ریزی راهبردی با نگاه به آینده فضای سایبر نیروهای مسلح و رصد علائم کم‌سو متناسب با رخدادهای محیطی باعث می‌گردد تا از غافلگیری راهبردی پیشگیری کرده و در صورت لزوم، واکنش سریع و مقتضی را نشان داد. ضمن این‌که منافع و دارایی‌های ارزشمند نیروهای مسلح شامل اطلاعات، زیرساخت‌های سایبری و ... را می‌توانیم صیانت امنیتی کنیم.

صیانت امنیتی فضای سایبر موضوع بسیار مهمی است و بسیار جلوتر از امنیت فضای سایبر است، زیرا در امنیت فضای سایبر به دنبال یک سری از الزامات برای ایمنی و امنیت این فضا هستیم، درحالی‌که صیانت امنیتی به دنبال موضوعاتی شامل ارزش‌ها، حریم خصوصی، سرمایه‌های مادی و معنوی، اسرار و اطلاعات، تخلفات و جرائم، خدمات و سرویس‌ها، قوانین و مقررات، پیاده‌سازی مراکز عملیات امنیت می‌باشد (حسینی، ۱۳۹۵: ۲۸۶). صیانت امنیتی دارای فرآیندی

است که در حوزه‌های دکترین، هدف‌گذاری، سیاست‌گذاری، برنامه‌ریزی، هدایت، سازمان‌دهی، هماهنگی، پیاده‌سازی و اجرا، نظارت و ارزیابی است (همان: ۵۰).

در حال حاضر در نیروهای مسلح دغدغه‌ها و چالش‌های زیادی در حوزه سایبر پیش رو هست که نیاز به چاره‌اندیشی دارد. برای نمونه دسترسی کارکنان به شبکه‌های اجتماعی (تلگرام، لاین، واتس آپ و ...) و عضویت آن‌ها در کانال‌های خصوصی شبکه‌های اجتماعی که همراه با ارائه اطلاعات در این کانال‌ها و شبکه‌های اجتماعی بوده و افشاء اطلاعات فراوانی را به همراه دارد؛ می‌توان نام برد. همچنین وجود سیاست‌ها، آیین‌نامه‌ها و دستورالعمل‌هایی که رویکرد صیانت امنیتی در تبیین آن‌ها ضعیف بوده و شکننده است را از دلایل عمده برای تدوین الگویی راهبردی و کلان در سطح نیروهای مسلح برای صیانت امنیتی فضای سایبر می‌توان نام برد که پاسخی کاربردی به دغدغه‌ها و سؤالات فوق در مواجهه با رویدادها، فرصت‌ها، ابهامات، تردیدهای موجود و در جهت ارتقاء توان امنیت سایبر نیروهای مسلح می‌باشد.

مسئله اصلی و سؤال کلیدی در این تحقیق آن است که با توجه به تغییر ماهیت و جنس تهدیدات امنیتی و عملکرد یکپارچه دشمن برای جاسوسی و خرابکاری در درون کشور علی‌الخصوص نیروهای مسلح و همچنین آسیب‌های ناشی از ضعف آموزش و فرهنگ برای مشارکت در حفاظت از اطلاعات سایبری نیروهای مسلح که شامل اطلاعات، زیرساخت ها، شخصیت‌ها و ... هست ابعاد و مؤلفه‌های و الگوی راهبردی صیانت امنیتی از فضای سایبر نیروهای مسلح چیست؟

اهمیت صیانت امنیتی فضای سایبر نیروهای مسلح از دو جنبه نظری و کاربردی حائز اهمیت است، زیرا به علت بنیادی بودن این تحقیق و عدم وجود کار پژوهشی مشابه موجب شناسایی و تبیین ابعاد، مؤلفه‌های صیانت امنیتی و تولید ادبیات بومی در این حوزه می‌گردد. همچنین کارکردهای کاربردی الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح جهت توسعه و اعتلاء علوم و فنون پدافندی و پیشگیرانه در فضای پر چالش امنیتی و محیط بی‌ثبات و پویای سایبر می‌گردد و باعث ایجاد و فراهم نمودن زمینه وفاق در فرآیند تصمیم‌سازی و تصمیم‌گیری امنیتی فضای سایبر بین فرماندهی و حفاظت اطلاعات می‌شود. این الگو موجب ایجاد پل و ارتباطی میان حوزه نظر و عمل و به عبارتی اجماع در خصوص چگونگی برخورد با موضوع صیانت امنیتی در فضای سایبر نیروهای مسلح است. تقسیم‌کار بین فرماندهی و حفاظت اطلاعات

و نهادهای مرتبط برای روشمند شدن دیدگاه‌های آن‌ها در فضای سایبر از جمله مواردی است که به‌عنوان اهمیت این تحقیق محسوب می‌گردد.

در خصوص ضرورت انجام این تحقیق می‌توان به سیاست‌های ابلاغی مقام معظم رهبری (مدظله‌العالی) بر لزوم توجه به توسعه فناوری اطلاعات و ارتباطات با رعایت ملاحظات امنیتی، سازوکار مناسب برای امن‌سازی ساختارهای حیاتی و حساس و مهم، صیانت از اسرار کشور، پایش مستمر، پیشگیری، دفاع و ارتقاء توان بازدارندگی در مقابل هرگونه تهدید در حوزه فناوری اطلاعات و ارتباطات اشاره نمود که صیانت امنیتی پایه اصلی این موارد است. در صورت نبود صیانت امنیتی در فضای سایبر؛ اتخاذ تصمیمات ناهمگن، نامنسجم، بخشی‌نگر، پراکنده، ناکارآمد و غیرمؤثر در حوزه‌های صیانت امنیتی فضای سایبر، علی‌الخصوص در تصمیمات امنیتی حوزه فرماندهی و حفاظت اطلاعات اجتناب‌ناپذیر می‌گردد.

بدیع بودن این تحقیق در قالب الگوی راهبردی برای نخستین بار در حوزه صیانت امنیتی فضای سایبر نیروهای مسلح با بهره‌گیری از گفتمان مقام معظم رهبری (مدظله‌العالی) و اسناد بالادستی و انجام مصاحبه و مستندسازی نظرات خبرگان نیروهای مسلح، دارای اهمیت بسزایی است و از آنجا که تاکنون در خصوص طراحی و ارائه الگوی راهبردی در این حوزه اقدامی نشده است، انجام این تحقیق ضرورت دارد.

مبانی نظری:

صیانت امنیتی: صیانت در لغت‌نامه دهخدا به معانی، نگه‌داشتن، نگهبانی، حفظ کردن، حفظ نگاهداری، محفوظ داشتن، مصون داشتن و در فرهنگ فارسی معین به معانی حفظ کردن و نگهداری می‌باشد. معادل انگلیسی کلمه صیانت (حفاظت، محافظت، حراست)[1] و (حفظ، نگهداری، حراست)[2] می باشد. صیانت امنیتی به مجموعه اقدامات دستگاه امنیتی برای کشف، شناسایی، خنثی‌سازی عملیات جاسوسی، براندازی، خرابکاری، عوامل ایجاد نارضایتی، اختلال در انجام مأموریت نیروهای مسلح و نفوذ جریانات سیاسی در آن‌ها به‌منظور کنترل امنیت فاوا و حفاظت از اسناد و مدارک، اماکن و تأسیسات، تسلیحات و تجهیزات نیروهای مسلح با رعایت ملاحظات و شرایط بومی هر سازمان اطلاق می‌گردد (اساسنامه ساحفاناجا). تعریف عملیاتی صیانت امنیتی عبارت است از فرآیندی سیستمی که از طریق شناسایی، حفاظت و پیشگیری، کشف

1-protection
2-preservation

و تشخیص، تحلیل، پاسخگویی و واکنش، بازیابی و بازسازی، بازدارندگی، مقابله مؤثر و با رویکرد تحول و نوآوری در اقدامات امنیت پایدار مراجع امنیتی سایبری را در مقابل تهدیدات تضمین می‌نماید.

صیانت امنیتی در سیره پیامبر اسلام (ص) و ائمه (ع): در روایات و احادیثی که توسط پیامبر اسلام و ائمه اطهار ارائه شده است اشاراتی به موضوع صیانت امنیتی گردیده است که برخی از مصادیق موضوع صیانت امنیتی در سیره پیامبر اسلام (ص) و ائمه (ع) به‌عنوان نمونه استخراج گردیده است.

قرار دادن موانع برای بازرسی: ابن اسحاق در حدیث مربوطه به جنگ فتح چنین بیان دارد: «پس رسول خدا (ص) فرمان داد راه‌ها را ببندند تا مردم مکه نتوانند اطلاعات مربوط به لشکر اسلام را به دست آورده و به فرماندهان و رهبران خود برسانند» (العاملی، ۱۳۷۶: ۲۹۴).

ثبت و ضبط اسامی کسانی که به بعضی از مناطق وارد می‌شوند: از امام صادق (ع) چنین روایتی را نقل می‌کند: «علی (ع) دستور داد تا اسامی هرکسی را که به شهر کوفه وارد می‌شود یادداشت کرده و مکتوب به حضرت (ع) گزارش دهند» (آشوب، ۱۳۹۰: ۲۷۱).

تشویق دیگران جهت مخفی نگاه داشتن اسرار محرمانه: حضرت علی (ع) فرمود: «هر چیزی که از تو مخفی داشته می‌شود، اجازه نداری که آن را اظهار و شایع کنی و نیز هر چیزی که تو می‌دانی و نسبت به آن آگاهی، مجاز نیستی که دیگران را از آن آگاه کنی» (شریف الرضی، ۱۳۴۳: ۳۳۶).

از کسانی که باید اسرار را مخفی نگاه داشت: از حضرت علی (ع) فرمود: «با دشمن خود مشورت نکن و اطلاعات خود را از او مخفی بدار» (آمدی، ۱۳۶۶: ۸۰۲). آنچه را که از اسرار در اختیار توست و آن را از دشمنت مخفی می‌کنی، همان‌طور نیز از دوستانت مخفی بدار و آن‌ها را از این اسرار باخبر نکن (شریف الرضی، ۱۳۴۳: ۲۶۰).

جلوگیری و ممانعت از مسافرین مخالف و مشکوک: حضرت علی (ع) در نامه‌ای چنین نوشت: «... به من خبر رسیده است که عده‌ای از مردم شهر به معاویه متمایل شده‌اند. پس هر کس را یافتن که چنین قصدی داشت از خروج او جلوگیری کن و هرکس که از دست تو بیرون رفت ناراحت نشو ...» (العاملی، ۱۳۷۶: ۲۹۸).

با توجه به مستندات ارائه شده در احادیث و روایات موجود در سیره پیامبر اسلام و ائمه اطهار، سه محور اصلی سیاست‌های امنیتی، اقدامات تدافعی و آگاه نمودن از مهم‌ترین محورهای صیانت امنیتی می‌باشد. لذا برای پیاده‌سازی یک مدل صیانتی باید خصوصیات زیر در آن وجود داشته باشد:

- باید یک دیواره آتش قبل از خاکریزهای اطلاعات ایجاد شود.
- محدودیت در دسترسی، برای کسانی که صلاحیت دسترسی ندارند.
- تسهیل در دسترسی، برای کسانی که صلاحیت دسترسی دارند (حسب مأموریت محوله).
- مستند نمودن اطلاعات واگذار شده به دیگران.
- برخورد مناسب با متخلفان و اخلال گران امنیت.

