فصلنامه پژوهش‌های حفاظتی ـ امنیتی
دانشگاه جامع امام حسین(علیه‌السلام)

سال نهم، شمارهٔ ۳۵ (پاییز ۱۳۹۹)صص۹۴-۶۵

طراحی الگوی مفهومی پایش تهدیدات سایبری جمهوری اسلامی ایران

■ کامیار ثقفی ■
استاد و عضو هیات علمی دانشگاه شاهد، تهران، ایران
■ علی اسماعیلی ■
دانشجوی دکترای مدیریت راهبردی امنیت فضای سایبر دانشگاه عالی دفاع ملی، تهران، ایران

تاریخ دریافت: ۱۳۹۹/۰۶/۲۰ تاریخ پذیرش: ۱۳۹۹/۰۹/۱۱

چکیده

در حال حاضر، بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی در همه‌سطوح، اعم از افراد، مؤسسه‌های غیر دولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد. بنابراین هر یک از این حوزه‌ها نیازمند مدل عملیاتی مختص خود برای پایش تهدیدها هستند. برای حفظ یکپارچگی این مدل‌ها لازم است یک الگوی مرجع راهبردی طراحی شود تا مدل‌های عملیاتی مذکور ذیل آن تعریف شوند. این الگو باید کمک کند تا هنگام طرح‌ریزی و تصمیم‌گیری‌های راهبردی، به عوامل و متغیرهای مؤثر و روابط آن‌ها توجه بیشتری شود. با تبیین مبانی نظری و پارادایم‌های حاکم بر این پژوهش و همچنین بررسی وضع موجود پایش تهدیدها، مطالعات تطبیقی، بررسی قوانین جاری کشور و استفاده از اسناد بالادستی، می‌توان الگوی مفهومی پایش تهدیدات سایبری ج.ا.ا را طراحی کرد.
با توجه به اینکه الگویی به‌منظور پایش تهدیدهای سایبری در کشور طراحی نشده، این پژوهش به‌دنبال چیستی آن است. این پژوهش با انجام مطالعات توصیفی و تکنیک تحلیل محتوا و همچنین بهره‌گیری از فن معادلات ساختاری، ضمن تأیید الگوی ارائه‌شده، مهم‌ترین ابعاد الگوی پایش تهدیدات سایبری ج.ا.ا را پویش و ارزیابی و واکنش در نظر گرفته است. بنابراین پیشنهاد می‌دهد با توجه به تقابل دائمی ج.ا.ا با استکبار جهانی و نظام سلطه، در ایجاد و ارتقای شبکه‌ملی اطلاعات که منجر به افزایش ظرفیت تاب‌آوری و ظرفیت انطباق می‌شود، تسریع شود.

کلید واژگان: *الگو، تهدیدات سایبری، پایش، فضای سایبر.*

مقدمه

حکومت‌هایی که رویکردهای سنتی به فضای مجازی دارند، به پدیده‌هایی که در درون و اطراف آن‌ها روی می‌دهد نگاه منفعلانه دارند. بنابراین در مواقع بروز تهدید سایبری غافلگیر شده و خسارت‌های زیادی را متحمل می‌شوند. در مقابل این رویکرد، نگاه دیگری وجود دارد که با تعاریف روش‌ها و فرایندهای مورد نیاز سعی می‌کند به‌صورت برنامه‌ریزی‌شده و هدفمند تهدیدات را رصد و پایش نماید و متناسب با آن‌ها اقدام پیشگیرانه و تدافعی را طراحی و اجرا نماید. همچنین سعی می‌کند به‌طور مداوم بر عملکرد آن نظارت داشته باشد و آن را ارتقا دهد. شناخت تهدیدات سایبری، تشخیص و ارزیابی ماهیت، نوع، شدت، دامنه و عمق آن در دستیابی به امنیت مطلوب و مد نظر در جامعه مبتنی بر فناوری، تأثیر بسزایی دارد. از سوی دیگر، پایش تهدیدات سایبری نقش مؤثری در محاسبه احتمال وقوع تهدید سایبری و ارزیابی شدت آن ایفا نموده و در سیاست‌گذاری موضوعات امنیتی نقش مهمی دارد.

پایش روندهای تهدیدات فضای سایبری نیازمند الگوی تصویری است که واقعیت‌ها، روابط و متغیرهای موجود، نحوه ارتباط آن‌ها و نتایج حاصل از کنش و واکنش آن‌ها را تبیین نماید. کشورهای پیشرو در حوزه سایبر این تهدیدات را به‌خوبی درک کرده‌اند و از قبل در سطوح مختلف راهبردی و عملیاتی الگوهایی را برای پیش‌بینی و سنجش آن‌ها، متناسب با کشورهای خود طراحی نموده و بر اساس این مدل‌ها، به ارزیابی و ارائه برآورد پرداخته‌اند. به‌عنوان نمونه، مؤسسه تحقیقاتی رند،[1] مؤسسه تحقیقاتی میتری[2] و همچنین سندیا[3] ازجمله مؤسسه‌های آمریکایی متعلق به نهادهای امنیتی‌نظامی آمریکا هستند که برای پایش و ارزیابی تهدیدات سایبری فعالیت‌های زیادی نموده‌اند.

با توجه به ویژگی‌های خاص حوزه‌های فعال در فضای سایبر، هر یک از این حوزه‌ها نیازمند مدل عملیاتی مختص خود برای پایش تهدیدات هستند. برای حفظ یکپارچگی این مدل‌ها نیاز است یک الگوی مرجع راهبردی طراحی شود تا مدل‌های عملیاتی مذکور ذیل آن تعریف گردند. از سویی، با توجه به بررسی‌های صورت‌گرفته در اسناد آشکار، چنین الگویی به‌منظور پایش تهدیدات سایبری در کشور طراحی نشده و عمدتاً اقدام انجام‌شده در دستگاه‌ها و سازمان‌ها در سطح مدل‌های عملیاتی است. با توجه به اینکه مدل‌های خارجی متناسب با مقتضیات ج.ا.ا نیستند و

1.Rand
2.MITRE
3.Sandia

از طرفی، وجود این الگو از نیازهای اساسی نظام مدیریت تهدیدات فضای سایبر ج.ا.ا است، باید به‌منظور طراحی آن اقدام نمود. از سویی بایست چیستی و شاخصه‌ها و رابطه میان آن‌ها به صورتی روشمند و قابل ارزیابی به تصمیم‌گیران کشور ارائه گردد. در این راستا، این پژوهش با هدف رفع این خلأ به تبیین آن‌ها می‌پردازد.

اهمیت و ضرورت پژوهش

در اهمیت این پژوهش از بُعد ایجابی می‌بایست به نکات ذیل اشاره نمود:

روابط عوامل تهدیدزا و سازوکارهای شناسایی تهدید را ترسیم نماید تا با به‌کارگیری این الگو زمینه‌های جلوگیری از غافلگیری و همچنین مقابله فعال را فراهم سازد.

در اسناد بالادستی همچون در فرمایش‌های امام خامنه‌ای(مدظله العالی) و سیاست‌های کلی نظام در حوزه افتا، سند افتا و همچنین راهبردهای دفاع سایبری کشور بر اهمیت‌داشتن چنین الگوهایی تأکید شده است (جمعی از محققان، ۱۳۹۵).

مدیریت تهدیدات سایبری شامل رصد و پایش تهدید، تحلیل تهدید، سنجش تهدید، طراحی و اجرای الگوی مناسب برای مدیریت واقعه و کنترل پیامدهای تهدید سایبری است (افتخاری،۱۳۹۲:۴۲).

این الگو بخش اول مدیریت تهدیدات را که همان پایش است، تبیین می‌نماید. نبود این الگو به‌منظور پایش و رصد تهدیدات، ممکن است چالش‌ها و نقایص ذیل را دربر داشته باشد:

ـ آمادگی برای مقابله با تهدیدات سایبری را کاهش دهد؛

ـ ابهام در تهدیددانستن یا ندانستن یک واقعه سایبری که در نهایت منجر به تصمیم‌گیری‌های غلط و هزینه‌های فراوان برای کشور می‌شود.

لذا این پژوهش با هدف تبیین بخش اول مدیریت تهدیدات سایبری و رفع نواقص مذکور به‌دنبال طراحی مفهومی یکی از نیازمندی اساسی کشور در حفاظت از ارزش‌ها و زیرساخت‌های حیاتی است.

اهداف پژوهش

ـ دستیابی به الگوی پایش تهدیدات سایبری ج.ا.ا؛

ـ دستیابی به ابعاد و مؤلفه‌ها و شاخص‌های پایش تهدیدات سایبری ج.ا.ا.

