فصلنامهٔ مطالعات حفاظت و امنیت انتظامی
نشریهٔ علمی (مقاله علمی- پژوهشی)
سال پانزدهم، شمارهٔ پنجاه و پنجم، تابستان ۱۳۹۹

تاریخ دریافت:۱۳۹۹/۰۲/۰۲
تاریخ پذیرش:۱۳۹۹/۰۵/۱۲

صیانت از مأموریت‌های سایبری در سازمان‌های امنیتی

اکبر استرکی[۱]، داود عبیری[۲]، احمدرضا فراشی[۳]

چکیده

زمینه و هدف: با توجه به حجم گستردهٔ وظایف و تنوع مأموریت‌های محوله سازمان‌های امنیتی نقش اساسی در استقرار امنیت عمومی و اجتماعی و متعاقب آن تثبیت امنیت ملی ایفا می‌کنند. گستردگی مأموریت‌های این سازمان، لزوم بهره‌گیری از سیستم‌ها و فناوری‌های نوین مانند فناوری اطلاعات و ارتباطات را بسیار پُررنگ کرده است. با توجه به وظایف مأموریت‌های حوزهٔ سایبری، کارکنان این حوزه به‌شدت در معرض تهدیدهای ناشی ازحضور و فعالیت در فضای سایبری هستند؛ بنابراین، حفاظت و صیانت در مقابل تهدیدهای فضای مزبور از قبیل جاسوسی رایانه‌ای، خرابکاری، براندازی، جنگ سایبری، جنگ الکترونیک، بدافزارها و سایر تهدیدها؛ با بهره‌گیری از اقدام‌های پیشگیرانه امری ضروری است.

روش‌شناسی: این پژوهش از حیث هدف کاربردی، از نظر ماهیت به‌صورت توصیفی- پیمایشی است. انجام پژوهش به شیوهٔ کمی؛ ابزار جمع‌آوری داده‌ها از طریق پرسش‌نامه انجام گردیده است که روایی آن پس از تنظیم اولیه، به تأیید متخصصان و خبرگان رسیده است. جامعه آماری در این پژوهش خبرگان مرتبط با حوزهٔ تخصصی فضای سایبری به تعداد ۱۵ نفر در سال ۱۳۹۸ بوده است.

یافته‌ها و نتیجه‌گیری: نتایج تحقیق حکایت از این دارد که مهم‌ترین عامل فضای سایبر داده‌ها و اطلاعات است که همین داده‌ها و اطلاعات به‌طور بالقوه بیشترین آسیب‌پذیری و تهدیدها را برای سازمان‌های امنیتی به‌دنبال دارد، مهم‌ترین هدف‌های امنیتی، راه‌کارهای پیشگیرانه محافظت و صیانت از مأموریت‌های سایبری است؛ از طرفی با توجه به سخنان مقام معظم رهبری(مدظله‌العالی) مبنی بر اقدام‌های آفندی به عنوان نوعی پیشگیری و صیانت؛ بنابراین پیشنهاد می‌گردد، در راستای صیانت از مأموریت‌ها تمامی مأموریت‌های سایبری در سازمان‌های امنیتی در رویکرد آفندی متمرکز گردد و با ایجاد بانک اطلاعاتی از جرائم سایبریِ رسیدگی‌شده بر ارتقای امنیت شبکه و صیانت از کارکنان اقدام کنند.

کلیدواژه: آسیب، پیشگیری، تهدید، سایبری، صیانت، مأموریت‌های سایبری.

---

۱ دکترای علوم ارتباطات، دانشیار دانشگاه علوم انتظامی.
۲ دکترای امنیت، مدرس دانشگاه علوم انتظامی.
۳ نویسندهٔ مسئول: کارشناس ارشد مدیریت دانشگاه علوم انتظامی.

مقدمه

استفاده از فناوری‌های فضای سایبری با توجه به رویکردهای جدید در دنیای کنونی امری اجتناب‌ناپذیر است؛ امروزه شاهد تحولات گسترده و عظیمی در زمینهٔ اطلاع‌رسانی و برقراری ارتباط در فضای مجازی هستیم و دهکدهٔ جهانی به ذهنیت جهانی تبدیل شده عصر اطلاعات به عصر ارتباطات و انفورماتیک تغییر ماهیت داده است.

در این میان فضای مجازی به‌عنوان یک رسانه، در نقش حلقه واسط و اتصال دهندهٔ نهادها، سازمان‌ها و گروهای مختلف اجتماعی در جامعهٔ کنونی عمل می‌کند؛ بنابراین، باید در ایجاد ارتباط بیشتر و پیشرفته‌تر، نقش حیاتی خود را متفاوت‌تر از سایر عناصر ایفا کند در چنین شرایطی، افزایش کمی و کیفی تقاضای دسترسی به فضای نوین ارتباطی را برای دریافت خدمات، اطلاعات و اطلاع‌رسانی و برقراری تعاملات بین، روش‌های ارتباطی، زندگی و کارامدی را تحت‌تأثیر خود قرار داده است (استرکی، ۱۳۹۱: ۱۲).

برای پیشگیری از تهدیدها می‌باید با شناخت و آگاهی و قدرتمندانه در این فضا وارد شد در روند پرشتاب توسعهٔ جهانی، فناوری ارتباطی با سرعتی غیرقابل وصف پیشرفت کرده و چهرهٔ جهان را دگرگون کرده است و گستره و عمق این دگرگونی به حدی است که جامعهٔ نوینی در حال پیدایش و شکل‌گیری و دورهٔ جدیدی از حیات بشر آغاز شده است.

فضای سایبری وسیله‌ای است که مدیریت و نظارت بخش عمده‌ای از امکانات آن مانند فضای اینترنت، آن را به ابزاری تبدیل کرده که به میزان بسیار زیادی مورد استفاده دشمنان و حریفان قرار می‌گیرد، بالطبع سازمان‌های اطلاعاتی نیز در راستای دست‌یابی

به هدف‌های خود در فعالیت‌هایی مانند جاسوسی، جمع‌آوری اخبار، هدایت منابع و ... از این فضا و امکانات موجود در آن استفاده می‌کنند از این رو فضای سایبری تهدیدی است که توسط دشمنان علیه ما استفاده می‌شود. با ورود فناوری به ن.م به‌ویژه سازمان‌های امنیتی به منظور قابلیت‌هایی چون سرعت، دقت، صحت، جامعیّت و مدیریت داده‌ها مورد توجه بوده و به‌عنوان فرصتی طلایی، چالش‌ها و تهدیدهایی را نیز به‌دنبال دارد. لازمهٔ حذف و کاهش قابل‌قبول تأثیر این تهدیدها، بهره‌گیری از تمهیدها و اقدام‌های صیانتی است.

عصر حاضر را به حق عصر فناوری اطلاعات نامیده‌اند. فناوری رایانه امروزه علاوه بر اینکه مورد استفاده مجریان قانون قرار می‌گیرد، مورد نظر و اقدام مجرمان نیز قرار گرفته است. آمارها نشان می‌دهد که به موازات گسترش اینترنت در جامعه و مبادلات اطلاعاتی و تجاری در این شاه‌راه اطلاعاتی، جرائم اینترنتی نیز افزایش یافته به همین منظور سازمان‌های امنیتی تلاش می‌کنند تا با تأمین امنیت فضای سایبر و برخورد با مجرمان سایبری قدرت بازدارندگی را برای وقوع جرائم را در فضای سایبر ایجاد کند؛ اما اتفاق می‌افتد که این سازمان‌ها به دلیل دسترسی آسان به بانک‌های اطلاعاتی و سامانه‌های ضدامنیتی خواسته یا ناخواسته به سوی فضاهای مخرب سایبر گرایش پیدا کرده یا سوق داده شوند یا اینکه حفاظت صحیح و اصولی از نرم‌افزارها و داده‌ها، سخت‌افزارها و تجهیزات و اماکن رایانه‌ای و نیروی انسانی این پلیس‌های تخصصی وجود نداشته باشد که زمینه‌ساز به فعلیت رسیدن تهدیدهایی از جمله همراهی و هم‌دستی با مجرمان سایبری تا حدی که در رخنه، سرقت و سوءاستفادهٔ بانک‌های اطلاعاتی، نفوذ، خرابکاری، نفی خدمات، کلاهبرداری، جاسوسی، استراق‌سمع، مواد مخدر، فساد و فحشاء و سرقت‌های اینترنتی و ... با باندها و مجرمان ارتباط و حتی تبانی داشته و موجب به خطر افتادن امنیت اجتماعی افراد (حقیقی و حقوقی) و بزرگ‌نمایی و سیاه‌نمایی برخی از مسائل اجتماعی، کمبودها و نارسایی‌های بخش‌های خصوصی و دولتی و سیاسی‌کردن هر مورد اجتماعی و فرهنگی و ایجاد جو ناامنی در

جامعه و حتی اخلال در روند مأموریت‌های سازمان‌های امنیتی و... که در نهایت موجب تهدید امنیت ملی می‌گردد.

یکی از تهدیدهای جدید در این‌باره جاسوسی رایانه‌ای است، جاسوسی رایانه‌ای ناظر بر کسب اسرار حرفه‌ای، تجاری، اقتصادی، سیاسی و نظامی و نیز افشا، انتقال و استفاده از اسرار است که به شکل ورود به دستگاه، پردازش داده‌ها و اعمال مشابه رخ می‌دهد. خرابکاری نیز به‌عنوان تهدیدی امنیت است. خرابکاری در اصطلاح به عملی گفته می‌شود که سبب از کارانداختن وسایلی تخریب تأسیسات و یا متوقف‌کردن وظایف سازمان و اشخاص به نفع دشمن می‌شود. براندازی نیز به‌عنوان تهدیدی امنیتی است، یکی از اقدام‌های مهم سازمان‌های اطلاعاتی در زمینهٔ براندازی، ایجاد نارضایتی مردمی است. سازمان‌های اطلاعاتی حریف ممکن است به منظور ایجاد نارضایتی در بین مردم ضمن تقرب به کارکنان آنان را به‌طور آگاهانه یا ناآگاهانه وادار به فعالیت‌هایی کنند که درنهایت منجر به نارضایتی مردم می‌شود؛ بنابراین پلیس در عرصهٔ جنگ رایانه‌ای هم به‌عنوان هدفی مناسب برای سازمان‌های اطلاعاتی است و به‌تبع نیازمند توسعه و گسترش تحولات بسیار زیاد و پیچیده در زمینهٔ فناوری اطلاعات و ارتباطات هم‌زمان با توسعه، سلامت، صیانت و صحت عمل پلیس است و برای حفاظت، صیانت و پیشگیری در برابر تهدیدها و آسیب‌پذیری‌هایی که متوجه مأموریت‌های سایبری می‌شود، نیازمند گرفتن تدابیر و تمهیدهای حفاظتی هدفمند است که می‌باید سازمان امنیتی به مورد اجرا بگذارد تا سازمان با وجود مواجههٔ دایمی با تهدیدهای مربوط به مأموریت‌های خود به دلیل برخورداری از قابلیت خودحفاظتی، خودنظارتی و مصونیت کافی، همواره آسیب‌ناپذیر باشند. سازمان مسئولیت دارد در این مقوله با گرفتن سیاست‌ها و محدودیت‌های حفاظتی متناسب در حوزهٔ سایبری اقدام کند؛ بنابراین نقش سازمان‌های امنیتی در تعیین قوانین و مقررات حفاظتی با تحلیل هوشمندانه صیانتی و پیشگیرانه و ارائه الگوهای امنیتی مناسب و مانع‌سازی برای حریف و برتری اطلاعاتی و انجام عملیات است تا بتواند مأموریت‌های سایبری را در برابر تهدیدها و آسیب‌پذیری

آن ایمن کند؛ و انجام این مهم بیانگر نقش سازمانی در تدوین این خط مشی و مشخص‌کردن اقدام‌های کارکنان در تحقق این هدف‌هاست. مسئله اصلی و دغدغه این پژوهش میزان تأثیرگذاری و نقش اقدام‌های پیشگیرانه در صیانت از مأموریت‌های سازمانی را بررسی می‌کند.

