Quarterly journal of strategic management attitude
Vol 1, No 4(4), winter2023
https://pmr.sndu.ac.ir

Type of Article: Reseach

Unknown threats and conceptual model of strategies to deal with them

Ebrahim Soltaninasab[1]

Received: 2023/12/14 **PP: 151-129** **Accepted:** 2023/10/24

Abstract

Extensive changes in today's world, in addition to providing opportunities for the individual and collective life of humanity, have created significant threats. The threats of the new world, which are more unknown than in the past, have wide-ranging effects and consequences on human social life. This has made the necessity of paying attention to them inevitable, and not paying attention to them endangers psychological and social stability and security and presents a future of unknowns and ambiguities. In this research, in order to conceptualize threats and unknown threats and strategies to deal with them, a descriptive method has been used. Using this approach, the nature of unknown threats and especially the strategy to deal with them are described in several steps. With the recognition of unknown threats and coping strategies, the model of the process of removing threats and dealing with unknown threats has been drawn as the conceptual model of this study. According to the research approach and model, in order to monitor continuous threats and deal with them, the following strategies are adopted and suggested: 1- having knowledge and awareness of the insider system, 2- discovering the attackers' behaviors and prioritizing threats under the title of "area of concern", 3- Discovering threats through the "Danger Discovery Center", 4- Identifying the source and destination of threats, 5- Preventing unknown threats using "Defense Game", "Smart Defense", "Moving Defense" and "Combating Combined Threats".

KeyWords: Unknown threats, threat recognition, threat detection.

Reference:
Soltaninasab, E. (2023). Unknown threats and conceptual model of strategies to deal with them. ***Strategic management attitude***, 1(4), 129-151.

[1] Ph.D. in future studies and Ph.D. in private law. Tehran. Iran. saeedsoltaninasab@gmail.com

فصلنامه نگرش مدیریت راهبردی
سال ۱/ شماره ۴(۴)/ زمستان ۱۴۰۲
https://pmr.sndu.ac.ir/

نوع مقاله: پژوهشی

تهدیدات ناشناخته و الگوی مفهومی راهبردهای مقابله با آنها

ابراهیم سلطانی‌نسب[1]

دریافت: ۱۴۰۲/۰۷/۰۲ صص: ۱۲۹-۱۵۱ پذیرش: ۱۴۰۲/۰۸/۲۳

چکیده

تحولات گسترده در جهان امروز، افزون‌بر آنکه فرصت‌هایی برای زیست فردی و جمعی بشریت فراهم ساخته است، زمینه‌ساز تهدیدات چشمگیری بوده است. تهدیدات دنیای جدید که بیش از گذشته دارای ماهیت ناشناختگی هستند، آثار و پیامدهای گسترده‌ای بر زندگی اجتماعی بشر دارند. همین امر ضرورت توجه به آنها را اجتناب‌ناپذیر ساخته است و عدم توجه به آنها، ثبات و امنیت روانی و اجتماعی را با مخاطره مواجهه می‌سازد و آینده‌ای از ناشناختگی‌ها و ابهامات را پیش‌روی انسان قرار می‌دهد. در این پژوهش به‌منظور مفهوم‌شناسی تهدید و تهدیدات ناشناخته و راهبردهای مقابله‌ای با آنها، از روش توصیفی استفاده شده است. با استفاده از این رویکرد، چیستی تهدیدات ناشناخته و به‌ویژه راهبرد مقابله با آنها در چند گام توصیف شده است. با شناخت تهدیدات ناشناخته و راهبردهای مقابله‌ای، الگوی فرایند دفع تهدید و مقابله با تهدیدات ناشناخته به‌عنوان الگوی مفهومی موردنظر این مطالعه ترسیم شده است. با توجه به رویکرد و الگوی پژوهش به‌منظور رصد تهدیدات مستمر و مقابله با آنها، راهبردهای ذیل اتخاذ و پیشنهاد می‌شود: ۱. داشتن دانش و آگاهی از سیستم خودی، ۲. کشف رفتارهای مهاجمان و اولویت‌بندی تهدیدات با عنوان «منطقه نگرانی»، ۳. کشف تهدیدات به واسطه «مرکز کشف خطر»، ۴. شناخت منبع و مقصد تهدیدات و ۵. پیشگیری از تهدیدات ناشناخته با استفاده از «بازی دفاع»، «دفاع هوشمند»، «دفاع متحرک» و «مقابله با ترکیبی شده تهدیدات».

کلیدواژه‌ها: تهدیدات ناشناخته، شناخت تهدید، کشف تهدید

استناددهی(APA): سلطانی نسب، ابراهیم (۱۴۰۲). تهدیدات ناشناخته و مدل مفهومی استراتژی‌های مقابله با آن‌ها. **فصلنامه نگرش مدیریت راهبردی**، ۱(۴)، ۱۲۹-۱۵۱.

[1] دکتری مطالعات آینده‌پژوهی و دکتری حقوق خصوصی. تهران. ایران. saeedsoltaninasab@gmail.com

مقدمه

بشر برای ادامه بقای خویش، همواره با تهدیدات فراوانی روبه رو بوده است. تعاریف متعدد و متکثری از تهدید ارائه شده است، اما درمجموع می‌توان گفت که تهدید وضعیتی است که در آن بخشی از ادراکات و تصورات انسان نسبت به پدیده‌ها و رابطه آنها با بقا، کمیت یا کیفیت ارزش مورد احترام، احساس خطر جدی یا نابودی را القا می‌کند. اغلب واکنش‌های انسان در طول تاریخ برای دفع خطرات و تهدیدات آشکار صورت می‌گرفته است، اما همواره تهدیدات پنهان و ناشناخته‌ای هم انسان‌ها را در معرض خطر قرار می دهند که عموماً آدمی از وجود آنها آگاه نیست، حال آنکه این تهدیدات وجود داشته، دارند و خواهند داشت. تهدیدات آشکار عموماً دارای اهداف، اجزاء و مراحل ایجاد، دامنه، سطوح و لایه‌ها و مصادیق گوناگونی می‌باشند، اما این ویژگی‌ها در تهدیدات ناشناخته کمی پیچیده‌تر هستند. براساس تعریف به‌دست‌آمده در این پژوهش، تهدیدات ناشناخته به تهدیداتی می‌گویند که هیچ علامت و امضای شناخته‌شده‌ای ندارد که بتوان آنها را شناسایی کرد. ازآنجایی‌که امروزه امکان خنثی‌سازی و فهم تهدیدات شناخته‌شده تا حدود زیادی تسهیل و فراهم شده است، شرایط برای ظهور تهدیدات ناشناخته بیش از گذشته مهیا شده است؛ با توجه به اثرگذاری تهدیدات ناشناخته، این مهم نقش برجسته‌ای در برنامه های راهبردی سیاسی، فرهنگی، نظامی و امنیتی دارد که مورد استقبال برنامه‌ریزان راهبردی نیز واقع شده است. برای مقابله با تهدیدات ناشناخته، مراحلی را با استفاده از سناریونویسی و مرور ادبیات مقالات و کتب مربوط به‌دست آورده‌ایم که به شرح ذیل در پژوهش کنونی پیشنهاد می‌کنیم: شناخت دارایی‌های سیستم، برآورد سطح تهدیدات، تعیین راهبرد دفاع، رصد و پایش تهدیدات ناشناخته، ایجاد شبکه کشف خطر و پیشگیری از تهدیدات ناشناخته با استفاده از روش‌هایی که در متن مقاله ارائه شده است. این پژوهش تلاش دارد بدواً بخش های حاکمیتی کشور را متوجه وجود تهدیدات ناشناخته کند و در مرحله بعد ضمن ارائه تعریف و دسته بندی از این تهدیدات، راه کار شناسایی و مقابله با آنها را پیشنهاد کند. به‌طور کلی پرسش‌های مشخصی که این پژوهش به دنبال پاسخگویی به آن می‌باشد، این است که ماهیت تهدیدات ناشناخته چیست؟ و راهبردهای مقابله‌ای با آنها کدام‌اند؟

مبانی نظری

بخش اول: ماهیت و مفهوم تهدید

تعریف تهدید:

تهدید در لغت به‌معنای ترساندن و بیم دادن است و در اصطلاح هر اقدام بالقوه که موجودیت و اهداف حیاتی سیستم را به خطر بیندازد (مرادیان، ۱۳۸۸). از نظر لرنر، هر چیزی که بتواند ثبات و امنیت سیستم را به خطر بیندازد، تهدید به‌شمار می‌رود. در برخی منابع امّا تهدید به‌معنای توانایی‌ها، نیّات و اقدامات دشمنان بالفعل و بالقوه برای جلوگیری از دستیابی سیستم به مقاصد امنیتی بیان شده است (عبداله‌خانی، ۱۳۸۹).

تعاریف دیگر از تهدید:

- به یک اعتبار تهدید، عنصر یا وضعیتی است که یکی از روش‌های حیاتی را به مخاطره می‌اندازد.
- تهدید، به مجموعه اقداماتی گفته می‌شود که اهداف و ارزش‌های حیاتی یک کشور را با هدف ایجاد تغییرات اساسی مورد هجوم قرار می‌دهد و غالباً نیز ریشهٔ خارجی دارد.
- تهدید، عبارت از توانایی‌ها، نیت‌ها و اقدامات دشمنان بالفعل و بالقوه داخلی و خارجی برای جلوگیری از دست‌یابی موفقیت‌آمیز خودی به علایق و مقاصد امنیت ملی به‌گونه‌ای است که دست‌یابی به این علایق، به خطر بیفتد (تاجیک، ۱۳۸۱).
- تهدید، به دیگر معنا یعنی نیّات، قابلیت‌ها و اقدامات بالفعل و بالقوه دشمنان که موجودیت یا اهداف و منافع حیاتی و ... دستاوردهای ... کشور را به خطر می‌اندازد یا عامدانه در مسیر تحقق آنها، مانع فیزیکی یا غیرفیزیکی جدی ایجاد کند (احمدیان، ۱۳۹۴).
- به‌عبارت دیگر تهدید، پدیده‌ای است که می‌تواند ثبات و امنیت را در یک کشور به خطر اندازد (مرادیان، ۱۳۸۹).
- بوزان و ویورالی، تهدید را هرگونه نشانه، حادثه یا شرایطی می‌دانند که توان ایجاد خسارت و ضرر علیه دارایی را داشته باشد (بوزان و ویورالی، ۱۳۸۶).
- تهدید، وضعیتی است که در آن مجموعه‌ای از ادراکات و تصورات انسان نسبت به پدیده‌ها و رابطه آنها با بقا، کمیت یا کیفیت ارزش مورد احترام، احساس خطر

جدی یا نابودی را القا می‌کند (ره‌پیک، ۱۳۸۷). البته درک چیزی به نام تهدید، درکی پسینی، زمینه‌ای و نسبی است. به‌عبارت دیگر شکل‌گیری تصوری که بیان‌کننده تهدید باشد، نیازمند به‌وجودآمدن تصوراتی مقدماتی است (کاظم‌پور و بهرامی، ۱۳۹۷).