پرسش‌های پژوهش

ـ الگوی پایش تهدیدات سایبری ج.ا.ا چیست؟

ـ ابعاد و مؤلفه‌ها و شاخص‌های تهدیدات سایبری ج.ا.ا چه هستند؟

روش تحقیق

با تبیین مبانی نظری و پارادایم‌های حاکم بر این پژوهش و همچنین بررسی وضع موجود، پایش تهدیدها، مطالعات تطبیقی، بررسی قوانین جاری کشور و استفاده از اسناد بالادستی، می‌توان الگوی پایش تهدیدات سایبری ج.ا.ا را طراحی کرد. بنابراین می‌شود نتیجه گرفت که نوع پژوهش در این زمینه توسعه‌ای خواهد بود. از طرف دیگر، تحقیق حاضر در پی یافتن مشکلات کشور و راه‌حل آن‌هاست؛ بنابراین از این منظر، کاربردی محسوب می‌شود و در مجموع توسعه‌ای‌کاربردی است.

برای انجام این پژوهش سه گام اصلی وجود دارد:

ـ شناسایی عناصر تشکیل‌دهنده الگو، شامل شاخص‌ها و مؤلفه‌ها و ابعاد؛

ـ به‌دست‌آوردن ارتباط و شدت همبستگی میان عناصر تشکیل‌دهنده الگو؛

ـ تأیید الگو.

در گام اول برای به‌دست‌آوردن شاخصه‌ها و مؤلفه‌های الگو از تکنیک خوشه‌بندی در تحلیل محتوای اسناد بهره‌گیری شده است. روش تجزیه و تحلیل خوشه‌ای، روشی آماری برای گروه‌بندی داده‌ها یا مشاهدات، با توجه به شباهت یا درجه نزدیکی آن‌هاست. از طریق تجزیه و تحلیل خوشه‌ای، داده‌ها یا مشاهدات به دسته‌های همگن و متمایز از هم تقسیم می‌شوند.

گام دوم، به‌دست‌آوردن ارتباط و شدت همبستگی میان عناصر الگو است. در این پژوهش از تکنیک معادلات ساختاری (SEM)[1] استفاده شده است. در این پژوهش با استفاده از آزمون

1. Structural Equation Modeling

کولموگروف اسمیرنوف توزیع نرمال داده‌ها بررسی شد و به‌دلیل نرمال‌نبودن توزیع داده‌ها، روش حداقل مربعات جزئی[1] و الگوسازی معادلات ساختاری مبتنی بر واریانس برای تأیید الگوی مفهومی پژوهش انتخاب شد.

گام سوم، تأیید الگو است که در این تحقیق از روش تحلیل عاملی استفاده شده است. این روش به بررسی همبستگی درونی تعداد زیادی از متغیرها می‌پردازد و در نهایت آن‌ها را در قالب عوامل کلی و محدود دسته‌بندی و تبیین می‌کند. تحلیل عاملی روشی هم‌وابسته بوده که در آن همه متغیرها به‌طور هم‌زمان مد نظر قرار می‌گیرند. در این تحقیق از روش مدل اندازه‌گیری انعکاسی استفاده شده است. در این مدل هر نشانگر معرف یک اندازه‌گیری توأم با خطا از متغیر مکنون است. همچنین در این مدل جهت علیت، از سازه به نشانگرهاست. به عبارتی، در این مدل فرض می‌شود اندازه‌گیری‌های مشاهده‌شده، تغییر در متغیر مکنون را منعکس می‌کنند. به بیان دیگر، با تغییر در سازه مدنظر تغییر در همه نشانگر بارز می‌شود. با توجه به اینکه در این مدل متغیر پایش تهدیدات سایبری دارای سه زیرمؤلفه است که تغییر در این سه مؤلفه بر روی متغیر پایش تهدیدات سایبری اثر می‌گذارد و همچنین چون هدف، تبیین اندازه‌گیری‌های مشاهده‌شده است؛ بنابراین در این تحقیق از مدل انعکاسی استفاده شده است. درمجموع این پژوهش، پژوهشی آمیخته است.

جامعه آماری و تعداد آن

بر اساس تحقیق، جامعه آماری پژوهش شامل گروه‌های ذیل است:

ـ متخصصان فضای سایبر و تهدیدات سایبری؛

ـ متخصصان علوم راهبردی.

از میان این دو گروه، به روش نمونه‌گیری هدفمند و در دسترس، تعداد ۷۰ نفر انتخاب شدند و پرسش‌ها در اختیار آن‌ها قرار داده شد.

1. Partial Least Squares

پیشینه‌پژوهش

در بررسی‌های صورت‌گرفته از بانک‌های اطلاعاتی آشکار داخلی، پژوهشی مجزا درخصوص الگوی پایش تهدیدات سایبری ج.ا.ا یافت نشد. فقط یک مقاله در سال ۱۳۹۴ به‌دست آقایان عبدالله‌خانی و حسینی با عنوان «سنجش تهدیدات سایبری» به دست آمد که توجه اصلی آن بر آسیب‌پذیری دارایی‌های کلیدی و اهداف مرجع است. با این حال، پژوهش‌های مفصلی در خارج از کشور از سوی نهادهای امنیتی و دفاعی همچون مؤسسه رند و سندیا در آمریکا صورت گرفته است که عناوین آن چنین است: مقاله «کشف تهدید سایبری مبتنی بر آنالیز رفتار حمله» در سال ۲۰۱۷ از سوی مؤسسه آمریکایی میتری منتشر شد. این پژوهش چارچوبی برای کشف حملات سایبری در سطح یک شبکه بزرگ را ارائه می‌دهد. انتشار طرح «ارزیابی تهدیدات سایبری مؤسسه میتری» در سال ۲۰۱۲ که با ارائه چارچوبی به‌دنبال ارزیابی تهدیدات سایبری با تکیه بر دو مؤلفه رفتار دشمن و هدف تهدیدگر است. مؤسسه سندیا در سال ۲۰۱۲ با ارائه یکسری شاخص‌ها به‌دنبال سنجش تهدیدات سایبری است. این چارچوب بر اساس توانایی و نیت تهدیدگر سایبری پایه‌گذاری شده است. مؤسسه میتری در طرح دیگری با عنوان «متدولوژی ارزیابی و اصلاح تهدیدات سایبری» در سال ۲۰۱۵ به‌دنبال ارائه یک مدل مهندسی در اولویت‌گذاری و پاسخ به تهدیدات سایبری از طریق به‌کارگیری اقدام برای کاهش استعداد آسیب‌پذیری در مقابل حملات سایبری است.

از دیگر پژوهش‌های انجام‌شده، رساله دکترای تئودور در سال ۲۰۱۲ با عنوان «چارچوب و نظریه برای ارزیابی امنیت فضای سایبر» است که به بررسی و ارزیابی تهدیدات سامانه‌های اسکادا می‌پردازد. همچنین رساله دیگری با عنوان «شناسایی و مقابله با تهدیدات سایبری در حوزه بانکی» نوشته لیناس در سال ۲۰۱۶، به بررسی بدافزارهای موبایل‌محور در عرصه بانکی می‌پردازد. مقاله‌ای با عنوان «مدل پیش‌بینی تهدیدات سایبری بر اساس پایش وقایع امنیتی سیستم» نوشته پارک در سال ۲۰۱۲ و همچنین مقاله‌ای با عنوان «امنیت سایبری: تهدیدات، دلایل، چالش‌ها، متدولوژی و راهکاری برای نرم‌افزارهای صنعتی» نوشته عبدالرزاق در سال ۲۰۱۳ به‌دنبال بررسی تهدیدات فنی در سطح شبکه از دید مهندسی بوده‌اند.

بررسی پیشینه‌های مذکور حاکی از آن است که با اینکه تهدیدات تکنیکی اثرات راهبردی دارند، اما بنا بر تحلیل‌های انجام‌شده، مقالات موجود فقط به جنبه‌های تکنیکی حملات سایبری، آن‌هم در سطح یک شبکه محدود پرداخته بودند و به تأثیر راهبردی آن توجهی نکرده بود.

مفهوم‌شناسی متغیرها

الگو

الگو تصویری است که از واقعیت‌ها و روابط موجود گرفته شده و نشانگر متغیرهای موجود، نحوه ارتباط آن‌ها و نتایج حاصل از کنش و واکنش آن‌هاست (حمیصی، ۱۳۹۱: ۱۶).

تهدیدات سایبری

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

تعریف عملیاتی پایش تهدیدات سایبری

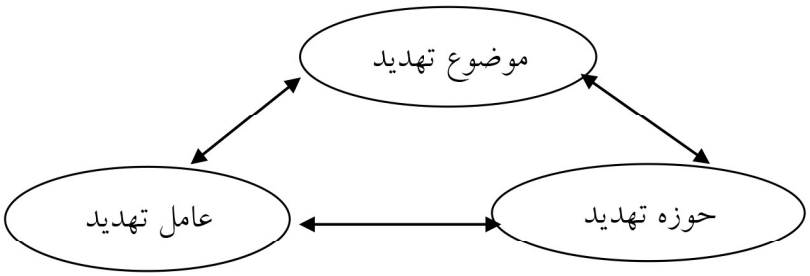
بر اساس تعریفی که وندل[1] از پایش نموده است، می‌شود پایش تهدیدات سایبری را فرایند مستمر پویش (جمع‌آوری)، آشکارسازی، تخمین‌زدن، ارزیابی، واکنش و ره‌گیری رویدادهای سایبری مرتبط با حوزه امنیت فضای مجازی دانست.

