فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره اول، زمستان ۱۴۰۰، صفحات ۱۵۶-۱۲۹

اولویت‌سنجی و رتبه‌بندی تهدیدات پرتکرار سایبری با محوریت فرایند زنجیره مرگ

محسن آقایی[۱]، علی معینی[۲]، احمد کاظمی[۳]

تاریخ دریافت: ۱۴۰۰/۰۳/۱۸ **تاریخ پذیرش: ۱۴۰۰/۰۸/۲۹**

چکیده

روند رو به تزاید تهدیدات سایبری بر ضد دولت‌ها و جوامع، زیرساخت‌ها و سازمان‌ها به شکلی غیرقابل پیش‌بینی و با سرعتی سرسام‌آور ادامه دارد. برنامه‌ریزی برای دفاع در مقابل تهدیدات منجر به حملات سایبری از مواردی است که در برنامه‌های کلان امنیتی دولت‌ها جایگاه ویژه‌ای پیدا کرده است. اقدامات مناسب در شناخت و تحلیل رفتار و ترغیب به توجه در مورد این پدیده خاص در فضای سایبر که به نوعی نقض‌کننده اصول محرمانگی، جامعیت و دسترس‌پذیری اطلاعات است به شکلی قابل توجه در بازدارندگی، مقابله و تاب‌آوری سایبری اثرگذار است. بر اساس نیازمندی به تقویت اقدامات شناسایی تهدیدات سایبری، در این پژوهش با هدف تعیین اولویت و تعیین رتبه تهدیدات پرتکرار اعلام‌شده از سوی منابع معتبر جهانی و بین‌المللی و با روش وزن‌دهی ساده با محوریت حضور تهدیدات موصوف در زنجیره مرگ و با استفاده از روش‌های مرسوم در نظریه گراف، نتایج در قالب رتبه‌بندی و تصویرسازی به شکل گراف‌های منتج از به‌کارگیری نرم‌افزار گفی ارائه شده است. نتایج این پژوهش بیانگر این موضوع مهم است که «تهدیدات دخلی» در صدر تهدیداتی است که در زنجیره مرگ قرار دارند.

کلید واژه‌ها: تهدیدات سایبری، زنجیره مرگ، گراف، وزن‌دهی

۱. دانش‌آموخته دکتری مدیریت سیستم‌ها از دانشگاه تهران، دبیر و پژوهشگر ارشد گروه سایبر دانشگاه عالی دفاع ملی (نویسنده مسئول)aghaee@sndu.ac.ir

۲.استاد و عضو هیأت علمی دانشکده علوم مهندسی پردیس دانشکده‌های فنی دانشگاه تهران.

۳.عضو هیأت علمی دانشگاه سیستان‌وبلوچستان و دانشجوی دکتری مدیریت فناوری اطلاعات دانشگاه تهران.

مقدمه

تهدیدات و حملات سایبری ازجمله معضلات امنیتی همه کشورهای جهان در دو دهه اول قرن بیست‌ویکم بوده است. حملات سایبری دولت‌ها بر ضد یکدیگر شدت یافته و این مسئله به‌تدریج در اولویت راهبردهای امنیتی حکومت‌ها جای گرفته است. به باور بسیاری از تحلیلگران مسائل دفاعی، تلفات و خسارت‌های جنگ سایبری نه‌تنها کمتر از جنگ‌های کلاسیک نخواهد بود، بلکه ممکن است محدوده و ابعاد گسترده‌تری را در بربگیرد. مؤسسه پست نوت[1] در سال ۲۰۱۷ میلادی اعلام نمود؛ آثار مخرب تهدید سایبری منجر به حمله در سال ۲۰۱۵ میلادی به زیرساخت توزیع نیروی برق کشور اوکراین شد و قطع برق ۲۲۵.۰۰۰ مشترک تا چند ماه ادامه داشت (پست نوت، ۲۰۱۷). به گزارش سایت آی‌تی‌ایران[2] تهاجم سایبری فروردین ۱۳۹۷ منجر به اختلال در فعالیت برخی از مراکز داده، سرویس‌دهنده‌ها و تعداد زیادی از سایت‌های جمهوری اسلامی ایران و برخی کشورها طور هم‌زمان شد (آی‌تی‌ایران، ۱۳۹۷).