اساساً تهدید، مفهومی انتزاعی است که درهم تنیدگی عمیقی با مفهوم امنیت ملّی دارد. بحث از امنیت و امنیت ملّی همراه با موضوع تهدید است و همچنین نمی‌توان سخن از تهدید به میان آورد، اما امنیت ملّی را نادیده گرفت. «باری بوزان» و «ویورالی» که از پایه‌گذاران مکتب کپنهاک هستند، با دیدگاه نئورئالیستی مفهوم امنیت را براساس گزاره تهدید - امنیت تبیین کرده‌اند، بدین معنا که امنیت را رهایی از تهدید معنا می‌کنند (احمدیان، ۱۳۹۴). اگرچه براساس گفتمان مثبت که جدیدتر از گفتمان مکتب نئورئالیستی است، امنیت و تهدید دو متغیر وابسته نیستند و هرکدام می‌توانند مستقل عمل کنند. براساس این تعریف جدید، فقدان امنیت تنها مرؤفه موردنیاز تهدید نیست، بلکه افزون‌بر آن، وجود شرایط مطلوب برای تحقق اهداف و خواسته‌های عوامل تهدید نیز مدنظر است.

هدف تهدید:

به‌طور کلی هدف هر نوع از تهدیدات، تأثیرگذاری بر عمل و اراده طرف مقابل است که با تهدید این تحمیل اراده به حریف صورت می‌پذیرد. اساساً اهداف تهدیدات یکی است و تفاوت آنها صرفاً در روش‌ها و ابزارهاست (هاشمی، ۱۳۹۰).

اجزاء و مراحل ایجاد تهدید:

هر تهدید از سه جزء تشکیل می‌شود: الف. کارگزار یا عامل تهدید، ب. حوزه تهدید و ج. موضوع تهدید (زروندی و یاری، ۱۳۹۶). به یک اعتبار، تهدید دارای دو مرحله است: مرحله **ذهنی** و مرحله **عملیاتی**. در مرحله ذهنی عامل تهدید بدواً به شناسایی نقاط آسیب‌پذیر جامعه هدف می‌پردازد و پس از بازتعریف اهداف و شناسایی ابزارهای موردنیاز، طرح حمله خویش را عملیاتی می‌کند.

انواع تهدید:

رایج‌ترین رویکرد در تقسیم‌بندی تهدید با توجه به حوزه‌ای که عامل تهدید در آن عمل می‌کند، به اشکال زیر قابل دسته‌بندی هستند: تهدیدات سیاسی، تهدیدات اقتصادی،

تهدیدات نظامی، تهدیدات اجتماعی و فرهنگی، تهدیدات زیست‌محیطی، تهدیدات فناورانه، سایبری و ترکیبی (زروندی و یاری، ۱۳۹۶).

دامنه تهدید:

منظور از دامنه تهدید، میزان شیوع یک تهدید از جنبه عاملی- ارزشی است. براساس این تعریف، دو اصل برای گستره تهدید شناسایی شده است:

- سطح ارزشی: در رابطه تهدیدآمیز، موضوعی وجود دارد که تهدید با توجه به آن معنا و مفهوم می‌یابد، براین‌اساس دامنه تهدید می‌تواند با توجه به موضوع تهدید مشخص شود.
- سطح عددی: منظور از دامنه تهدید در این سطح، تعداد بازیگران درگیر در تهدید است که بیشتر به‌عنوان یک شاخص اصلی از سوی برخی تحلیلگران به آن اشاره شده است (احدی و مرادیان، ۱۳۹۵).

سنجش تهدید:

مهم‌ترین موضوع پس از شناخت و گونه‌شناسی تهدید، سنجش تهدیدات است. طراحی نظام سنجشی تهدید می‌بایست براساس شاخص‌های متعدد کمی- کیفی باشد (گار، ۱۳۷۷). برای این منظور سازوکار سنجش دولایه‌ای وجود دارد که در دو سطح ظرفیت‌های بیرونی و درونی به بررسی میزان شدت تهدید می‌پردازد (افتخاری، ۱۳۸۵).

سطح اول: ظرفیت‌های بیرونی؛ شاخص‌هایی که بیشترین روایی را برای شناخت سنجش تهدیدات دارا هستند، عمق تهدید، دامنه تهدید، زمان تهدید، مکان تهدید، میزان قدرت عامل تهدید و موقعیت تهدیدات» هستند.

سطح دوم: ظرفیت‌های بیرونی؛ سنجش یک تهدید، ارتباطی مستقیم با توانمندی هر بازیگر دارد، به همین دلیل برای سنجش تهدیدات دو عامل «توان درون سیستمی و منافع سیستم» به‌عنوان شاخص اصلی بیان ظرفیت درونی بازیگر در نظر گرفته شده است (ساوه درودی، اسماعیلی و حیدری ۱۳۹۵). برخی نیز شاخص‌های سنجش تهدید را این‌گونه بیان نموده‌اند: عمق تهدید، منافع بنیادین، منافع مهم و منافع حاشیه‌ای (زروندی و یاری، ۱۳۹۶).

الگوی ارزیابی تهدیدات:

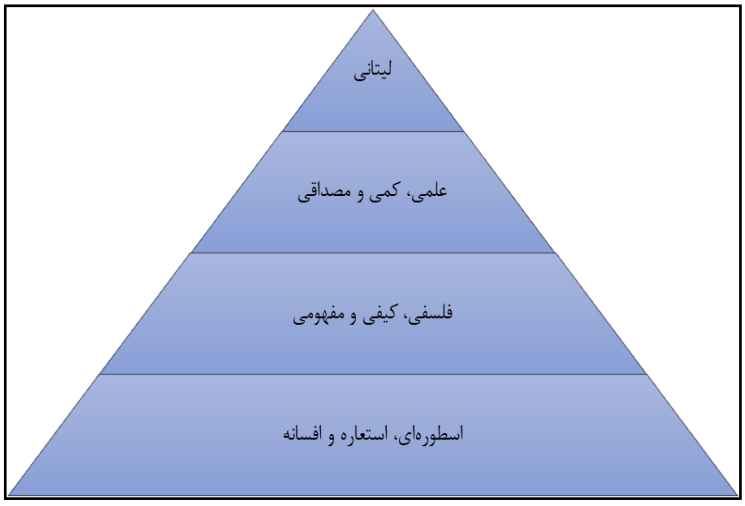
برای ارزیابی تهدید می‌توان از چند روش کلی استفاده کرد:

- شناسایی تهدید مبتنی‌بر اهداف مرجع؛
- ارزیابی تهدیدات از طریق طراحی سناریو؛
- ارزیابی تهدیدات و اولویت‌بندی تهدیدات شناسایی‌شده؛
- ارزیابی تهدیدات براساس اهداف مرجع و اولویت‌بندی تهدیدات؛
- ارزیابی تهدیدات به روش موازنه تهدید؛
- ارزیابی تهدید به روش سنجش تهدید؛
- روش ماتریس تحلیل و ارزیابی تهدیدات (کاظم‌پور و بهرامی، ۱۳۹۷).

لایه‌های تهدید:

پیش از این بیان شد که تهدید یک لایه ذهنی دارد و یک لایه عملیاتی که این دو می‌بایست با ساختار محیط درونی و محیط عملیاتی ارتباط ایجاد کنند تا به یک مسئله امنیتی تبدیل شود. اما اگر بخواهیم اندکی عمیق‌تر بنگریم، انگاره تهدید در مرحله ذهنی از یک ساختار و لایه‌های پیشینی تشکیل می‌شود که میزان موفقیت ما در از بین‌بردن تهدید به شناخت و تحلیل لایه‌های علل ایجاد این انگاره و ذهنیت، بستگی مستقیم دارد. برای شناخت و تحلیل لایه‌لایه علت‌های ایجاد مرحله ذهنی تهدید می‌توان از الگوی لایه‌لایه‌ای علت‌ها بهره جست.

تحلیل لایه‌لایه‌ای علت‌ها یکی از روش‌های آینده‌پژوهی است که سهیل عنایت‌الله، آینده‌پژوه پاکستانی، آن را ابداع و توسعه داده است. هدف از پیاده‌سازی تحلیل لایه‌لایه‌ای علت‌ها، شناخت پدیده‌های اجتماعی و رسیدن به درکی عمیق از لایه‌های زیرین مسائل و مشکلات است. پس از آشکار شدن لایه‌های مختلف پدیده‌ها، نوبت به تدوین و ارائه سناریوهای بدیل آینده می‌رسد. در تحلیل لایه‌لایه‌ای علت‌ها، حالت‌های مختلف دانستن اعم از علمی- تجربی، تفسیری- تأویلی و فلسفی- انتقادی، یکپارچه می‌شوند. ارزش و سودمندی این روش در پیش‌بینی بهتر و دقیق‌تر آینده نیست، بلکه با ایجاد فضاهای گذار، زمینه لازم را برای خلق آینده‌های بدیل فراهم می‌کند.



شکل ۱. هرم تحلیل لایه‌لایه‌ای علت‌ها

تحلیل لایه‌لایه‌ای علت‌ها از چهار سطح تشکیل می‌شود که عبارت‌اند از: لیتانی، علت‌های اجتماعی، جهان‌بینی و گفتمان مسلط و درنهایت اسطوره- استعاره.