ادبیات و مبانی نظری

معنای تهدیدات امنیتی

تهدید از سه بخش اساسی کارگزار یا عامل تهدید، حوزه تهدید و موضوع تهدید تشکیل شده است. عامل تهدید در واقع هویت (شخصی یا سازمانی) یا چیزی است که به‌طور بالفعل یا بالقوه توانایی ایجاد، انتقال یا پشتیبانی از تهدید را دارد؛ درحالی‌که حوزه تهدید، هویت یا چیزی است که موجودیت یا دارایی‌های حیاتی آن در معرض خطر قرار گرفته است. موضوع تهدید، وضعیت، پدیده، فعالیت یا رخدادی است که به نظر می‌رسد قابلیت‌های درونی و بیرونی انتقال، پشتیبانی یا ایجاد خطر را در موجودیت یا دارایی‌های حیاتی بازیگر مورد آماج در خود دارد (عبداللّه‌خانی، ۲۱:۱۳۸۶).

1.Wendel



شکل۱: اجزای سازمان تهدید

دسته‌بندی تهدیدات سایبری

دارایی‌ها همواره در معرض انواع تهدیدها قرار دارند. تهدید عبارت است از عامل بالقوه یک رویداد امنیتی نامطلوب که می‌تواند موجب واردآمدن خسارت به سیستم یا سازمان شود. در واقع، تهدید عاملی است که می‌تواند موجب بروز یک حادثه امنیتی شود. غالباً عاملی را تهدید می‌نامند که به‌شکل بالقوه در کمین امنیت است. تهدیدی که به فعلیت درآید، حمله نامیده می‌شود. معمولاً یک سازمان، یا کنترل کمی نسبت به یک تهدید دارد یا اصلاً کنترلی ندارد که علت این امر ریشه در خارجی‌بودن منبع تهدید دارد.

در ذیل به برخی از دسته‌بندی‌های تهدیدات سایبری موجود منتشرشده در مستندات علمی اشاره شده است.

- دسته‌بندی تهدیدات اشاره‌شده در سند افتا (سند افتا، ۱۳۸۷)
- طبقه‌بندی تهدیدهای سایبری در گزارش کنگره آمریکا (USGAO, 2010)
- طبقه‌بندی AVOIDIT برای تهدیدهای سایبری (Simmons, 2009)
- طبقه‌بندی حملات سایبری بر اساس اطلاعات تهیه‌شده توسط سرت (Kjaerland, 2005)
- دسته‌بندی با چهار بعد برای پوشش حملات کامپیوتری و شبکه (Hansman, 2005)
- طبقه‌بندی حمله‌محور روی چهار دلیل اصلی خطاهای امنیتی (Lough, 2001)
- طبقه‌بندی از حملات منع سرویس توزیع‌شده (Mirkovic, 2004)
- طبقه‌بندی بر اساس ریسک‌های امنیتی سایبری (محمدی، ۱۳۹۱: ۹۴)
- تعریف ماکروسافت برای تقسیم‌بندی تهدیدات (morana, 2011)
- دسته‌بندی هوارد از حمله سایبری (Cohen, 2009)
- تقسیم‌بندی سازمان پدافند غیر عامل (محمدی، ۱۳۹۱: ۹۶).

اگر در یک مدل مفهومی ابعاد فضای سایبر را حوزه‌های محتوا، سرویس، زیرساخت، ماشین‌های هوشمند، حاکمیت و کاربر تعریف نماییم، دسته‌بندی‌های ذکرشده اغلب در ابعاد سرویس و زیرساخت

بوده‌اند و اشاره‌ای به تهدیدات در بعدهای محتوا، کاربر و حاکمیت ننموده‌اند. در این راستا، لازم است تهدیدات این حوزه‌ها نیز احصا و دسته‌بندی شود.

درخصوص ابعاد سرویس و زیرساخت نیز لازم به ذکر است که این طبقه‌بندی‌ها با فراهم‌کردن اطلاعات مفید درباره حملات، به مدافعان کمک می‌کند تا از شبکه خود در مقابل مهاجمان سایبری دفاع کنند. با این شیوه‌ها می‌توان انواع حملات را پیش‌بینی کرد. با توجه به اینکه روش‌های دفاعی بسیار زیاد هستند، بنابراین نیاز است که دسته‌بندی‌ها توسعه یابند و انواع روش‌های دفاعی ممکن برای آسیب‌پذیری‌هایی نیز که کشف می‌شوند، در نظر گرفته شود.

تعریف عملیاتی فرایند پایش

پایش[1] : رویه‌ای روش‌شناختی است که با هدف ارزیابی رویدادهای در حال شکل‌گیری، هم‌زمان با روی‌دادن یا در کوتاه‌ترین زمان ممکن پس‌ازآن، انجام می‌پذیرد (خزایی، ۱۳۸۴: ۴۹). پایش معمولاً دربرگیرنده چندین بخش متفاوت است.

پویش[2] : پویش جستجوی علائم و نشانه‌های رویدادها یا فرایندها در محیطی ویژه مانند شگفتی‌ساز تا علائم ضعیف تغییر، پیشران‌ها و متغیرهای کلیدی است (همان). برخی از محورهای جمع‌آوری بدین‌گونه هستند: تغییرات روند جابه‌جایی بستر ارتباطات از کابل به حوزه بی‌سیم؛ روند همگرایی علوم فناوری اطلاعات و ارتباطات با بیوتکنولوژی؛ ظهور تکنولوژی‌های جدید در ساخت و معماری رایانه‌ها، مانند سامانه‌های مبتنی بر فیزیک کوانتوم.

آشکارسازی[3] : توجه به یافته‌های مربوط به فرایند در حال پایش (همان)؛ به‌عنوان مثال، برجسته‌سازی وضعیت حکمرانی اینترنت با استفاده از پیشران‌های فضای سایبر، مانند توجه به ظهور اینترنت اشیا و قابلیت کنترل و مدیریت آینده بر اساس این فناوری.

تخمین‌زدن[4]: پیش‌بینی آینده یک پدیده و پاسخ احتمالی آن به شرایط متغیر (همان)؛ به‌عنوان مثال پیش‌بینی انتقال از آی‌پی ورژن ۴ به آی‌پی ورژن ۶ در راستای ایجاد زیرساخت اینترنت اشیا.

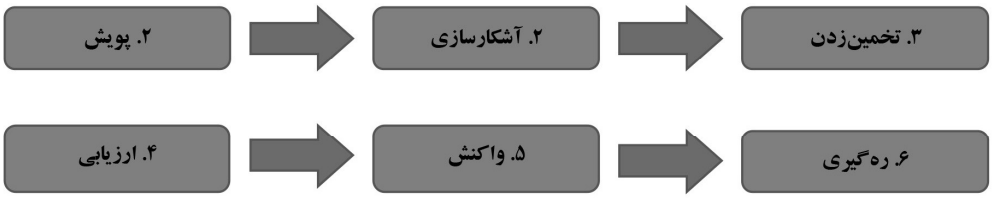
1.moitoring
2. scanning
3.detecting
4. projecting

ارزیابی[1]: قضاوت درباره مفهوم یافته‌های مرحله آشکارسازی، البته اگر روشن نباشند (همان)؛ برای نمونه، برآورد قدرت نرم جبهه استکبار به‌خاطر گسترش اشرافیت اطلاعاتی راهبردی ناشی از تجمیع اطلاعات حاصله نزد آن‌ها در سامانه یا سرویس‌هایی چون رایانش ابری.

واکنش[2]: تصمیم‌گیری درباره نحوه برخورد یا پاسخ مطلوب با توجه به ماهیت پدیده آشکارشده (همان)؛ برای مثال اعلام وضعیت‌هایی چون بحران، هشدار و... درخصوص گسترش شبکه‌های اوترنت.[3]

ره‌گیری[4]: پیگیری مستمر پدیده‌ای که شناسایی و کشف شده است (همان، ۸۵)؛ برای مثال امکان‌سنجی پدیده‌هایی چون شبکه‌های اینترنت چمدانی یا روزآمدکردن اطلاعات مربوط به پیامدهای گسترش تارنماهای سیاه.[5]

دقت در اندازه‌گیری پدیده پایش‌شده، جامع‌بودن پویش، قطعیت در کشف و آشکارسازی پدیده‌های هدف (به‌هنگام وقوع آن‌ها) و وجود ابزارهای نظری و مفهومی و فنی مناسب برای ارزش‌یابی درست معنای پدیده‌ها، عواملی هستند که تا حد زیادی سودمندی و کارآمدی پایش را تحت‌تأثیر قرار می‌دهند.