تهدیدات سایبری از جنبه‌های مختلفی مورد توجه هستند. جوزف ساموئل‌نای[3] نویسنده کتاب آینده قدرت، تأکید دارد «لایه اطلاعاتی فضای سایبر، از بازده فزاینده نسبت به مقیاس برخوردار و عرصه آن برای کنترل قانونی مشکل است. پس بهتر است از حوزه اطلاعاتی با هزینه‌های پایین، تهدید را بر ضد لایه فیزیکی با منابع کمیاب و گران اعمال نمود» (جوزف ساموئل نای،۲۰۱۰، ۲۲). برخی تهاجم‌های سایبری گسترده سال‌های اخیر بر ضد زیرساخت‌های حیاتی کشورها را می‌توان بر اساس این رویکرد در نظر گرفت. از طرفی دوگان[4] و میچالکسی[5] (۲۰۰۹)، نیز در پژوهشی چنین نتیجه‌گیری کرده‌اند که تحلیل و گونه‌شناسی تهدیدات سایبری زیرساخت‌های حیاتی مؤلفه کلیدی امنیت آن‌ها و پیش‌بینی، کنترل و رفع آثار این تهدیدات مستلزم درک صحیح آن‌ها است (دوگان‌ومیچالسکی،۲۰۰۹، ۱۲). در پژوهشی دیگر، آقایی و همکاران (۱۳۹۸)، چنین نتیجه‌گیری کرده‌اند که برای مدیریت و

1.POSTNOTE (Cyber Security of UK Infrastructure).
2.https://itiran.com
3.Joseph Nye.
4.David P. Duggan.
5.John T. Michalski.

کاهش آثار تهدیدات سایبری به‌عنوان یکی از پدیده‌های فناناپذیر فضای سایبر، ارتقای قدرت تصمیم‌سازی و تصمیم‌گیری، ایجاد و استمرار امنیت سایبری زیرساخت‌های حیاتی اطلاعاتی و ارتباطی ضروری است شناسایی تهدیدات سایبری در ابعاد مختلف برای مواجهه فعال و خردمندانه در شرایط قبل از وقوع، در زمان وقوع و بعد از وقوع انجام شود(آقایی و همکاران، ۱۳۹۸، ۳).

با توجه به موارد فوق و لزوم شناخت عمیق تهدیدات سایبری به روش‌های مختلف، قابلیت تفکر در عمق ماهیت تهدیدات، روش‌های حمله و برنامه‌ریزی برای دفاع سایبری فعال ازجمله اقداماتی است که می‌تواند توسعه تفکر مواجهه با این چالش فضای سایبر را شکل‌دهی کند. مطالعه وضعیت تهدیدات پرتکرار از سوی منابع رسمی و توجه به آن‌ها بر اساس استفاده در فرایندها و سناریوهای حملات سایبری، ضمن افزایش توجه به تهدیدات، کاهش هزینه‌ها در برنامه‌های دفاع سایبری را به همراه خواهد داشت. بر این اساس، شناخت تهدیدات سایبری، ضمن ارتقای دانش و آگاهی در این حوزه، عامل ارتقای قدرت تصمیمات راهبردی و امنیت سایبری زیرساخت‌های حیاتی نیز قلمداد می‌شود.

نظر به موارد فوق و در ارتباط با توسعه شناخت وضعیت تهدیدات سایبری، مسئله مورد نظر این پژوهش اولویت‌سنجی و رتبه‌بندی تهدیدات سایبری بر اساس نرخ حضور آن‌ها در سناریوهای مدون حملات سایبری است که یکی از معروف‌ترین روندهای مدون‌شده در این حوزه، فرایند زنجیره مرگ است. بر این اساس هدف اصلی پژوهش تعیین اولویت‌ها و رتبه تهدیدات سایبری پرتکرار اعلام‌شده از سوی منابع معتبر با محوریت میزان حضور در زنجیره مرگ است. اهداف فرعی این پژوهش در حوزه‌های سنجش وزن تهدیدات موصوف، تعیین اولویت آن‌ها و رتبه‌بندی تهدیدات با استفاده از روش وزن‌دهی ساده[1] و ارائه نتایج با به‌کارگیری فرایندها در نظریه گراف است.