فضای سایبری را می‌توان به تیغ دو لبه‌ای تشبیه کرد چنانچه از آن استفاده درست شود در راه پیشرفت و سازندگی است و اگر نادرست استفاده گردد باعث تباهی و نابودی خواهد شد.

حضرت امام خامنه‌ای(مدظله‌العالی) دربارهٔ نقش رسانه‌ها می‌فرمایند: مجموعه زنجیرهٔ به هم پیوستهٔ رسانه‌های گوناگون که حالا اینترنت هم داخلش شده است و ماهواره‌ها و تلویزیون‌ها و رادیوها در جهت مشخصی حرکت می‌کنند تا سررشتهٔ تحولات جوامع را به عهده بگیرند. حالا که دیگر خیلی آسان و روراست شده است (۱۸ آبان ۱۳۸۵).

بیل گیتس معتقد است تحت تأثیر فضای مجازی جدید که در آن تلویزیون‌ها و رایانه‌ها به یک شبکه جهانی هوشمند مرتبط هستند، عناصر رفتاری انسان‌ها شکل خواهد گرفت و این شبکه‌ها ستون فقرات ساختار اجتماعی ما را تشکیل می‌دهند (کاریزی، ۱۳۸۱: ۳۲۹). با رشد شتابان فناوری ارتباطات، دو روند بزرگ و اثرگذار و متعامل «جهانی‌شدن و مجازی‌شدن» و انتقال زندگی انسان‌ها به فضاهای سایبر، مجازی‌شدن به عامل اصلی تغییر الگوهای فکری و رفتاری بخش عظیمی از انسان‌ها به‌ویژه جوانان است (اوحدی، ۱۳۸۰: ۹).

توجه به تهدیدهای فضای سایبری و انجام تحقیقات کاربردی در این حوزه از اهمیت زیر برخوردار است:

۱. شناخت تهدیدهای فضای سایبری می‌تواند نقش مؤثری در محاسبه احتمال وقوع و ارزیابی شدت آن ایفاء کرده و سیاست‌گذاری‌های موضوع‌های امنیتی در سازمان نقش تأثیرگذاری داشته باشد؛

۲. اشراف اطلاعاتی سازمان بر حوزهٔ تهدیدهای فضای سایبری در مأموریت‌های سایبری را افزایش خواهد داد؛

۳. با جرائم سایبری به‌طور مناسب، قبل، حین و بعد از وقوع برخورد می‌شود؛

٤. از تهدیدها و آسیب‌پذیری‌ها به موقع پیشگیری می‌شود؛

۵. می‌توانیم دشمن و حریف را غافل‌گیر کرده و از غافل‌گیری نیروهای خودی جلوگیری کنیم؛

٦. زمینهٔ سوءاستفادهٔ حریف و دشمن از کارکنان مأموریت‌های سایبری را از بین ببریم؛

۷. پیشگیری و مقابله مؤثر با براندازی، خرابکاری، جاسوسی و سایر تهدیدهای مرتبط با مأموریت‌های سایبری اعمال می‌گردد.

بنابراین، صیانت از کارکنان در مقابل تهدیدهای فضای مزبور از قبیل جاسوسی، جاسوسی رایانه‌ای، خرابکاری، براندازی، جنگ سایبری، جنگ الکترونیک، بدافزارها و سایر تهدیدها؛ با بهره‌گیری از اقدام‌های آفندی امری ضروری بوده و از اهمیت بالاتری برخوردار است که در این میان سازمان با انجام اقدام‌های آفندی در حوزهٔ جمع‌آوری، عملیات، برآورد هوشمندانه و ارایه الگوهای حفاظتی مناسب می‌تواند گام‌های مؤثر در پیشگیری از تهدیدها بردارد.

از این رو انجام پژوهش‌های مفید و جدی در حوزهٔ فضای سایبری امری ضروری به‌نظر می‌رسد تا با شناخت نقاط قوت و ضعف و عوامل تأثیرگذار، بتوان آینده‌نگری کرد و افق پیش روی کارکنان مأمورت‌های سایبری را ترسیم کرد.

هدف اصلی: راه‌های صیانت از مأموریت‌های سایبری سازمان‌های امنیتی؛

سؤال‌های تحقیق

سؤال اصلی: صیانت از مأموریت‌های سایبری در سازمان‌های امنیتی چگونه است؟

سؤال‌های فرعی

۱. مأموریت‌های اصلی سایبری سازمان‌های امنیتی کدام‌اند؟

۲. تهدیدهای اصلی اجرای مأموریت‌های سایبری سازمان کدام‌اند؟

۳. آسیب‌پذیری‌های اصلی اجرای مأموریت‌های سایبری سازمان کدام‌اند؟

٤. ابعاد و مؤلفه‌های صیانت از مأموریت‌های سایبری کدام‌اند و کدام مؤلفهٔ بیشترین تأثیر را دارند؟

مبانی نظری: تعاریف

فضای سایبری: «مجموعه‌ای از سیستم‌ها و شبکه‌های رایانه‌ای شامل نیروی انسانی، زیرساخت‌ها، تجهیزات، سخت‌افزار، نرم‌افزار و سیستم‌های ارتباطی، نظارتی و مدیریتی است که به منظور تولید، ذخیره‌سازی، پردازش، تبادل و بهره‌برداری از اطلاعات ایجاد و سازماندهی شده‌اند» (یادگاری، ١٣٩٤: ٤٢).

حفاظت: معنای لغوی حفاظت: حفاظت، در لغت به معنای نگهداری است. مفهوم حفاظت: مجموعه اقدام‌ها و تمهیدهایی که موضوع‌های حفاظتی را در برابر تهدیدها و خطرهای مربوط حفظ کند (پورمراد، ۱۳۸۹: ۱۵۹).

پیشگیری: مفهوم لغوی پیشگیری: پیشگیری از نظر لغوی: جلوگیری، دفع، صیانت، حفظ صحت (دهخدا، ۱۳۷۷: ٤٥) پیشگیری از ریشه لاتین (Prevention) در فرهنگ به معنای جلوگیری‌کردن، مانع‌شدن و پیش‌بینی کردن آمده است (معین، ۱۳۸۱: ۹۳۳).

صیانت: صیانت از نظر لغوی: نگه‌داشتن، نگهبانی، خویشتن بازداشتن (دهخدا) صیانت از ریشهٔ لاتین (Protection) در فرهنگ به معنای حفظ‌کردن؛ خویشتن نگاهداشتن، نگهداری آمده است. (معین). صیانت: میل‌هایی مربوط به بدن را که اغلب به لفظ حس حیات یا حس ذات تعبیر می‌شوند، می‌توان احتیاجات بدنی یا مشتهیات جسمانی نامید، یا صیانت نفس، صیانت ذات آمده است.

صیانت امنیتی: مجموعه اقدام‌هایی است برای پیشگیری، کشف، شناسایی، خنثی‌سازی تهدیدهای جاسوسی، خرابکاری و براندازی، اختلال در روند انجام مأموریت انجام می‌پذیرد (چراغی و قدسی‌فر، ۱۳۹۰).

تهدید: تهدید به مجموعه اقدام‌هایی اطلاق می‌شود که هدف‌ها و ارزش‌های حیاتی یک کشور را با هدف ایجاد تغییرهای اساسی مورد هجوم قرار می‌دهد و اغلب نیز ریشهٔ

خارجی دارد (شایگان، ۱۳۹٤) تهدید نقطهٔ مقابل امنیت قرار دارد. زمانی امنیت وجود دارد که تهدید نباشد و برعکس. هرگاه تهدیدی احساس شود، امنیت رخت برمی‌بندد.

سایبری: از لحاظ لغوی در فرهنگ‌های مختلف سایبر به معنای مجازی و غیرملموس است که با توجه به گستردگی مفهوم سایبر و اطلاق آن به تمام افعال و اقدام‌ها واقع شده در محیط شبکه‌های بین‌المللی از جمله اینترنت و بی‌شمار بودن مصادیق سایبر به توصیه متخصصان و دانشمندان صاحب نام این رشته، یافتن لغت معادل یا ترجمه آن به زبان‌های دیگر، به دلیل مفهوم لغوی این واژه در سطح بین‌المللی، مجاز نیست چرا که ممکن است دایره شمول و مفهوم آن را محدود کند؛ به همین دلیل برگردان آن به فارسی نیز کمی مبهم است؛ سایبر یعنی علم فرمان، یعنی هوش مصنوعی از نظر اهل فن دنیای صفر و یک (خوش‌عمل، ۱۳۹۱: ٤۹).

فضای سایبری: منظور از فضای سایبر یا فضای مجازی ترکیبی از ده‌هاهزار رایانهٔ به‌هم پیوسته، خدمات دهنده‌ها، شبکه‌های ارتباطی، سوئیچ‌ها و کابل‌های فیبر نوری است که امکان ایجاد ارتباطات را در یک سامانهٔ جامع فراهم می‌آورد (افتخاری، ۱۳۸۲: ۵). برخی فضای سایبر را با اینترنت یکی می‌گیرند که اشتباه است. چرا که فضای سایبر ارتباط صورت گرفته مبتنی بر سامانه‌های مخابراتی را نیز شامل می‌شود و تعریف کامل‌تری دارد. در اصل می‌توان این‌گونه مطرح کرد که اینترنت یکی از ظرفیت‌های فضای سایبر است که البته به دلیل کاربرد فراوان، گاهی به صورت عرف، تعریف کلی فضای سایبر را به خود اختصاص داده است (یادگاری و همکاران، ۱۳۹٤: ٤۳).