- سطح اول، لیتانی نام دارد که در فرهنگ مسیحی به‌معنای مراسم دعا و مناجات دسته‌جمعی است. لیتانی، سطحی‌ترین لایه بوده و معرف دیدگاه رسمی و پذیرفته‌شده از واقعیت است.
- سطح دوم، سطح علت‌های اجتماعی و معرف دیدگاه نظام‌مند است. در این سطح، داده‌های سطح لیتانی توضیح داده شده و مورد سؤال قرار می‌گیرند.
- سطح سوم، نمایانگر جهان‌بینی و گفتمان است. در این سطح، فرض‌های استدلالی که بر بستر جهان‌بینی‌ها و ایدئولوژی‌ها قرار داشته و ناخودآگاه هستند، واکاوی می‌شوند.
- سطح چهارم، نشانگر اسطوره‌ها و استعاره‌هاست. این سطح درواقع معرف ابعاد انگیزشی ناخودآگاه موضوع است (مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، تحلیل لایه‌لایه‌ای علت‌ها).

اگرچه این روش در آینده‌پژوهی مورد استفاده قرار می‌گیرد، اما می‌توان تهدیدات را با تکیه بر این روش تحلیل کرده و علت ایجاد آنها را برای یافتن روش صحیح مقابله با تهدیدات پیدا کرد.

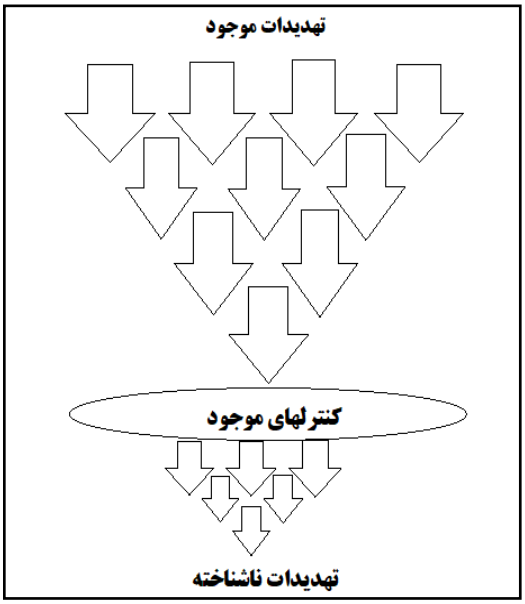
مصادیق تهدید:

آسیب، خطر و بحران (زروندی و یاری، ۱۳۹۶) که مواجهه با این مصادیق بـه شـناخت و توجه به سه جزء مهم ذیل بستگی دارد: نوع و جنس تهدید، زمان و غافلگیری (کـاظمی، ۱۳۸۹).

بخش دوم: تهدیدات ناشناخته

تعریف تهدیدات ناشناخته:

در تعریف تهدید ناشناخته باید گفت: «تهدید ناشناخته، تهدیدی است که هیچ علامت و امضای شناخته‌شده‌ای ندارد که بتوان آن را شناسایی کـرد». بـه دیگـر عبـارت «تهدیـد ناشناخته، تهدیدی است که توانسته (بتواند) از کنترل‌هـای امنیتـی موجـود در سیسـتم مورد آماج عبور کند، بدون اینکه هیچ یک از کنترل‌های امنیتی نشانه‌ای از وجود و وقوع آن را دریافت و اعلام نمایند». جـنس تهدیـدات ناشـناخته و بـازیگران آنهـا (بسـته بـه تهدیدات معمول)، پیچیده‌تر و فنـی‌تـر شـده اسـت. امـروزه تهدیـدات مـاهیّتی مرکّـب یافته‌اند.



شکل ۲. فرایند ایجاد تهدیدات ناشناخته

هدف تهدیدات ناشناخته:

هدف تهدیدات ناشناخته، «بقا، دارایی‌ها و ارزش‌های اساسی سیستم، فرد یا جامعه است». به‌طور کلی تهدید، عاملی ضدامنیّت به‌شمار می‌رود. تهدید عاملی نامطلوب است که می‌تواند خارج از کنترل و اراده ما عمل کند.

تقسیم‌بندی تهدیدات ناشناخته

الف. تهدیدات با منشأ فنّاوری که عبارت‌اند از: تهدیدات؛ سایبری، بیولوژیک، پرتوی و شیمیایی؛

ب. تهدیدات سخت و کالبدی؛

ج. تهدیدات انسان‌محور که عبارت‌اند از: تهدیدات؛ اقتصادی، فرهنگی- اجتماعی و امنیتی (سند راهبردی سازمان پدافند غیرعامل کشور).

با وجود تصور متداول که اغلب، تهدیدات را عاملی خارجی می‌دانند، امروزه لزوماً تهدیدات را به‌عنوان یک عامل خارجی نمی‌شناسند، بلکه در تحلیل ریشه‌های تهدیدات به داخلی یا درون‌سازمانی بودن تهدیدات توجه می‌شود.

سطح تهدیدات:

سطح تهدیدات دربرگیرنده حجم تهدیدات از کوچکترین جزء تا کلان‌ترین حجم آن می‌باشد که عبارت‌اند از: تهدیدات فردی، تهدیدات گروهی، تهدیدات ملّی، تهدیدات منطقه‌ای، تهدیدات بین‌المللی و تهدیدات جهانی (افتخاری، ۱۳۸۵).

ارکان و سازمان تهدیدات:

الف. عامل تهدیدات: که عبارت است از هویت، موجودیت یا موضوع خاص یا چیزی است که به‌طور بالفعل یا بالقوه توانایی ایجاد خطر یا پشتیبانی از تهدیدات را دارد.

ب. حوزه تهدیدات: عبارت است از هویت، موجودیت یا چیزی که موجودیت یا دارایی‌های حیاتی یا ارزش‌های آن در معرض خطر قرار گیرد.

موضوع تهدیدات:

وضعیت، پدیده، فعالیت یا رُخدادی است که به‌نظر می‌رسد قابلیت‌های درونی و بیرونی انتقال، پشتیبانی یا ایجاد خطر در موجودیت یا دارایی‌های حیاتی یا ارزش‌های بازیگر خود را مورد آماج قرار می‌دهد. راه‌کنش (تاکتیک)ها و تکنیک‌های تهدیدات ناشناخته جدید، با استفاده از فناوری‌های روز دنیا، از روش‌های بسیار پیشرفته و

سیستم‌های آفندی و کنترل و نظارت برخوردار هستند، به‌نحوی‌که توان پشت سر گذاردن آخرین فناوری‌های روز و نفوذ در آنها را دارا هستند.

باید دانست که مهمترین ویژگی تهدیدات ناشناخته، عدم شناخت ما نسبت به نوع، ابعاد، حجم، کیفیت و میزان اثرگذاری آنهاست. ما باید در تشخیص تهدیدات ناشناخته، ابتدا به بررسی نقاط ضعف خویش بپردازیم و نظام پیشگیری از تهدیدات را براساس نقاط ضعف خود طراحی نماییم. باید در تشخیص تهدیدات ناشناخته همیشه این اصل را مدنظر قرار دهیم که تهدیدات ناشناخته، دنباله‌ای از وقایع و رفتارهای همبسته است که در طی یک دوره زمانی اتفاق می‌افتد. «هیچگاه یک تهدید را نقطه‌ای و به‌طور دفعی نباید مورد بررسی قرار داد، بلکه سلسله علل و عوامل زمینه‌ای هستند که با استفاده از موقعیت زمانی و مکانی، امکان ایجاد تهدید را فراهم خواهند آورد».

سان تزو در کتاب هنر جنگ می‌نویسد: اگر خودتان و دشمن‌تان را بشناسید، از هیچ جنگی هراس به دل راه نمی‌دهید. اگر خودتان را بشناسید، ولی شناختی از دشمن خویش نداشته باشید، به‌ازای هر پیروزی که به‌دست می‌آورید، باید منتظر یک شکست سنگین باشید. امّا اگر نه خودتان و نه دشمنتان را نمی‌شناسید، در هر نبردی شکست سنگینی خواهید خورد.

برای شناخت تهدیدات ناشناخته، عناصری لازم است که در صورت وجود این عناصر می‌توان به رصد و شناخت تهدیدات مزبور پرداخت (صیادی، ۱۳۹۷).

الف. شناخت دارایی و ارزش‌هایی که با داشتن آن تهدید می‌شویم؛

- ما چه داریم که مورد تهدید قرار می‌گیریم؟
- آیا دارایی ما یک محصول یا یک فناوری است؟
- آیا ما برای داشتن یک ثروت طبیعی مورد تهدید واقع می‌شویم؟
- آیا ما به‌دلیل قرار داشتن در یک موقعیت خاص جغرافیایی تهدید می‌شویم؟
- آیا ما به خاطر یک مقام یا جایگاه ملّی، منطقه‌ای یا جهانی تهدید می‌شویم؟
- آیا ما برای هم‌پیمانی و همکاری با یک گروه یا کشور در جهان مورد هجمه و تهدید دشمنان هستیم؟

هر کدام از موارد یادشده می‌تواند دلیلی باشد که دارایی‌های ما از سوی دشمنان مورد حمله قرار بگیرد. برای مقابله با تهدیدات (شناسا یا غیر شناسا) شناخته یا ناشناخته،

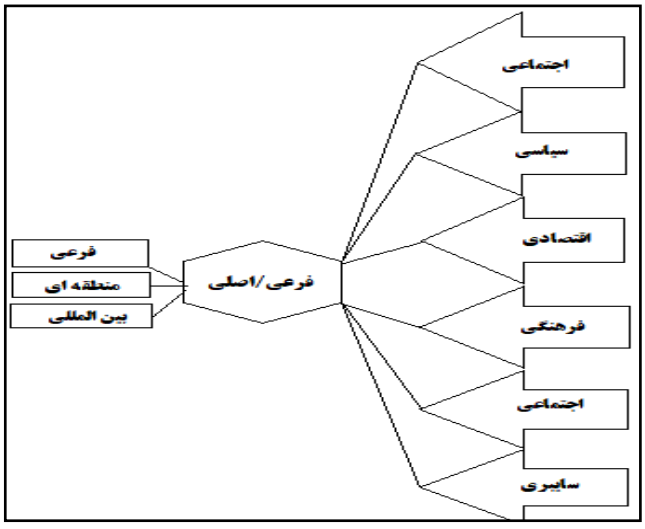
اولین چیزی که می‌بایست مورد بررسی قرار دهیم، علّت و منشأ ایجاد تهدید است و در این امر باید همه ابعاد و جوانب امر را مورد بررسی قرار داده و شناخت منشأ ایجاد تهدیدات را به‌طور کامل انجام دهیم و هیچ موردی را از قلم نیندازیم.