این پژوهش از این نظر حائز اهمیت است که به اولویت و رتبه تهدیدات، میزان توجه و استفاده مهاجمان فضای سایبر، سناریوها و برنامه‌های این گروه در اجرای اقدامات

1.Simple Additive Weighting (SAW).

تهدیدآمیز با محوریت به‌کارگیری تهدید مورد نظر در فرایند زنجیره مرگ به‌عنوان یکی از سناریوهای مدون مهاجمان سایبری تا حد زیادی تمرکز دارد و به این ترتیب تدوین برنامه‌های دفاع سایبری با دوراندیشی بهتر و هزینه‌های کمتر انجام می‌شود. ضرورت انجام این پژوهش نیز از این نظر مورد توجه است که بدون توجه به وزن و میزان اثر تهدیدات سایبری اقدامات مربوط به ارتقای قدرت بازدارندگی، مقابله و تاب‌آوری سایبری را نمی‌توان به شکل برنامه‌ریزی‌شده به انجام رساند. نظر به موارد فوق مسئله اصلی این پژوهش تعیین ارتباط تهدیدات سایبری با میزان نقش‌آفرینی در مراحل زنجیره مرگ برای شناسایی بهتر و بیشتر آثار این تهدیدات در وقوع حملات سایبری است. بر این اساس؛ هدف اصلی پژوهش تعیین اولویت و تعیین رتبه تهدیدات با فرکانس زیاد فعالیت بر اساس حضور در سناریو زنجیره مرگ سایبری و سنجش وزن تهدیدات، اولویت‌سنجی و ارائه ارتباط تهدیدات سایبری در قالب گراف به‌عنوان اهداف فرعی پژوهش است.

بنابراین سؤال اصلی پژوهش این است که اولویت و رتبه تهدیدات پرتکرار سایبری در زنجیره مرگ چگونه است و سؤالات فرعی نیز بر این اساس هستند که:

۱. سنجش وزن تهدیدات سایبری با محوریت حضور در زنجیره مرگ به چه ترتیب است؟

۲. اولویت‌سنجی تهدیدات سایبری بر اساس حضور در مراحل زنجیره مرگ چگونه است؟

۳. بررسی تهدیدات سایبری در قالب گراف بر ارتقای قدرت دفاع سایبری چگونه است؟

ادبیات و مبانی نظری

مفهوم‌شناسی

«تهدید سایبری» در واژه‌نامه امنیت سایبری مشترک ایالات متحده و روسیه (۲۰۱٤) به‌عنوان «خطری با قابلیت برقراری ارتباط با آسیب‌پذیری سایبری برای فعال نمودن آن» تعریف شده است (واژه‌نامه امنیت سایبری مشترک ایالات متحده و روسیه، ۲۰۱٤، ۳۸). این مفهوم در سند

راهبردی پدافند سایبری جمهوری اسلامی ایران چنین آمده است: «هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به مأموریت‌ها، وظایف، تصویر دستگاه متولی، سرمایه ملی سایبری یا کارکنان دستگاه به‌واسطه سامانه اطلاعاتی، دسترسی غیرمجاز، تخریب (انهدام)، افشا، تغییر اطلاعات یا ممانعت از (ایجاد اختلال در) ارائه خدمت، معرف تهدید سایبری است» (سند راهبردی پدافند سایبری جمهوری اسلامی ایران، ۱۳۹٤، ۲٤). نظر به موارد ارائه‌شده، تعریف عملیاتی این متغیر «رویداد یا واقعه‌ای با قابلیت وارد نمودن ضربه به اهداف، عملکرد و کارکنان مرتبط با سرمایه ملی سایبری، با به‌کارگیری آسیب‌پذیری موجود از طریق دسترسی غیرمجاز، انهدام، افشا، تغییر اطلاعات یا ممانعت از ارائه خدمت» است.