صیانت امنیتی در اندیشه ها، نظرات، فرامین و تدابیر مقام معظم رهبری (مدظله العالی): با توجه به اهمیت موضوع صیانت امنیتی، به برخی از فرمایشات و تأکیدات مقام معظم رهبری در موضوع صیانت امنیتی که خطاب به نیروهای مسلح ابلاغ نموده‌اند، اشاره می‌گردد. لازم به ذکر است برخی از موضوعات که مصداق قوی‌تری دارند به علت طبقه‌بندی در اینجا اشاره نشده است.

آمادگی علمی و فنی و خوداتکایی: فراگرفتن دانش اطلاعاتی، مجهز شدن به مدرن‌ترین ابزار لازم اطلاعاتی جهت پیشگیری از جاسوسی و نفوذ دشمن از طریق فناوری ...و در داخل و توسط خودتان ساخته شود (۱۳۸۸/۰۹/۰۸).

طبقه‌بندی و حیطه‌بندی اطلاعات: ...در همه بخش‌ها طبقه‌بندی‌ها را بدون ملاحظه رعایت بکنید، نگذارید که دشمن از بی‌مبالاتی ما در مورد حفاظت از کارهای طبقه‌بندی شده و اسناد طبقه‌بندی شده، سوءاستفاده کند (۱۳۹۰/۰۴/۰۱).

پیشگیری و مراقبت: بر پیشگیری اصرار بیشتری دارم تا علاج؛ فکر کنید راه پیشگیری چیست؟ (۱۳۸۴/۱۱/۰۲)

برخورد با تخلفات: باید با تخلف برخورد شود و این سازمان انقلابی از همه آفت‌ها دور باشد تا صیانت گردد (۱۳۹۰/۰۴/۰۴).

نظارت و صیانت کارکنان: لزوم نظارت قوی و دائم بر کارکنان نیروهای مسلح با (همراهی و مساعدت) فرماندهان (۱۳۹۰/۰۴/۰۴).

دفاع و حمله سایبری (آفند و پدافند سایبری) و دیوار آتش: دشمن دید خاکریز نرم و سستی است نفوذ و رخنه می‌کند. ... تلاش کنید که یک دیواره آتش درست کنید که کسی نتواند نزدیک شود (۱۳۹۰/۱۰/۲۷).

جلوگیری از درز اطلاعات: لزوم اتخاذ تمهیدات لازم به‌منظور جلوگیری از درز اطلاعات به خارج (۱۳۹۰/۰۴/۰۴).

موضوعات، دشمن‌شناسی، شناخت تهدیدات و آسیب‌پذیری‌ها، رصد و مراقبت، آمادگی علمی و فنی، طبقه‌بندی و حیطه‌بندی اطلاعات، پیشگیری و مراقبت، اشراف اطلاعاتی، آمادگی دفاعی، هشداردهی، برخورد با تخلفات، دفاع و حمله، جلوگیری از درز اطلاعات، تصمیم‌گیری، پیگیری و دنبال‌گیری از مصادیق صیانت امنیتی از منظر معظم‌له می‌باشد.

ابعاد فضای سایبر نیروهای مسلح:

فضای سایبر عبارت است از شبکه‌های وابسته به یکدیگر، از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای، پردازنده‌های تعبیه‌شده (جاگذاری‌شده)، کنترل‌گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات. این فضا ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد یا تنها قابلیت اتصال به محیط پیرامونی در آن تعبیه شده باشد (سند راهبردی پدافندی سایبری کشور، ۱۳۹۲: ۶).

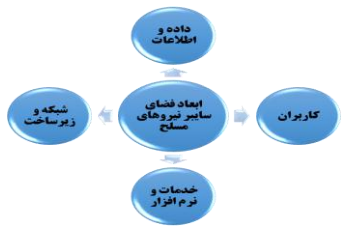
فضای سایبر نیروهای مسلح شامل تمامی سامانه‌هایی است که با تجهیزات و سامانه‌های فاوا مرتبط بوده و از طریق آن اجرای مأموریت انجام می‌گردد. به عبارتی فضای سایبر نیروهای مسلح مشتمل بر تمامی شبکه‌های صوت، دیتا، نرم‌افزارهای عملیاتی، سخت‌افزارهای ارتباطی رایانه‌ای، تجهیزات و ادوات نظامی مجهز به سامانه‌های فاوا به‌صورت مستقل یا مرتبط، محدود یا گسترده که در آن تبادل اطلاعات در راستای اجرای مأموریت ایجاد و در حال توسعه است؛ می‌باشد (طرح ارتقاء امنیت و افزایش قدرت دفاع سایبری در نیروهای مسلح، ۱۳۹۴: ۱۳).

بر اساس تعریف مشترک فضای سایبر که توسط روسیه و آمریکا ارائه شده، ارتباطات، اطلاعات، کاربران، سخت‌افزار و نرم‌افزار را مهم‌ترین ابعاد می‌دانند. محیط، قدرت و توان، سخت‌افزار، نرم‌افزار، شبکه، محتوی، انسان و سیاست به‌عنوان ابعاد فضای سایبر معرفی نموده

است (Rauscher and Yaschenko:2011,17). دیوید کلارک ویژگی‌های فضای سایبری و اجزای آن را شامل انسان‌ها، اطلاعات، بلوک‌های پیش‌ساخته منطقی و شالوده فیزیکی معرفی کرده است (Clark:2010,35). در مدل معماری مرجع امنیت که در سال ۱۳۹۶ ارائه شده، داده‌ها و اطلاعات، نرم‌افزار سیستم و سرویس، دارایی‌های فیزیکی و زیرساخت و تجهیزات، کاربران، شبکه‌ها و سیستم‌های ارتباطی به‌عنوان ابعاد فضای سایبر معرفی شده است (شورای عالی فناوری اطلاعات کشور، ۱۳۹۶)[1].

فضای سایبر دارای ابعاد مختلفی می‌باشد که برخی از آن‌ها توسط محققان ارائه شده است. در پژوهشی که توسط ستاد کل نیروهای مسلح انجام گردیده است، ابعاد فضای سایبر در چهار بعد کاربران، اطلاعات، خدمات (سرویس‌ها) و زیرساخت معرفی شده است (ولوی، ۱۳۸۵: ۲۵). همچنین در تحقیق دیگری ابعاد فضای سایبر دارای لایه‌های اجتماعی، اطلاعاتی، کاربردی، نرم‌افزاری، سخت‌افزاری و فیزیکی است (محمدی،۱۳۹۲: ۱۱۵).

در آئین‌نامه جامع امنیت فناوری اطلاعات و ارتباطات نیروهای مسلح، مهم‌ترین ابعاد فناوری اطلاعات و ارتباطات عبارتند از: نرم‌افزار و برنامه‌های کاربردی، سخت‌افزار و تجهیزات، بسترهای ارتباطی، اطلاعات الکترونیکی، شبکه‌ها، نیروی انسانی و کاربران.



شکل (۱): ابعاد فضای سایبر نیروهای مسلح

با توجه به تعاریف ارائه شده و همچنین بر اساس مطالعه اسناد و مدارک معتبر علمی در حوزه سایبر مهم‌ترین ابعاد فضای سایبر علی‌الخصوص فضای سایبر نیروهای مسلح که باید صیانت شود تا از هرگونه آسیب و تهدید حفظ گردد دارای ۴ رکن اصلی می‌باشد که عبارتند از **داده و اطلاعات، کاربران، شبکه و زیرساخت، خدمات و نرم‌افزار** در شکل ۱ ابعاد فضای سایبر نیروهای مسلح ترسیم گردیده است.

1-www.ieaf.ir

تهدیدات فضای سایبر نیروهای مسلح: تهدیدات سایبری عبارت از هر رویداد با قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف سازمان، سرمایه سایبری یا کارکنان سازمان از طریق دسترسی غیرمجاز، انهدام (تخریب)، افشاء، تغییر اطلاعات و یا ایجاد اخلال در ارائه خدمت و سرویس است (سند راهبردی پدافندی سایبری کشور، ۱۳۹۲: ۸).

تهدیدات سایبری یک عامل بالقوه برای نقض امنیت در فضای سایبری است. تهدید سایبری در صورتی وجود خواهد داشت که یک پیشامد، قابلیت، کنش، یا رخداد که می‌تواند در امنیت سایبری رخنه ایجاد نموده و منجر به صدمه شود، وجود دارد. این بدان معنی است که یک تهدید سایبری، یک خطر بالقوه است که ممکن است منجر به بهره‌برداری از یک آسیب‌پذیری امنیتی شود . (Stallings:2011,145) روش‌های مختلفی برای دسته‌بندی تهدیدات سایبری ارائه شده است. برای نمونه تهدیدهای سایبری به دو دسته اصلی تهدیدات خارجی و داخلی تقسیم شده‌اند. منشاء تهدیدهای خارجی در خارج از شبکه محلی یا ملی است و عمدتاً از جانب نفوذگران خارجی است؛ اما منشاء تهدیدهای داخلی در داخل شبکه و از جانب نفوذگران داخلی است (Libicki:2009,55). موضوعات تهدیدات فضای سایبر که توسط اسناد کتابخانه‌ای و مطالعات مختلف ارائه شده است بسیار متنوع می‌باشد. در جدول ۱ این تهدیدات از منظرهای مختلف ارائه شده است.