ب. برآورد سطح تهدیدات:

یکی دیگر از نکات مهم در شناخت تهدید، ترسیم کامل سطوح تهدید سازمان است. متناسب با اندازه و ابعاد سازمان می‌بایست شناسایی و ترسیم سطوح تهدید صورت پذیرد و همراستای با این شناسایی، پایش سطح تهدید از ضروریات می‌باشد. پایش و ترسیم سطوح تهدید به دو شکل صورت می‌گیرد:

اول. بُردارهای تهدید: همان شیوه‌ها و نقاطی هستند که محل تلاقی تهدیدات با ساختار درونی سازمان می‌باشند؛ ورودی‌های و خروجی‌های سازمان، نقاط حیاتی و راهبردی، تقاطع‌های کلیدی، نقاط ضعف، نقاط قوت و روش‌های جاری امور حیاتی و راهبردی.

دوم. حوزه‌ها و دامنه‌های عملیاتی سازمان: شیوه دیگر پایش و ترسیم سطوح تهدید، دسته‌بندی سطوح تهدید در قالب حوزه‌ها و دامنه‌های عملیاتی سازمان است.



شکل ۳. دسته‌بندی سطوح تهدیدات

هر یک از حوزه‌های یادشده را می‌توان پایش کرده و به ترسیم سطح‌بندی آنها پرداخت. هرقدر حوزه‌های عملیاتی وسیع‌تر باشد، سطوح تهدید بیشتری را می‌بایست پایش و ترسیم کرد.

- تعیین اولویت‌ها:

پس از شناخت دارایی‌ها و ارزش‌های سیستم و تعیین محل استقرار آنها و دسته‌بندی سطوح تهدید می‌بایست به اولویت‌گزینی ارزش‌ها و دارایی‌های در معرض تهدید بپردازیم و اولین نکته مهم و حائز اهمیت دراین‌خصوص این است که بدانیم در سامانه‌های موردنظر ما، چه اتفاقی در حال رُخدادن است، پس ضمن اتخاذ یک سیاست اجرایی برای اولویت‌گزینی، یک مرکز تعیین سطوح تهدید و تجمیع همه داده‌های به‌دست‌آمده در یک نقطه متمرکز، ایجاد کرده و سازمان و ساختار متناسب با انجام این مأموریت را تشکیل دهیم. این مرکز را می‌توان «مرکز شناسایی و شکار تهدیدات» نامید.

پیش‌بینی و تحلیل رفتار مهاجم:

هنگامی که ما بردارهای تهدید و حوزه‌ها و دامنه‌های آن را شناسایی کرده باشیم و سپس اولویت‌های اهداف نیروهای متخاصم را پیش‌گزینی کرده‌ایم، حالا نوبت به پیش‌بینی و تحلیل رفتار مهاجمان می‌رسد. با ترسیم الگوریتم رفتاری دشمن برمبنای تجربه‌های گذشته می‌توان نقشه‌های عملیاتی مهاجمان را بازخوانی کرد و با خواندن دست دشمن، او را به مسیر دلخواه خود هدایت کرد، به‌نحوی‌که پیکربندی زمین‌بازی با مدیریت و نظر ما صورت بپذیرد.

ترسیم سناریوهای بازی:

بازخوانی نقشه عملیات دشمن و به‌اصطلاح خواندن دست دشمن می‌تواند ما را در تعیین زمین و زمان بازی بسیار کمک نماید، افزون‌بر این ما خواهیم توانست که سناریوهای بازی را در زمین و زمانی که خودمان تعیین کرده‌ایم، پیاده کنیم، بدون اینکه دشمن و مهاجمان متوجه این موضوع باشند که آنها صرفاً یک بازیگر در سناریوهای القایی ما هستند.

بسته به نوع نگرش و هدف ما از اجرای کلان سناریوها، سناریوی بازی‌های میانی می‌تواند به روش‌های ذیل طراحی و اجرا شود:

- سناریوی بلک‌جک:

در این سناریو، هدف ما صرفاً حذف هدف با حداقل امکانات ضروری است.

- سناریوی معمّا:

ما در این سناریو عامل تهدید را درگیر حلّ معمّاهایی می‌نماییم که از پیش طراحی و پیاده کرده‌ایم. دشمن به گمان حلّ معمّاهای بزرگ درگیر آنها خواهد شد، بدون اینکه بداند بازیگر سناریوی معمّای ازپیش‌طراحی‌شدهٔ ماست.

- سناریوی روباه و شکارچی:

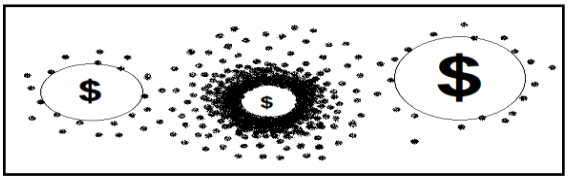
هدف از اجرای این سناریو، حذف مهاجم در محل استقرارش است، به‌طوری‌که با دنبال‌کردن عامل مهاجم و تهدید، او را در محل اختفا و استقرارش یا به قولی در لانه‌اش برای همیشه حذف نماییم.

- سناریوی بازی بی‌پایان:

بهترین روش برای مدیریت تهدیدات ناشناخته، تدوین و اجرای سناریوی بازی بی‌پایان است. ذهن‌خوانی از دشمن و شناخت قواعد بازی، ما را در تعیین زمان و مکان بازی، توانمند خواهد ساخت، آنگاه با پیش‌بینی رفتار مهاجم، او را به سناریویی بی‌پایان هدایت خواهیم کرد که با وجود بازی در زمین‌وزمان تعیین‌شده از سوی ما، هیچگاه متوجه نشود که در حال دویدن در یک گردونه است، امّا لازمه این امر اجرای شرایط ذیل است:

- تغییر زمان و مکان صحنه اجرای سناریو به‌دلخواه مهاجم؛
- تعیین بازیگران مخالف‌خوان، به‌نحوی‌که مهاجم به بازیگران صحنه بازی شکّ ننماید؛
- اعطای امتیازهایی در بازی بی‌پایان برای نگه‌داشتن حریف در زمین‌بازی به طمع امتیازات بیشتر؛
- تغییر متناوب سناریوهای بازی به‌نحوی‌که سناریوها همزمان با تغییر زمان و مکان و بازیگران تغییر کند و هر سناریوی جدید همبسته با سناریوهای پیشین باشد. توالی سناریوهای پی‌درپی، راز بازی بی‌پایان است.

«هنر اصلی ما در حفظ و بقای امنیت خود، پیش‌بینی بازی تهدید و طراحی سناریوهای مقابله با آنهاست»، درغیراین‌صورت، تفاوت ما با یک سیستم واکنش‌گرای منفعل، چه خواهد بود؟! یکی از راه‌های شناسایی تهدیدات ناشناخته، رفتارهای غیرعادی شبکه‌ای است که بر دارایی‌های مهم ما متمرکز شده است.



شکل ۴. تمرکز تهدیدات بر دارایی‌های مهم

روش تحقیق

در این مطالعه پژوهشگر با رویکردی توصیفی و تبیینی، ضمن صورت بندی مفهوم تهدید و تهدیدات ناشناخته، با ترسیم الگویی به ارائه مهم ترین راهبردهای مقابله با این تهدیدات پرداخته است. به‌منظور جمع‌آوری اطلاعات در این پژوهش، از روش کتابخانه‌ای استفاده شده است. تحقیق کتابخانه‌ای ، فرایندی منظم و گام‌به‌گام است که برای گردآوری اطلاعات مورد استفاده قرار می گیرد. در طول فرایند یک مطالعه کتابخانه‌ای، همواره لازم است که پژوهشگر به عمق برگردد و اطلاعات قبلی را دستکاری، تعدیل و بازنویسی کند. روش کتابخانه‌ای، یک فرایند گام‌به‌گام برای جمع‌آوری اطلاعات از منابع موجود است. برای به‌کارگیری روش کتابخانه‌ای در یک تحقیق، مراحل زیر را در نظر بگیرید.

۱- بررسی کلمات کلیدی و اصطلاحات پژوهش

پس از این که ایده اصلی مقاله مشخص شد، روی کلمات کلیدی و اصطلاحات تخصصی به‌کار رفته در آن ایده، متمرکز می‌شویم. سپس رابطه بین این کلمات کلیدی مشخص می‌شود. بدین منظور ابتدا مفهوم تهدید و تهدیدات ناشناخته و اجزای آن مفهوم‌پردازی شده است.

۲- جمع‌آوری و دریافت منابع معتبر علمی مرتبط با موضوع مقاله

مقالات و پژوهش‌های مرتبط با کلیدواژه‌ها را جمع‌آوری می‌کنیم و تلاش می‌شود منابعی را انتخاب کنیم که معتبر، اساسی و جدید باشند. سپس این منابع اطلاعاتی را با دقت مطالعه کرده و نکات مهم آن را با ذکر منبع یادداشت می کنیم. با توجه به بدیع بودن موضوع، تدوین پیشینه پژوهش با دشوارهایی روبه‌رو بوده است و مطالب ارائه‌شده در این زمینه پراکنده و متکثر می باشند؛ بدین منظور پژوهشگر با جمع آوری مطالب پراکنده برای ترسیم صورت‌بندی مفهوم تهدید و تهدیدات ناشناخته، اقدام به طبقه‌بندی آنها در یک چارچوب منطقی نموده است.