«زنجیره مرگ»، زنجیره مرگ سایبری[1] که به‌عنوان «زنجیره کشتار نفوذ یا زنجیره کشتار سایبری» نیز از آن یاد می‌شود، مفهومی است که در ابتدا جهت شناسایی، آماده‌سازی در مقابل حملات و مقابله و از بین بردن آن‌ها در سال ۱۹۹۵ میلادی در شرکت ساخت تجهیزات نظامی و هوایی لاکهید مارتین به وجود آمد، اما رفته‌رفته و با گذشت زمان این چارچوب جهت پیش‌بینی و شناخت تهدیدات، مهندسی اجتماعی[2]، مقابله با باج افزارها[3]، نشت‌های امنیتی[4] و همچنین تهدیدات مداوم پیشرفته[5] توسعه یافت. در این تحقیق به‌کارگیری این مفهوم به‌عنوان مبنایی برای سنجش میزان استفاده تهدیدات سایبری از سناریو مدون‌شده در این زنجیره برای نابودی اهداف سایبری است.

«سناریو حملات سایبری»، مالوری[6] (۲۰۲۱) در مقاله خود با عنوان «چه نوع سناریوهای حمله را می‌توانید در یک محدوده سایبری شبیه‌سازی کنید؟» چنین نتیجه‌گیری می‌کند که: هر بار که سازمانی سناریوی حمله اجرا می‌کند، متخصصان امنیتی در معرض آزمایش قرار می‌گیرند، آموزش‌های خود را به کار می‌گیرند، مهارت‌های جدید را یاد می‌گیرند، از تجارب و ابزارهای جدید استفاده می‌کنند و با آخرین تهدیدات دست اول در

1.Cyber Kill Chain.
2.Social Engineering.
3.Ransomware.
4.Security breaches.
5.Advanced Persistent Threat.
6. Patrick Mallory.

یک محیط فنی بسیار واقع‌بینانه مقابله می‌کنند. با گذشت زمان، تیم‌های امنیتی می‌توانند سرعت شناسایی و پاسخ‌گویی به تهدیدات و حملات را بهبود ببخشند، کنترل‌ها یا قوانین امنیتی اضافی را ادغام کنند و بیاموزند که کدام رفتارهای سیستم غیرعادی هستند و چگونه می‌توان حفاظت‌های مرتبط را به اجزای زیرساخت حیاتی برای حفظ تداوم مرتبط نمود(مالوری، ۲۰۲۱).

«گراف»، مفهومی است که نقطه آغاز پیدایش آن در قالب نظریه‌ای در قرن هجدهم میلادی در رابطه با مسئله پل‌های کونیگسبرگ شکل گرفته است. مسئله «پل‌های کونیگسبرگ»، به هفت پل شهر کونیگسبرگ برمی‌گردد که امروزه از نظر جغرافیایی در کالینگراد روسیه واقع شده است. این هفت پل، برای ارتباط بین خشکی‌های دو طرف رودخانه‌ای به نام پرگِل احداث شده بود؛ اما مسئله‌ای که به این پل‌ها ارتباط داشت این بود: «آیا می‌توان از نقطه‌ای شروع به قدم زدن کرد و همه پل‌ها را پیمود؟» که به این منظور، اویلر (۱۷۳۶) نشان داد که این کار غیرممکن است. اویلر ثابت کرد برای آنکه مسیر از یک رأس شروع شود و از همه یال‌ها یک بار عبور شود و به همان رأس بازگردد، باید گراف هم‌بند باشد و مرتبه هر یک از رأس‌های آن نیز زوج باشد (کریمی، فتانه و میرافضل، سیدمرتضی، ۱۳۹۸). در این تحقیق از مفهوم و نرم‌افزار تحلیل گراف جهت ارائه بهتر موقعیت تهدیدات سایبری در نقاط شماتیک گراف و تعداد تمرکز تهدیدات در یک نقطه استفاده می‌شود.