مستند	تهدیدات
حمید نادی – ۱۳۹۳	سرویس‌های اطلاعاتی دشمن، جاسوسی و خرابکاری
Landwehr, 1994	افشا، جعل یا تخریب، تغییر یا دستکاری، انکار، از کاراندازی، منع سرویس، منع سرویس توزیع شده، ابزارهای بهره‌برداری، بمب‌های منطقی، صیادی (فیشینگ)، شنودگر، اسب تروا، ویروس، ویشینگ (نوعی از فیشینگ که با استفاده از مکالمات صوتی در اینترنت انجام می‌شود)، واردرایوینگ (استفاده از لپ‌تاپ برای ورود به شبکه‌های بی‌سیم) کرم و بهره‌برداری روز صفر.
AVOIDIT, 1994	ایمیل‌های مشکوک، بدافزار، هک و نفوذ، حملات مختل‌سازی خدمات، فریب، نقض قوانین مالکیت معنوی
معاونت پژوهش و تولید علم ۱۳۹۶	حملات سایبری به سایت ها و زیرساخت های حیاتی، تولید بدافزارهای مخرب، اقدامات جاسوسی و جمع آوری اطلاعات، استفاده از فیشینگ و کشف رمز عبور کاربران، قطع سرویس و خدمات به مشتریان و ... از مهم‌ترین تهدیداتی به شمار می‌آیند.
Rauscher 2011 Yaschenko	اختلال، ازکاراندازی یا نابودی زیرساخت‌های ملی (ارتباطات، برق، آب، بانک‌ها، سازمان‌های دولتی، سازمان‌های خدماتی ملی، انرژی) یا سازمان‌های نظامی
Stouffer 2014 کنترل صنعتی	فاجعه‌های محیطی طبیعی یا ایجاد شده توسط انسان، آتش، طغیان – طوفان دریایی، توفان – گردباد،

مستند	تهدیدات
	زلزله، بمب‌گذاری، اشغال/ بیماری، اپیدمیک/ آلودگی وسیع محیطی، وقایع طبیعی غیرمنتظره مثل کسوف، خطاهای زیرساخت / قطعی، ارتباطات، قطع انرژی الکتریکی
سازمان اف. بی. آی	سرویس‌های اطلاعات، نفوذ سایبری از سوی گروه‌های جنایی، هکرها، هکتیویسم به حمله‌هایی با انگیزه سیاسی، کارمند داخلی ناراضی، تروریست‌ها درصدد تخریب، عدم دسترسی به سرویس، ابزارهای اکسپلویت، بمب منطقی، استراق سمع داده‌ها (اسنیفر)، اسب تروجان، ویروس، کرم‌ها، جاسوس‌افزار، ردیابی با شماره تلفن، حمله به شبکه‌های بی‌سیم، اسپم ساختن، فیشینگ (کپی همانندسازی شده از یک وب‌سایت)، جعل پست الکترونیکی، فارمینگ (تله هرزنامه‌ای)
سند راهبردی پدافند سایبری، ۱۳۹۲	انواع تهدیدات سایبری که در سند راهبردی پدافند سایبری به آن‌ها اشاره شده است بر اساس تهدیدات ملی می‌باشد و این تهدیدات عبارتند از: دسترسی، نفوذ، دریافت اطلاعات، دستکاری اطلاعات، جابجایی اطلاعات، تخریب اطلاعات، توقف سرویس، آسیب رساندن به زیرساخت ارتباطی، تخریب زیرساخت اجرایی، آتش‌سوزی و تخریب و انفجار زیرساخت

جدول (۱): برخی از تهدیدات فضای سایبر نیروهای مسلح

با توجه به بررسی‌های انجام شده در اسناد علمی و همچنین بر اساس تدابیر و فرامین، اسناد بالادستی کشور تهدیدات فضای سایبر را می‌توان در ۴ دسته کلی دسته‌بندی نمود و هر یک از تهدیدات دارای هدف مشخص و ابزارهایی می‌باشد که در جدول ۲ به آن‌ها اشاره شده است.

نوع تهدید	هدف تهدید	ابزار تهدید
جاسوسی	شنود، سرقت، نفوذ، افشاء، دسترسی، دریافت اطلاعات	بدافزار، فیشینگ، هک، جعل هویت، فریب، حملات سایبری
خرابکاری	نابودی و تخریب، اختلال یا قطع سرویس، دستکاری یا تغییر، درز اطلاعات	باج افزار و بدافزار، فیشینگ، هک، جعل هویت، فریب، حملات سایبری
عوامل ناراضی و مجرمان	سرقت، نابودی و تخریب، انکار، دستکاری یا تغییر، درز اطلاعات	بدافزار، جعل هویت، ابزارهای ذخیره‌ساز
آسیب‌پذیری‌ها	انکار، اختلال یا قطع سرویس، نابودی و تخریب، درز و نشت اطلاعات، افشاء	بدافزار، ابزارهای ذخیره‌ساز، رایانه‌های تک‌کاربره و همراه، پیکربندی نامناسب شبکه، عدم کنترل شبکه اینترنت، عدم تنظیمات در بستر شبکه، منابع انسانی فاقد صلاحیت

جدول (۲): دسته‌بندی تهدیدات فضای سایبر نیروهای مسلح

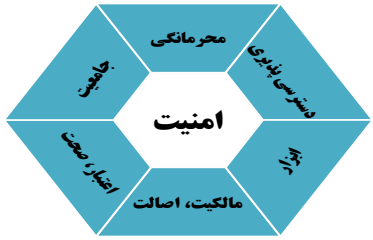
با توجه به دسته‌بندی انجام شده در تهدیدات فضای سایبر نیروهای مسلح، مدل تهدیدات به توجه به ۴ نوع تهدید اصلی به شرح شکل ۲ می‌باشد.

شکل (۲): مدل تهدیدات فضای سایبر نیروهای مسلح

امنیت فضای سایبر: امنیت سایبری یکی از دسته‌بندی‌های امنیت بر پایه فضای سایبری است که در چهره درون سایبری بر دو دسته امنیت اطلاعات و امنیت سامانه و شبکه و در چهره برون سایبری بر سه دسته امنیت کاربران و مشترکین (امنیت فردی)، امنیت زیرساخت‌های نهادهای عمومی (امنیت اجتماعی) و امنیت ملی است. امنیت اطلاعات با سه سنجه بنیادین تبلور می‌یابد: نخست قابلیت اعتماد و رازداری است تا به‌واسطه آن اطلاعات به‌صورت غیرمجاز افشاء نشوند. با این معیار سعی در پیشگیری از دسترسی اشخاص ناصالح به اطلاعات می‌شود. دوم صحت و تمامیت است تا از تغییر یا حذف غیرمجاز اطلاعات پیشگیری شود. سوم قابلیت دسترسی است تا با تحقق این معیار، ممانعت غیرمجاز از دسترسی به اطلاعات و منابع آن پیش نیاید. غیر از این سه معیار ماهوی، باید پارامترهای قابلیت استناد (شناسایی قبلی طرفین مبادله)، قابلیت پاسخگویی (تعریف و اجرای مسئولیت‌های طرفین) و عدم انکار (اثبات اینکه اطلاعات به دریافت‌کننده واقعی ارسال شده) نیز مدنظر قرار بگیرد تا از حیث شکلی نیز پشتوانه امنیت اطلاعات تضمین گردد (عالی پور، ۱۳۹۳: ۱۵).

امنیت فضای سایبر در دیدگاه‌های مختلف دارای ابعاد متفاوتی است ولی تمامی این دیدگاه‌ها دارای یک هدف واحد هستند. در مقاله‌ای که توسط اویزینیس و لاپری در سال ۲۰۰۴ ارائه شده است، سیستم‌های اطلاعاتی به سه مؤلفه اصلی سخت‌افزار، نرم‌افزار و ارتباطات تقسیم می‌شوند. در نتیجه، صفات امنیت باید در هر سه مؤلفه دیده شود تا امنیت اطلاعات فراهم شود. در این دیدگاه

صفات امنیت اطلاعات را محرمانگی، جامعیت و قابلیت دسترسی[1] تعریف می‌کنند. بـه عـلاوه بایـد لایه‌های امنیتی دیگری نیز بر روی آن فراهم شود که شـامل امنیـت فیزیکـی (محصـولات)، امنیـت کارکنان (انسان‌ها) و امنیت سازمانی (رویه‌ها) است. در شکل ۳ این سه بعد نمایش داده شده است (Avizienis and Laprie: 2004,18).



شکل (۳): مولفه‌های اصلی امنیت اطلاعات

در مقاله‌ای که پندر در سال ۲۰۱۲ منتشر نمود، مدل توسعه‌یافته امنیـت فضـای سـایبر را در ۶ بُعد ارائه نموده است (Pender: 2012, 10). محرمانگی، دسترسی‌پـذیری، یکپـارچگی و جامعیـت، اصالت و مالکیت، اعتبار و صحت، ابزار

در مقاله «مروری بر امنیت شبکه‌های کامپیوتری» مباحث مربـوط بـه مشـکلات امنیتـی، انـواع رخنه در شبکه‌ها، روش‌های جلوگیری از نفوذ، مسائل امنیتی در اینترنت و پروتکل آی پی پرداخته است. در این مقاله مهم‌ترین اقدامات امنیتی به شرح زیر معرفی شده است:

- پیشگیری (جلوگیری از خسارت)
- ردیابی (تشخیص) – (میزان خسارت، هویت دشمن، کیفیت حمله (زمان، مکـان، دلایـل حمله، نقاط ضعف و ...))
- واکنش (بازیابی و جبران خسارات، جلوگیری از حملات مجدد) (بختیاری، ۱۳۸۰: ۵).

همچنین در این مقاله مهم‌ترین روش‌های کنترلی برای ایجاد امنیت اشاره شده است که عبارتند از:

- روش رمزنگاری شامل (عمل رمز، تمامیت، تعیین هویت، امضای الکترونیکی)
- کنترل‌های نرم‌افزاری شامل (کنترل برنامه کـاربردی توسـط سیسـتم عامـل، پیـدا نمـودن نقطه‌ضعف‌های برنامه کاربردی، کنترل در طراحی یک نرم‌افزار (قبل از پیاده‌سازی))

1 -CIA(Confidentiality- Integrity- Availability)

- کنترل‌های سخت‌افزاری شامل (سخت‌افزار به‌عنوان رابط بین کاربر و سیستم (کارت هوشمند))
- تعیین سیاست‌های امنیتی شامل (ایجاد سیاست‌های امنیتی کارا (تغییر متناوب کلمه عبور))
- سایر روش‌های شامل (استفاده از شمارنده‌ها، ثبت هرگونه دسترسی به سیستم، استفاده از دیوار آتش) (همان: ۶).

یکی دیگر از اقدامات برای برقراری امنیت پایدار و به عبارتی حفاظت از فناوری اطلاعات و ارتباطات که همواره در معرض آسیب، تعرض و تهدید قرار دارد، استفاده از تیم های واکنش اضطراری رویدادهای رایانه‌ای یا CERT[1] می‌باشد. در مقاله‌ای که اولاف کوریدف در سال ۲۰۱۴ به بررسی اهداف تیم‌های واکنش اضطراری به رویدادهای رایانه‌ای می‌پردازد مهم‌ترین اهداف یک سرت را به شرح زیر ارائه می‌نماید:

- شناسایی تهدیدات امنیتی و رویدادهای بالقوه
- تشخیص تهدیدات امنیتی و رویدادها
- هماهنگی فعالیت‌های واکنش به رویداد
- مهار و کاهش رویدادهای امنیتی
- استمرار کسب و کار علی‌رغم تهدیدات امنیتی
- انعطاف‌پذیری فناوری اطلاعات و ارتباطات در برابر تهدیدات امنیتی.

شاخص‌های جهانی امنیت سایبری[2] -۲۰۱۷: اتحادیه بین‌المللی مخابرات، اولین نسخه از راهنمای راهبرد امنیت سایبر را در سال ۲۰۰۸ و نسخه اصلاحی این شاخص را برای اندازه‌گیری کمی سطح پیشرفت امنیت سایبری در کشورها طراحی کرده است. هدف نهایی اتحادیه بین‌المللی مخابرات از تهیه این شاخص تقویت فرهنگ جهانی امنیت سایبری است. این شاخص شامل پنج مؤلفه‌های قوانین و مقررات[3]، اقدامات فنی[4]، ساختارهای اجرایی و سازمانی[5]، ظرفیت‌سازی[1]، همکاری[2] ملی و بین‌المللی می‌باشد.