ویژگی‌های فضای سایبر

۱- ذخیرهٔ اطلاعات در فضای مجازی (دیجیتالی‌کردن اطلاعات)؛ ۲- فضای واقعی مجازی؛ ۳- جهانی و فرامرزی بودن؛ ٤- دست‌یابی آسان به آخرین اطلاعات؛ ۵- جذابیت و تنوع؛ ٦- آزادی اطلاعات و ارتباطات؛ ۷-گمنامی؛ ۸- در دسترس بودن؛ ۹- تعدد بازیگران در فضای سایبری؛ ۱۰- پایین بودن احتمال تنبیه و بازخواست.

تهدیدهای فضای سایبری

۱- جاسوسی: جاسوسی، به‌عنوان تهدیدی امنیتی است که به‌طور عام متوجه تمامی کارکنان از جمله کارکنان پلیس. از آنجایی که ماهیت کار و محیط فعالیت پلیس فتا در فضای تولید و تبادل اطلاعات از جمله اینترنت شکل می‌گیرد، کارکنان این پلیس بیش از سایر کارکنان در معرض ارتباط با بیگانگان و سازمان‌های اطلاعاتی حریف بوده و به همین میزان تهدیدهای متنوع‌تر و جدی‌تری در این حوزه متوجه آنهاست (پورمراد، ۱۳۹۳: ٤٣)؛

۲- جاسوسی رایانه‌ای: جاسوسی رایانه‌ای ناظر بر کسب اسرار حرفه‌ای، تجاری، اقتصادی، سیاسی و نظامی و نیز افشا، انتقال و استفاده از اسرار است که به شکل ورود به سامانه، پردازش داده‌ها و اعمال مشابه رخ می‌دهد. از ویژگی‌های جاسوسی رایانه‌ای می‌توان به موارد زیر اشاره کرد:

- محدودهٔ اسرار در جاسوسی رایانه‌ای شامل اسرار نظامی، سیاسی، تجاری، اقتصادی و... است؛
- تمامی مراحل جاسوسی که به شکل تفتیش غیرمجاز، افشا، انتقال، استفاده از ترفندهای برنامه‌نویسی و استفاده از ترفندهای نفوذ است در رایانه رخ می‌دهد؛
- در جاسوسی رایانه‌ای وجود ارکان متشکله فضای مجازی لازم است؛
- در جاسوسی رایانه‌ای ممکن است جاسوسی فقط به دلیل ضعف سامانه‌های امنیتی انجام شود و فرد ثانی وجود نداشته باشد.

مستند به قانون جرائم رایانه‌ای اصلی‌ترین جاسوسی رایانه‌ها، با ارزش (سری) بودن داده‌ها و اطلاعات است طبق تبصره (۱) ماده (۳)، دادهٔ ارزشمند داده‌ای است که افشای آن به امنیت کشور یا منافع ملی آسیب می‌زند؛ بنابراین، اگر فردی به داده‌های ارزشمند دسترسی پیدا کند یا آنها را تحصیل کند یا محتوای در حال انتقال آنها را نظارت کند به‌عنوان مجرم شناخته شده و طبق قانون با وی برخورد می‌شود. قانون‌گذار هرکس را که به قصد دسترسی به داده‌های سری، تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را

نقض کند مجرم می‌داند؛ به عبارت دیگر قانون‌گذار شروع به جاسوسی رایانه‌ای را نیز جرم دانسته است (پورمراد، ۱۳۹۳: ٤٥ و ٤٦).

۳- خرابکاری: خرابکاری در اصطلاح به عملی گفته می‌شود که سبب از کار انداختن وسایل یا تخریب تأسیسات و یا متوقف‌کردن وظایف سازمان و اشخاص به نفع دشمن می‌شود. هرچند در مورد تجهیزات و تأسیسات رایانه‌ای اقدام‌های خرابکارانه به صورت‌های مختلف متداول (انفجار، آتش‌سوزی، مکانیکی، روانی، مدرن و فنی) صورت می‌گیرد، ولی خرابکاری فنی چه در بُعد سخت‌افزاری و چه در بعد نرم‌افزاری با عنایت به وضعیت سامانه‌های رایانه‌ای تهدیدی جدی‌تر به حساب می‌آید. خرابکاری می‌تواند در هر یک از قسمت‌های سامانه مثل قسمت منابع تغذیه، از قبیل موتور برق، برق شهر، سرقت باتری، قطع یا اتصال خطوط، اضافه‌کردن مواد نامناسب یا نشت سوخت و غیره صورت گیرد (پورمراد، ۱۳۹۳: ٤٧).

٤- براندازی: براندازی نیز به‌عنوان تهدیدی امنیتی است که به‌طور عام متوجه تمامی کارکنان از جمله کارکنان پلیس. یکی از اقدام‌های مهم سازمان‌های اطلاعاتی در زمینهٔ براندازی، ایجاد نارضایتی بین مردم است. سازمان‌های اطلاعاتی حریف ممکن است به‌منظور ایجاد نارضایتی در بین مردم ضمن تقرب به کارکنان پلیس فتا آنان را به‌طور آگاهانه یا ناآگاهانه وادار به فعالیت‌هایی کنند که درنهایت منجر به نارضایتی مردم می‌شود (پورمراد، ۱۳۹۳: ٤٨).

۵- جنگ رایانه‌ای (جنگ سایبری): جنگ رایانه‌ای اشاره به وضعیتی دارد که در آن عملیات نظامی بر اساس اطلاعات رایانه‌ای نظارت شوند یا به‌منظور جلوگیری از عملیات دشمن برای ایجاد اختلال در ارتباطات و جلوگیری از دسترسی به اطلاعات تلاش شود. معنای دیگر جنگ رایانه‌ای، تلاش برای کسب اطلاعات هرچه بیشتر از دشمن و جلوگیری از کسب اطلاعات توسط وی دربارهٔ شماست یا به تعبیری، تلاش برای توازن اطلاعات و دانش به‌نفع شما، به‌خصوص در وضعیتی که توازن نیروهای نظامی به‌نفع شما نیست و درنهایت جنگ رایانه‌ای به معنای استفاده از اطلاعات برای

به‌حداقل رساندن سرمایه، جنگ‌افزار و نیروی انسانی موردنیاز برای کسب پیروزی در جنگ است. این نوع جنگ، نیازمند فناوری‌های مختلفی است. به‌ویژه برای صدور فرمان‌ها و پایش میدان جنگ، جمع‌آوری هوشمندانه اطلاعات و پردازش و صدور آنها، ارتباطات راه‌کنشی، موقعیت‌یابی، تشخیص دوست از دشمن و سرانجام برای استفاده از سلاح‌های هوشمند که قادرند به‌صورت خودکار بر اساس اطلاعات دریافتی از ماهواره علیه دشمن بجنگند (پورمراد، ۱۳۹۳: ٤٩). گفتنی است نبرد سایبری در دو حوزهٔ آفندی و پدافندی انجام می‌شود.

آفند رایانه‌ای: به عملیاتی گفته می‌شود که از سامانه‌های اطلاعاتی برای ایجاد اختلال در افکار، تضعیف یا انهدام اطلاعات موجود در رایانه‌ها و شبکه‌های رایانه‌ای دشمن استفاده می‌شود. رایانه‌ها و شبکه‌های ارتباطی، تسلیحات مورد استفاده در آفند رایانه‌ای است؛ به‌عبارت دیگر با استفاده از آنها می‌توان به رایانه و سامانه‌های ارتباطی دشمن حمله کرد. تفاوت بین آفند رایانه‌ای با آفند فیزیکی که ممکن است سامانه‌های اطلاعاتی مشابه را مورد حمله و تخریب قرار دهد، در نوع ابزار مورد استفاده آنهاست. در تخریب یا حملهٔ فیزیکی، از موشک، بمب و این قبیل ابزار استفاده می‌شود در حالی که در آفند رایانه‌ای از تسلیحاتی چون رایانه و سامانه‌های رایانه‌ای استفاده می‌شود (پورمراد، ۱۳۹۳: ۵۰).

به‌طورکلی آفند رایانه‌ای شامل اقدام‌هایی است که باعث کاهش کارایی دشمن از طریق ممانعت در استفاده او از رایانه‌ها می‌شود. این اثر به کمک تأثیرگذاری بر توانایی تجهیزاتی دشمن حاصل می‌شود. در آفند رایانه‌ای مفاهیمی همچون «جنگ بر روی شبکه، مانور مجازی، رخنه رایانه‌ای، تروریسم رایانه‌ای، جنگ اینترنتی، جنگ مجازی، رخنه و نفوذ به رایانه‌ها، تجهیز سخت‌افزارها و نرم‌افزارها، جنگ الکترونیک، بدافزارها و برنامه‌های مزاحم، آفند فیزیکی، جرائم رایانه‌ای، پاک‌کردن اطلاعات ذخیره شده، تحریف یا تغییر اطلاعات ذخیره شده، یا پردازش شده یا ارسال شده توسط رایانه‌ها و شبکه‌های ارتباطی و...» مطرح است. در عرصهٔ جنگ اطلاعات، نبرد رایانه‌ای به‌عنوان یکی از میادین جنگ مطرح بوده و همان‌گونه که خود مکمل سایر عملیات است، سایر

عملیات نیز تکمیل کننده آن محسوب می‌شوند؛ بنابراین، در یک آفند رایانه‌ای که در چارچوب جنگ اطلاعات انجام می‌شود اقدام‌های زیر متصور است:

الف) تجهیز سامانه‌ها به ابزارهای جاسوسی؛

ب) حمله رایانه‌ای (رخنه و نفوذگری)؛

ج) به‌کارگیری و استفاده از بدافزارها (پورمراد، ۱۳۹۳: ۵۱).

٦- بدافزارها: یک بدافزار، یک برنامهٔ رایانه‌ای است که به‌طور غیرمجاز به رایانه یا شبکه منتقل شده و عملیات خاصی را که به‌طورمعمول مطلوب ما نیست انجام می‌دهد. استفاده از بدافزارها در شبکه رواج بیشتری دارد زیرا یک شبکه رایانه‌ای میدان مناسبی برای این‌گونه نرم‌افزارهاست. یک کرم در یک شبکه رایانه‌ای به سرعت منتشر می‌شود و میدان عمل وسیعی را به خود اختصاص می‌دهد. یکی از بدافزارهای مهم در شبکه‌های رایانه‌ای اسب تروا‌ست، یک اسب تروا می‌تواند یک سرور را به‌عنوان درپشتی به دستگاه قربانی منتقل و نصب کند و بدین‌سان میزبانی نفوذگر را عهده‌دار شود. در یک شبکه گسترده مهم‌ترین دغدغه امنیتی پیشگیری و مقابله با بدافزارهاست (پورمراد، ۱۳۹۳: ٦۰).

امنیت سایبری: مفهوم امنیت به‌طور کلی یک ارزش مناقشه‌آمیز سیاسی غیرمتکامل، مبهم، توسعه نیافته و ضعیف؛ اما از نظر سیاسی قدرتمند و در حال تحول است. این مفهوم با مسائلی درباره ادامهٔ بقا، رفاه و حفاظت از کشور ارتباط مستقیم دارد (باری‌بوزان، ۱۳۷۸: ۲۹).