«وزن‌دهی ساده»، روشی است که به‌عنوان یکی از ساده‌ترین روش‌های تصمیم‌گیری چند معیاره در سال ۱۹۸۱ میلادی توسط هدانگ و یون ارائه شده است (عطایی، ۱۳۸۹). در این روش که با نام روش ترکیب خطی وزن‌دار نیز شناخته می‌شود، پس از بی‌مقیاس کردن ماتریس تصمیم، با استفاده از ضرایب وزنی معیارها، ماتریس تصمیم بی‌مقیاس وزن‌دار به دست می‌آید و با توجه به این ماتریس، امتیاز هر گزینه محاسبه می‌شود (حائریان اردکانی، علی و همکاران، ۱۳۹۵).

پیشینه‌شناسی

نظر به اینکه در این پژوهش هدف بر موضوع اولویت‌سنجی و رتبه‌بندی تهدیدات سایبری متمرکز است، برخی منابع و گزارش‌های معتبر داخلی و بین‌المللی که با توجه به اهمیت شناخت ابعاد و تکرار تهدیدات سایبری اقدام به انتشار و ترویج اطلاعات آن‌ها می‌کنند در این پژوهش مورد نظر قرار گرفته‌اند.

در مقاله‌ای با عنوان «امنیت سایبری زیرساخت‌های حیاتی»، مگ‌لاراس[1] (۲۰۱۸) چنین عنوان نموده است که: برای سیستم‌های پیچیده و توزیع‌شده‌ای که علاوه بر تهدیدات جدید مستعد متعارف بودن هستند؛ بسیاری از روش‌های امنیتی را می‌توان برای چنین سیستم‌هایی[2] اعمال کرد. با در نظر گرفتن اینکه هم کارایی بالا، هم شناسایی نفوذ در زمان واقعی و هم سربار کم مورد نیاز است (مگ‌لاراس و همکاران، ۲۰۱۸).

ازجمله پژوهش‌های مرتبط، مواردی است که پژوهشگران گروه «ارزیابی امنیتی شبکه‌ها و سامانه‌ها» در پژوهشکده امنیت ارتباطات و فناوری اطلاعات (۱۳۹۶) ارائه نموده‌اند. در گزارش تحقیقاتی[3] مربوطه، پیشران‌های امنیتی را در چهار مرحله: مفاهیم، پیشران‌های امنیتی سایبری، روندهای کلان امنیت سایبری شناسایی و سپس صورت‌بندی نموده‌اند(عرب‌سرخی و همکاران، ۱۳۹۶).

توماس ای‌جانسون[4] (۲۰۱۵) در کتاب حفاظت از زیرساخت‌های حیاتی[5]، با نگاه به موارد قدرت‌ساز و آسیب‌پذیر زیرساخت‌های حیاتی آمریکا با ارائه آمار، طیف تهدیدات سایبری زیرساخت‌های حیاتی، ابزارها و منطق تهدیدات را به شکلی مدون ارائه و اولویت‌های تحقیق و توسعه برای حفاظت از زیرساخت‌ها را با در نظر گرفتن ارتقای امنیت سایبری و شناخت تهدیدات داخلی سایبری معرفی نموده است (جانسون، ۲۰۱۵).

---

1. Leandros A. Maglaras.

۲.منظور زیرساخت‌های حیاتی و کلیه زیرساخت‌هایی هستند که از سیستم‌ها و سامانه‌های سرپرستی و گردآوری داده (SCADA) استفاده می‌کنند.

۳. تبیین ملاحظات امنیتی در حوزه ارتباطات و فناوری اطلاعات.

4.Thomas A. Johnson.

5.CYBERSECURITY, Protecting Critical Infrastructuresfrom Cyber Attack and Cyber Warfare.

آقایی و همکاران (۱۳۹۸)، با ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی، طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی را با در نظر گرفتن نگاه سیستم از دیدگاه نفوذگر، توصیف سیستم، منابع شناسایی تهدیدات و ارتباط محورهایی همچون نوع تهدید، عوامل تهدید و مشخصات تهدید را در قالب ابعاد منطق طبقه‌بندی این نوع از تهدیدات معرفی نموده‌اند (آقایی و همکاران، ۱۳۹۸).