شکل ۲: فرایند عملیاتی پایش (wendel, 2008: 292)

مدل مفهومی

مدل مفهومی که در این مرحله حاصل گردیده، نتیجه تحلیل و مستخرج از ادبیات و مبانی نظری و اسناد بالادستی و مطالعه تطبیقی و محیطی است. این مدل حاکی از ساخت‌های اساسی مفهوم پایش تهدیدات سایبری است که در سطح خود، قادر به تبیین و ارائه ابعاد یا همان عوامل تشکیل‌دهنده آن و همچنین تعاریف عملیاتی آن (مؤلفه‌ها) است. برای رسیدن به این مدل بر مبنای تعریف ارائه‌شده در موضوع پایش ابعاد مدل احصا گردید. این ابعاد از سوی جمعی از

1.evaluating
2.reacting
3.Outernet
4.Tracking
5.Dark Web

خبرگان ارشد فضای سایبر در دو حوزه مدنی و نظامی (از طریق مصاحبه‌های عمیق) تأیید شد. سپس عبارات مهم قابل تأکید موضوعات مطرح‌شده مانند جدول شماره ۱ استخراج شد و پس از دسته‌بندی آن‌ها بر اساس بیشترین فراوانی، این کلیدواژه‌ها به‌عنوان مؤلفه و شاخص‌های الگو بهره‌برداری شد. این جداول مبتنی بر عناصر تشکیل‌دهنده الگوی پژوهش (مفهوم) به‌همراه منبع آن مستخرج از مراجعی است که در پژوهش بررسی شده‌اند. به‌عنوان مثال مؤلفه «منابع» دارای چندین شاخص است که مشخص گردیده هر کدام از چه مرجعی استخراج گردیده و در کجای پژوهش به‌صورت مفصل تبیین شده است

مفهوم	ارجاع	منبع
مؤلفه	منابع	
نفوذ	مبانی نظری؛ دشمن‌شناسی	مقام معظم رهبری در دیدار با مدرسان و فضلا و طلاب حوزه علمیه مشهد، ۲۰ تیر ۱۳۶۸
	ادبیات تحقیق؛ تاریخچه و مفاهیم	Sandia, 2012, cyber metrics
	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱
منشأ	مبانی نظری؛ دشمن‌شناسی	مقام معظم رهبری در دیدار گروه کثیری از بسیجیان سراسر کشور، ۳۰ آبان ۱۳۷۵
	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱
	مبانی نظری؛ طبقه‌بندی تهدیدهای سایبری در گزارش کنگره آمریکا	USGAO, 2010
	مبانی نظری؛ دسته‌بندی هوارد از حمله سایبری	Cohen, 2009
	مطالعه تطبیقی؛ انگلیس	Uk cyber security, 2014

هم‌پیمانان	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع‌تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیرعامل، ۱۳۹۱
دانش تخصصی فضای مجازی	مفاهیم و ادبیات تحقیق؛ ژئوپلیتیک فضای سایبر	احمدی‌پور، ابعاد ژئوپلتیک فضای سایبری در عصر فن‌آوری اطلاعات، ۱۳۹۱
	ادبیات تحقیق؛ تاریخچه و مفاهیم	Sandia, 2012, cyber metrics
دانش جنبی	ادبیات تحقیق؛ تاریخچه و مفاهیم	Sandia, 2012, cyber threat metrics
مؤلفه تمایل		
پافشاری	مفاهیم و ادبیات تحقیق؛ سازمان معنایی تهدید	علی عبداللّه‌خانی، تهدیدات امنیت ملی، ۱۳۸۶
	ادبیات تحقیق؛ تاریخچه و مفاهیم	Sandia, 2012, cyber threat metrics
	مفاهیم و ادبیات تحقیق؛ شاخص انگیزه در طبقه‌بندی تهدیدات	اصغر افتخاری، برآورد تهدید؛ رویکردی نظام‌واره، ۱۳۹۲
	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱
زمان	مفاهیم و ادبیات تحقیق؛ سنجش شدت تهدیدات	اصغر افتخاری، برآورد تهدید؛ رویکردی نظام‌واره، ۱۳۹۲
	ادبیات تحقیق؛ تاریخچه و مفاهیم	Sandia, 2012, cyber metrics
	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱
سابقه تهدید	ادبیات تحقیق؛ تاریخچه و مفاهیم	The MITRE Corporation,2012

قابلیت / توانایی	مفاهیم و ادبیات تحقیق؛ ظرفیت‌های درونی	اصغر افتخاری، برآورد تهدید؛ رویکردی نظام‌واره، ۱۳۹۲
	ادبیات تحقیق؛ تاریخچه و مفاهیم	The MITRE Corporation, 2012
	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱
احتمال موفقیت	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱
شدت تهدید سایبری	مبانی نظری؛ تقسیم‌بندی سازمان پدافند غیر عامل	ارزیابی تهدیدات سایبری، سازمان پدافند غیر عامل
	ادبیات تحقیق؛ تاریخچه و مفاهیم	Sandia, 2012, cyber metrics
	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱
نهان‌کاری	مبانی نظری؛ مطالعه تطبیقی آمریکا	America ‘s cyber future, 2011
	ادبیات تحقیق؛ تاریخچه و مفاهیم	Sandia, 2012, cyber threat metrics
جذابیت	ادبیات تحقیق؛ تاریخچه و مفاهیم	America ‘s cyber future, 2011
	ادبیات تحقیق؛ تاریخچه و مفاهیم	آیین‌نامه فنی سایبری، پدافند غیر عامل، ۱۳۸۸
	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱
پیامدهای منفی	ادبیات تحقیق؛ تاریخچه و مفاهیم	The MITRE Corporation, 2012
	مبانی نظری؛ دشمن‌شناسی	مقام معظم رهبری در مراسم بیعت مردم زنجان، ۱۵ تیر ۱۳۶۸
	ادبیات تحقیق؛ تاریخچه و مفاهیم	آیین‌نامه فنی سایبری، پدافند غیر عامل، ۱۳۸۸
	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱

تمایل	ادبیات تحقیق؛ تاریخچه و مفاهیم	The MITRE Corporation,2012
	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱
افشا	ادبیات تحقیق؛ تاریخچه و مفاهیم	The MITRE Corporation, 2012
مؤلفه آسیب‌پذیری		
بازدارندگی	ادبیات تحقیق؛ تاریخچه و مفاهیم	علی عبداللّه‌خانی، تهدیدات امنیت ملی، ۱۳۸۶
بازدارندگی	ادبیات تحقیق؛ تاریخچه و مفاهیم	جمعی از محققان، ۱۳۹۵
بازدارندگی	ادبیات تحقیق؛ تاریخچه و مفاهیم	سیاست‌های کلی نظام در حوزه پدافند غیر عامل
ظرفیت انطباق	ادبیات تحقیق؛ تاریخچه و مفاهیم	علی عبداللّه‌خانی، تهدیدات امنیت ملی، ۱۳۸۶
تاب‌آوری	ادبیات تحقیق؛ تاریخچه و مفاهیم	جمعی از محققان، ۱۳۹۵
تاب‌آوری	ادبیات تحقیق؛ تاریخچه و مفاهیم	The DOD cyber strategy, 2015
تاب‌آوری	ادبیات تحقیق؛ تاریخچه و مفاهیم	علی عبداللّه‌خانی، تهدیدات امنیت ملی، ۱۳۸۶
تاب‌آوری	ادبیات تحقیق؛ تاریخچه و مفاهیم	جمعی از محققان، ۱۳۹۵
مؤلفه پیامد تهدید سایبری		
عمق تهدید سایبری	ادبیات تحقیق؛ تاریخچه و مفاهیم	انواع تهدیدات و نحوه بررسی آن‌ها، سازمان پدافند غیر عامل، ۱۳۹۱
عمق تهدید سایبری	ادبیات تحقیق؛ تاریخچه و مفاهیم	علی عبداللّه‌خانی، تهدیدات امنیت ملی، ۱۳۸۶