1- CERT (Computer emergency response team)
2- Global Cybersecurity Index(GCI): 2017
3- Legal Measures
4- Technical Measures
5- Organizational Measures

این پنج مؤلفه بنیان شاخص جهانی امنیت سایبری را شکل می‌دهند، زیرا اجزاء تشکیل دهنده فرهنگ ملی یک کشور در زمینه امنیت سایبری می‌باشند. هدف نهایی اتحادیه بین‌المللی مخابرات از این اقدام، بومی‌سازی و یکپارچه‌سازی امنیت سایبری در مقیاس جهانی می‌باشد. مقایسه راهبردهای ملی امنیت سایبری کشورهای مختلف می‌تواند منجر به شناسایی راهبردهای موفق و بهتر گردد. همچنین زمینه تبادل اطلاعات ما بین کشورها و بهره‌مندی کشورهای کمتر توسعه‌یافته را فراهم می‌نماید. از آنجا که همه کشورها به سمت محیطی شبکه‌ای و دیجیتال در حرکت می‌باشند، بومی‌سازی به‌موقع امنیت سایبری می‌تواند زیرساخت‌هایی امن‌تر و منعطف‌تر با قابلیت خودترمیمی ایجاد نماید. شاخص امنیت سایبری از پنج مؤلفه اصلی تشکیل شده است و هرکدام دارای تعدادی شاخص می‌باشند. با ارزش‌گذاری هر یک از این شاخص‌ها می‌توان امتیاز امنیت سایبری هر کشور را به دست آورد. طبق امتیازبندی انجام شده در سال ۲۰۱۷، سنگاپور با امتیاز ۰/۹۲ در رتبه اول و آمریکا با امتیاز ۰/۹۱ در رتبه دوم و کشورمان ایران با امتیاز ۰/۴۹۴ در رتبه ۶۰ قرار دارد (GCI:2017,55).

تدابیر و فرامین مقام معظم رهبری (مدظله‌العالی) در حوزه امنیت و فضای سایبر: فرماندهی معظم کل قوا اعتقاد عمیق و بنیادی به عدم توسعه فاوا بدون برقراری امنیت دارند و همواره بر تقدم امنیت تأکید نموده‌اند. در همین راستا اندیشه‌ها، نظرات، تدابیر و فرامین معظم‌له در حوزه امنیت و فضای سایبر احصاء گردیده است. برخی از موضوعات که مصداق قوی‌تری دارند به علت طبقه‌بندی در اینجا اشاره نشده است.

دستورالعمل‌ها و آیین‌نامه‌ها: در طرح‌های فنی توسعه و ساخت اماکن ... دستورالعمل استاندارد نحوه استقرار شبکه‌های رایانه‌ای ... را با لحاظ نمودن موارد امنیتی، حفاظتی و تأسیساتی تهیه و ابلاغ نماید (۱۳۹۲/۰۱/۱۵).

تحقیق، پژوهش و آموزش‌های تخصصی حوزه امنیت فضای سایبر: برنامه جامعی را جهت ارتقای سطح دانش فاوا ... با همکاری سازمان‌ها ... تهیه و در سیر مراحل تصویب قرار دهد. (۱۳۹۲/۰۱/۱۵). تعریف و اجرای پروژه‌های تحقیقاتی و فناورانه امن در حوزه فناوری‌های نوین با رویکرد جلوگیری از موازی‌کاری‌ها و تقسیم کار (۱۳۹۳/۰۴/۲۴).

1-Capacity Building
2- Cooperation

بومی‌سازی ابزار و تجهیزات حوزه امنیت فضای سایبر: به ودجا و سازمان‌ها ابلاغ کنید تکیه بر تولید داخلی و خوداتکایی در فاوا لازم است (۱۳۹۲/۰۱/۱۵). برنامه‌ریزی مناسب را برای ... تولید نرم‌افزارهای پایه بومی (سیستم عامل، بانک اطلاعات و...) و سایر نرم‌افزارهایی که می‌تواند در جهت افزایش امنیت و کاهش آسیب‌پذیری‌ها مؤثر باشد (۱۳۹۲/۰۱/۱۵).

طرح، برنامه ساختار و سازمان امنیت سایبر: سازمان مناسبی را ... جهت انجام جنگ الکترونیک در محدوده فاوا (پیشگیری از نفوذ، تخریب و فریب) پیش‌بینی و در سیر مراحل تصویب قرار دهد (۱۳۹۲/۰۱/۱۵).

راهبردها، سیاست‌ها ابلاغی حوزه امنیت و فضای سایبر: رایانه بدون امنیت، خطرآفرین است. سخت‌افزار بدون آموزش و تأمین امنیت نبایستی رشد بی‌تناسب داشته باشد (۱۳۸۵/۰۶/۰۱).

موضوعات، بودجه و اعتبارات، همکاری و تعامل بین دستگاه‌ها، دستورالعمل‌ها و آیین‌نامه‌ها، تحقیق و پژوهش و آموزش‌های تخصصی، بومی‌سازی تجهیزات سایبری و نرم‌افزارهای پایه، استاندارد بومی، سیاست‌گذاری و راهبردهای امنیتی مناسب در حوزه امنیت فضای سایبر از مهم‌ترین مصادیق امنیت فضای سایبر از منظر معظم‌له می‌باشد.

اهمیت امنیت فضای سایبر و نقش آن در صیانت امنیتی فضای سایبر: با عنایت به نفوذ و تأثیرگذاری روزافزون فضای سایبر در تمام امور جوامع و سازمان‌ها و همچنین مخاطرات و تهدیدات این فضا در عرصه‌های مختلف از قبیل اقتصاد، فرهنگ، سیاست و دفاعی، امنیتی و ...، ضرورت دارد به‌منظور صیانت امنیتی از جامعه و سازمان‌ها در برابر تهدیدات احتمالی، حکومت‌ها امنیت کامل و جامع این فضا را مدنظر قرار دهند. در جمهوری اسلامی ایران نیز به‌منظور ایفای نقشِ حاکمیت در تأمین امنیتِ این حوزه در مقابل حملات الکترونیکی، مرکز مدیریت راهبردی افتای ریاست جمهوری مأموریت یافته است در تعامل با دستگاه‌های ذی‌ربط، نسبت به امن‌سازی زیرساخت‌های دستگاه‌های حیاتی اقدام کند (افتا[1]: ۱۳۸۹).[2] بر همین اساس امنیت فضای سایبر به‌عنوان یکی از الزامات اولیه صیانت امنیتی فضای سایبر محسوب می‌گردد.

دفاع و پدافند سایبری و نقش آن در صیانت امنیتی فضای سایبر: بر اساس تعریفی که در سند راهبردی امنیت سایبری انگلستان[3] آمده است، دفاع سایبری فعال اصلی برای اجرای اقدامات

۱- سند راهبردی امنیت فضای تولید و تبادل اطلاعات

2- www.ict.gov.ir

3 -National Cyber Security Strategy 2016 - UK

امنیتی به‌منظور تقویت یک شبکه و یا سامانه است که در برابر حمله مقاوم است. دفاع سایبری فعال به‌طور معمول به تحلیل‌گران امنیت سایبریِ در حال توسعه درک درستی از تهدید در شبکه را می‌دهد و سپس به ابداع و اجرای اقدامات فعالانه در مبارزه و یا دفاع در برابر این تهدیدات اشاره دارد (سند راهبردی امنیت سایبری انگلستان، ۲۰۱۶: ۳۳).

بر اساس تعریف سازمان پدافند سایبری کشور، پدافند سایبری عبارت است از: مجموعه اقداماتی که موجب بازدارندگی، پیش‌گیری، ممانعت از انجام، تشخیص به موقع، مقابله مؤثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری توسط متخاصمین سایبری، اعم از نیروی نظامی (ارتش سایبری) کشورهای متخاصم، گروه‌های تحت حمایت پنهان دولت‌های متخاصم، جاسوسان سایبری، تروریسم‌های سایبری می‌شود. (سند راهبردی پدافند سایبری کشور، ۱۳۹۲)

مراحل دفاع سایبری که در سند راهبردی پدافند سایبری کشور ارائه شده است دارای ابعاد و مؤلفه‌های زیر می‌باشد:

بازدارندگی: نامطلوب جلوه دادن حمله نه لزوماً جلوگیری از آن (کنترل‌های امنیتی، قوانین، مجازات‌ها، اقدامات تلافی‌جویانه)

جلوگیری: ممانعت از وقوع حمله و دستیابی مهاجم به منبع اطلاعات (پنهان‌سازی اطلاعات، احراز هویت، کنترل دسترسی، ارزیابی امنیت و رفع آسیب‌پذیری‌ها)

هشداردهی: شناسایی حمله بالقوه قبل از شروع یا در مراحل اولیه وقوع (تشخیص بالقوه، پیام ترک مخاصمه)

شناسایی: مانیتور کردن و شناسایی حمله پس از وقوع (نگهبان، دوربین، ضدویروس، سیستم تشخیص نفوذ، دیوار آتش)

آمادگی اضطراری: توانایی بهبود و بازیابی منبع اطلاعات پس از حمله (بهبود دفاع، بازیابی اطلاعات)

واکنش: هدایت اوضاع، جبران خسارات، تقویت دفاع و یا مقابله به مثل

چرخه پدافند سایبری شامل مجموعه اقداماتی است که به‌صورت یک زنجیره متصل به هم بوده و با انجام این اقدامات صیانت امنیتی فضای سایبر ارتقاء یافته و تضمین امنیت پایدار مراجع امنیتی سایبری به وجود می‌آید. در این چرخه اقداماتی از قبیل رصد، پایش و تشخیص تهدید،

استخراج آسیب‌پذیری، تجزیه و تحلیل ریسک، مدیریت دفاعی صحنه، بازیابی اطلاعات، ایمن‌سازی و پایداری اطلاعات، مصون‌سازی سایبری، ارتقاء آمادگی پدافند سایبری، تولید قدرت پاسخگویی به تهدید، به‌روزرسانی تهدیدات و مقایسه با وضع موجود را شامل می‌گردد (سند راهبردی پدافند سایبری کشور، ۱۳۹۲).

همان‌طور که در ابعاد دفاع سایبری مشخص است یکی از ارکان صیانت امنیتی داشتن رویکرد دفاع سایبری در اقدامات مربوط به حفاظت از اطلاعات در برابر تهدیدات می‌باشد. بر همین اساس دفاع و پدافند سایبری به‌عنوان یکی از ارکان اصلی در صیانت امنیتی به شمار می‌آید.

روش تحقیق:

پژوهش حاضر در پی رفع نیازها و حل مشکلات مطرح در فضای سایبر نیروهای مسلح و ارائه راه‌حل آن‌ها هست، لذا پژوهش حاضر توسعه‌ای – کاربردی است. روش تحقیق به‌صورت آمیخته (کمی و کیفی) بوده و در روش کیفی با روش تحلیل مضمون[1] که یکی از روش‌های ساده و کارآمد تحلیل کیفی است و دارای انعطاف‌پذیری نسبت به سایر روش‌های تحلیل کیفی است، استفاده می‌گردد. تحلیل مضمون به دنبال استخراج مضامین برجسته یک متن در سطوح مختلف است و شبکه مضمون‌ها نیز به دنبال تسهیل ساختاردهی و ترسیم این مضمون‌ها است. شبکه مضامین بر اساس یک رویه مشخص، مضمون‌ها در قالب مفاهیم و مضمون‌های پایه، مقولات و مضمون‌های سازمان دهنده، مضمون‌های فراگیر نظام‌مند می‌کند (درخشه و دیگران: ۱۳۹۴، ۵۵).