۳- یادداشت اطلاعات مربوط به مسئله تحقیق و پرسش پژوهش

یکی از مشکلاتی که در روش تحقیق کتابخانه ای وجود دارد، این است که پژوهشگر با خیل عظیمی از اطلاعات مواجه می‌شود. ازاین‌رو بسیار مهم است که او نخست منابع اطلاعاتی معتبر مانند مقالات علمی را انتخاب کند. سپس اطلاعاتی را که درراستای پرسش پژوهش است، باید برای نگارش مطالعه خود به کار گیرد و از مطالب غیرمرتبط چشم‌پوشی کند.

تحلیل اطلاعات:

در این مرحله، پژوهشگر داده‌های جمع‌آوری‌شده را با هم مقایسه و نتیجه‌گیری می‌کند. بدین ترتیب ابتدا اجزای تهدیدات ناشناخته، واکاوی شده و در ادامه نیز مهم‌ترین شیوه‌های مقابله با این تهدید به صورت الگوی مفهومی ترسیم شد.

مزیت روش پژوهش کتابخانه‌ای:

روش کتابخانه‌ای در قیاس با سایر روش‌های پژوهش، روشی کم‌هزینه است که زیاد به تخصص آنچنانی نیاز ندارد؛ معمولاً در نگارش بیشتر تحقیقات، از روش تحقیق کتابخانه‌ای در مرحله اول استفاده می‌شود. چراکه این روش، روشی سهل و ارزان بوده و می‌توان بیشتر اطلاعات اولیه را به‌راحتی با این روش جمع‌آوری کرد. ازاین‌رو روش پژوهش کتابخانه‌ای در پژوهش‌ها به‌کار گرفته می‌شود.

یافته‌های تحقیق

بخش سوم: راهبرد دفاع در تهدیدات ناشناخته:

اولین مرحله دفاع در برابر بازیگران تهدیدات ناشناخته، دانش و آگاهی کافی ما از سیستم خودی است، یعنی پیش از هر چیزی می‌بایست ما از همه ابعاد سیستم یا جامعه خود اعم از نقاط ضعف و قدرت و فرصت‌ها و تهدیدات مربوط به سیستم خود آگاه باشیم، به‌نحوی‌که هیچ نقطه تاریک و ابهام‌آمیزی درباره سیستم خودی، نزد ما وجود نداشته باشد.

سایر مراحل دفاع در برابر تهدیدات ناشناخته عبارت‌اند از:

۱. کشف رفتارهای مهاجمان

برای کشف رفتارهای ناهنجار مهاجمان تهدیدات ناشناخته در سیستم یا جامعه ما، صرفاً یک الگوریتم یا تکنیک واحد، چاره‌ساز نخواهد بود. بلکه مجموعه‌ای از الگوریتم‌ها و

تکنیک‌ها براساس رفتارهای نوظهور تهدیدات ناشناخته باید به‌کار گرفته شود. چراکه تهدیدات ناشناخته صرفاً از یک الگوی رفتاری ثابت تبعیت نمی‌کنند و سناریوهای متعدد همبسته را در تهاجم خویش به‌کار می‌گیرند، بنابراین دفاع در برابر تهدیدات ناشناخته نیز می‌بایست متحرک، پویا و متناسب با حمله و تهدید باشد که این امر نیازمند پیش‌بینی و تحلیل رفتار مهاجمان برای به‌دست‌آوردن الگوهای رفتاری تهدیدات ناشناخته می‌باشد.

پس از به‌دست‌آمدن الگوهای رفتاری عوامل تهدیدات ناشناخته باید نسبت به مشخص‌کردن اولویت مهمترین تهدیدات با همبستگی و توالی ترتیب آنها برای پیش‌بینی سناریوهای دفاع اقدام نماییم. با اولویت‌بندی تهدیدات مهم و مؤثر، آنها را با عنوان «**منطقه نگرانی**» طبقه‌بندی نماییم، سپس تحلیلگران با استفاده از نقشه‌برداری مبتنی‌بر وضعیت، اهمیت و زمان اجرای این تهدیدات، به بررسی مناطق نگرانی می‌پردازند تا افزون‌بر کسب بینش عمیق نسبت به این تهدیدات، اقدامات تجویزی مناسبی را انجام دهند. برای تبیین رفتارها یا واکنش‌های محیطی می‌بایست از منابع متمایز اطلاعات و داده‌ها استفاده نماییم، یعنی در تشخیص تهدیدات یا آفندها و پدافندهای اجرایی نباید از یک منبع داده و با یک روش به‌طور مداوم استفاده نماییم، چرا که بسیاری از مواقع، تهدیدات و حملات برای برآورد میزان، سطح و قدرت پاسخ سیستم دفاعی است تا براساس تکنیک‌های استخراج‌شده توسط هوش مصنوعی، فرایند یادگیری ماشین و توالی شناختی نسبت به طراحی برنامه‌های نفوذ در سیستم تدافعی اقدام کنند. در فرایند شناسایی تهدیدات، برای احراز هویت تهدید می‌بایست با استفاده و بهره‌گیری از دایرکتورهای فعال تحلیل و ارزیابی و ابرداده‌ها نسبت به شناسایی و ارزیابی کامل تهدید اقدام کرده و به‌دنبال یک نشانه از ظهور رفتارهای غیرعادی و غیرمنطبق با پروتکل‌های امنیتی باشیم.

۲. کشف تهدیدات

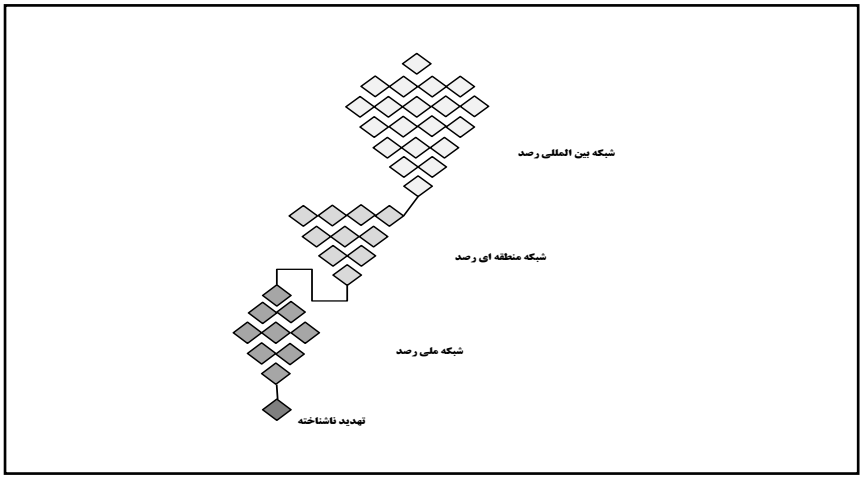
در یک دسته‌بندی برای کشف تهدیدات دو نوع رویکرد بیان شده است:

- رویکرد مقطعی (دوره‌ای) برای شناسایی تهدیدات کوتاه‌مدت مورد استفاده قرار می‌گیرد.
- رویکرد هویتی (ذاتی) که با بقای سیستم تداوم دارد، یعنی تا ما هستیم، مورد تهدید

هستیم (احمدیان، ۱۳۹۴).

با توجه به رویکردهای پیش‌گفته و به‌منظور رصد تهدیدات مستمر در همه سطوح، می‌توان با ایجاد مرکز شناسایی، تحلیل و ارزیابی تهدیدات به نام «**مرکز کشف خطر**»، همه داده‌های تولیدشده از سوی مراکز رصد و پایش ملّی و منطقه‌ای را در قالب یک شبکه به‌هم‌پیوسته، تحلیل کرده و دقت تشخیص تهدیدات ناشناخته را تقویت نمود. این مرکز به‌عنوان یک مرکز جمع‌آوری و رصد داده‌ها و اطلاعات، در امر پایش داده‌ها و اطلاعات و دفع تهدیدات ناشناخته باید شبکه‌محور باشد. در این صورت می‌بایست به طریق ذیل عمل نماید:

الف. شبکه رصد و پایش تهدیدات: در این بخش مرکز می‌بایست با طراحی یک شبکه جامع از جست‌وجوگرهای تهدیدات نسبت به جمع‌آوری داده‌ها و اطلاعات مربوط به تهدیدات ناشناخته به صورت شبکه‌ای عمل کند، یعنی هر یک از مراکز ورود و تولید داده‌ها و اطلاعات را در سطح کشور، منطقه و بین‌المللی در قالب یک شبکه جمع‌آوری و داده‌های سازمانی را تحلیل نموده و با استفاده از یک الگوریتم دقیق نسبت به جداسازی، طبقه‌بندی، درجه‌بندی، تحلیل و تشخیص تهدید اقدام نماید.



شکل ۵. شبکه رصد و پایش تهدیدات

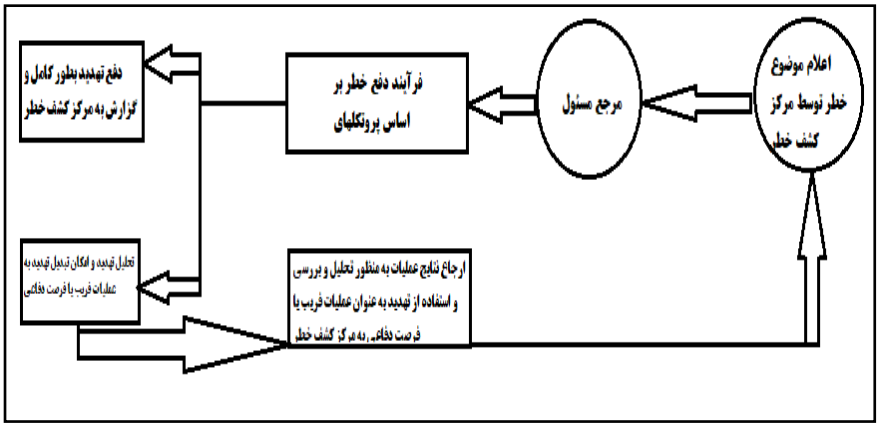
بر اساس این الگو، همه داده‌ها و اطلاعات در سطح بین‌المللی، منطقه‌ای و ملّی مورد بررسی، ارزیابی، طبقه‌بندی، درجه‌بندی و ارزیابی قرار می‌گیرند و پس از تحلیل و تشخیص آنها و تطابق با استانداردهای مربوط به تهدیدات ناشناخته و کشف نوع و

ارتباط آن عامل با مؤلفه‌های امنیتی کشور در هر یک از سطوح سه‌گانه یادشده، برای دفع این عامل تهدید براساس تدابیر ازپیش‌تعیین‌شده امنیتی و پروتکل‌های مربوط به دو صورت عمل می‌شود:

اول. براساس اختیارات مرکز کشف خطر به‌طور مستقیم با آن تهدید برخورد لازم صورت می‌پذیرد.