عمق تهدید سایبری	ادبیات تحقیق؛ تاریخچه و مفاهیم	باری بوزان، ۱۳۷۸
شدت تهدید سایبری	ادبیات تحقیق؛ تاریخچه و مفاهیم	علی عبداللّه‌خانی، تهدیدات امنیت ملی، ۱۳۸۶
شدت تهدید سایبری	ادبیات تحقیق؛ تاریخچه و مفاهیم	باری بوزان، ۱۳۷۸
گستره تهدید سایبری	ادبیات تحقیق؛ تاریخچه و مفاهیم	علی عبداللّه‌خانی، تهدیدات امنیت ملی، ۱۳۸۶
گستره تهدید سایبری	ادبیات تحقیق؛ تاریخچه و مفاهیم	باری بوزان، ۱۳۷۸
مؤلفه اقدام و اعلام		
ره‌گیری	ادبیات تحقیق؛ تاریخچه و مفاهیم	Metayer, 2011
اشتراک و تحلیل اطلاعات	ادبیات تحقیق؛ تاریخچه و مفاهیم	David , 2017
اشتراک و تحلیل اطلاعات	ادبیات تحقیق؛ تاریخچه و مفاهیم	FACT SHEET, 2015
اطلاع‌رسانی	ادبیات تحقیق؛ تاریخچه و مفاهیم	William, 2005
اطلاع‌رسانی	ادبیات تحقیق؛ تاریخچه و مفاهیم	EE-ISAC, 2017
اعلام وضعیت	ادبیات تحقیق؛ تاریخچه و مفاهیم	Matt Loeb, 2015
اعلام وضعیت	ادبیات تحقیق؛ تاریخچه و مفاهیم	ITL BULLETIN, 2017
اطلاع‌رسانی	ادبیات تحقیق؛ تاریخچه و مفاهیم	ITL BULLETIN, 2017

ره‌گیری	ادبیات تحقیق؛ تاریخچه و مفاهیم	NIST, 2016
اشتراک و تحلیل اطلاعات	ادبیات تحقیق؛ تاریخچه و مفاهیم	NIST, 2016
اطلاع‌رسانی	ادبیات تحقیق؛ تاریخچه و مفاهیم	NIST, 2016

جدول ۱: شاخصه‌ها و مؤلفه‌های الگو

بر اساس تعریفی که وندل[1] از پایش ارائه نموده، می‌شود به‌صورت کلی ابعاد الگوی پایش تهدیدات سایبری را به سه بخش اصلی تقسیم نمود: ۱. پویش تهدیدات سایبری؛ ۲. ارزیابی تهدیدات سایبری؛ ۳. واکنش تهدیدات سایبری.

این ابعاد با مدل‌هایی چون OODA تطابق دارد که جان بوید،[2] استراتژیست نظامی آمریکا، آن را در سال ۱۹۹۷ درخصوص فرایند عملیات نظامی (در حوزه نیروی هوایی) ارائه داده بود.

OODA مدلی برای تصمیم‌گیری است که به انجام یک تصمیم‌گیری سریع، اثربخش و پیشگیرانه کمک می‌کند. این مدل از چهار بعد تشکیل شده است:

ـ مشاهده:[3] جمع‌آوری اطلاعات جاری از کلیه منابع موجود و در دسترس.

ـ جهت‌گیری:[4] تجزیه و تحلیل اطلاعات گردآوری‌شده و استفاده از آن برای به‌روزکردن وضعیت فعلی.

ـ تصمیم‌گیری: [5]تعریف انجام مجموعه‌ای از اقدامات.

ـ اقدام:[6] پیگیری و اجرای تصمیم اتخاذشده (Frans Osinga, 2006).

برای تبیین بیشتر این مفاهیم، هر کدام از این کلیدواژه‌ها تعریف شد. گفتنی است که مرجع این مفاهیم همان ستون منبع در جدول ۱ است.

1.Wendel
2.John Boyd
3.Observe
4.Orient
5.Decide
6.Act

پویش تهدیدات سایبری

جمع‌آوری داده‌های مرتبط با امنیت سایبری یا نقض امنیت سایبری از کلیه منابع را پویش گویند. در این بعد تمرکز جمع‌آوری اطلاعات بر وضعیت تهدیدگر (دشمن) است. مؤلفه‌های این بعد عبارت‌اند از: منابع و تمایل.

منابع:[1] منظور از منابع، همان ویژگی‌های زیرساختی و توانمندی‌های تهدیدگر سایبری و امکانات به‌کارگیری‌شده از سوی دشمن برای انجام، انتقال یا پشتیبانی تهدید سایبری است.

شاخص‌های منابع عبارت‌اند از:

نفوذ:[2] مجموعه اقداماتی را نفوذ گویند که دشمن در راستای ایجاد دسترسی در دارایی‌های سایبری انجام می‌دهد؛ مثلاً بهره‌گیری از عوامل انسانی نفوذی با هدف شکستن الزامات حفاظتی.

دانش سایبری و تنوع تخصص‌های آن: میزان و سطح بهره‌گیری از علوم اطلاعات و ارتباطات در طراحی و تولید و به‌کارگیری تهدید. ممکن است تهدید ترکیبی از چند دانش مختلف در حوزه‌های فنی باشد؛ مانند تولید ویروس‌های روز صفر[3] و انتشار آن در شبکه‌های ارتباطی.

دانش مرتبط:[4] اشاره به دانش‌های جنبی (غیر سایبری) در تولید و اجرای تهدید سایبری دارد؛ به‌عنوان مثال بهره‌گیری از دانش هسته‌ای در تولید و انتشار ویروس استاکس‌نت.

تجهیزات سخت‌افزاری و نرم‌افزاری: سطح، پیچیدگی و شدت بهره‌گیری از تجهیزات فناوری اطلاعات در تولید و به‌کارگیری تهدید.

تعدد هم‌پیمانان: اشاره به همکاری جمعیِ تهدیدگران علیه دارایی سایبری دارد؛ به‌عنوان مثال همکاری چند کشور متخاصم علیه ج.ا.ا در طراحی و انجام تهدید علیه زیرساخت‌های هسته‌ای.

منشأ: منشأ تهدید اشاره به ویژگی هویت تهدیدگر سایبری دارد که شامل دولت‌ها، گروه‌های هکری، تروریست‌ها و... می‌شود. هر سطحی از این منشأها به کارگیری شود نوع حمله و اثرات تخریبی آن متمایز خواهد بود.

تمایل:[5] منظور از مؤلفه تمایل ویژگی‌های مرتبط با میزان و شدت اشتیاق تهدیدگر سایبری به اقدام، پشتیبانی یا انتقال تهدید برای رسیدن به اهداف خود است.

1.Resource
2.Access
3. zero day
4.Kenetic knowledge
5.Willingness

شاخص‌های تمایل عبارت‌اند از:

نهان‌کاری:[1] اشاره به میزان اختفا و پنهان‌کاری اقدامات تهدیدگر سایبری دارد. هر چه میزان اهمیت و تمایل دشمن (تهدیدگر) بیشتر باشد، اقدامات خود را به‌صورت نهان‌تر انجام می‌دهد.

سابقه تهدید: اشاره به تعداد و همچنین تناوب انجام تهدید سایبری مشخص در گذشته دارد. هر چه تهدیدگر سایبری از انجام تهدید جواب مطلوب خود را کسب کرده باشد، باز هم تمایل به انجام آن در آینده دارد.

زمان: اشاره به میزان زمان طراحی و اجرای تهدید سایبری از سوی دشمن (تهدیدگر) دارد. هر چه این زمان طولانی‌تر باشد اهمیت تهدید و تمایل تهدیدگر برای انجام آن، بیشتر است.

افشا:[2] در صورتی که تهدید سایبری به هر نحوی افشا شود و دشمن همچنان به‌دنبال انجام آن باشد یا آن را ترک نماید حاکی از میزان تمایل وی برای انجام یا پشتیبانی تهدید است.

جذابیت دارایی:[3] میزان ارزشی که دارایی سایبری برای تهدیدگر دارد. به‌عنوان مثال اثرات تخریبی ناشی ازبین‌رفتن زیرساخت‌های انرژی در دیگر زیرساخت‌ها جذابیت این حوزه را برای تهدیدگر مضاعف می‌نماید.

تبعات منفی: غالباً تهدیدگر سایبری به‌دنبال انجام تهدیداتی است که برای وی تبعاتی به‌دنبال نداشته باشد یا حداقل در پایین‌ترین سطح هزینه باشد؛ به‌عنوان مثال درج نام تهدیدگر در فهرست‌های ممنوعه یا تحریم و...، در صورت اثبات حمله از سوی تهدیدگر.

میزان موفقیت تهدید: میزان احتمال موفقیت‌آمیزبودن تهدید سایبری از نظر تهدیدگر.

ارزیابی تهدیدات سایبری

پیش‌بینی آینده نحوه برخورد تهدید سایبری با دارایی‌ها مستلزم بررسی آسیب‌پذیری‌های دارایی سایبری و همچنین پیامد تحقق آن تهدیدات است؛ زیرا تهدیدات به‌خودیِ‌خود و فارغ از محیط دارایی‌ها، بی‌خطر هستند. لذا می‌بایست بر اساس شاخص‌های آسیب‌پذیری دارایی‌ها و پیامد تحقق تهدیدات، اطلاعات را جمع‌آوری و تحلیل کرد.