در این تحقیق ابتدا فرامین و تدابیر مقام معظم رهبری و اسناد بالادستی در حوزه سایبر مورد تحلیل قرار گرفته و مضامین پایه و مفاهیم استخراج شده و با بهره‌گیری از روش گروه خبرگی و مصاحبه با خبرگان چارچوب مدل مفهومی، تحقیق ایجاد گردید و در نهایت کلیه ابعاد و مؤلفه‌های احصاء شده و همچنین مدل مفهومی مورد تأیید خبرگان قرار گرفته است.

در بخش کمی، پس از اینکه ابعاد و مؤلفه‌های صیانت امنیتی فضای سایبر نیروهای مسلح مورد شناسایی قرار گرفت، پرسشنامه‌ای توسط محقق طراحی گردید و پس از انجام مراحل روایی و پایایی آن، با مراجعه به جامعه آماری اقدام به نمونه‌گیری شد. با توجه به جامعه آماری که در این تحقیق در نظر گرفته شده است (۸۰ نفر)، پرسشنامه‌ها به افراد مورد نظر ارسال گردید و تعداد ۶۸ پرسشنامه جمع‌آوری شد و برای تجزیه و تحلیل داده‌های جمع‌آوری شده از روش‌های آمار

1 -Thematic analysis

توصیفی جهت تشریح و تبیین پاسخ‌ها مورد استفاده قرار گرفت. لازم به ذکر است در آمار تحلیلی این تحقیق از آزمون‌های آمار توصیفی ضریب همبستگی (آزمون)، معادلات ساختاری (تحلیل عاملی تأییدی) و برای رتبه‌بندی هر یک از مؤلفه‌های الگوی راهبردی از آزمون فریدمن استفاده شد. برای تعیین اعتبار و پایایی سؤالات پرسشنامه، در این تحقیق با استفاده از نرم‌افزار spss ضریب آلفای کرونباخ پرسشنامه طیف لیکرت به دست آمد که بیش از نه‌دهم (0.922) می‌باشد و نشان‌دهنده پایایی بالای پرسشنامه است.

تحلیل مضامین موضوع صیانت امنیتی فضای سایبر از منظر فرامین و تدابیر مقام معظم رهبری و اسناد بالادستی حوزه سایبر:

با توجه به تأکیدات فراوان مقام معظم فرماندهی کل قوا در خصوص فرصت‌ها و تهدیدات فضای سایبری و اهمیت فراوان به ایجاد امنیت و همچنین تأکید معظم‌له در فضای سایبر «اصل را بر پیشگیری بگیرید»، لذا امنیت این فضا را اصل اول توسعه می‌دانند. در همین راستا کلیه فرمایشات معظم له از سال‌های ۸۶ تاکنون که در قالب فرامین، تدابیر، سخنرانی‌ها، بازدیدها و ... ارائه گردیده و مرتبط با موضوعات صیانت امنیتی فضای سایبر، شامل (امنیت، فضای مجازی و فضای سایبر، فاوا، جنگال، مراقبت، پیشگیری و ...) است احصاء گردیده (تعداد ۷۸ تدبیر و فرامین) که در متن مقاله به برخی از آن‌ها اشاره شده است و بر پایه روش تحلیل مضامین مورد بررسی تحلیلی قرار گرفته است.

همچنین مهم‌ترین اسناد بالادستی حوزه سایبر که مورد بررسی قرار گرفته است عبارتند از: سیاست‌های کلی برنامه ششم و پنجم توسعه، سیاست‌های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات، سیاست‌های کلی نظام در امور پدافند غیر عامل، سیاست‌های ابلاغی به شورای عالی فضای مجازی، قانون برنامه پنج ساله ششم جمهوری اسلامی ایران (۱۴۰۰ – ۱۳۹۶)، برخی مواد قانون برنامه پنجم توسعه کشور مرتبط با فضای سایبر، قانون جرائم رایانه‌ای کشور است.

همچنین راهبردها و مأموریت‌های مراکز و سازمان‌ها در حوزه صیانت امنیتی فضای سایبر نیز مورد تحلیل قرار گرفته است که برخی از آن‌ها عبارتند از: مرکز مدیریت راهبردی افتای ریاست جمهوری، سند راهبردی امنیت فضای تولید و تبادل اطلاعات (افتا)، سازمان پدافند غیرعامل در حوزه فناوری اطلاعات، قرارگاه پدافند سایبری کشور، پلیس فتا (فضای تبادل اطلاعات)، مرکز

بررسی تهدیدات سایبری، کمیسیون امنیت و کنترل امنیت ارتباطات و فناوری اطلاعات نیروهای مسلح، آئین‌نامه جامع امنیت فناوری اطلاعات و ارتباطات نیروهای مسلح، صنعت امنیت فناوری اطلاعات و ارتباطات نیروهای مسلح (صاافتا)

با توجه به تحلیل مضامین انجام شده، در مجموع تعداد ۳۱۶ مضمون پایه استخراج گردید و در قالب تعداد ۷۰ مضمون سازمان دهنده و ۹ مضمون پایه دسته‌بندی گردید. با توجه به اصلاحات انجام شده توسط گروه خبرگی و برخی از خبرگان مضامین سازمان دهنده و مضامین فراگیر در حوزه اقدامات و راهکارهای صیانت امنیتی فضای سایبر احصاء گردید که نتیجه آن به شرح جدول ۳ ارائه می‌گردد.

مضامین فراگیر	توضیحات	مضامین سازمان دهنده
شناسایی (منابع و دارایی‌های سایبری)	درک زمینه کسب و کار، منابع و خطرات مربوط به امنیت سایبری	مدیریت دارایی‌های فضای سایبر (داده‌ها، کارکنان، سخت‌افزار، سامانه‌ها)
		شناخت کسب و کار و مأموریت
		شناخت حاکمیت (راهبردها، سیاست‌ها، روش‌های مدیریت و نظارت)
		ارزیابی ریسک و خطرات
		راهبردهای مدیریت خطرات (فرایند شناسایی، ارزیابی و پاسخ به خطر)
		شناسایی قوانین، مقررات و دستورالعمل‌های بازدارنده و پیشگیرانه داخلی و بین‌المللی
محافظت (ایمن‌سازی و پایداری امنیت)	طراحی و پیاده‌سازی راهکارهای ایمنی و امنیتی مناسب برای اطمینان از خدمات و سرویس‌های فضای سایبر	کنترل و نظارت دسترسی کاربران و سامانه‌ها
		آموزش، آگاه‌سازی و فرهنگ‌سازی (عمومی و تخصصی) و تبیین تهدیدات فضای سایبر
		امنیت داده‌ها و اطلاعات
		صیانت سرمایه انسانی و امنیت کارکنان (صلاحیت حین ورود، حین خدمت و رهایی خدمت)
		فرآیندهای حفاظت از اطلاعات، کارکنان و شبکه
		مشارکت و تعامل بخش دولتی و خصوصی، فرماندهی و حفاظت، نهادهای امنیتی و نظارتی
		تعمیر و نگهداری و به‌روزرسانی سامانه‌های موجود و تداوم پایداری امینت
		فناوری‌های حفاظتی و امنیتی شامل راهکارهای فنی، امنیتی و مدیریتی
		یکپارچه‌سازی سامانه‌های نرم‌افزاری و سخت‌افزاری با رعایت لایه‌بندی استقلال بخش‌ها
		آزمایشگاه مرجع کنترل امنیت سایبر و ارزیابی امنیتی محصولات سایبری
		رمزنگاری مستقل و بومی
		پیاده‌سازی و استقرار استانداردهای امنیت سایبر بومی
		ممیزی، اعتبارسنجی و اعطای گواهی در حوزه امنیت سایبر
		استقرار ابزارهای کنترل امنیت سایبری بومی
		طبقه‌بندی و حیطه‌بندی اطلاعات

مضامین فراگیر	توضیحات	مضامین سازمان دهنده
		توسعه مرکز عملیات امنیت بومی (حداقل نرم‌افزار)
		آگاهی و دانش تخصصی
		بهره‌برداری از سرویس‌های مبتنی بر ابرداده بومی
		امنیت فیزیکی
تشخیص و کشف (تهدیدات و آسیب‌های امنیتی)	طراحی و پیاده‌سازی فعالیت‌های مناسب برای تشخیص، کشف و شناسایی وقوع یک رویداد امنیتی در فضای سایبر	شناسایی به‌موقع ناهنجاری‌ها، رویدادها، تخلفات و شکست‌ها
		شناسایی و رفع آسیب‌پذیری‌های سایبری
		نظارت مستمر بر امنیت، باهدف اثربخشی اقدامات حفاظتی
		فرایندهای تشخیص، آگاهی وضعیتی از حوادث و فعالیت‌های غیرعادی
		رصد و پایش مستمر تهدیدات محتمل و شناسایی مقدمات وقوع یک رویداد
		پیشگیری از بروز تهدیدها و حملات احتمالی
		حسگرها، سنسورها و سامانه‌های مراقبتی و هشداردهی
تحلیل (مخاطرات)	طراحی و پیاده‌سازی فعالیت‌های مناسب برای جمع‌آوری و پالایش رویدادها و انتخاب راه‌حل مناسب امنیتی در فضای سایبر	جمع‌آوری و نگهداری سوابق رویدادها
		غربالگری و پاک‌سازی سوابق رویدادها
		پالایش هوشمند اطلاعات و رویدادها
		اشراف اطلاعاتی با اشتراک‌گذاری اطلاعات نهادهای امنیتی و نظارتی
		تصمیم‌گیری، اتخاذ تدبیر مناسب و انتخاب راه‌حل مناسب برای واکنش
		پیش‌بینی مخاطرات و رویدادها
پاسخ و واکنش (رویدادهای امنیتی)	طراحی و پیاده‌سازی فعالیت‌های عملیاتی در واکنش به یک رویداد امنیتی فضای سایبر	برنامه‌ریزی برای پاسخگویی و واکنش (روش‌های اجرایی و فرآیندهای پاسخ)
		ارتباطات و تعاملات هماهنگ‌کننده با نهادها و سازمان‌های داخلی و خارجی
		تجزیه وتحلیل (حمایت از بهبود فعالیت‌ها برای حصول اطمینان پاسخ)
		کاهش و جلوگیری از انجام و گسترش یک رویداد
		بهبود و ارتقاء سطح توانمندی و فعالیت‌های ترکیبی جهت مقابله
		نظارت بر فرایند پاسخ به رویداد
		هوشمندی در پاسخگویی و مقابله
		هشداردهی (هشدارها و اخطارها و اطلاع‌رسانی)
		حفظ آمادگی اضطراری پاسخ (انجام رزمایش سایبری در جهت پاسخ)
		برخورد مناسب با تخلفات و انجام توجیه و ارشاد
بازیابی (حفظ و بهبود وضعیت)	پیاده‌سازی فعالیت‌های متناسب برای حفظ انعطاف‌پذیری و بازگرداندن هرگونه قابلیت به خدمات مختل شده	برنامه‌ریزی برای بازیابی و بازسازی به موقع سیستم
		ارتقاء (برنامه‌ریزی و فرآیندهای بازیابی با نگاه به آینده)
		تداوم و استمرار خدمات‌رسانی و جلوگیری از قطع خدمات، تخریب و ...
		انعطاف‌پذیری فاوا در برابر تهدیدات امنیتی و پیش‌بینی راهکارهای موازی
بازدارندگی (توان و قدرت	طراحی و پیاده‌سازی	تدوین قوانین و مجازات‌های بازدارنده
		مأیوس‌سازی و ممانعت از اشراف اطلاعاتی دشمن