مؤسسه انیسا (۲۰۱۷) در گزارش سالیانه[1]، تهدیدات سایبری با فرکانس تکرار زیاد را مشخص، تشریح و رتبه‌بندی نموده است و بر موارد: تهدید، بردار حمله و عوامل تهدید به‌عنوان سه مؤلفه اصلی در حوزه سنجش تهدیدات توجه نموده است (انیسا،۲۰۱۷)، جدول(۱).

جدول (۱)- لیست تهدیدات سایبری، گزارش ۲۰۱۷

ردیف	عنوان تهدید	ردیف	عنوان تهدید	ردیف	عنوان تهدید	ردیف	عنوان تهدید	ردیف	عنوان تهدید
۱	بدافزار	٤	فیشینگ	۷	باج افزار	۱۰	دست‌کاری/ آسیب/ سرقت	۱۳	نشت اطلاعات
۲	حملات مبتنی بر وب	٥	هرزنامه	۸	شبکه‌های طعمه	۱۱	نقض اطلاعات	۱٤	کیت‌های بهره‌برداری
۳	حملات برنامه‌های کاربردی وب	٦	منع سرویس	۹	تهدیدهای داخلی	۱۲	سرقت هویت	۱٥	جاسوسی سایبری

در تحقیق دیگری نیز آقایی و همکاران (۱۳۹۹)، برای دست‌یابی به الگوی مفهومی ساختارشناسی تهدیدات سایبری مراکز داده، با استفاده از روش فراترکیب اقدام به گردآوری اطلاعات و ارائه مدل مفهومی با ساختاری مبتنی بر نُه بعد: فناوری، منشأ، ماهیت، انگیزه، دامنه بروز، آثار و پیامدها، دامنه اثرگذاری، شیوه تحقق و آسیب‌پذیری و ۳٦ مؤلفه نموده‌اند و بررسی اعتبار مدل با استفاده از روش ضریب کاپا انجام شده است(آقایی و همکاران، ۱۳۹۹). همچنین مؤسسه انیسا (۲۰۱۹) نیز در گزارش سالیانه[2]، تهدیدات

۱. پانزده تهدید و روند مرتبه بالا در سال ۲۰۱۷.

۲. پانزده تهدید و روند مرتبه بالا در سال ۲۰۱۹.

سایبری با فرکانس تکرار زیاد را مشخص، تشریح و رتبه‌بندی نموده است و همچنان بر مواردی همچون: تهدید، بردار حمله و عوامل تهدید به‌عنوان سه مؤلفه اصلی در حوزه سنجش تهدیدات توجه نموده است (همان)، جدول (۲).

جدول (۲)- لیست تهدیدات سایبری، گزارش ۲۰۱۹

رتبه	عنوان تهدید	رتبه	عنوان تهدید	رتبه	عنوان تهدید	رتبه	عنوان تهدید	رتبه	عنوان تهدید
۱	بدافزار	٤	فیشینگ	۷	شبکه‌های طعمه	۱۰	دست‌کاری/ آسیب/ سرقت	۱۳	رمزگذاری
۲	حملات مبتنی بر وب	٥	منع سرویس	۸	نقض داده	۱۱	نشت اطلاعات	۱٤	باج‌افزار
۳	حملات برنامه‌های کاربردی وب	٦	هرزنامه	۹	تهدیدهای داخلی	۱۲	سرقت هویت	۱٥	جاسوسی سایبری