آسیب‌پذیری دارایی‌های سایبری را می‌توان به ناتوانی در جلوگیری از حمله سایبری، ناآگاهی

1.Stealth
2.Exposure
3.Attraction

درخصوص چگونگی وقوع و مدیریت تهدید و نبودِ قدرت در دفع حمله سایبری بیان نمود. لذا ظرفیت آسیب‌پذیری دارایی سایبری را می‌شود در سه مرحله قبل و حین و بعد از حمله سایبری ارزیابی نمود. شاخص اول، بازدارندگی است که عبارت است از فعالیت‌های طرف خودی برای اعمال نفوذ در تهدیدگر سایبری، به نحوی که وی را از اقدام به تهدید باز دارد؛ یعنی اقدامات انجام‌شده در راستای جلوگیری از واردآمدن تهدید یا همان مرحله قبل از حمله. شاخص بعدی تاب‌آوری است. بدین معنا که آیا امکان بازگشت دارایی سایبری به حالت سابق وجود دارد یا خیر؟ یا حداقل در میان‌مدت امکان چنین کاری امکان‌پذیر هست؟ به‌عنوان مثال با ایجاد قابلیت افزونگی پیش از حمله، شاهد استمرار سرویس در حال ارائه هستیم. این بدان معنی است که سامانه دارای تاب‌آوری است. در مرحله سوم، یعنی بعد از حمله و زمان مدیریت بحران موضوع ظرفیت انطباق مطرح است. یعنی آیا دارایی سایبری تهدیدشده می‌تواند در زمانی معقول و قابل اتکا خود را با وضعیت تهدید وفق دهد؟ به‌عبارت دیگر، آیا دارایی تهدیدشده سایبری از قابلیت مانور و چرخش مناسب در تحول سریع و مناسب در زمان حمله برخوردار است و می‌تواند شرایط مدیریت تهدید را برای خود فراهم آورد؟

مؤلفه بعدی در ارزیابی تهدید، پیامد تهدید سایبری است که نتیجه یک رویداد یا موقعیت است و به‌صورت کیفی، کمی، آسیب یا ضرر بیان می‌شود و با شاخص‌های ذیل قابل اندازه‌گیری است (علمداری، ۱۳۹۱: ۱۱۳):

ـ عمق تهدید: عمق تهدید به میزان نفوذ آن در لایه‌های درونی زیرساخت یا دارایی سایبری بستگی دارد.

ـ شدت تهدید: به میزان آثار تخریبی آن تهدید بر زیرساخت‌ها و دارایی سایبری بستگی دارد.

ـ گستره تهدید: پوشش محیطی تهدید را مد نظر قرار می‌دهد. هر قدر محیط اعمال تهدید سایبری وسیع‌تر باشد، تهدید گستردگی بیشتری دارد.

واکنش به تهدیدات سایبری

سومین بُعد از مدل مفهومی اشاره به تصمیم‌گیری درباره نحوه برخورد با تهدید سایبری و پیگیری مستمر این تهدیدات دارد. پُرواضح است واکنشی که در این سطح از مدل مفهومی پایش تهدیدات سایبری مد نظر است با واکنشی که در مدیریت حملات سایبری شامل بازیابی، پاسخ حمله و... است، متفاوت باشد.

مؤلفه‌های این بعد عبارت‌اند از: اعلان و اقدام.

اعلان: مجموعه فعالیت‌هایی را گویند که به حوزه اعلام مربوط می‌شوند. شاخص‌های اعلان عبارت‌اند از:

ـ اطلاع‌رسانی: اطلاع‌رسانی به نهادها و سلسله‌مراتب ذی‌ربط درخصوص تهدید سایبری کشف‌شده.

ـ اعلام وضعیت: هشداردهی و سطح‌بندی تهدید سایبری با مشخص‌نمودن سه وضعیت بحرانی و مخاطره‌انگیز و هشدار.

ـ وضعیت بحرانی: وضعیتی که بر اثر وقوع تهدیدات سایبری تمامیت آن دارایی مورد هدف باشد و تهدیدگر نیز تمایل و توانمندی مناسب برای چنین هدفی داشته باشد.

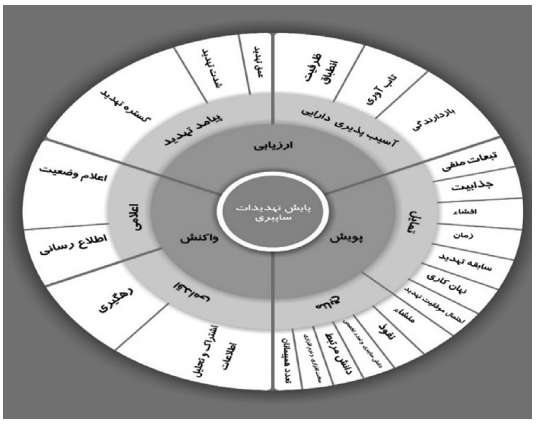
ـ وضعیت مخاطره‌انگیز: وضعیتی که تأثیر جدی بر سطوح عملیاتی و تاکتیکی دارایی سایبری گذاشته و هسته مرکزی تداوم چرخه خدمات در آن زیرساخت مورد هدف قرار گرفته شده باشد.

ـ وضعیت هشدار: وضعیتی که در صورت وقوع تهدید سایبری، اختلال در تداوم تولید و چرخه خدمات در دارایی مورد هدف در گستره محدودی از محیط است (سازمان پدافند غیر عامل، ۱۳۹۱).

اقدام: مجموعه فعالیت مرتبط با پیگیری تهدید که با شاخص‌های ذیل تبیین می‌گردد:

ـ ره‌گیری:[1] ردیابی پیوسته تهدید سایبریِ شناسایی و کشف‌شده است با امکان‌سنجی وقوع مجدد آن، به‌همراه به‌روزآمدکردن اطلاعات مربوطه.

ـ اشتراک و تحلیل اطلاعات تهدید: مبادله و تحلیل اطلاعات تهدید سایبری با دیگر نهادهای متولی پایش در زیرساخت‌های مرتبط.



شکل ۳: مدل مفهومی پایش تهدیدات سایبری

1.Tracking

تحلیل داده‌ها

آزمون الگو

در این پژوهش با استفاده از آزمون کولموگروف اسمیرنوف توزیع نرمال داده‌ها بررسی شد و به‌دلیل نرمال‌نبودن توزیع داده‌ها، روش حداقل مربعات جزئی[1] یا الگوسازی معادلات ساختاری مبتنی بر واریانس برای آزمون الگوی مفهومی پژوهش انتخاب شد. در روشPLS دو الگو آزمون می‌شود. الگوی اول، بیرونی یا الگوی اندازه‌گیری است که شامل سؤالات و متغیر مکنون مربوطه است. الگوی دوم، درونی یا الگوی ساختاری است که نشان‌دهنده متغیرهای مکنون و روابط میان آن‌هاست. شرط برقراری پایایی سازه این است که اندازه پایایی مرکب (CR) از ۰/۷ بزرگ‌تر و همچنین اندازه متوسط واریانس استخراج‌شده (AVE) از ۰/۵ بزرگ‌تر باشد (فورنل و لارکر،۱۹۸۱). برای بررسی ارتباط میان ابعاد، مؤلفه‌ها، شاخص‌ها و همچنین همبستگی آن‌ها، پرسشنامه بازطراحی شد و پس از آنالیز اطلاعات دریافتی از خبرگان، در نهایت پایایی سازه و پایایی مرکب به‌نحو خیلی خوب تأیید شد.

ملاک کلی برازش (GOF) [2] الگو را می‌توان با محاسبه میانگین هندسی میانگین اشتراک و R^2 به دست آورد.

$$GOF=\sqrt{AVRAGE(COMUNALITIE)}*R^2$$

$$GOF=\sqrt{0.75}*0.63=0.68$$

شاخص برازش در مدل PLS را می‌توان برای بررسی اعتبار یا کیفیت مدل PLS به‌صورت کلی استفاده کرد. این شاخص نیز همانند شاخص‌های برازش مدل لیزرل عمل می‌کند و بین صفر تا یک قرار دارد و مقادیر نزدیک به یک نشانگر کیفیت مناسب مدل هستند (Tenenhaus, 2004:740). مقدار (GOF) محاسبه‌شده برای مدل، نزدیک به مقدار ۰/۶۸ بود کـه بـر خـوبی برازش مدل برای داده‌ها دلالت دارد.

تحلیل الگو و نتیجه‌گیری

با توجه به اینکه الگو در کنار سادگی می‌بایست چارچوب کلی پایش را تبیین کند، این الگو بر اساس فرایند شش مرحله‌ای تعریف‌شده در موضوع پایش، خلاصه‌سازی شد و بر اساس ضرورت

1.Partial Least Squares
2.Good of Fitness

افرازبودن ابعاد، این سه بعد انتخاب شد. گفتنی است که به مراحل فرایند پایش، مانند ره‌گیری و آشکارسازی در این سه بعد اشاره شده است؛ به نحوی که بندهای آشکارسازی و تخمین‌زدن در بعد ارزیابی و بند ره‌گیری در بعد واکنش در نظر گرفته شده است. به هر حال، پس از انتخاب این سه بعد با خبرگان حوزه تهدیدات سایبری درخصوص ابعاد الگو مصاحبه شد و این ابعاد از سوی آن‌ها تأیید شد. در مرحله بعد یکسری کلمات کلیدی از ادبیات تحقیق، مبانی نظری، اسناد بالادستی و فرمایشات امام خامنه‌ای انتخاب شد و فراوانی آن‌ها در این مستندات به‌دست آمد که نتایج آن‌ها منجر به مشخص‌شدن مؤلفه‌ها و شاخص‌های الگو شد. تحلیل‌های آماری بالا نیز حاکی از ارتباط خیلی خوب میان ابعاد، مؤلفه‌ها و شاخص‌ها هستند.