سطوح امنیت در فضای سایبری

• سطح اول امنیت: در فضای سایبری، امنیت در حوزهٔ زیرساخت‌ها و شریان اطلاعاتی است. وابستگی به شبکه‌های پر سرعت و پردازشگرهای قدرتمند روز به روز افزایش می‌یابد که دستگاه‌ها را در معرض مخاطراتی از آتش و طوفان تا بزه‌کاری و تروریسم سایبری قرار داده که نیاز مدیریت و نظارت دارد (کیان‌خواه، ۱۳۸۹: ۳۵).

• سطح دوم امنیت: در فضای سایبری، امنیت در حوزهٔ فرد و اجتماع است. ابعاد چالش در بعد فردی و اجتماعی موجب طرح‌ریزی امنیت فرهنگی و هویتی و امنیت اخلاقی و دینی می‌شود. امنیت اخلاقی و هویتی فرد و اجتماع در فضای سایبر حافظ دین و اخلاق پایبند به فطرت الهی است. امنیت فرهنگی و هویتی، حافظ انسانیت انسان است که هویت و فرهنگش ریشه در آداب و سنتی است که بر اساس ویژگی‌ها و نژاد و قومش شکل گرفته است (کیان‌خواه، ۱۳۸۹: ۷).

• سطح سوم امنیت: در فضای سایبر، امنیت در حوزهٔ ملی و حاکمیتی است. تهدیدها در حوزهٔ ملی و حاکمیتی، مجموعه تهدیدهایی است که حیاتی‌ترین منافع ملی و حاکمیتی یک نظام را به چالش می‌کشاند. این حوزه از تهدیدهای بخشی در حوزهٔ زیرساخت و شریان‌های اطلاعاتی قرار داشته و بخشی در حوزهٔ امنیت سیاسی و اقتصادی است. فضای سایبری که ذاتا ابزاری برای تعامل و ارتباط افراد و جوامع است فضایی را برای جنگ روانی ایجاد می‌کند. در این جنگ اطلاعات علیه فکر و ذهن افراد استفاده می‌شود و منجر به عملیات علیه اراده ملی، عملیات علیه عناصر نظامی، ایجاد تضاد فرهنگی و ایجاد تنش و هرج و مرج می‌شود (کیان‌خواه، ۱۳۸۹: ۸).

جرائم سایبری: به‌طور کلی، جرائم سایبری را در چهار دسته یا طبقه کلی می‌توان جای داد (یادگاری و دیگران، ۱۳۹٤: ۵۱).

۱- جرائم کلاسیک با توصیف سایبری: جرائمی در این دسته قرار می‌گیرند که جرائم سنتی تلقی می‌شوند؛ اما در حال حاضر به علت پیشرفت فناوری، با وسایل نوینی انجام می‌شوند. از جمله این جرائم، می‌توان به کلاهبرداری سایبری، جعل سایبری، تخریب سایبری، جاسوسی سایبری و ... اشاره کرد (یادگاری و دیگران، ۱۳۹٤: ۵۱)؛

۲- جرائم علیه محرمانه‌بودن داده‌ها و سامانه‌ها: هر نمادی از موضوع‌ها، مفاهیم یا دستورکارها از جمله متن، صوت یا تصویر را که برای برقراری ارتباط میان سامانه‌های رایانه‌ای ایجاد می‌گردد، داده محتوا می‌گویند. از جمله جرائمی که در این دسته جای

می‌گیرند می‌توان به شنود غیرمجاز داده‌های مخابراتی در ارتباطی خصوصی یا داده‌های سری اشاره کرد که واجد ارزش برای امنیت داخلی و خارجی کشور هستند (یادگاری، ۱۳۹٤: ۵۱)؛

۳- جرائم علیه صحت و تمامیت داده‌ها و سامانه‌ها: تغیر، ایجاد، محو یا متوقف‌کردن رایانه‌ای و مخابراتی به قصد تقلب، غیرقابل استفاده‌کردن، تخریب یا اخلال در داده‌ها یا امواج الکترومغناطیسی، ممانعت از دست‌یابی اشخاص مجاز به داده‌ها با تغییر رمز ورود یا رمزنگاری، از جمله جرائمی هستند که در این دسته قرار می‌گیرند (یادگاری، ۱۳۹٤: ۵۱)؛

٤- جرائم مرتبط با محتوا: این دسته از جرائمی را تحت شمول خود قرار می‌دهد که در آنها، رایانه به‌عنوان ابزار و وسیله توسط مجرم برای ارتکاب جرم به‌کار گرفته می‌شود و فقط فناوری اطلاعات، زمینهٔ ارتکاب آنها را فراهم می‌سازد. برای مثال انتشار محتویات مستهجن، تبلیغ یا تحریک یا تشویق به انحراف‌های جنسی یا خودکشی از طریق سامانه رایانه‌ای یا مخابراتی در این دسته قرار می‌گیرند (یادگاری، ۱۳۹٤: ۵۲).

پیشگیری

مفهوم پیشگیری: بزه یک پدیدهٔ پیچیده، با قابلیت تفسیر بالا و مفهومی متغییر در بستر زمان و مکان است. نقطه تلاقی دیدگاه‌های مختلف نسبت به جرم، اعمال نظارت بر آن است. برای سالیان متمادی تصور می‌شد نه‌تنها شیوه‌های سنجیده نظارت جرم در قالب دستگاه عدالت کیفری شکل می‌گیرد و از رهگذر مجازات اعمال می‌گردد. امروز می‌توان گفت نوعی هم‌گرایی بر سر این مفهوم وجود دارد که فرایند جرم‌انگاری یک پیش‌شرط ضروری برای پیوستگی اجتماعی و پایش اجتماعی نیست؛ به عبارت دیگر نظارت تنها در اشکال رسمی ظاهر نمی‌گردد. از سوی دیگر بر پیوستگی جرم با زمینهٔ بروز و ظهور آن تأکید می‌گردد. از این منظر جرم نمی‌تواند به منزله یک امر التزامی و جدای از بستری که در آن قرار گرفته است بررسی و نظارت شود. این رویکرد درنهایت به غنی‌سازی جرم‌شناسی و پدیدآمدن جرم‌شناسی پیشگیرانه می‌انجامد که به مفهومی مضیق از پیشگیری قائل است. «واژهٔ پیشگیری» امروزه در معنای جاری و

متداول آن دارای دو بعد است: پیشگیری یا جلوگیری کردن، هم به معنای پیش‌دستی کردن، پیشی‌گرفتن و به جلوی چیزی رفتن است و هم به معنای «آگاه‌کردن، خبر چیزی را دادن و هشدار دادن» اما در جرم‌شناسی پیشگیرانه، پیشگیری در معنای اول آن مورد استفاده واقع می‌شود یعنی کاربرد فنون مختلف به منظور جلوگیری از وقوع بزه‌کاری، هدف به جلوی جرم‌رفتن و پیشی‌گرفتن از بزه‌کاری است (نجفی ابرندآبادی، ۱۳۷۸: ۱۳۰-۱۲۹).

پیشگیری از لحاظ لغوی: پیشگیری از نظر لغوی؛ جلوگیری، دفع، صیانت، حفظ صحت (دهخدا، ۱۳۷۷: ٤٥). پیشگیری از نظر لغوی به معنای جلوگیری‌کردن، مانع شدن، جلو بستن و نیز اقدام‌های احتیاطی برای جلوگیری از رخدادهای بد و ناخواسته است (معین، ۱۳۸۱: ۹۳۳).

اقدام‌های پیشگیرانه: به یک‌سری از امور گفته می‌شود که ضمن تعیین روش‌ها و اصول حفاظتی با وضع مقررات و دستورکار اجرایی موجب گسترش فرهنگ پیشگیری و ایجاد آمادگی برای پیشگیری و یا کاهش سوانح و حوادث می‌گردد (جمشیدی، ۱۳۸۰: ۵۱)

الگوهای صیانتی یا پیشگیرانهٔ مأموریت‌های سایبری

۱- تعیین صلاحیت کارکنان: یکی از شیوه‌های پیشگیری از بروز تهدیدهای امنیتی و غیرامنیتی به کارگیری کارکنان در محل‌ها و مشاغل مناسب با توجه به نوع تخصص، نقاط ضعف و قوت و سایر معیارهای تعیین صلاحیت است؛

۲- آموزش و آگاه‌سازی: همچنین در آیین‌نامه حفاظت اسناد مدارک مصوبه فرماندهی معظم کل قوا فرماندهان و رؤسا را موظف کرده تا با همکاری حفاظت اطلاعات برنامه‌های توجیهی آموزش در مورد حفاظت اسناد را برای کارکنان تحت امر خود که با اسناد و مدارک طبقه‌بندی شده سر و کار دارند تنظیم و اجرا کنند. در این راستا بهره‌گیری از فناوری اطلاعات برای آموزش افراد تازه استخدام و توجیه آنان و... لازم است؛

۳- حفاظت اسناد و مدارک: به کلیه اقدام‌هایی که به منظور نگهداری اسناد و مدارک درمقابل خطرهای طبیعی (سیل، زلزله و...) و خطرهای مصنوعی (جاسوسی،

خرابکاری، سرقت، سهل‌انگاری و...) به‌عمل آمده و از دسترسی افراد غیرمجاز به آن جلوگیری کند، حفاظت اسناد و مدارک گویند (کریمایی، ۱۳۸٤: ۸٤). تعیین محدودیت‌های لازم (دسترسی، حیطه‌بندی، طبقه‌بندی) برای دسترسی به آن و جلوگیری از دسترسی غیرمجاز و افشای آن (جمشیدی، ۱۳۸۰: ۸۷-۸٦)؛

٤- حفاظت فیزیکی: حفاظت فیزیکی یکی از اقدام‌های تدافعی (غیرعامل) سازمان حفاظت اطلاعات است. منظور از حفاظت فیزیکی کلیه اقدام‌هایی است که به منظور حفظ تأسیسات در مقابل خطرهای طبیعی و مصنوعی اتخاذ می‌گردد؛ به عبارت دیگر حفاظت فیزیکی یک‌سری موانع متحدالمرکزی است که به دور تأسیسات کشیده می‌شود تا از ورود متجاوز جلوگیری گردد (جمشیدی، ۱۳۷۸: ۲۰)؛

۵- صیانت از مأموریت‌های سایبری با پدافند غیرعامل: پدافند غیرعامل یا دفاع غیرعامل به مجموعه اقدام‌هایی اطلاق می‌گردد که به‌کارگیری جنگ‌افزار نیاز ندارد و با اجرای آن می‌توان از واردشدن خسارات مالی به تجهیزات و تأسیسات حیاتی و حساس نظامی و غیرنظامی و تلفات انسانی جلوگیری کرده و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد. عملیات ثابت روانی، جنگ نرم، تهدیدهای اقتصادی و حملات سایبری از جمله تهدیدهای دشمن در پدافند غیرعامل است. لازمه حذف و کاهش قابل‌قبول تأثیر این تهدیدها بهره‌گیری از تمهیدها و اقدام‌هایی است که به آن حفاظت می‌گویند. در واقع حفاظت سلسله اقدام‌هایی است که برای حفظ و تامین تأسیسات و تجهیزات، اسناد و مدارک، اخبار و اطلاعات و اشخاص در برابر تهدیدهای دشمن و خطرهای طبیعی انجام می‌شود (چراغی و قدسی‌فر، ۱۳۹۰: ۵).