روش‌شناسی

به‌منظور تدوین رتبه‌بندی تهدیدات سایبری با محوریت حضور در زنجیره مرگ، چنین برنامه‌ریزی شد که ابتدا اقدامات جمع‌آوری اطلاعات در خصوص انتخاب تهدیدات سایبری و میزان فعالیت آن‌ها در بخش‌های مختلف فرایند زنجیره مرگ با روش مطالعه کتابخانه‌ای و بهره‌گیری از منابع مرتبط انجام شود و سپس با استفاده از روش وزن‌دهی ساده، تحلیل گراف با به‌کارگیری نرم‌افزار گفی در حوزه تحلیل شبکه‌ای اقدام به تعیین وزن و میزان حضور تهدیدات سایبری در مراحل مختلف سناریو زنجیره مرگ شود. بر این اساس؛ ارائه مدلی با توان توصیف شکل تمرکزی تهدیدات سایبری در بخش‌های مختلف فرایند زنجیره مرگ و نتایج عملیاتی آن که دربرگیرنده برنامه دفاع سایبری و تصمیم‌سازی و تصمیم‌گیری در این حوزه است، این تحقیق جنبه کاربردی دارد. علاوه بر این با توجه به گسترش دانش در این حوزه، تحقیق حاضر توسعه‌ای است؛ بنابراین فعالیت حاضر بر اساس هدف از نوع توسعه‌ای-کاربردی است.

تحقیق حاضر با رویکرد آمیخته (کیفی و کمی) انجام شده است. در بخش کیفی با استفاده از روش مطالعات کتابخانه‌ای و با مراجعه به منابع معتبر نسبت به جمع‌آوری

مقالات و کتاب‌ها و اسناد و گزارشات پژوهشی اقدام و با بررسی نتایج و تفسیر آن‌ها مبنای سنجش و رتبه‌بندی تعیین شد. کنترل یافته‌ها و ارزیابی آن‌ها با روش ضریب کاپا انجام شد. همچنین با استفاده از روش وزن‌دهی ساده[1] که با نام روش ترکیب خطی وزن‌دار نیز شناخته می‌شود، پس از بی‌مقیاس کردن ماتریس تصمیم، با استفاده از ضرایب وزنی معیارها، ماتریس تصمیم بی‌مقیاس وزن‌دار به دست می‌آید و با توجه به این ماتریس، امتیاز هر گزینه محاسبه می‌شود. اگر در یک مسئله تصمیم‌گیری چندمعیاره n معیار و m گزینه وجود داشته باشد، به‌منظور انتخاب بهترین گزینه با استفاده از روش وزن‌دهی ساده مراحل به شرح زیر است:

۱. **تشکیل ماتریس تصمیم:** این روش شامل جدولی است که ستون‌های آن معیارها یا زیرمعیارها و سطرهای آن را گزینه‌ها تشکیل می‌دهند.

۲. **بی‌مقیاس کردن ماتریس تصمیم:** برای بی‌مقیاس کردن ماتریس تصمیم در روش SAWبه طریق زیر عمل می‌کنیم.

۳. **اگر معیار مثبت باشد:** تک‌تک اعداد آن ستون را بر بزرگ‌ترین عدد تقسیم می‌کنیم.

٤. **اگر معیار منفی باشد:** مینیمم آن ستون تقسیم بر تک‌تک اعداد می‌شود.

۵. **تشکیل ماتریس وزن‌دار:** در این گام با توجه به وزن‌های محاسبه‌شده از روش‌های دیگر ماتریس وزن‌دار را به دست می‌آوریم.

٦. **انتخاب گزینه برتر:** با جمع سطری ماتریس وزن‌ها امتیاز هر گزینه محاسبه می‌شود و بر اساس آن گزینه‌ها رتبه‌بندی می‌شوند.

یکی از جداول موجود در گزارش ارائه‌شده در پژوهشگاه ارتباطات و فناوری اطلاعات، مربوط به تعیین وضعیت و جایگاه هرکدام از تهدیدها در زنجیره مرگ است. بر اساس گزارش[2] ارائه‌شده از سوی شرکت لاکهید مارتین[3]، مطالعه «زنجیره مرگ

1. Simple Additive Weighting (SAW).
2.Understanding The Cyber Kill Chain.
3.Lockheed Martin, an American aerospace defense, security, and technology company.

سایبری» ابزاری برای مفهوم‌یابی در مورد چگونگی عملیات سایبری است[1]. این مفهوم در حقیقت بیان‌کننده فازهای یک تهاجم سایبری است که در نهایت راهبردهای مهاجم را مشخص می‌کند. در این بخش فرایند زنجیره مرگ سایبری در قالب اصلی خود ارائه می‌شود و در بخش‌های بعدی عملکرد هر فاز از فرایند معرفی و شرح داده خواهد شد.