با توجه به تعریفی که از سازمان تهدیدات در ادبیات پژوهش به‌عمل آمد، یک تهدید سایبری شامل سه مؤلفه عامل تهدید سایبری، حوزه تهدید سایبری و موضوع تهدید سایبری است؛ به‌عنوان مثال انجام حملات منع سرویس توزیع‌شده از سوی آمریکا در زیرساخت‌های اقتصادی مانند بانک‌ها. در این مثال، عامل تهدید آمریکا از طریق حملات DDOS (موضوع تهدید سایبری) به زیرساخت‌های اقتصادی (حوزه تهدید سایبری) حمله کرده است. با توجه به اینکه این پژوهش به‌دنبال یک الگوی راهبردی مرجع است، از بررسی حملات که غالباً جنبه تکنیکی دارند صرف‌نظر و به دو حوزه تهدیدگر و تهدیدشونده توجه شده است. این الگو برای شناخت حوزه تهدیدگر با دو مؤلفه منابع و تمایل و شاخص‌های مرتبط با آن، وضعیت دشمن را پایش نموده و با بررسی دو مؤلفه آسیب‌پذیری و پیامد تهدید سایبری و همچنین شاخص‌های آن به‌دنبال تبیین وضعیت خودی یا حوزه تهدید است.

ابعاد پایش تهدیدات سایبری ج.ا.ا چیست؟

بر مبنای الگوی به‌دست‌آمده، ابعاد پایش تهدیدات سایبری ج.ا.ا شامل پویش، ارزیابی و واکنش می‌شود. پویش اشاره به جمع‌آوری اطلاعات بر اساس مؤلفه‌ها و شاخص‌های وضعیت تهدیدگر سایبری (دشمن) دارد و ارزیابی نیز اشاره به جمع‌آوری اطلاعات بر اساس مؤلفه‌ها و شاخص‌های وضعیت تهدیدشونده (خودی) دارد. همچنین واکنش توجه به تصمیم‌گیری، اقدام مناسب و به‌موقع نسبت به تهدید کشف‌شده یا تهدیدی دارد که در آینده ظهور خواهد نمود. البته بدیهی است این واکنش از اقداماتی که در مدیریت حملات سایبری در پاسخ به حمله است، متفاوت است.

ضریب همبستگی میان متغیر مستقل پویش و متغیر وابسته پایش تهدیدات سایبری برابر ۰٫۶۸ است و این بدان معنی است که رابطه مثبت خوب میان این دو متغیر وجود دارد. به همین صورت است برای ارزیابی و پایش که ضریب همبستگی آن‌ها برابر ۰٫۶۹ است؛ یعنی رابطه مثبت خوب میان این دو متغیر نیز وجود دارد. در نهایت، ضریب همبستگی ۰٫۵۹ میان پایش تهدیدات سایبری با واکنش نیز نشان می‌دهد که رابطه مثبت و قابل قبولی میان این دو متغیر وجود دارد.

آنچه از ضریب همبستگی ابعاد الگو به دست می‌آید، حاکی از اولویت بُعدهای ارزیابی و پویش بر واکنش است. از سویی، اختلاف معناداری میان پویش و ارزیابی مشاهده نشد.

مؤلفه‌های پویش عبارت‌اند از: تمایل و منابع.

ضریب همبستگی تمایل و پویش برابر است با ۰٫۹۱ یعنی رابطه مثبت خیلی خوب میان این دو متغیر وجود دارد. از طرفی، ضریب همبستگی دو متغیر منابع و پویش نیز برابر ۰٫۵۶ است؛ یعنی رابطه مثبت قابل قبولی میان آن‌ها برقرار است.

مؤلفه‌های ارزیابی عبارت‌اند از: آسیب‌پذیری دارایی‌ها و پیامد تهدیدات.

ضریب همبستگی ارزیابی و آسیب‌پذیری دارایی‌ها برابر ۰٫۸۷ است؛ یعنی رابطه مثبت خیلی خوب میان این دو متغیر برقرار است. ضریب همبستگی ارزیابی و پیامد تهدیدات سایبری نیز برابر با ۰٫۶۱ است؛ یعنی رابطه خوب مثبت میان آن‌ها وجود دارد.

مؤلفه‌های واکنش عبارت‌اند از: اقدامی و اعلامی.

ضریب همبستگی دو متغیر واکنش و اقدام برابر با ۰٫۷۷ است؛ یعنی رابطه خوب مثبت میان آن دو وجود دارد. ضریب همبستگی واکنش و اعلام نیز برابر با ۰٫۶۹ است؛ به‌عبارت دیگر رابطه مثبت خوب میان دو متغیر واکنش و اعلام برقرار است.

شاخص‌های پایش تهدیدات سایبری ج.ا.ا چیست؟

شاخص‌های تمایل: تبعات منفی، جذابیت دارایی سایبری برای تهدیدگر، افشا، زمان، سابقه تهدید، نهان‌کاری و احتمال موفقیت تهدید از منظر دشمن.

شاخص‌های منابع: منشأ تهدید سایبری، امکان نفوذ و دسترسی، دانش سایبری و تعدد تخصص‌های آن، دانش مرتبط، تجهیزات سخت‌افزاری و نرم‌افزاری.

شاخص‌های اقدامی: اشتراک و تحلیل اطلاعات، ره‌گیری.

شاخص‌های اعلامی: اطلاع‌رسانی و اعلام وضعیت.

شاخص‌های پیامد تهدید: عمق تهدید، شدت تهدید و گستره تهدید.

شاخص‌های آسیب‌پذیری دارایی: بازدارندگی، تاب‌آوری و ظرفیت انطباق.

تحلیل رگرسیون

بر اساس معادلات رگرسیون به‌دست آمده، می‌توان گفت:

$$M=2.07+0.14V+0.13I+0.13R+0.17W+0.15P+0.13D$$

پایش تهدیدات سایبری[1] برابر است با عدد ثابت ۲,۰۷ به اضافه چهارده‌صدم آسیب‌پذیری[2]، به علاوه سیزده‌صدم پیامد تهدید سایبری[3] ،به علاوه سیزده‌صدم منابع[4]، به علاوه هفده‌صدم تمایل[5]،به‌علاوه پانزده‌صدم اقدام[6]، به علاوه سیزده‌صدم اعلام[7]. آنچه از این فرمول به دست می‌آید بالابودن ضریب تمایل دشمن برای انجام تهدید سایبری است که می‌بایست بر اساس شاخص‌های تمایل نسبت به کاهش آن راهبردهای لازم طراحی گردد.

پیشنهادها

با توجه به مدل مفهومی و فرمول ریاضی استخراج‌شده از آن، مؤلفه تمایل ضریب بیشتری از دیگر مؤلفه‌ها دارد. این بدین معنی است که در پایش تهدیدات سایبری توجه جدی به شاخص‌های آن اثربخشی پایش را مضاعف می‌کند.

مؤلفه «تمایل» ناظر به تحرکات سایبری دشمن است. از سویی «آسیب‌پذیری دارایی» و «پیامد تهدیدات» نیز ناظر به اقدامات طرف خودی (تهدیدشونده) است. شاخص‌های دو بعد پویش و ارزیابی به‌تنهایی نیز قابل فهم و تجزیه و تحلیل است و هر کدام هویت مستقل دارند. اما در نگاه کلان پایش تهدیدات سایبری باید یک رابطه دوسویه متأثر از هم در نظر گرفت. این دو رابطه

1.Monitoring
2.Vulnerability
3.Impact
4.Resource
5.Willingness
6.Performance
7.Declaration

تعاملی با یکدیگر داشته و با یکدیگر معنی کامل‌تری می‌یابند و در کنار هم بهتر فهمیده می‌شوند. به‌عبارتی، افزایش آسیب‌پذیری دارایی‌ها بر تمایل دشمن برای بهره‌برداری از تهدید تأثیر افزایشی خواهد داشت یا اینکه پیامدهای تهدید عنصر تأثیرگذاری در انجام یا عدم انجام تهدید خواهد بود.

با توجه به تأیید الگو، پیشنهاد می‌شود مدل عملیاتی این الگو به همراه راهبرد و برنامه‌های اقدام طراحی گردد.