مضامین فراگیر	توضیحات	مضامین سازمان دهنده
پاسخگویی به تهدیدات)	اقدامات عملیاتی در خصوص تصمیمات دشمن به یک رویداد امنیتی فضای سایبر	تهدید در مقابل تهدید به‌صورت نامرئی و غیرعلنی
		جلوگیری از بازتاب فرهنگ و رفتار دشمن
		پیاده‌سازی معماری پدافندی در جهت پایداری فضای سایبر در مقابل آسیب‌پذیری
		قدرت پاسخگویی در برابر تهدیدات و توان تهاجمی بالا
		مقاومت و تاب‌آوری بدون آسیب دیدن و توانایی مقابله به مثل
		پاسخ به موقع و قدرت پشیمان کنندگی دشمن
		دنبال‌گیری تا رفع اثر تهدید دشمن
مقابله مؤثر (توان روبه‌رو شدن و تلافی)	پیاده‌سازی اقدامات عملیاتی در روبه‌رو شدن و تلافی خسارت وارده توسط دشمن در امنیت فضای سایبر	دشمن‌شناسی و تجزیه و تحلیل رفتارهای دشمن
		آمادگی عالمانه و دفاعی جهت مقابله با دشمن
		دفاع در مقابل حملات سایبری دشمنان
		حمله سایبری و مقابله اثربخش
نوآوری و تحول (سیاست‌ها، منابع، زیرساخت)	طراحی و پیاده‌سازی اقدامات و فعالیت‌های آموزشی، نوآورانه و تحول‌زا در جهت ارتقاء صیانت امنیتی فضای سایبر	بومی‌سازی استاندارد امنیت سایبر
		تولید بومی محصولات و زیرساخت‌های سایبری (سیستم عامل بومی و ...)
		تدوین منابع علمی بومی در حوزه سایبر
		تحقیق و پژوهش، تحول و نوآوری در امنیت فضای سایبر
		آموزش و ارتقاء کمی و کیفی منابع انسانی حوزه سایبر و امنیت سایبر

جدول ۳- جمع‌بندی تحلیل مضامین فرامین، تدابیر و اسناد بالادستی در حوزه فضای سایبر

الگوی مفهومی صیانت امنیتی فضای سایبر نیروهای مسلح

با توجه به بررسی اسناد راهبردی فضای سایبر کشورها، مدل‌ها و الگوهایی که برای صیانت امنیتی فضای سایبر ارائه شده است، دارای مدل‌های متنوعی برای تبیین امنیت فضای سایبر می‌باشند و ضرورت وجود الگویی بومی برای نیروهای مسلح که به‌عنوان الگوی صیانت امنیتی فضای سایبر باشد؛ بسیار مشهود است. در همین خصوص با مطالعه کلیه نظریه‌ها و مدل‌ها در فضای سایبر و امنیت فضای سایبر و همچنین با مطالعه فرامین و تدابیر فرماندهی معظم کل قوا و اسناد بالادستی فضای سایبر در کشور، الگوی مفهومی پیشنهادی که ابعاد و مؤلفه‌های آن بر اساس مطالعه اکتشافی از فرامین و اسناد بالادستی به دست آمده است، تبیین می‌گردد. مدل مطالعه بر پایه اهداف سه‌گانه چیستی، چرایی و چگونگی پایه‌گذاری شده است و در پاسخ به سؤال ابعاد و مؤلفه‌های صیانت امنیتی فضای سایبر نیروهای مسلح جدول ۴ می‌تواند به شناخت موضوع کمک نماید.

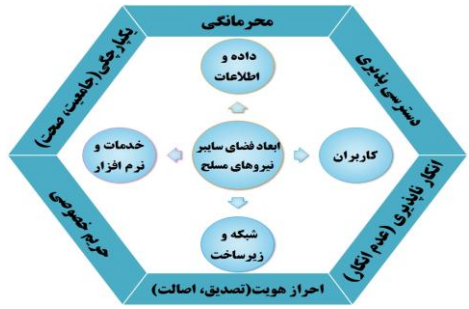
ابعاد و مؤلفه‌های صیانت امنیتی فضای سایبر نیروهای مسلح		
چیستی	چرایی	چگونگی
این بخش بر ماهیت و عوامل اصلی که در فضای سایبر نیروهای مسلح می‌بایست صیانت امنیتی شوند دلالت دارند.	این بخش به علل و اهدافی که برای صیانت امنیتی فضای سایبر نیروهای مسلح لازم است دلالت دارند.	این بخش به کلیه بایدها و نبایدها، الزامات و اقداماتی که برای صیانت امنیتی فضای سایبر لازم است پرداخته می‌شود.

جدول (۴) ابعاد و مؤلفه‌های صیانت امنیتی فضای سایبر نیروهای مسلح

چیستی: عوامل اصلی فضای سایبر نیروهای مسلح: با مطالعه اسناد و مدارک معتبر علمی در حوزه سایبر مهم‌ترین ابعاد و مراجع امنیتی فضای سایبر که باید صیانت امنیتی شود تا از هرگونه آسیب و تهدید حفظ گردد بر ۴ پایه اصلی استوار بوده که عبارتند از: داده و اطلاعات، کاربران، شبکه و زیرساخت، خدمات و نرم‌افزار است. در شکل ۴ ابعاد و عوامل اصلی فضای سایبر نیروهای مسلح ترسیم گردیده است.

چرایی: علل و اهدافی امنیتی فضای سایبر نیروهای مسلح: هدف اصلی صیانت امنیتی، تضمین پایدار امنیت فضای سایبر است. بر اساس مطالعه اسناد و مدارک معتبر علمی در حوزه سایبر مهم‌ترین اهداف امنیتی که می‌بایست از آن‌ها صیانت امنیتی شود در ۶ موضوع یکپارچگی، محرمانگی، دسترسی‌پذیری، انکارناپذیری، احراز هویت، حریم خصوصی سازمان احصاء گردیده است. اهداف امنیتی یکپارچگی، محرمانگی، دسترسی‌پذیری، احراز هویت توسط پندر در سال ۲۰۱۲ معرفی شده است (Pender: 2012, 10) . انکارناپذیری (عدم انکار) نیز به‌عنوان یکی دیگر از اهداف امنیتی شناسایی گردیده است (Landwehr: 1994, 17). محافظت از حریم خصوصی سازمان در رساله دکتری آقای حسینی به‌عنوان یکی دیگر از اهداف امنیتی معرفی شده است (حسینی، ۱۳۹۵: ۲۸۶).

با توجه به تأیید خبرگان در خصوص ۶ هدف امنیتی در فضای سایبر نیروهای مسلح، در شکل ۵ کلیه اهداف امنیتی که برای فضای سایبر نیروهای مسلح لازم و ضروری می‌باشد ترسیم شده است و صیانت امنیتی از این اهداف امنیتی باید صورت پذیرد.



شکل (۴): چرخه صیانت امنیتی فضای سایبر

چگونگی: اقدامات و راهکارهای صیانت امنیتی فضای سایبر نیروهای مسلح: در این بخش با هدف صیانت امنیتی از اهداف امنیتی شش‌گانه در فضای سایبر نیروهای مسلح و با مطالعه کلیه فرامین و تدابیر فرماندهی معظم کل قوا، اسناد بالادستی در فضای سایبر کشور، مدارک معتبر علمی در حوزه سایبر و همچنین اسناد راهبردی فضای سایبر کشورهای منتخب، کلیه بایدها و نبایدها، الزامات و اقداماتی که برای صیانت امنیتی فضای سایبر لازم است، احصاء گردید و در قالب مؤلفه و زیر مؤلفه دسته‌بندی شده است که در جدول ۳ ارائه شده است. این مؤلفه‌ها در ۹ مضامین فراگیر دسته‌بندی شده است که بر اساس اسناد علمی معتبر دارای یک فرآیند سیستمی می‌باشد که طبق انجام مصاحبه‌ها و نظرات خبرگان و جلسات خبرگی انجام شده این فرآیند در قالب چرخه صیانت امنیتی فضای سایبر مورد تأیید خبرگان قرار گرفته است.

شکل (۵): چرخه صیانت امنیتی فضای سایبر

مدل مفهومی ابعاد و مؤلفه‌های صیانت امنیتی فضای سایبر نیروهای مسلح

در این بخش مدل مفهومی ابعاد و مؤلفه‌های صیانت امنیتی فضای سایبر نیروهای مسلح که در سه بعد ترسیم شده است ارائه می‌گردد:

برای دستیابی به پایه‌های اصلی مدل مفهومی با انجام مصاحبه با ۱۰ نفر از خبرگان، نهایتاً مشخص گردید که مدل از ۳ بُعد اصلی و ۱۹ مؤلفه تشکیل می‌شود و همان‌گونه که فضای سایبر توانمندساز فضای فیزیکی است و لذا مشابه فضای فیزیکی طول، عرض و ارتفاع معرف آن است و مدل اصلی بر همین اساس تبیین گردیده و در شکل ۶ مشاهده می‌شود.

شکل (۶): مدل مفهومی ابعاد و مؤلفه‌های صیانت امنیتی فضای سایبر نیروهای مسلح

مطالعه تطبیقی اسناد راهبردی امنیت فضای سایبر کشورهای منتخب با موضوع صیانت امنیتی: بر اساس جمع‌بندی‌های انجام شده و مطالعه اسناد راهبردی امنیت فضای سایبر کشورها که توسط محقق شناسایی گردید و با توجه به ابعاد و مؤلفه‌های الگوی صیانت امنیتی فضای سایبر که از فرامین و تدابیر و اسناد بالادستی کشور احصاء شده است، همان‌طور که در جدول ۵ مشهود

است، ابعاد و مؤلفه‌های شناسایی شده یا مورد تأیید اسناد راهبردی امنیت فضای سایبر کشورهای مورد بررسی و الگوهای امنیت فضای سایبر می‌باشد و یا بخشی از ابعاد و مؤلفه‌های آن مورد تأیید است و لذا می‌توان نتیجه گرفت که سمت و سوی مطالعات با اسناد راهبردی تطبیق داشته و می‌تواند به‌عنوان یک پشتیبان برای این موضوع به شمار آید.