دوم. به دلیل شرایط تهدید موضوع، به مرجع تخصصی آن ارجاع و درخواست دفع تهدیدات از آن مرجع می‌شود.

ب. شبکه دفع تهدید: در این مرحله پس از رصد و پایش، شناسایی تهدیدات و تحلیل و ارزیابی خطر و نیز تشخیص نوع، میزان و درجه اهمیت آن به‌دلیل تخصصی‌بودن موضوع و تقسیم وظایف و مسئولیت‌های ازپیش‌تعیین‌شده، موضوع به یکی از مراجع مربوط ارجاع می‌شود.



شکل ۶. فرایند دفع تهدیدات

کشف خطر

برای به‌دست‌آوردن یک دید جامع درباره آنچه که در محیط رصد چه در سطح بین‌المللی و منطقه‌ای و چه در سطح ملّی اتفاق می‌افتد، در عین اینکه باید با بسط دید خویش در مرکز کشف خطر، داده‌های بسیار متعددی را جست‌وجو نماییم، اما می‌بایست به این پرسش پاسخ مناسب دهیم: اول. با چه ابزاری جست‌وجو می‌کنیم، دوم. به دنبال چه می‌گردیم و سوم. وقتی موضوع موردنظر را پیدا کردیم، می‌خواهیم با آن چکار کنیم. ازآنجاکه هدف عملیات عوامل تهدیدات ناشناخته، تضعیف و انهدام مبانی قدرت و

دارایی‌ها و ارزش‌های مهم ماست، بنابراین باید توجه کرد که گاهی اوقات بخشی از سیستم یا جامعه مورد حمله اینگونه تهدیدات قرار می‌گیرد، درحالی‌که ما برای آن بخش هیچگونه ارزشی قائل نیستیم و در ره‌نامه (دکترین) دفاعی ما هیچ جایگاهی ندارد. حال آنکه آن بخش یک قطعه از معمای (پازل) راهبرد آفندی دشمن است و ما از ارتباط آن بخش با دارایی‌های مهم خویش بی‌خبر یا غافل هستیم. این گونه دارایی‌ها و ارزش‌ها را می‌توان «دارایی‌ها و ارزش‌های واسط» نامید. یعنی شاید این دارایی سیستم رأساً فاقد ارزش قابل‌توجه و اهمیت راهبردی خواهند بود، اما به دلیل نقش کلیدی آنها در جغرافیای تهدیدات می‌بایست در ارزیابی طرح‌های دفاعی خویش این قبیل دارایی‌ها و ارزش‌ها را نیز مورد توجه ویژه قرار دهیم، چراکه دشمن هیچگاه نیروی خویش را صرف تضعیف یا از بین بردن دارایی‌های کم‌اهمیّت ما نمی‌کند، بلکه تلاش می‌کند با حداقل امکانات و بودجه، حداکثر ضربه را به ما و سیستم دفاعی ما وارد نماید، پس ارزش‌های به‌ظاهر کم‌اهمیّت از نظر ما، ممکن است نقاط راهبردی مورد توجه دشمن باشد، بنابراین هیچگاه نباید با دست‌کم‌گرفتن این نقاط و ارزش‌ها دچار خطای محاسباتی و راهبردیی شویم، چراکه درغیراین‌صورت می‌بایست منتظر تحمّل خسارت‌های جبران‌ناپذیری در حوزه امنیّتی باشیم. بررسی رفتارهای غیرمعمول تهدیدات ناشناخته می‌تواند یکی از راه‌های شناسایی نقاط راهبردی ما باشد، رصد رفتارهای غیرمعمول و بررسی رفتارشناسانه تحرکات دشمن، ما را در شناخت الگوریتم‌های رفتاری وی یاری می‌کند.

الگوریتم‌های رفتاری دشمن می‌تواند شامل داده‌ها و اطلاعات غیرمعمول بدون ساختار یا نیمه‌ساختاریافته باشد. این اطلاعات ممکن است شامل رفتارها، کاراکترها و پیام‌های معنایی، عددی و غیرعددی بوده و در صورت رصد دقیق و با وضوح بالا و درک روابط بین آنها، ما را به بسته‌های اطلاعاتی و جغرافیای تهدیدات بالقوه و بالفعل ناشناخته جهانی، منطقه‌ای و ملّی رهنمون کنند. نقشه‌برداری از الگوریتم عملیاتی رفتارهای عوامل تهدید می‌تواند صحت وقوع تهدیدات ناشناخته را برای ما روشن نماید. قطعاً جهان برای نیروهای کنشگرا، مملو از خطرات و تهدیدات شناخته و ناشناخته است و این امر ایجاب می‌کند که با استفاده از الگوریتم‌های عملیاتی موجود نسبت به مدیریت و رصد ترافیک رفتارها و عملیات‌های موجود بپردازیم تا نسبت به تمایز رفتارهای

مخاطره‌آمیز در مناطق خاص نگرانی و دارای خطر بالای امنیتی اقدام نموده و ضمن وزن‌دهی به آنها، زمینه‌های نگرانی درراستای ارتباط خطر با دارایی‌های سازمان را در اولویت قرار داده و نقشه رفتاری سناریوهای تهدید درحال‌وقوع را ترسیم نماییم. بنابر آنچه که گفته شد، «نقشه‌برداری از الگوریتم‌های عملیاتی رفتارهای مخاطره‌آمیز و مدیریت ترافیک تهدیدات»، امری ضروری به‌نظر می‌رسد.

هر تهدید، منشعب از خاستگاهی است که تحلیل لایه‌های علّی و معلولی آن برای شناخت ریشه‌ها و علل به‌وجود آمدن آن تهدید، بسیار ضروری است. تقریباً هیچ پدیده‌ای را نمی‌توان یافت که بدون ریشه‌ها و علل شناختی به‌وجود آمده باشد. برای تحلیل یک تهدید و شناسایی مؤلفه‌های غیرشناسا، حتماً می‌بایست ریشه‌های آن، مورد شناسایی و ارزیابی قرار گیرد. هرچند عامل به‌وجود آمدن تهدیدات، قصد دشمنان و رقبا برای به‌دست آوردن یا ازبین‌بردن دارایی‌ها و ارزش‌های سازمان ما می‌باشد، اما شناسایی ریشه‌ها و عوامل به‌وجود آورنده تهدیدات می‌تواند به نحوه برخورد ما با آن تهدیدات کمک شایانی نماید. شناسایی ریشه‌های عوامل تهدیدات را می‌توانیم «تبارشناسی تهدیدات ناشناخته» نیز بنامیم.

بزرگترین توانمندی یک سیستم هوشمند دفاعی پویا در برابر تهدیدات ناشناخته، «پیش‌بینی امکان وقوع تهدیدات شناسا و غیرشناسای آینده و کشف الگوهای ترکیبی تهدیدات متعدد» است.

۳. منبع و مقصد تهدیدات:

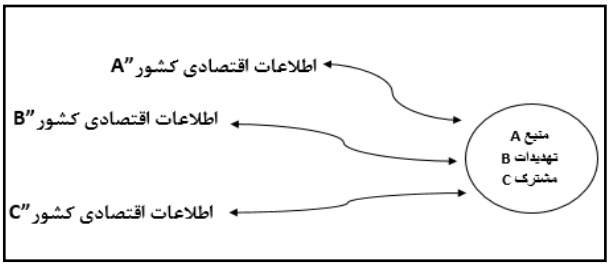
حسب موارد پیش‌گفته ممکن است که مهاجمان چه به صورت مشترک و هماهنگ و چه به صورت ناهماهنگ و غیرمشترک براساس وجوه ذیل به دارایی‌های با ارزش سازمان حمله‌ور شوند:

حالت اول: منبع تهدیدات غیرمشترک، مقصد تهدیدات غیرمشترک؛

در این حالت نیروهای تهدیدکننده، هر یک از مبداء و مسیری جداگانه بدون هماهنگی با یکدیگر به اهدافی غیرمشترک و متفاوت حمله‌ور شده و هر یک به شیوه خود به‌دنبال دستیابی به مقاصد خویش هستند. برای نمونه: کشور الف به دنبال دستیابی به اطلاعات اقتصادی کشور ب است. کشور ج به دنبال دستیابی به اطلاعات نظامی کشور د است. کشور پ به دنبال دستیابی به اطلاعات امنیتی کشور ح است.

حالت دوم: منبع تهدیدات مشترک، مقصد تهدیدات غیرمشترک؛

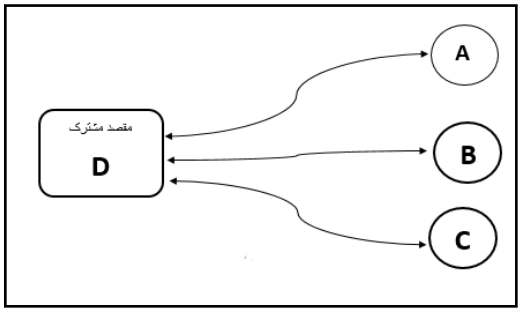
در این حالت نیروهای تهدیدکننده از یک مبداء و منبع، عملیات را آغاز می‌کنند امّا مقصد این تهدیدات غیرمشترک هستند.



ویژگی این نوع از تهدیدات این است که براساس یک نقشه و الگوی ازپیش‌طراحی‌شده از سوی یک منبع واحد متخاصم برای به‌دست‌آوردن اطلاعات حیاتی اهداف غیرمشترک یا ضربه زدن به دارایی‌ها و ارزش‌های اهداف متعدد، اقدام صورت می‌پذیرد. البته این تعدد اهداف به معنای پراکندگی هدف عملیاتی نیست، بلکه این تعدد و تکثر می‌تواند در قالب یک کلان‌پروژه چندوجهی، طراحی و اجرا شده باشد.