٦- حفاظت مخابرات (فناوری ارتباطات): حفاظت مخابرات عبارت است از تمامی اقدام‌هایی که سبب می‌شود تا اشخاص غیرمجاز نتوانند به اسناد و مدارک باارزش و طبقه‌بندی مخابراتی و شبکه‌های ارتباطی دسترسی پیدا کنند و یا در تفسیر و تجزیه و تحلیل اطلاعات به‌دست آمده دچار فریب و گمراهی شوند (اروسخانی، ۱۳۷۹: ۱٤).

پیشینهٔ تحقیق: با بررسی که در بانک اطلاعاتی پایان‌نامه‌های دانشگاه علوم انتظامی امین صورت گرفت، مشخص گردید تاکنون پژوهشی با این عنوان و یا در ارتباط با این موضوع در ناجا انجام نشده است و با بررسی صورت گرفته در پایگاه اینترنتی کتابخانه ملی ایران، مشخص گردید کتاب یا پژوهشی با این موضوع تهیه و یا تألیف نشده است، گفتنی است پژوهش‌های متعددی در حوزهٔ فضای سایبری صورت گرفته است که مرتبط با موضوع پژوهش نبوده است.

با بررسی‌های صورت گرفته در پایگاه اینترنتی اسناد ایران (ایران‌داک)، پایگاه اطلاعات علمی جهاد دانشگاهی[1]، پایگاه مجلات ایران[2]، مشخص گردید از میان این پژوهش‌های انجام شده هیچ‌کدام در خصوص نقش اقدام‌های پیشگیرانه در صیانت از مأموریت‌های سایبری یکی از سازمان‌ها نبوده و پژوهشی‌هایی که تا حدودی مرتبط با موضوع این تحقیق هستند به شرح زیر است:

۱- خلیلی‌پور رکن‌آبادی و نورعلی‌وند (۱۳۹۱) مقاله‌ای باعنوان «تهدیدهای سایبری و تأثیر آن بر امنیت ملی» نوشته‌اند؛ این مقاله به‌دنبال پاسخ‌گویی به این است که تهدیدهای سایبری چگونه بر امنیت ملی تأثیر می‌گذارند و این اثرگذاری در چه ابعادی خود را نمایان می‌سازد؛ و در این مقاله به این نتیجه رسیده است ویژگی‌های فضای سایبری چون قیمت پایین ورود، گمنامی و تأثیرگذاری شگرف، پدیده‌ای به نام انتشار قدرت را به وجود آورده است که نه‌تنها باعث شده دولت‌های کوچک از ظرفیت‌های بیشتری برای اعمال قدرت در این فضا برخوردار شوند، بلکه منجر به ورود بازیگران جدیدی همچون شرکت‌ها و گروه‌های سازمان یافته و افراد به معاملات قدرت جهانی شده است؛ که تغیرهای عمده‌ای را در نوع، ابعاد و گستردگی تهدیدها به‌وجود آورده است که برای مقابله با آنها همکاری مؤثر و دو جانبه دولت‌ها و بخش خصوصی را که دارای منافع مشترکی در برخورد با این تهدیدها هستند را می‌طلبد؛

1 SID
2 MAG IRAN

۲- مرتضی اشرفی و مجتبی اشرفی (بی‌تا) مقاله‌ای با عنوان «تحلیلی بر جاسوسی و جنگ سایبری» چاپ شده در فصلنامه درس‌هایی از مکتب اسلام شماره ٦٦١، در این مقاله به بحث جمع‌آوری اخبار به وسیله جاسوسی پرداخته شده است؛ و به این نتیجه رسیده شده است که فعالیت‌های متعدد در زمینه مسائل امنیتی دولت‌ها باید در درون یک نظام کلی حفاظتی و سازمان یافته اجرا شود و همچنین شناخت عوامل و مراحل تعیین و تدوین اطلاعات و جاسوسی امری بسیار مهم و قابل توجه است و هر کشور برای آمادگی برای رفع مخاطرات باید با شناخت لایه‌های گوناگون اطلاعاتی و جاسوسی و استفاده از عوامل تعیین کننده برای آینده خود، برنامه‌ریزی کند و در مرحلهٔ بعد از همهٔ ظرفیت‌های خود برای بازنگری و اجرای مؤثر آن بهره گیرد؛

۳- پورمراد (۱۳۸٦) در مقاله‌ای با عنوان «نگاهی به اینترنت و تهدیدهای آن» به ارائه تعریفی از اینترنت و تهدیدهای متصور آن پرداخت و درنهایت نتیجه گرفت؛ اینترنت همانند هر پدیدهٔ دیگر دارای وجوه مثبت و منفی بسیاری است و باید به وجوه منفی آن توجه بیشتری شود؛

٤- آذری‌فر (۱۳۹۵) در پایانامهٔ کارشناسی ارشد خود به بررسی نقش ارتباطات و اطلاعات در امنیت سایبری با رویکرد پدافند غیرعامل پرداخته است.

پژوهش‌هایی نیز در خصوص فضای سایبری در خارج از کشور در خصوص موضوع تهدیدهای فضای سایبری انجام شده که در ادامه به بررسی یکی از آنها پرداخته می‌شود: آرن لازکاو[1] و چند نفر دیگر از نویسندگان در سال ۲۰۱٤ در کتاب *معاملات ACM در فناوری اینترنت* مقاله‌ای را با عنوان «ترکیب امن تیم برای خنثی‌کردن تهدیدهای داخلی و جاسوسی سایبری» را تدوین کردند که در این مقاله به توسعه ترکیب امن برای مقابله با جاسوسی سایبری برای محافظت از اسرار سازمانی در برابر مهاجمان که تلاش می‌کنند در کنار استفاده از ابزارهای فنی، اعضای گروه را نیز با خود همراه سازند پرداخته شده است.

1 Aaron Laszk


الگوی مفهومی تحقیق
صیانت از تهدیدهای فضای سایبر
اشراف اطلاعاتی
تمرکز بر اطلاعات آفندی و تهاجمی
تحلیل صیانتی و پیشگیرانه
الگوهای صیانتی
• توسعه اشراف اطلاعاتی بامحوریت فضای سایبری
• رصد فضای مجازی به منظور شناسایی نقاط ضعف و قوت آن
• حضور مؤثر در تمامی نقاط و لایه‌های سازمانی
• رصد دائمی مأموریت‌های سایبری و محیط آن
• دارا بودن چشم بینا، تیزبین و دقیق
• شناخت زمینه‌ها، قرائن و شواهد حوادث قبل از وقوع و ممانعت از آن
• انعکاس به موقع اطلاعات، گزارش‌ها و هشدارها و انجام اقدام‌های مقتضی و مؤثر
• دسته‌بندی، استنتاج و تحلیل اطلاعات و انتشار به‌موقع و بهره‌برداری به‌موقع
• تعامل و همکاری حداکثری با دستگاه‌های مرتبط با حفظ حیطه‌بندی
• شناسایی نرم‌افزارهای جاسوسی و سایر اقدام‌های سخت‌افزاری جاسوسی و نفوذ به ساختار مأموریت‌های سایبری
• اقدام‌های آفندی و تهاجمی با تأکید بر اقدام‌های صیانتی و پیشگیرانه
• تمرکز بر اقدام‌های آفندی
• هدف‌های عملیات آفندی و تهاجمی شامل (فرصت طرح‌ریزی، کاهش هزینه‌ها و آسیب‌ها، تمرکز بر نقاط ضعف دشمن و حریف، قابلیت پاسخگویی، خلق توانایی‌های جدید، بالا بردن توان مقابله، ایجاد سردرگمی و استیصال در سازمان‌های جاسوسی حریف و دشمن)
• استحکام سازمانی با توجه به دیدگاه مقام معظم رهبری و فرماندهی معظم کل قوا (مدظله‌العالی) شامل (تمرکز بر دشمن، اشراف اطلاعاتی، صیانت امنیتی، بازدارندگی و پیشگیری، زیرساخت‌های مأموریتی، سرمایهٔ انسانی)
• اقدام‌های آفندی با شناسایی و اولویت‌بندی تهدیدها و آسیب‌پذیری‌ها مأموریت‌های سایبری، عملیات آفندی، تحلیل آفندی و پیشگیرانه و در نهایت ارائه الگوهای صیانتی و پیشگیرانه
• تأکید بر الزام‌های سایبری در زیرساخت‌های مأموریت‌ها در فضای سایبر
• استفاده ازداده‌کاوی در اقدام‌های آفندی
• انجام اقدام‌های تحلیلی درخصوص پرونده‌های عملیاتی رسیدگی‌شده مرتبط با جرائم جاسوسی، خرابکاری و براندازی در فضای سایبری برای شناسایی آسیب‌ها
• انجام اقدام‌های تحلیلی درخصوص پرونده‌های عملیاتی رسیدگی‌شده مرتبط با جرایم جاسوسی، خرابکاری و براندازی در سایبری برای شناسایی تهدیدها
• تحلیل هوشمند و به‌موقع وقایع رخدادها در فضای سایبری
• بهره‌گیری از تحلیل هوشمندانه به منظور تصمیم‌گیری صحیح و به‌موقع
• ارایه الگوهای صحیح پیشگیری از تهدیدهای فضای سایبری در مأموریت‌های سایبری بااستفاده از تحلیل هوشمندانهٔ آفندی
• توسعه امن زیرساخت‌ها و رعایت اصول پدافند غیرعامل در مراکز فاوا به منظور ارتقای ضریب امنیت، ایمنی و پایداری
• ارایه الگوهای خودحفاظتی در فضای سایبری به کارکنان
• فرهنگ‌سازی نحوهٔ استفاده از فضای سایبری در بین کارکنان با معرفی الگوهای مطلوب
• هشداردهی منظم و به‌موقع به کارکنان باتوجه به شیوه و شگردهای جدید به‌دست آمده از اقدام‌های آفندی در قالب الگوهای مطلوب
• نظارت از طریق معاونت پیشگیری بر مأموریت‌ها
• نظارت عملکرد کارکنان در فضای سایبری و احصای موارد سوء
• توجه جدی به تأیید صلاحیت کارکنان

روش‌شناسی تحقیق: روش این تحقیق از نظر نوع کاربردی و از نظر روش تحلیلی توصیفی با رویکرد کیفی از طریق مصاحبه است. جامعه آماری شامل تعداد۱۵ نفر از مدیران عالی مستقر در شهر تهران بوده است؛ و برای تحلیل آماری از نرم‌افزار مسکیودا استفاده شده است.