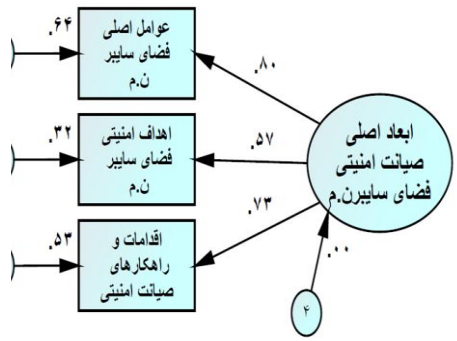
ردیف	عنوان سند راهبردی	سال انتشار	عوامل اصلی فضای سایبر				اهداف امنیتی فضای سایبر					اقدامات و راهکارهای صیانت امنیتی فضای سایبر							
			داده و اطلاعات	کاربران	شبکه و زیرساخت	خدمات و نرم‌افزار	یکپارچگی	محرمانگی	دسترسی‌پذیری	انکارناپذیری	احراز هویت	حریم خصوصی	شناسایی	محافظت	تشخیص و کشف	تحلیل	پاسخ و واکنش	بازیابی	بازدارندگی	مقابله مؤثر	نوآوری و تحول
۱	شاخص‌های جهانی امنیت سایبری	۲۰۱۷	*	*	*	*	*	*	*				*	*	*	*	*	*			*
۲	دکترین امنیت اطلاعاتی فدراسیون روسیه	۲۰۱۶	*	*	*	*	*	*	*				*	*	*		*		*		*
۳	راهبرد امنیت فضای سایبری ملّی چین	۲۰۱۶	*	*	*	*	*	*	*		*	*	*	*	*	*	*	*	*	*	*
۴	راهبرد امنیت ملی سایبری انگلستان	۲۰۱۶	*	*	*	*	*	*	*				*	*	*		*		*	*	*
۵	راهبرد امنیت سایبری آلمان	۲۰۱۶	*	*	*	*	*	*	*				*	*	*	*	*		*	*	*
۶	راهبرد سایبری وزارت دفاع آمریکا	۲۰۱۵	*	*	*	*	*	*	*				*	*	*	*	*	*	*	*	
۷	سیستم حفاظت امنیت سایبری ملی آمریکا	۲۰۱۵	*	*	*	*	*	*	*				*	*	*	*	*	*	*		*
۸	راهکارهای امنیت ملی سایبری بین‌المللی – ناتو	۲۰۱۴	*	*			*	*	*					*			*				*
۹	کنترل امنیتی برای دفاع سایبری- شورای امنیت سایبری آمریکا	۲۰۱۴	*	*	*	*	*	*	*		*	*	*	*	*	*	*				*
۱۰	مدل مرجع ایمنی و تضمین اطلاعات	۲۰۱۳	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*				

۱۱	برنامه حفاظت از اطلاعات طبقه‌بندی‌شده وزارت دفاع آمریکا	۲۰۱۳	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
۱۲	راهبرد امنیت سایبری ملی- اتحادیه بین‌المللی مخابرات - ITU	۲۰۱۱	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*
۱۳	چارچوب مدیریت امنیت اطلاعات در استاندارد ایزو ۲۷۰۰۱	۲۰۱۱	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
۱۴	چارچوب مدل سازمان‌دهی فناوری اطلاعات (کوبیت)	۲۰۱۰	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*					
۱۵	معماری امنیت در استاندارد ۸۰۵ اتحادیه بین‌المللی مخابرات	۲۰۰۶	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*				
۱۶	مدل معماری فراسازمانی مؤسسه ملی استاندارد آمریکا (NIST)	۲۰۰۵	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
۱۷	چارچوب معماری امنیتی سابسا	۱۹۹۵	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	*	

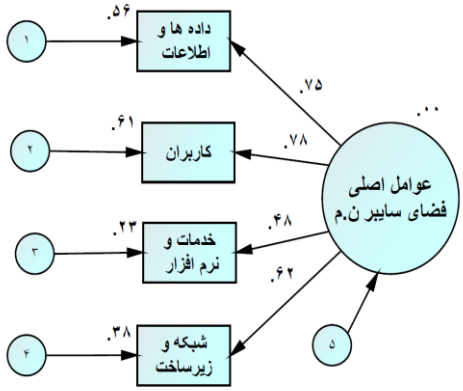
جدول (۵): مطالعه تطبیقی صیانت امنیتی فضای سایبر

تحلیل عاملی تأییدی ابعاد و مؤلفه‌های شناسایی شده صیانت امنیتی فضای سایبر نیروهای مسلح: در ابتدا برای تحلیل عاملی تأییدی الگوی راهبردی مورد نظر، ابعاد و مؤلفه‌های شناسایی شده صیانت امنیتی فضای سایبر نیروهای مسلح مطابق شکل با نرم‌افزار آموس[1] و بر اساس داده‌های جمع‌آوری شده مورد بررسی قرار گرفت و نتایج به دست آمده حکایت از تأیید و برازش مدل را دارد. اعدادی که روی یال‌های مدل قرار دارند، این عدد نقش میزان تأثیر بار عاملی بر روی مؤلفه‌های مربوط به هر بُعد را نشان می‌دهد و حکایت از آن دارد که کلیه بارهای عاملی برآورد شده نیز از حیث آماری معنادار است (بر اساس استاندارد نرم‌افزار آموس بار عاملی بزرگ‌تر از ۰/۳ دارای اعتبار بالایی است)

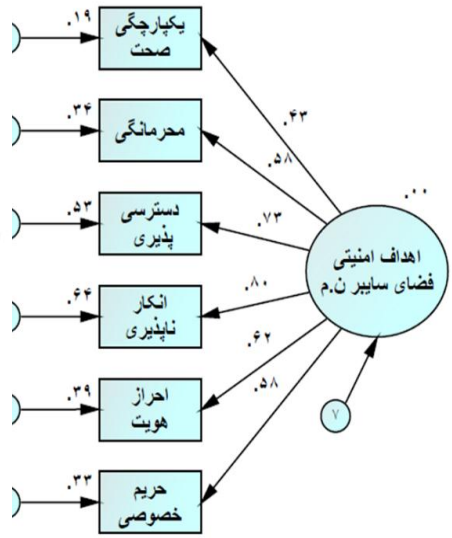
1 -Amos



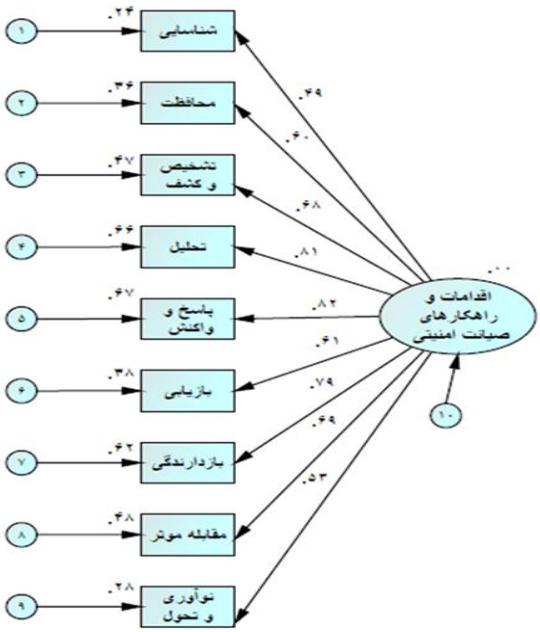
شکل (۷): تحلیل عاملی ابعاد اصلی الگوی راهبردی



شکل (۸): تحلیل عاملی مؤلفه‌های بُعد عوامل اصلی



شکل (۹) تحلیل عاملی مؤلفه‌های بُعد اهداف امنیتی



شکل (۱۰): تحلیل عاملی مؤلفه‌های بُعد اقدامات و راهکارهای صیانت امنیتی

نتیجه‌گیری:

ابعاد و مؤلفه‌های الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح، پس از بررسی الگوهای منتج شده از تئوری‌ها و کارکردها همراه با بررسی تطبیقی اسناد بالادستی و اسناد راهبردی ۱۳ کشور و همچنین از طریق مراجعه به آرای خبرگان در حوزه‌های راهبردی و امنیتی فضای سایبر، به‌طور منطقی و مفهومی استنباط گردید و با ساده‌سازی مفاهیم به دست آمده موضوع و مفهوم صیانت امنیتی به‌صورت الگویی متشکل از ابعاد، مؤلفه‌ها بر اساس فرامین، تدابیر فرماندهی معظم کل قوا و اسناد بالادستی و همچنین تطبیق با اسناد راهبردی کشورها با استفاده از روش پژوهش آمیخته با روش توصیفی استخراج گردید.

الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح از سه بعد اصلی و ۱۹ مؤلفه تشکیل شده است.

- بُعد عوامل اصلی فضای سایبر (با ۴ مؤلفه)
- بُعد اهداف امنیتی فضای سایبر نیروهای مسلح (با ۶ مؤلفه)
- بُعد اقدامات و راهکارهای صیانت امنیتی فضای سایبر نیروهای مسلح (با ۹ مؤلفه و ۷۰ زیر مؤلفه)

با توجه به نتایج به دست آمده از تحلیل داده‌های کمی تحقیق، رتبه‌بندی ابعاد و مؤلفه‌ها که با استفاده از آزمون رتبه‌بندی فریدمن انجام گردیده است به شرح زیر است:

مؤثرترین بُعد، اهداف امنیتی فضای سایبر نیروهای مسلح و سپس عوامل اصلی فضای سایبر نیروهای مسلح و در نهایت بُعد اقدامات و راهکارهای صیانت امنیتی فضای سایبر نیروهای مسلح می‌باشد.

در بُعد اهداف امنیتی فضای سایبر نیروهای مسلح مهم‌ترین مؤلفه‌ها به ترتیب رتبه‌بندی عبارتند از محرمانگی، احراز هویت، یکپارچگی، دسترسی‌پذیری، عدم انکار و در نهایت حریم خصوصی سازمان است.

در بُعد عوامل اصلی فضای سایبر نیروهای مسلح مهم‌ترین مؤلفه‌ها به ترتیب رتبه‌بندی عبارتند از داده‌ها و اطلاعات، کاربران، شبکه و زیرساخت و در نهایت خدمات و نرم‌افزار می‌باشد.

در بُعد اقدامات و راهکارهای صیانت امنیتی فضای سایبر نیروهای مسلح مهم‌ترین مؤلفه‌ها بـه ترتیب رتبه‌بندی عبارتند از بازدارندگی، تشخیص و کشف، محافظت، مقابله مؤثر، تحلیل، نـوآوری و تحول، پاسخ و واکنش، بازیابی و در نهایت شناسایی می‌باشد.

الگوی راهبردی تبیین شده، نه تنها از ویژگی‌های بومی برخوردار است بلکه با داشتن رویکـرد بازدارندگی و مقابله تأکیدات فرماندهی معظم کل قوا را نیز در این حوزه پاسخگو می‌باشد.