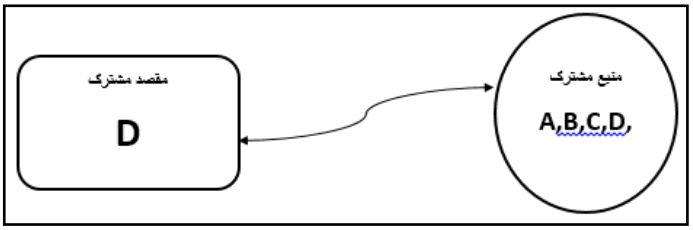
حالت سوم: منبع تهدیدات غیرمشترک، مقصد تهدیدات مشترک؛

در این شکل، نیروهای تهدیدکننده هر یک از مبداء و مسیری جداگانه و احیاناً بدون هماهنگی یکدیگر به یک هدف مشترک حمله‌ور شده و هر یک به شیوه خود به‌دنبال دستیابی به دارایی‌های حیاتی کشور یا سیستم هدف می‌باشند.

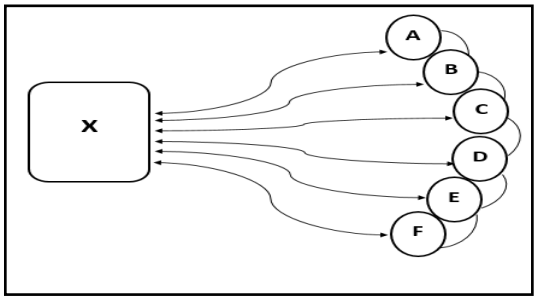


حالت چهارم: منبع تهدیدات مشترک، مقصد تهدیدات مشترک؛

در این شکل از حالات تهدید، با وجود تعدد منبع تهدیدات، به‌طور مشترک به یک هدف و مقصد مشترک حمله‌ور می‌شوند.



حالت پنجم: منبع تهدیدات غیرمشترک مرتبط، مقصد تهدیدات مشترک؛
در این صورت از حالات پیش‌گفته، اگرچه منبع تهدیدات غیرمشترک هستند، امّا با هماهنگی و ارتباط با هم و یک تقسیم‌کار، به یک مقصد مشترک حمله‌ور می‌شوند و ارزش‌ها و دارایی‌های با ارزش را مورد تهاجم قرار می‌دهند.



۴. پیشگیری از تهدیدات ناشناخته:

برای پیشگیری از تهدیدات ناشناخته می‌بایست ضمن روایتگری داستان تهدیدات آینده از قبل، با شناخت محیط درونی و بیرونی سازمان، همه سکانس‌های سناریوی مقابله با این تهدیدات را پیش‌طراحی و آماده نماییم. برای مقابله با هر تهدید ناشناخته باید یک سناریوی متفاوت و جداگانه طراحی کرد، زیرا اگرچه ممکن است در مقابله با تهدیدات متعدد بتوان از یک طرح یا راهبرد بهره برد، اما همیشه یادمان باشد که هر تهدید، دفاع مختص به خود را می‌طلبد، چراکه زمان و مکان دو مؤلفه تغییرپذیر هستند و تهدیدات در بستر این دو مؤلفه با شکل‌ها و چهره‌هایی متفاوت ظاهر می‌شوند. یک عامل تهدید در زمان و مکانی مشخص، چهره‌ای از خود نشان می‌دهد که همان عامل در زمان و مکانی دیگر چهره و عملکرد و شدت میزان تهدید و تخریبش متفاوت با چهره قبلی اوست!

- **بازی دفاع**[۱]

برای دفاع مؤثر در برابر تهدیدات می‌بایست سناریوهای متعدد دفاع را از پیش طراحی کرده و در یک «**بازی دفاع**» نسبت به کارایی سناریوهای ازپیش‌طراحی‌شده اطمینان حاصل کرد. بدین ترتیب که با ارزیابی و پیش‌بینی رفتار تهدیدات آتی یا گروه‌های مظنون به تهدید و تحلیل آنها به یک پیش‌بینی نسبی از توان تخریب عوامل تهدید دست می‌یابیم، سپس با قراردادن مختصات این توان تخریب در بازی دفاع، میزان و قدرت هماوردی توان دفاعی سیستم را در برابر تهدید می‌سنجیم. این عملیات می‌تواند به برآورد توان دفاعی ما در برابر تهدیدات ناشناخته کمک شایانی کند. درحقیقت بازی دفاع، روشی برای جلوگیری از غافلگیری راهبردی است.

- **دفاع هوشمند**[۲]

مزیّت یک سیستم آماده در برابر تهدیدات شناسا و غیرشناسا، هوشمندی سامانه تشخیص، تفکیک، اطلاع‌رسانی و دفع حملات عوامل تهدید است. «دفاع هوشمند» یک تکنیک روزآمد در صحنه هماوردی سیستم با تهدیدات است که به دفع بهینه خطر از مجموعه خودی خواهد پرداخت. لازمه ایجاد سامانه دفاع هوشمند؛

- شناخت و ارزیابی دقیق از توان دشمن و تهدیدات آن؛
- یکپارچگی سیستم شناسایی، تحلیل، اطلاع‌رسانی و دفاع؛
- درست‌اندازگی سیستم و استفاده بهینه از حداقل فرایندها با بازدهی حداکثری؛
- چابکی سیستم هوشمند در دفع خطر، به‌نحوی که از مرحله پیش‌بینی تا دفع خطر و ارزیابی توان تهدیدات، کمترین زمان و توان ممکن صرف شود.
- کوتاه بودن سطوح تصمیم‌گیری تا اجرا، اگرچه ممکن است یک ویژگی در درست‌اندازگی پیش‌بینی شود، اما همگی به این نکته واقفیم که نقش تصمیم‌گیری نیروی انسانی و مدیران آنقدر بسزاست که می‌تواند همه معادلات را به‌هم بزند، بنابراین به‌نظر می‌رسد که نقش سطوح تصمیم‌گیری در مدیریت دفاع، صرف‌نظر از به‌کارگیری سیستم هوشمند دفاعی، بسیار حائز اهمیت است.

---

۱. Defense game
۲. Smart defense

- **دفاع متحرک**[1]

«دفاع متحرک» درحقیقت به‌معنای گشودن جبهه‌های جدید در مقابل تهدیدات است، به‌گونه‌ای که نیروی متخاصم وقتی حمله را آغاز می‌کند، با واکنشی روبه‌رو شود که مجبور به عقب‌نشینی گردد، یعنی اگر دشمن اقدام به حمله در یک جبهه نمود، برای وادار نمودن دشمن به بازگشت باید ما در چندین جغرافیای امنیتی دیگر علیه او جبهه‌های جدید باز کنیم تا در محاسبات عملیاتی خود به این نتیجه برسد که بهتر است هرچه سریع‌تر از حملات خویش دست بردارد. این راهبرد اگرچه در نظر اول شباهت‌هایی به راهبرد ضربه متقابل دارد، اما در عمل و راهبرد، تفاوت‌های فراوانی با آن دارد، ازجمله اینکه دفاع متحرک بر پایه بازدارندگی طرح‌ریزی شده است.

- **ترکیب تهدیدات**

یکی از اهداف بسیار مهم و اصلی سناریوهای دفاعی، مقابله با تهدیدات ناشناخته، جلوگیری از پیوند منابع تهدیدات در خارج از حیطه نفوذ سیستم و نیز جلوگیری از همگرایی آنهاست. چراکه هر یک از تهدیدات ناشناخته به صورت ذاتی قابل رصد، مقابله و اطفا هستند، اما هنگامی که این تهدیدات پیش از ورود به محیط عملیاتی هدف، با هم ترکیب شوند، قابلیت و توان تخریب آنها به صورت تصاعدی بالا خواهد رفت. ممکن است عوامل تهدید در شرایط غیرمتعارف در ترکیب و پیوند با یکدیگر به عاملی ناشناخته‌تر و مخرب‌تر تبدیل شوند که در آن صورت امکان مهار آن با روش‌های معمول به‌هیچ‌وجه امکان‌پذیر نباشد؛ بنابراین بهترین راهبرد ما در برابر این موضوع، جلوگیری از ترکیب تهدیدات و مهار قدم‌به‌قدم هر یک از آنها به صورت انفرادی است.

باتوجه‌به تجربه و رفتارشناسی تهدیدات موجود در عرصه تنازعات، ممکن است تهدیدات ناشناخته با یکی از حالت‌های ذیل ترکیب شوند؛

الف. ترکیب همگن:

عبارت‌اند از تهدیداتی که از یک نوع و یک جنس و با کارکرد همسو هستند، برای نمونه: خسارت‌های نظامی= تهدید نظامی ۳ + تهدید نظامی ۲ + تهدید نظامی ۱

ب. ترکیب غیرهمگن:

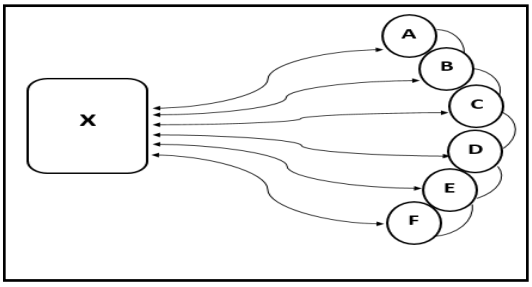
عبارت‌اند از ترکیب تهدیدات غیر هم‌جنسی که با توجه به نوع زیانی که به سیستم وارد

[1]. Animated defense

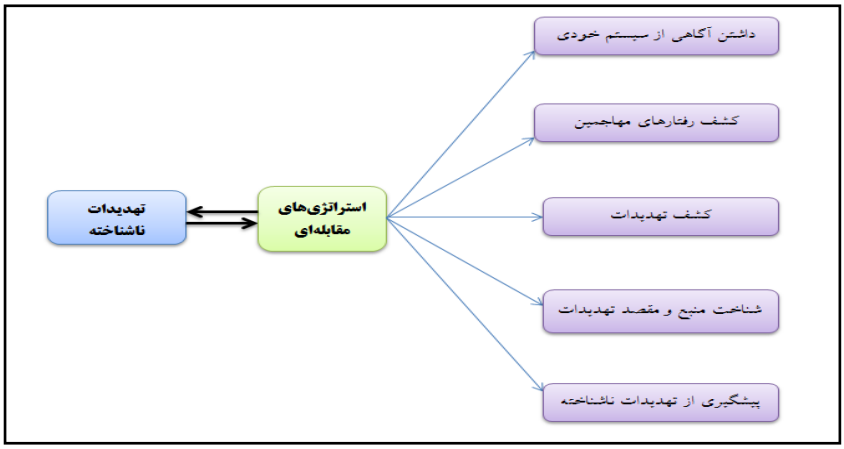
می‌نمایند و تقارن یا توالی زمانی آن، موجب تکمیل‌شدن حملات و خسارات سایر عوامل تهدید به سیستم می‌شوند، مثلاً؛

فروپاشی = تهدید اقتصادی + تهدید نظامی + براندازی از طریق جنبش‌های مدنی + تهدید بیولوژیک

همان‌گونه که در الگوی پنجم از تهدیدات ناشناخته گفته شد، «منبع تهدیدات غیرمشترک مرتبط، مقصد تهدیدات مشترک»، در این حالت اگرچه منبع تهدیدات، غیرمشترک و از هم جدا هستند، اما با هم مرتبط بوده و به تبادل اطلاعات با یکدیگر می‌پردازند که این امر خطرات فراوانی را برای سیستم ما فراهم می‌آورد، به این صورت که عوامل تهدیدکننده از طریق ارتباط با یکدیگر، نقاط ضعف خود را در هنگام حمله به منافع حیاتی ما جبران می‌نمایند!