یافته‌های تحقیق

الف) یافته‌های توصیفی: از لحاظ محل خدمت، ۸٦۰٦ درصد از پاسخ‌دهندگان مرکز سازمان و ۱۳.٤ درصد هم از مراکز استان بوده است. به لحاظ سطح تحصیلات، بیشتر افراد (٦٦/۷ درصد) از پاسخ‌دهندگان کارشناسی ارشد بوده است.۲۰ درصد کارشناسی و ۱۳/۳ درصد هم دکترا بوده‌اند. از نظر سابقهٔ خدمت هم افراد افراد با سابقه خدمت بین ۱٦ تا ۲۰ سال به میزان ٤٦/۷ درصد بیشترین میزان و افراد بالای ۲٦ سال هم به میزان ۱۳/۳ کمترین افراد هستند.

ب) یافته‌های تحلیلی

سؤال یک: مأموریت‌های سایبری چیست؟ در بررسی مأموریت‌های سازمانی مصاحبه‌شوندگان معتقدند در خصوص مأموریت‌ها گویه «بررسی و رصد وب‌گاه‌های داخلی و خارجی» با ۱۷/۰۷ درصد در رتبهٔ اول؛ گویه‌های «پیشگیری و مقابله با جرائم و تخلفات سایبری» و «اینترانت داخلی کشور» با ۱٤/٦۳ در رتبهٔ دوم و گویه‌های «ارتقای امنیت فضای سایبر کشور» و «اجرای قوانین و مقررات ابلاغی در حوزهٔ فضای سایبر» با ۱۲/۲۰ در رتبهٔ سوم قرار دارند. در خصوص مأموریت‌ها گویه «رصد فضای سایبر» با ۲۱/۹۵ درصد در رتبهٔ اول، گویه «جمع‌آوری اخبار و اطلاعات مربوط به تجمعات و گروه‌های غیرقانونی» با ۱۹/۵۱ درصد در رتبهٔ دوم و گویه «فروش لوازم و کالاهای غیرقانونی» با ۱۷/۰۷ درصد در رتبهٔ سوم قرار دارد. در خصوص پلیس آگاهی گویه «جرائم سرقت» با ۵۳/۳۳ در رتبهٔ اول و گویه «قاچاق کالا و ارز» با ٤٦/٦۷ درصد در رتبهٔ دوم قرار دارند.

سؤال دوم: تهدیدهای اجرای مأموریت‌های سایبری کدام‌اند؟ با توجه به دیدگاه مصاحبه‌شدگان ۲۸/۵۷ درصد تهدیدها را طبیعی و ۷۱/٤۲ درصد را تهدیدهای مصنوعی اعلام کردند و با توجه به حساسیت تهدیدهای مصنوعی این مقوله مورد بررسی و تحلیل قرار گرفته است.

جدول فراوانی نظر پاسخ‌دهندگان در خصوص ابعاد تهدیدهای مصنوعی مأموریت‌های سایبری

ابعاد	مقوله‌های مورد تأکید	فراوانی	درصد
تهدیدهای مصنوعی	بعد امنیتی	۱۵	۲۸/۸٤
	بعد اجتماعی	۹	۱۷/۳۰
	بعد سیاسی	۷	۱۳/٤٦
	بعد بین‌الملل	۵	۹/٦۲
	بعد فرهنگی	۸	۱۵/۳۸
	بعد روانی	۸	۱۵/۳۸

در تهدیدهای مصنوعی ابعاد امنیتی و اجتماعی بیشترین اهمیت را دارند. در بررسی ابعاد امنیتی و اجتماعی، گویه‌های «تجمعات و اجتماعات»، «ترویج ارتباط‌های غیراخلاقی» با ۸/۹۱ درصد در رتبهٔ اول، گویه‌های «جاسوسی رایانه‌ای»، «براندازی» و «حمله رایانه‌ای با رخنه و نفوذگری» با ۷/۹۲ درصد در رتبهٔ دوم و گویه «جاسوسی» و «خرابکاری» و «تهدید بنیان‌های خانواده» با ٦/۹۳ درصد در رتبهٔ سوم قرار دارند.

سؤال سوم: آسیب‌پذیری‌های اجرای مأموریت‌های سایبری چیست؟ در بررسی پاسخ مصاحبه‌شوندگان، گویه‌های «پایین‌بودن فرهنگ استفاده از فضای مجازی»، «بومی‌نبودن سامانه‌ها و سیستم‌عامل و نرم‌افزارها و سیستم‌عامل»، «ناآگاهی و آموزش نیروهای تازه‌خدمت به سخت‌افزارها، نرم‌افزارها و نحوهٔ واپایش اطلاعات آنها» با ٤/۸۹ درصد در رتبهٔ اول قرار دارند. در خصوص گویه‌های «گرانی و مشکل‌بودن امنیت»، «امنیت کامل دست‌نیافتنی»، «برقراری امنیت توسط انسان»، «استفاده از اینترنت بدون فیلتر»، «نبود شناخت از نرم‌افزارهای مورداستفاده و ماهیت آنها»، «ناآگاهی و ضعف آموزش کاربری و امنیتی کاربران و بهره‌برداران فضای مجازی»، «رعایت‌نکردن قوانین و مقررات»، «مشخص‌نبودن نقش سازمان در مأموریت‌های سایبری با ٤/۳۵ درصد در رتبهٔ دوم، گویه‌های «فقدان زیرساختار رمزنگاری» «نیروی انسانی متناسب با کار نیست و نارضایتی کارکنان از فشار کاری» و «استفاده از گوشی‌های هوشمند و رعایت‌نکردن ملاحظه‌های امنیتی» «ضعف تجهیزاتی و ضعف دانش کارکنان» «کمبود منابع، تحریم‌هاو آشنا نبودن به مباحث روز فناوری‌های نوین» با ۳/۸۰ درصد در رتبهٔ سوم قرار دارد.

سؤال چهارم: ابعاد و مؤلفه‌های صیانت از مأموریت‌های سایبری کدام‌اند و کدام مؤلفه‌ها بیشترین تأثیر را دارند؟

بعد اول: عوامل اصلی فضای سایبر (چیستی): عوامل اصلی فضای سایبر؛ یعنی شناخت مراجع امنیتی که لازم است در فضای سایبر صیانت امیتی شود که شامل مؤلفه‌های ذیل است:

مؤلفهٔ ۱- داده‌ها و اطلاعات: کلیه نظام‌ها و سامانه‌های اطلاعاتی و ارتباط آنها با یکدیگر و طبقه‌بندی و گردش اطلاعات را شامل می‌گردد؛

مؤلفهٔ ۲- کاربران: کلیه بهره‌برداران سامانهٔ اطلاعات و ارتباطات و افرادی که به‌عنوان تولیدکننده، مصرف‌کننده و یا پردازش کنندهٔ اطلاعات هستند؛

مؤلفهٔ ۳- شبکه و ارتباطات: کلیه سامانه‌های سخت‌افزاری و نرم‌افزاری که تبادل اطلاعات را از طریق باسیم و بی‌سیم فراهم می‌کنند؛

مؤلفهٔ ٤- خدمات و نرم‌افزار: کلیه خدمات برای مبادله پیام‌ها و اطلاعات کاربران در بستر نرم‌افزار؛

مؤلفهٔ ۵- زیرساخت و سخت‌افزار: کلیه تجهیزات و ابزارهای سخت‌افزاری که امکانات لازم برای شبکه و سامانه‌هاست.

جدول فراوانی نظر پاسخ‌دهندگان در خصوص عوامل اصلی فضای سایبر

مقوله‌های مورد تأکید	فراوانی	درصد
داده‌ها و اطلاعات	۱۱	۲۵
کاربران	۸	۱۸/۱۸
شبکه و ارتباطات	۹	۲۰/٤۵
خدمات و نرم‌افزار	۷	۱۵/۹۱
زیرساخت و سخت‌افزار	۹	۲۰/٤۵

در نظر مصاحبه‌شوندگان، گویه «داده‌ها و اطلاعات» با ۲۵ درصد در رتبهٔ اول، گویه‌های «شبکه و ارتباطات» و «زیرساخت و سخت‌افزار» با ۲۰/٤۵ درصد در رتبهٔ دوم و گویه «کاربران» با ۱۸/۱۸ در رتبهٔ سوم قرار دارد.

بعد دوم: هدف‌های امنیتی فضای سایبر (چرایی):

هدف‌های امنیتی فضای سایبر؛ یعنی کلیه هدف‌هایی که لازم است به‌صورت پایدار صیانت شود تا امنیت فضای سایبر فراهم گردد و شامل مؤلفه‌های ذیل است:

مؤلفهٔ ۱- یکپارچگی (جامعیت، صحت): فرایندی که اطمینان ایجاد می‌کند تا داده در مقابل تغییرهای تصادفی و یا تعمدی حفاظت شود؛

مؤلفهٔ ۲- محرمانگی: حفاظت از فاش‌شدن غیرمجاز یا جلوگیری از درک شدن آنها هست؛

مؤلفهٔ ۳- دسترسی‌پذیری: فرایندی که اطمینان ایجاد می‌کند تا داده برای کاربران مجاز در دسترس و قابل‌استفاده خواهد بود؛

مؤلفهٔ ٤- انکارناپذیری (عدم‌انکار): فرایندی است که گیرنده یا فرستنده یا عمل‌کننده روی اطلاعات نباید قادر به انکار عمل خود باشد؛

مؤلفهٔ ٥- احراز هویت (تصدیق، اصالت): فرایندی است که در آن تعیین می‌کنیم شخصی یا چیزی درواقع همان است که اعلام می‌کند؛

مؤلفهٔ ٦- حریم خصوصی: فرایندی که یک فرد یا گروه اطلاعات مربوط به خود را مجزا می‌کند و بتواند اطلاعاتش را با انتخاب خودش برای دیگران آشکار سازد.

جدول فراوانی نظر پاسخ‌دهندگان در خصوص هدف‌های امنیتی فضای سایبر

مقوله‌های مورد تأکید	فراوانی	درصد
محرمانگی	۱۲	۲۱/٤۳
یکپارچگی (جامعیت و صحت)	۱۰	۱۷/۸٦
دسترسی‌پذیری	۸	۱٤/۲۹
انکارناپذیری (عدم‌انکار)	۹	۱٦/۰۷
احراز هویت (تصدیق، اصالت)	۹	۱٦/۰۷
حریم خصوصی	۸	۱٤/۲۹

در بررسی بعد دوم (هدف‌های امنیتی فضای سایبر) مشخص می‌شود، گویه «محرمانگی» با ۲۱/٤۳ درصد در رتبهٔ اول، گویه «یکپارچگی (جامعیت و صحت)» با

۱۷/۸٦ درصد در رتبهٔ دوم و گویه‌های «انکارناپذیری (عدم‌انکار)» و «احراز هویت (تصدیق، اصالت)» با ۱٦/۰۷ در رتبهٔ سوم قرار دارند.