مهم‌ترین محورهایی که می‌توان از نتایج این تحقیق برشمرد عبارتند از:

- شناسایی و تبیین ابعاد، مؤلفه‌های الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح
- تولید ادبیات در خصوص صیانت امنیتی فضای سایبر در نیروهای مسلح
- ایجاد و فراهم نمودن زمینه وفاق در فرآیند تصمیم سازی و تصمیم‌گیری امنیتی فضای سایبر بین فرماندهی و حفاظت اطلاعات در چارچوب طراحی الگوی راهبردی صیانت امنیتی فضای سایبر
- تقویت و ارتقا تفکر راهبردی در حوزه صیانت امنیتی فضای سایبر در نیروهای مسلح
- ایجاد پل و ارتباطی میان حوزه نظر و عمل و به عبارتی اجماع در خصوص نحوه و چگونگی برخورد با موضوع صیانت امنیتی در فضای سایبر نیروهای مسلح
- بی‌نیاز نمودن مسئولین امنیتی و فرماندهان نیروهای مسلح در مراجعه به الگوهای غیربومی
- ایجاد تقسیم‌کار بین فرماندهی و حفاظت اطلاعات، برای روشمند شدن دیدگاه‌ها در فضای سایبر نیروهای مسلح
- فراهم آوردن زمینه لازم برای مواجهه هوشمندانه و مقتدرانه با تحولات پرشتاب فضای سایبر

الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح

بر اساس تعاریف و الگوهای نظری موجود، فرآیند صیانت امنیتی همانند یک چرخه پدافند سایبری است که دائماً در چرخش بوده و تمام مؤلفه‌ها با نگاه به فرامین و اسناد بالادستی بروز گردیده و همواره در حال رصد، کشف و شناسایی تهدیدات، آسیب‌پذیری‌ها می‌باشد و این فرآیند همواره حفظ پایداری اهداف امنیتی فضای سایبر نیروهای مسلح را دنبال می‌نماید، به‌گونه‌ای که کلیه عوامل اصلی فضای سایبر نیروهای مسلح از هرگونه آسیب و تهدیدی صیانت گردد.

در همین راستا الگوی راهبردی که بتواند فرآیندهای اصلی صیانت امنیتی را تبیین نماید به‌صورت شکل ۱۱ است. الگوی راهبردی معرفی شده، دارای این ویژگی می‌باشد که با نگاه به بیرون کلیه تهدیدات و مخاطرات را رصد و شناسایی نموده و با تحلیل مخاطرات و ارائه راهکارهای مقابله‌ای و پیشگیرانه درصدد پاسخگویی به تهدیدات است. البته حفظ وضع موجود و بازیابی و برگشت به وضعیت عادی و تاب‌آوری در برابر تهدیدات نیز از دیگر ویژگی‌های این الگو است.

در این الگو همواره توجه و نگاه با اتکاء به قدرت درونی و تولید محصولات و ابزار بومی، انجام تحقیق و پژوهش، تولید منابع بومی است و همواره درصدد رفع نقاط ضعف و آسیب‌پذیری‌ها است. نگاه به آینده و انجام پیش‌بینی و ارائه راهکارهای پیشگیرانه از دیگر ویژگی‌های این الگوی راهبردی است.

شکل (۱۲): الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح

پیشنهادات اجرایی:

با توجه به تحقیقات عمیقی که در اسناد و مقالات علمی انجام شده است، نتایج حاصله از این تحقیق، قابلیت تبدیل شدن به یک نظریه قابل اتکاء در حوزه صیانت امنیتی فضای سایبر را دارد؛ بنابراین با توجه به نتایج به دست آمده، چند پیشنهاد به شرح زیر ارائه می‌گردد:

- فرماندهان نیروهای مسلح و ساحفاهای نیروهای مسلح که در حوزه صیانت امنیتی فضای سایبر نیروهای مسلح دارای وظیفه می‌باشند، از نتایج این تحقیق برای ارتقاء سطح صیانت امنیتی فضای سایبر و تداوم امنیت استفاده نمایند.
- شناخت مأموریت و خطرات و تبیین راهبردها و سیاست‌های صیانت امنیتی با استفاده از تدوین شیوه‌نامه‌ها، آیین‌نامه‌ها و مقررات پیشگیرانه و بازدارنده توسط متولیان فضای سایبر نیروهای مسلح.
- انجام اقدامات صیانتی از قبیل کنترل، نظارت، آموزش، استقرار استاندارد بومی، حیطه‌بندی با استفاده از نیروی انسانی متعهد، جهادی در جهت تداوم و استمرار امنیت فضای سایبر.
- رصد، شناسایی و کشف تهدیدات و آسیب‌پذیری‌ها، تخلفات و شکست‌های فضای سایبر نیروهای مسلح و انجام اقدامات صیانت امنیتی جهت استمرار و تداوم امنیت و حفظ اطلاعات و منابع سایبری نیروهای مسلح.
- ایجاد ارتباطات و تعاملات سازنده نهادهای نظارتی و امنیتی در سطح نیروهای مسلح در جهت پاسخگویی و واکنش به تهدیدات با اشتراک‌گذاری اطلاعات در جهت اشراف اطلاعاتی.
- با توجه به نقش بومی‌سازی در جهت صیانت امنیتی فضای سایبر، مسئولین امر در سطح نیروهای مسلح ضمن توجه به این موضوع حمایت‌های لازم از اقدامات و محصولات امنیتی بومی به انجام رسانند.
- افزایش سطح آگاهی‌های عمومی و تخصصی در حوزه امنیت و صیانت امنیتی فضای سایبر نیروهای مسلح با اتخاذ تدابیر مدیریتی مناسب ارتقاء یابد.
- تقویت و توسعه زیرساخت‌های امنیت فضای سایبر به‌عنوان پیش‌نیاز صیانت امنیتی در فضای سایبر با تقویت نیروی انسانی متخصص، تخصیص بودجه و اعتبارات، ایجاد ساختارهای اجرایی و مأموریتی و تبیین راهبردهای صیانت امنیتی در فضای سایبر.

- ساختار سیاست‌گذاری حاکمیتی در سطح نیروهای مسلح در جهت تدوین سیاست‌های صیانت امنیتی با رویکرد منسجم‌سازی و نظارت بر اجرای آن ایجاد گردد.
- اعتبارات لازم و مکفی در جهت انجام تحقیق و توسعه هدفمند و تولید منابع بومی توسط متولیان امر تخصیص یابد.
- رصد و شناسایی فناوری‌های نوین حوزه صیانت امنیتی فضای سایبر با توجه به شناخت نقاط قوت، ضعف و توانمندی‌های دشمنان در فضای سایبر.

منابع:

- امام خامنه‌ای (مدظله‌العالی)، مجموعه فرامین و تدابیر ابلاغی در نیروهای مسلح.
- امام خامنه‌ای (مدظله‌العالی)، ***مجموعه بیانات***، WWW.Khamenei.ir
- معاونت پژوهش و تولید علم، (۱۳۹۶)، ***راهبردهای امنیت سایبری- سیاست‌گذاری***، گردآوری و تدوین: معاونت پژوهش و تولید علم، دانشگاه اطلاعات و امنیت ملی.
- بختیاری، شهرام، (۱۳۸۰)، ***امنیت شبکه‌های کامپیوتری***، پژوهشکده الکترونیک دانشگاه شریف.
- دعموش العاملی، علی، (۱۳۷۶)، ***دائرةالمعارف اطلاعات و امنیت در آثار و متون اسلامی***، مؤسسه چاپ و انتشارات دانشگاه امام حسین (ع)، جلد سوم.
- آشوب، محمدبن‌علی ابن‌شهر، (۱۳۹۰)، ***مناقب آل ابی‌طالب***، جلد دوم، نشر مکتبه الحیدریه.
- شریف‌الرضی، محمدبن‌حسین، (۱۳۴۳)، ***شرح نهج البلاغه***، جلد ۲۰، قم: نشر مرکز آیت‌اله مرعشی.
- آمدی، عبدالواحد ابن محمد، (۱۳۶۶)، ***غررالحکم و دررالکلم***، جلد ۲، قم: نشر مرکز النشر التابع لمکتب الاعلام الاسلامی.
- محمدی، علی، (۱۳۹۲)، ***اصول و مبانی فضای سایبر***، انتشارات دانشگاه عالی دفاع ملی.
- درخشه، جلال؛ افتخاری، اصغر و ردادی، محسن، (۱۳۹۴)، ***تحلیل مضمونی اعتماد در اندیشه آیت‌الله خامنه‌ای***، پژوهشگاه علوم انسانی و مطالعات فرهنگی، تهران: سال ششم، شماره سوم.
- عالی‌پور، حسن، (۱۳۹۳)، ***امنیت سایبری در افق ۱۴۰۴ (چالش‌ها و راهکارهای حقوقی رویارویی با بزه‌های امنیتی سایبری)***، تهران: همایش ملی دفاع سایبری.
- شورای عالی فناوری اطلاعات کشور، (۱۳۹۶)، ***مدل مرجع امنیت***، وزارت ارتباطات و فناوری اطلاعات، قابل دسترس در www.ieaf.ir.
- حسینی، پرویز، (۱۳۹۵)، ***ارائه الگوی راهبردی در حوزه امنیت فناوری اطلاعات و ارتباطات بر اساس گفتمان امام (ره) و رهبری، قانون اساسی، تجارب جمهوری اسلامی ایران و بهره‌گیری از تجارب موفق بشری***، تهران: دانشگاه عالی دفاع ملی، دانشکده امنیت ملی.
- نادی، حمیدرضا، (۱۳۹۲)، ***ارائه الگوی راهبردی حفاظت اطلاعات ملی جمهوری اسلامی ایران***، تهران: دانشگاه عالی دفاع ملی، دانشکده امنیت ملی.
- اداره کل فناوری اطلاعات ستاد کل نیروهای مسلح، (۱۳۹۴)، ***طرح ارتقا امنیت و افزایش قدرت دفاع در فضای سایبر در نیروهای مسلح***.

- ولوی، محمدرضا، (۱۳۸۵)، ***سیستم ارتباطی مطمئن برای نیروهای مسلح و چگونگی تأمین از سیستم ارتباطی کشور و مخصوص نیروهای مسلح***، گروه بررسی توان ملی در حوزه آماد و پشتیبانی مرکز تحقیقات راهبردی ستاد کل نیروهای مسلح.
- ***آیین‌نامه جامع امنیت فاوا*** نیروهای مسلح- ابلاغی ستاد کل ۹۱/۱۲/۰۲.
- ***سند راهبردی پدافندی سایبری کشور***، (۱۳۹۲)، سازمان پدافند غیرعامل کشور

- M. C. Libicki, Cyberdeterrence and Cyberwar, RAND Corp. 2009
- David Clark, Characterizing Cyberspace: Past, Present and Future, MIT CSAIL, Version 1.2, March 2010.
- K.F. Rauscher and V. Yaschenko (Eds.), Russia-U.S. Bilateral on Cybersecurity Critical Terminology Foundations, 2011
- C. E. Landwehr, et al. "A Taxonomy of Computer Program Security Flaws, with Examples," ACM Computing Surveys, Vol. ٢٦, No. ٣ (Sept. ١٩٩٤).
- A. Avizienis, J.C. Laprie, B. Randell and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, 2004, pp. 11-33.
- Pender-Bey, Georgie. "THE PARKERIAN HEXAD.". 2012
- W. Stallings, Cryptography and Network Security: Principles and Practice, 5th Edition, Prentice-Hall, 2011.
- Olaf Kruidhof_ Evolution of National and Corporate CERTs - Trust, the Key Factor - 2014
- S. L. P. A. H. Keith Stouffer, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology, 2014
- Global Cybersecurity Index(GCI), International Telecommunication Union(ITU), Swizerland Geneva, 2017
- National Cyber Security Strategy 2016 - UK
- Federal Bureau of Investigation (FBI) Information Technology Strategic Plan FY 2010 – 2015