با توجه به موارد پیش‌گفته و شناخت نوع و ترکیب تهدیدات، به الگویی از راهرد مقابله با تهدیدات ناشناخته «الگوی مفهومی راهبردهای مقابله با تهدیدات ناشناخته» دست می‌یابیم که با الهام گرفتن از آن می‌توانیم به ترسیم نقشه‌راه دفاعی در برابر تهدیدات ناشناخته دست یابیم. هر چند این الگو تنها یک پیش‌نمونه از الگوهای دفاعی در این زمینه است، اما در آینده با تکمیل این الگو به نمونه‌های پیشرفته‌تری از راهبردهای شناسایی و مقابله با تهدیدات ناشناخته، دست خواهیم یافت.



شکل ۷. الگوی مفهومی راهبردهای مقابله با تهدیدات ناشناخته

بحث و نتیجه‌گیری

مطالعه کنونی ضمن تبیین و مفهوم سازی تهدیدات ناشناخته، مهم‌ترین راهبردهای مقابله با این تهدیدات را در قالب یک الگوی مفهومی ترسیم نموده است. هنر ما در مدیریت این نوع از تهدیدات، کشف رابطه‌های پنهان تهدیدات و شناسایی همبستگی‌های عملیاتی بین آنهاست که این امر می‌تواند ما را به شاهراه اطلاعات تبادلی بین عوامل تهدید برساند. البته این موضوع در صورتی محقق می شود که ما از طریق کنترل و مدیریت محیط های عملیاتی بتوانیم عوامل تهدیدزا را در تور امنیتی خویش وارد نموده و با الگوی بازی بی‌پایان، آنها را در منطقه رصد و تحلیل نماییم.

یک بازی دومینو، هنگامی به نتیجه می رسد که همه مهره های بازی در محیط عملیاتی خویش به‌طور زنجیره‌ای تعیین موقعیت شده باشند. چرا که درغیراین‌صورت و با قطع شدن زنجیره سقوط، امکان ادامه حرکت مهره های بازی دومینو وجود نخواهد داشت. در بازی با عوامل تهدیدات ناشناخته، کافی است فقط یک مهره کلیدی را جابه جا کنیم، در آن صورت است که؛

- از دستیابی دشمن به منابع ارزش و اطلاعات خود جلوگیری می‌نماییم؛
- مانع تکمیل پازل آفندی دشمن خواهیم شد؛
- می توانیم دشمن را در تور فریب خویش گرفتار کرده و سناریوهای دلخواه خویش را پیاده سازیم.

البته جابه‌جایی مهره کلیدی صرفاً به‌معنای انتقال مهره‌ها نیست، این امر می‌تواند با حذف یا تبخیر مهره‌های کلیدی محقق شود. با تغییر جوامع و فناوری‌های اطلاعات پایه، تهدیدات ناشناخته نیز به‌طرز چشمگیری دچار تحول شده‌اند. ویژگی این نوع از تهدیدات، خاموش بودن و ناشناخته بودن آنهاست. شاید یک‌روند عادی یا محصول تکنولوژیکال که سال‌ها مورد استفاده مردم قرار می‌گرفته، درحقیقت یک تهدید ناشناخته بوده است، اما هیچ‌کس به ماهیت تهدیدزای آن پی نبرده و سال‌ها به‌عنوان یک عامل خودی و سفید در جامعه وجود داشته است!

تهدید ناشناخته لزوماً صورت تهاجمی ندارد. ابزارهای امنیتی موجود که ناظر بر محیط‌های پیرامونی و درونی ما هستند، صرفاً می‌توانند به شناسایی و دفع بخشی از تهدیدات بپردازند که ابزار، فناوری و تواناییشناخت آنها را داشته باشند. تنها راه دفع کامل تهدیدات ناشناخته جدید، شناخت دقیق محیط خودی برای امکان تشخیص تهدیدات ناشناخته از رفتارهای عادی و روزمره شبکه است. تنها در این صورت است که می‌توان عملیات مهاجمان ناشناخته را پیش از ورود به رینگ امنیتی دارایی‌های ارزشمند خود، شناسایی و خنثی کرده و به عنوان مدخلی برای ورود به سیستم مهاجمان از آن استفاده کرد، چرا که؛

«سیاه‌چاله‌ها همواره دو محیط را به هم متصل می‌کنند، فضای کیهان ما به فضای پشت سیاه‌چاله و فضای پشت سیاه‌چاله به فضای کیهان ما».

منابع

احدی، محمد، و مرادیان، محسن(۱۳۹۵). سنجش و ارزیابی تهدیدهای کشورهای منطقه علیه ج. ا. ا با استفاده از الگوی مرکز مطالعات راهبردی آجا برای ارزیابی تهدید. فصلنامه راهبرد دفاعی، سال ۱۴، ش۵۶.

احمدیان، علی‌اکبر(۱۳۹۴). تهدیدشناسی از منظر رهبران انقلاب اسلامی ایران. مجله سیاست دفاعی، سال ۲۳، ش ۹۱، ۳۹-۹.

افتخاری، اصغر(۱۳۸۵). کالبدشکافی تهدیدات. تهران: مرکز مطالعات دفاعی و امنیت ملی، دانشگاه امام حسین (علیه‌السلام).

افتخاری،اصغر(۱۳۸۵). کالبدشکافی تهدید. تهران: دافوس سپاه پاسداران، مرکز مطالعات دفاعی و امنیت ملّی.

بوزان، باری، و ویورالی، دووبلد پاپ(۱۳۸۶). چارچوبی تازه برای تحلیل امنیت. ترجمه علیرضا طیب. تهران: پژوهشکده مطالعات راهبردی.
تاجیک، محمدرضا(۱۳۸۱). مقدمه بر استراتژی‌های امنیت ملی جمهوری اسلامی ایران. تهران: مرکز بررسی‌های استراتژیک ریاست جمهوری.
ره‌پیک، سیامک(۱۳۸۷). تهدیدات قدرت ملّی، مظاهر و نشانگان. تهران: انتشارات مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.
زروندی، مهدی، و یاری، مریم(۱۳۹۶). کالبدشکافی تهدیدات با تأکید بر مفهوم امنیت ملی. فصلنامه مدیریت و پژوهش دفاعی، سال ۱۶،ش ۸۵، ۱۴۴-۱۱۷.
ساوه درودی، مصطفی، اسماعیلی، مهدی، و حیدری، دانیال(۱۳۹۵). الگوی تهدیدشناسی از منظر مقام معظم رهبری. فصلنامه راهبرد دفاعی، سال ۱۴، ش ۵۴.
سند راهبردی سازمان پدافند غیر عامل کشور.
عبداله‌خانی، علی(۱۳۸۹). فرهنگ استراتژیک. تهران: مؤسسه فرهنگی ابرار معاصر.
عناصر شناخت یک تهدید، شکار تهدیدات و اطلاعات تهدید، ۵ عنصر اصلی در برنامه هوشمندی امنیت که برای شکار تهدید لازم دارید، مهدی صیادی، ۱۳۹۷/۸/۱، سایت hypersec.ir آخرین بازدید ۱۳۹۸/۱۲/۳.
کاظم‌پور، ذکریا، و بهرامی، محسن(۱۳۹۷). الگویابی تهدیدات هوشمند آینده به روش تحلیل کالبدی تهدید. فصلنامه آینده‌پژوهی دفاعی، سال ۳، ش ۱۰.
کاظم‌پور، ذکریا، و بهرامی، محسن(۱۳۹۷). الگویابی تهدیدات هوشمند آینده به روش تحلیل کالبدی تهدید. فصلنامه آینده‌پژوهی دفاعی، سال ۳، ش ۱۰.
کاظمی، سیدعلیاصغر(۱۳۸۹). مدیریت بحران‌های بین‌الملل، تهران: دفتر مطالعات سیاسی بین‌الملل.
گار، تد رابرت(۱۳۷۷). چرا انسان‌ها شورش می‌کنند. ترجمه علی مرشدی‌زاده. تهران: پژوهشکده مطالعات راهبردی.
مرادیان، محسن(۱۳۸۸). تهدیدات، اصول و مبانی. تهران: انتشارات شهید صیاد شیرازی.
مرادیان، محسن(۱۳۸۹). مبانی نظری امنیت. تهران: دانشکده علوم و فنون فارابی.
مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، تحلیل لایه‌لایه‌ای علت‌ها. نظریه و موردکاوی‌های یک روش‌شناسی یکپارچه و متحول‌ساز آینده‌پژوهی.
هاشمی، سیدحمید(۱۳۹۰). جنگ نرم در دنیای معاصر. تهران: دفتر مطالعات فرهنگی و برنامه‌ریزی وزارت علوم، تحقیقات و فناوری.