بعد سوم: اقدام‌ها و راه‌کارهای صیانت امنیتی فضای سایبر (چگونگی) شامل اقدام‌ها و راه‌کارها صیانت‌های امنیتی به مجموعه اقدام‌هایی گفته است که امنیت پایدار مراجع امنیتی فضای سایبر را تضمین می‌کند و شامل مؤلفه‌های ذیل است:

مؤلفهٔ ۱- شناسایی (منابع و دارایی‌های سایبری): پیاده‌سازی درک زمینه کسب‌وکار، منابع و خطرهای مربوط به امنیت سایبری، مطابق با راهبرد مدیریت ریسک؛

مؤلفهٔ ۲- محافظت (ایمن‌سازی و پایداری امنیت): پیاده‌سازی راه‌کارهای ایمنی مناسب برای اطمینان از خدمات فضای سایبر؛

مؤلفهٔ ۳- تشخیص و کشف (تهدیدها و آسیب‌های امنیتی): پیاده‌سازی فعالیت‌های مناسب برای شناسی و کشف وقوع رویدادی امنیتی در فضای سایبر؛

مؤلفهٔ ٤- تحلیل (مخاطرات): پیاده‌سازی فعالیت‌های مناسب برای جمع‌آوری و پالایش رویدادها و انتخاب راه‌حل مناسب امنیتی در فضای سایبر؛

مؤلفهٔ ۵– تحلیل، پاسخ و واکنش (رویدادهای امنیتی): پیاده‌سازی فعالیت‌های عملیاتی درواکنش به یک رویداد امنیت فضای سایبر؛

مؤلفهٔ ٦- بازیابی (حفظ و بهبود وضعیت): پیاده‌سازی فعالیت‌های متناسب برای حفظ انعطاف‌پذیری و بازگرداندن هرگونه قابلیت به خدمات مختل شده؛

مؤلفهٔ ۷- بازدارندگی (توان و قدرت پاسخ‌گویی به تهدید): پیاده‌سازی اقدام‌های عملیاتی در خصوص تصمیم‌های دشمن به یک رویداد امنیت فضای سایبر؛

مؤلفهٔ ۸- مقابله مؤثر (توان رودررویی و تلافی): پیاده‌سازی اقدام‌های عملیاتی در روبه‌رو شدن و تلافی خسارت وارده توسط دشمن در امنیت فضای سایبر؛

مؤلفهٔ ۹- نوآوری و تحول (سیاست‌ها، منابع، زیرساخت): پیاده‌سازی اقدام‌ها و فعالیت‌های نوآورانه و تحول‌زا برای ارتقای صیانت امنیتی فضای سایبر

جدول فراوانی نظر پاسخ‌دهندگان در خصوص اقدام‌ها و راه‌کارهای صیانت امنیتی فضای سایبر

مقوله‌های مورد تأکید	فراوانی	درصد
شناسایی (منابع و دارایی‌های سایبری)	۱۱	۱۳/۱۰
محافظت (ایمن‌سازی و پایداری امنیت)	۱۲	۱٤/۲۹
تشخیص و کشف (تهدیدها و آسیب‌های امنیتی)	۹	۱۰/۷۱
تحلیل (مخاطرات)	۹	۱۰/۷۱
پاسخ و واکنش (رویدادهای امنیتی)	۸	۹/۵۲
بازیابی (حفظ و بهبود وضعیت)	۸	۹/۵۲
بازدارندگی (توان و قدرت پاسخ‌گویی به تهدید)	۹	۱۰/۷۱
مقابلهٔ مؤثر	۱۰	۱۱/۹۰
نوآوری و تحول (سیاست‌ها، منابع، زیرساخت)	۸	۹/۵۲

در بررسی دیدگاه مصاحبه‌شدگان در بعد سوم (اقدام‌ها و راه‌کارهای صیانت امنیتی فضای سایبر (چگونگی) مشخص می‌شود، گویه «محافظت (ایمن‌سازی و پایداری امنیت)» با ۱٤/۲۹ درصد رتبهٔ اول، گویه «شناسایی (منابع و دارایی‌های سایبری)» با ۱۳/۱۰ درصد در رتبهٔ دوم و گویه «مقابله مؤثر» با ۱۱/۹۰ در رتبهٔ سوم قرار دارند.

سؤال‌های فرعی مربوط به سؤال چهارم: در بررسی دیدگاه مصاحبه‌شدگان:

- در اقدام‌ها و راه‌کارهای شناسایی منابع و دارایی‌های سایبری، مقوله «شناخت حاکمیت راهبردها، سیاست‌ها، روش‌های مدیریت و نظارت» با ۲۰/٤۵ درصد در رتبهٔ اول قرار دارد.
- در اقدام‌ها و راه‌کارهای محافظت مقوله «پیاده‌سازی و استقرار استاندارد امنیت سایبر» با ۸/۸٦ درصد در رتبهٔ اول، قرار دارد.
- در اقدام‌ها و راه‌کارهای تشخیص و کشف (تهدیدها و آسیب‌های امنیتی)، مقوله‌های «شناسایی تهدیدها و آسیب‌پذیری‌های سایبری» و «فرایندهای تشخیص» با ۲۰ درصد در رتبهٔ اول قرار دارد.
- در اقدام‌ها و راه‌کارهای تحلیل مؤلفه‌های «پالایش هوشمند اطلاعات» و «اشراف اطلاعاتی و اشتراک‌گذاری اطلاعات رویدادهای سایبری» با ۲۰/٤۵ درصد در رتبهٔ اول قرار دارد.

- در اقدام‌ها و راه‌کارهای تحلیل، پاسخ و واکنش مؤلفه‌های «کاهش (جلوگیری از انجام و گسترش یک رویداد)» و «بهبود» با ۱۳/۸۵ درصد در رتبهٔ اول قرار دارد.
- در اقدام‌ها و راه‌کارهای بازیابی مؤلفه «ارتقاء (برنامه‌ریزی و فرایندهای بازیابی با نگاه به آینده)» با ۲۹/۰۳ درصد در رتبهٔ اول قرار دارد.
- در اقدام‌ها و راه‌کارهای بازدارندگی مقوله «تدوین قوانین و مجازات بازدارنده» با ۱٦/۳٦ درصد در رتبهٔ اول قرار دارد.
- در اقدام‌ها و راه‌کارهای مقابله مؤثر مؤلفه «حمله سایبری و مقابل اثربخش» با ۳۱/۲۵ درصد در رتبهٔ اول قرار دارد.
- در اقدام‌ها و راه‌کارهای نوآوری و تحول مقوله «ارتقای کمی و کیفی منابع انسانی حوزهٔ سایبر و امنیت سایبری» با ۲۳/٦۸ درصد در رتبهٔ اول قرار دارد.

سؤال پنجم: با توجه به اقدام‌ها و راه‌کارهای صیانتی حفاظتی در سؤال‌های بالا نقش اقدام‌های پیشگیرانه تا چه میزان بر پیشگیری و صیانت از تهدیدهای فضای سایبری تأثیر دارد؟

جدول فراوانی نظر پاسخ‌دهندگان در خصوص اقدام‌ها و راه‌کارهای صیانتی

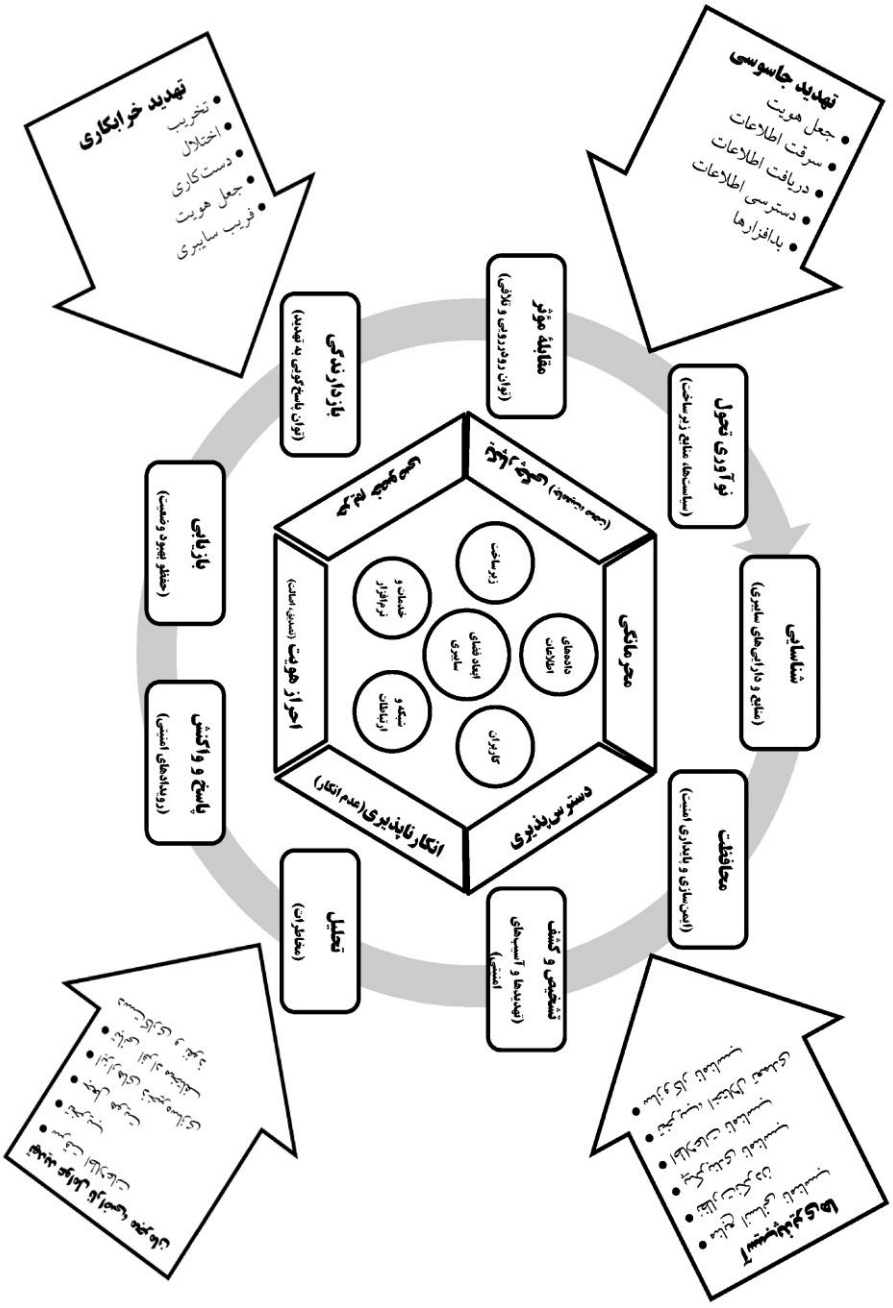
مقوله‌های مورد تأکید	فراوانی	درصد
خود حفاظتی	۱۱	۱۰/۷۸
آموزش	۹	۸/۸۲
توجیه و ارشاد	٦	۵/۸۸
آگاه‌سازی	۷	٦/۸٦
نظارت و کنترل	۱۰	۹/۸۰
امنیت کارکنان (صلاحیت کارکنان مأموریت‌های سایبری حین گزینش، ورود و حین خدمت و رهایی)	۱۳	۱۲/۷۵
امنیت فیزیکی و اجرایی‌کردن اصول پدافند غیرعامل	۹	۸/۸۲
ایجاد سیاست‌های دسترسی و حیطه‌بندی و طبقه‌بندی	۱۰	۹/۸۰

اشراف اطلاعاتی	۱۲	۱۱/۷٦
شناسایی عوامل مؤثر بر ارتباطات و اطلاعات	۸	۷/۸٤
تدوین و اجرای سناریوهای محتمل ناشی از تهدیدهای سایبری و سطح‌بندی آنها	۷	٦/۸٦

برابر دیدگاه مصاحبه‌شدگان امنیت کارکنان با ۱۲/۷۵ درصد در رتبهٔ اول و اشراف اطلاعاتی با ۱۱/۷٦ درصد در رتبهٔ دوم و خودحفاظتی با ۱۰/۷۸ درصد در رتبهٔ سوم قرار دارد.