با مقایسه وضعیت موجودِ پایش تهدیدات سایبری با الگوی طراحی‌شده، پیشنهاد می‌شود با ایجاد مراکز اشتراک و تحلیل اطلاعات به‌منظور افزایش توان پایش تهدیدات سایبری اقدام لازم صورت پذیرد.

نظر به نبود نظام پایش تهدیدات، پیشنهاد می‌شود در دو سطح نظامی و مدنی این نظام با مشارکت نهادهای متولی به‌همراه فرایندهای لازم طراحی گردد.

با توجه به مطالعات انجام‌شده در کشورهای پیشرو، فناوری‌های برهم‌زن[1] یکی از پیشران‌های تغییرات و زمینه‌های ایجاد تهدیدات آتی هستند که لازم است در این حوزه برای سرمایه‌گذاری کافی به‌منظور روندشناسی و بومی‌سازی این فناوری‌ها اقدامات لازم صورت گیرد.

با توجه به وضعیت نظام ج.ا.ا و تقابل دائمی آن با استکبار جهانی و نظام سلطه، تسریع در ایجاد و ارتقای شبکه ملی اطلاعات گوشزد می‌شود که منجر به افزایش ظرفیت تاب‌آوری و ظرفیت انطباق می‌شود.

1.Disruptive technology

منابع و مآخذ

الف) منابع فارسی

۱. افتخاری، اصغر، ۱۳۹۲، ***«برآورد تهدید»***؛ رویکردی نظام‌واره، دانشگاه عالی دفاع ملی.

۲. حمیصی، مرتضی، ۱۳۹۱، ***«الگوی راهبردی تأسیس و توسعه سازمان‌های مردم‌نهاد ایرانی با تأکید بر منافع امنیت ملی جمهوری اسلامی ایران»***، رساله دکتری، دانشگاه عالی دفاع ملی، دانشکده مدیریت راهبردی.

۳. جمعی از محققان، ۱۳۹۲، ***«بررسی فرصت‌ها و تهدیدهای شبکه‌های اجتماعی مجازی از منظر امنیت ملی و ارائه الگوی مناسب»***، دانشگاه عالی دفاع ملی.

۴. جمعی از محققان، ۱۳۹۵، ***«طراحی نظام دفاع سایبری ج.ا.ا»***، مطالعه گروهی دانشجویان دوره اول امنیت فضای سایبر، دانشگاه عالی دفاع ملی.

۵. جلالی، غلامرضا و محسن خواجوی، ۱۳۹۳، ***«بررسی تهدیدات و آسیب‌پذیری‌های سایبری در حوزه ارتباطات زیرساختی کشور»***، اجلاس ملی دفاع سایبری.

۶. خزایی، سعید، ۱۳۸۴، ***«دیده‌بانی»***؛ مبانی و مفاهیم، مرکز آینده‌پژوهی علوم و فناوری دفاعی.

۷. سازمان پدافند غیر عامل، ۱۳۹۱، ***«انواع تهدیدات و نحوه بررسی و ارزیابی آن‌ها»***.

۸. داوری، ع و رضازاده، آ، ۱۳۹۲، ***«مدل‌سازی معادلات ساختاری با نرم‌افزار PLS»***، تهران: جهاد دانشگاهی.

۹. عبدالله‌خانی، علی، ۱۳۸۶، ***«تهدیدات امنیت ملی»***، تهران: ابرار معاصر.

۱۰. عبدالله‌خانی، علی و پرویز حسینی، ۱۳۹۴، ***«سنجش تهدیدات سایبری»***، فصلنامه امنیت ملی، ش ۱۶.

۱۱. علمداری، شهرام، ۱۳۹۱، ***«روش‌های ارزیابی آسیب‌پذیری زیرساخت‌ها و مدیریت بحران»***، بوستان حمید.

۱۲. کرم‌نیا، رضا، ۱۳۹۱، ***«ارائه الگوی راهبردی دفاعی بر اساس اندیشه دفاعی حضرت امام خمینی»***، رساله دکتری، دانشگاه عالی دفاع ملی.

۱۳. محمدی، علی، ۱۳۹۱، ***«اصول و مبانی امنیت فضای سایبر»***، دانشگاه عالی دفاع ملی.

ب)منابع لاتین

1.Abdul Razzaq, Ali Hur, H Farooq Ahmad, Muddassar Masood,(2013) ،Cyber Security: Threats,Reasons, Challenges, Methodologies and State ofthe Art Solutions for Industrial Applications , National University of Sciences and Technology, Islamabad, Pakistan,

2.C. Simmons, S. Shiva, C. Ellis, D. Dasgupta, S. Roy, and Q. Wu, "AVOIDIT،2009، A Cyber Attack Taxonomy," Technical Report, University of Memphis.

3. David A. Powner (15 May 2017). "Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities". DIANE Publishing – via Google Books.

4.EE-ISAC,2017, The European threat landscape, accessible : http://www.ee-isac.eu/seminar

5.FACT SHEET,2015, Executive Order Promoting Private Sector Cybersecurity Information Sharing, The White House

6. J. Mirkovic and P. Reiher,2004،"A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM ،CCR

7. Frans Osinga,2006,Science, Strategy and War: The Strategic Theory of John Boyd Strategy and History Series

8. ITL BULLETIN,2017, CYBER-THREAT INTELLIGENCE AND INFORMATION SHARING, accessible : https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2017-05.pdf

9.Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2014. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), Sage: Thousand Oaks.

10.M. Kjaerland, 2005،"A Taxonomy and Comparison of Computer Secu-

rity Incidents from the Commercial and ‹Government Sectors," Computers and Security, Vol. 25,

11.Morana, Marco; UcedaVelez, Tony (2011). Application threat modeling. Oxford: Wiley-Blackwell. p. 37. ISBN 978-0-470-50096-5.

12.Matt Loeb, 2015, Cybersecurity Global Status Report ,acceissble : https://www.isaca.org/pages/cybersecurity-global-status-report.aspx

13.NIST,2016, Guide to Cyber Threat Information Sharing , National Institute of Standards and Technology

14.S. Hansman and R. Hunt,2005‹ "A Taxonomy of Network and Computer Attacks," Computer and Security.

MITRE, 2012, How Do You Assess Your Organization's Cyber Threat Level, The MITRE Corporation

15.Neo Park ,Won Hyung Park,(2012) Cyber Threat Prediction Model Using Security Monitoring System Event, Springer Netherlands

16.The MITRE Corporation, 2015, "Cyber Operations Rapid Assessment - Examining the State of Cybersecurity Assessment Methodologies and Introducing a New Alternative

17.Medina Llinás,2016, Identifying and combating cyber-threats in the field of online banking, Universitat Politècnica de Catalunya.

18.SHAW,2010, CYBERSPACE: WHAT SENIOR MILITARY LEADERS NEED TO KNOW accessible in ,http://handle.dtic.mil/100.2/ADA520146

19.Sandia, 2012, Cyber Threat Metrics, Sandia National Laboratories,Susana B. Adamo, 2013, State and Trends of the Environment, accessible in http://www.unep.org/geo/pdfs/geo5/geo5_report_c1.pdf

20.Sommestad , teodor , 2012, A framework and theory for cyber security

assessments, Industrial Information and Control Systems KTH, Royal Institute of Technology Stockholm, Sweden

21.Tenenhaus, M. Amato, S. Esposito Vinzi, V. 2004. A Global Goodness-Of-Fit Index for Pls Structural Equation Modeling. In Proceedings of the Xlii Sis Scientific Meeting, 739-742

22.USGAO,2010، United States Faces Challenges in Addressing Global Cybersecurity and Governance, United States Government Accountability Office.

23. Wendell Bell ,2008, Foundations of Futures Studies, Volume 1: Human Science for a New Era, transaction Publisher

24.William F. Pelgrin,2005, Cyber Security Awareness, MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER (MS-ISAC)

ج)تارنما

۱. امام خامنه‌ای، ۱۳۹۴، بیانات در دیدار دبیر و کارشناسان دبیرخانه شورای عالی امنیت ملی، قابل دسترس در: www.khamenei.ir

۲. امام خامنه‌ای، ۱۳۹۱، بیانات در دیدار علما و روحانیون استان خراسان شمالی، قابل دسترس در: www.khamenei.ir

۳. امام خامنه‌ای، ۱۳۹۴، حکم انتصاب اعضای جدید شورای عالی فضای مجازی، قابل دسترس در: www.khamenei.ir

۴. امام خامنه‌ای، ۱۳۹۰، حکم تشکیل شورای عالی فضای مجازی، قابل دسترس در: www. khamenei.ir

۵. امام خامنه‌ای،۱۳۹۰، ابلاغ سیاست‌های کلی برنامه ششم توسعه، قابل دسترس در: www. khamenei.ir_ امام خامنه‌ای، ۱۳۹۲، دیدار با رئیس‌جمهور و اعضای هیئت‌دولت، قابل دسترس در: www.khamenei.ir