بحث و نتیجه‌گیری

در نتیجه‌گیری نهایی از این پژوهش با توجه به اسناد بالادستی، فرامین، تدابیر و اسناد راهبردی فضای سایبر ابعاد و مؤلفه‌های فضای مجازی شکل ورود تهدیدها و آسیب‌پذیری‌ها به آنها و درنهایت اقدام‌های صیانتی و پیشگیرانه نمایان‌گر است. با توجه به نظر مصاحبه‌شدگان مبنی بر اینکه کاربران به‌عنوان مهم‌ترین عامل فضای سایبر هستند و در هدف‌های امنیتی فضای سایبر مهم‌ترین بعد دسترس‌پذیری و حریم خصوصی اعلام شده است در اقدام‌ها و راه‌کارهای پیشگیرانه در صیانت از مأموریت‌های سایبری اقدام‌های صیانتی کارکنان در استخدام و گزینش، حین خدمت و آگاه‌سازی، اشراف اطلاعاتی بر عملکرد کارکنان، نظارت و درنهایت ایجاد فرهنگ خود حفاظتی مهم‌ترین مؤلفه‌ها اعلام شده است. البته ارزیابی ریسک و خطرها و مدیریت تهدیدها، امنیت داده‌ها و اطلاعات، فرایندهای حفاظت اطلاعات، طبقه‌بندی و حیطه‌بندی اطلاعات امنیت فیزیکی، شناسایی تهدیدها و آسیب‌پذیری‌های سایبری، کاهش، بهبود، نظارت، هوشمندی و هشداردهی، حفظ آمادگی و برخورد به‌موقع با تخلفات، تدوین قوانین و مجازات‌های بازدارنده، قدرت پاسخ‌گویی، قدرت پشیمان‌سازی دشمن و رفع اثر تهدید نیز قابل‌توجه بوده و نقش مهمی در صیانت از مأموریت‌های سایبری دارد.



شکل ۱) الگوی صیانتی مأموریت‌های سایبری در سازمان‌های امنیتی

پیشنهادها

۱) پیشنهادهای مرتبط با سؤال اول (مأموریت‌های سایبری) آنچه مشخص و مبرهن است مأموریت‌های سایبری کاملاً مشخص و جامع نیست؛ بنابراین پیشنهاد می‌گردد:

- برای شناسایی تهدید و آسیب و ارائه راه‌کارهای پیشگیرانه لزوم شناسایی، تفکیک و دسته‌بندی انواع مأموریت‌های برای انجام مدیریت و حفاظت از آن امری ضروری است.
- مشخص‌شدن مأموریت‌های سایبری از لحاظ ماهیت، کیفیت و نحوهٔ اقدام‌های سازمانی.

۲) پیشنهادهای مرتبط با سؤال دوم (تهدیدهای اجرای مأموریت‌های سایبری): با توجه به تنوع تهدیدهای سایبری در کلیه ابعاد به‌خصوص در تهدیدهای امنیتی (جاسوسی، خرابکاری، براندازی، نفوذ و...) پیشنهاد می‌شود:

- سازمان در عملیات آفندی برای پیشگیری از تهدیدهای فضای سایبری اقدام‌های خود را متمرکز کند؛
- شناسایی عوامل حریف با پوشش مناسب برای شناسایی هدف‌ها، توانایی شیوه و شگردها؛
- تهیه مستند از ضعف‌ها و آسیب‌پذیری‌های کارکنان مأموریت‌های سایبری از موارد به‌دست آمده از پرونده‌های عملیاتی رسیدگی شده.

۳) پیشنهادهای مرتبط با سؤال سوم (آسیب‌پذیری‌های اجرای مأموریت‌های سایبری)

- انجام اقدام‌های تحلیلی درخصوص وقایع و پرونده‌های عملیاتی رسیدگی‌شده مرتبط با جرائم در فضای سایبری؛
- بهره‌برداری از بانک‌های اطلاعاتی تشکیل شده برای شناسایی آسیب‌پذیری‌ها و ارایه تحلیل هوشمندانه؛

٤)پیشنهادهای مرتبط با سؤال چهارم (اقدام‌های پیشگیرانه در صیانت از مأموریت‌های سایبری)

- ارائه الگوهای حفاظتی به منظور نظارت عملکرد کارکنان مأموریت‌های سایبری؛
- احصای موارد سوء و اعلام به‌مبادی ذی‌ربط برای صیانت از کارکنان؛

- درنهایت با ایجاد و تقویت نقش خودنظارتی و خودحفاظتی در بین کارکنان موجب صیانت و پیشگیری از مأموریت‌های سایبری گردند.
- نظارت مداوم این کارکنان برای سنجش این امر باید مدنظر باشد و در حصول موردی اقدام‌های پیشگیرانه و صیانتی و درنهایت بازدارنده لازم به‌عمل آید.

۵)پیشنهادها به مراکز پژوهشی و دانشجویان آینده:

- راه‌های بهینه‌کردن و اجرایی‌کردن آموزش (مداوم) کارکنان مأموریت‌های سایبری به تغییرهای روز فناوری‌های نوین (تهدیدها و آسیب‌پذیری‌های فضای سایبری)؛
- نهادینه‌کردن تقوا، ایمان در بین کارکنان به منظور ایجاد خودحفاظتی، صیانت و پیشگیری؛
- طراحی و پیاده‌سازی سیستم‌عامل امن بومی، بانک‌های اطلاعاتی، زیرساخت‌های طراحی و پیاده‌سازی که در تمامی فازهای تلاقی تولید زیرساخت سخت‌افزاری بومی؛
- به‌روزرسانی کلیه دستورکارهای جرائم سایبری؛
- سرعت همگام با تولید علم سایبری در برنامه‌های کلان؛
- ایجاد قوانین بازدارنده و به‌روز؛
- استفاده از افراد متخصص غیرسازمانی واجد صلاحیت امنیتی برای ارتقای امنیت شبکه‌های سازمان.

منابع

استرکی، اکبر (۱۳۹۱)، «شبکه‌های اجتماعی مجازی؛ مفاهیم، اصول و مبانی»، فصلنامه جامعه اطلاعاتی، سال چهارم، شماره ۱، تهران: انتشارات مرکز آموزشی پژوهشی شهید سپهبد صیاد شیرازی.

بابایی، محمد و بنی‌مسلم حیدری (۱۳۹۲)؛ «ارایه الگویی برای تحلیل و پیش‌بینی اطلاعات در سازمان‌های امنیتی»، *فصلنامه پژوهش‌های حفاظتی امنیتی دانشگاه جامع امام حسین*، شماره ٤ صفحه ۵۵ به نقل از دانش اطلاعاتی.

بوزان، باری (۱۳۷۸)؛ *مردم دولت‌ها و هراس*، تهران: پژوهشکدهٔ مطالعات راهبردی.

پورمراد، مجید (۱۳۸۹)، *دانستنی‌های حفاظت از فناوری اطلاعات و ارتباطات* (ویژه کارکنان ناجا و کاربران رایانه)، تهران: حدیث کوثر.

پورمراد، مجید (۱۳۹۳)، *حفاظت اطلاعات ویژه پلیس فتا* (ویژه مربیان مقطع کارشناسی)، تهران: حدیث کوثر.

چراغی، احمد و رحمت‌اله قدسی‌فر (۱۳۹۰)، *آنچه باید یک حفاظتی بداند*، تهران: حدیث کوثر.

خوش‌عمل، حسین (۱۳۹۱)؛ *پدافند غیرعامل در حوزهٔ سایبر*، تهران: مرکز آموزشی و پژوهشی شهید سپهبد شیرازی.

دهخدا، علی‌اکبر (۱۳۷۷)؛ *لغت‌نامه*، تهران: انتشارات دانشگاه تهران.

سخنان مقام معظم رهبری و فرماندهی معظم کل قوا(مدظله‌العالی) (۱۳۸۵)؛ ۱۸ آبان‌ماه.

سلحشور، مسعود (۱۳۹۲) *جمع‌آوری اخبار در فضای سایبری*، تهران: حدیث کوثر.

عمید، حسن (۱۳۸۲)، *فرهنگ فارسی*، تهران، امیر کبیر.

فرقانی، جمشید و مصطفی امکانی (۱۳۸۱)، *دانش نظامی عمومی*، تهران: انتشارات معاونت آموزشی نزاجا.

کتولی‌نژاد، خدابخش (۱۳۹٤)، *رهیافت امنیتی بر تهدیدها و آسیب‌پذیری‌ها*، تهران: حدیث کوثر.

کیان‌خواه احسان و سعید علوی‌وفا (۱۳۹۰)؛ «مفهوم‌شناسی امنیت سایبری»، *مجموعه مقالات نخستین همایش ملی دفاع سایبری*، تهران: سازمان انتشارات جهاد دانشگاهی.

کریمایی، علی‌اعظم (۱۳۸۷)؛ *حفاظت اطلاعات دافوس*، تهران: حدیث کوثر.

مشیری، مهشید (۱۳۷٤)، *فرهنگ اصطلاحات عامیانه جوانان*، تهران: ناشر آگاهان ایده.

معین، محمد (۱۳٦۲)، *فرهنگ فارسی معین*، تهران: انتشارات سپهر، جلد اول، چاپ پنجم.

یادگاری، وحید؛ رضا طلایی و علیرضا هاشمی (۱۳۹٤)؛ «آینده‌پژوهی جرائم سایبری علیه کارکنان ناجا»، *فصلنامه مطالعات حفاظت و امنیت انتظامی*، شماره ۳۵، تهران: حدیث کوثر.