شکل (۱)- فرایند زنجیره مرگ سایبری، شرکت لاکهید مارتین (چپ) و معادل‌سازی شده آن (راست)

ـ فاز اول: «شناسایی»[2] هدف بر اساس مجموعه اقدامات است.

ـ فاز دوم: «ابزاریابی»[3] برای حمله بر اساس آسیب‌پذیری‌های شناسایی‌شده یا «تسلیحات»

ـ فاز سوم: «آمادگی برای اقدام»[4] یا «نصب»

---

۱. این گزارش توسط محقق مورد مطالعه و بررسی قرار گرفت و اقدامات مشابهت‌سنجی با گزارش تهیه شده در پژوهشگاه ارتباطات و فناوری اطلاعات انجام شد. در این گزارش هفت مرحله مشخص به عنوان زنجیره مرگ سایبری و به منظور نقشه راه مهاجم مورد بررسی قرار می‌گیرد.

2.Reconnaissance.
3.Weaponization.
4.Delivery.

ـ فاز چهارم: «اجرای حمله»[1] یا اجرای کد تخریب‌کننده در محیط هدف یا «بهره-برداری»

ـ فاز پنجم: «نصب»[2] یا «تحویل» ابزار به سیستم هدف

ـ فاز ششم: «فرمان و کنترل»[3] به‌وسیله سلاح سایبری یا «دستور و کنترل»

ـ فاز هفتم: «اقدام بر مبنای هدف»[4] یا «اقدام برای هدف»

همان‌طور که قبلاً اشاره شد، یکی از اهداف این پژوهش ارائه ارتباط بین تهدیدات سایبری مورد نظر است تا بر این اساس بتوان در موقعیت‌های تشخیص سناریوهای حملات به اهداف مختلف از اطلاعات ارتباط تهدیدات در قالب سناریوها استفاده نمود و با تحلیل در مورد آن‌ها ضمن تدوین و برنامه‌ریزی اقدامات به برنامه‌های حملات سایبری مهاجمان دست یافت. به این منظور و با استفاده از نظریه گراف که قبلاً شرح داده شد و با معرفی روش تحلیل شبکه اقدام به تعیین روابط بین تهدیدهای سایبری در قالب سناریوهای مختلف می‌شود.

تحلیل شبکه (های اجتماعی)[5]

درک ارتباط بین مجموعه تهدیدات سایبری در سناریو حملات بر ضد اهدافی همچون زیرساخت‌های حیاتی می‌تواند دیدگاه‌های مفیدی را برای تصمیم‌سازی و تصمیم‌گیری در برنامه‌های پدافند و آفند سایبری توسعه دهد. به این منظور می‌توان با الگوبرداری در حوزه تحلیل ارتباط بین اجزای یک مجموعه از ایده تحلیل شبکه‌های اجتماعی فریمن[6] (۲۰۰۰) با هدف مشاهده وابستگی عناصر یا اعضای مورد مطالعه و تعاملات و روابط میان آن‌ها در علوم رفتاری استفاده نمود. این تجزیه‌وتحلیل به‌منظور کشف الگوهای روابط میان اعضا و همچنین سوابق و پیامدهای چنین الگویی است (فریمن، ۲۰۰۰) (نویدی، فاطمه و همکاران، ۱۳۹۶).

1.Exploitation.
2.Installation.
3.Command and Control.
4.Actions on Objectives.
5. Social Network Analysis (SNA).
6. Freeman.

تحلیل شبکه‌های اجتماعی تحلیل روشمندی است که نشان‌دهنده روابط اجتماعی در نظریه شبکه و متشکل از گره‌ها (بازیگران درون شبکه) و روابط است (کارلوس[1]، ۲۰۱۱)؛ به عبارت دیگر تحلیل شبکه‌های اجتماعی مجموعه‌ای از فن‌ها، ابزارها و متدولوژی‌ها برای ترسیم نمودن و اندازه‌گیری روابط بین افراد و سازمان است (چاکینگال[2]، ۲۰۱۳). همچنین یکی از مسائل مهم در شبکه‌ها وضعیت تبادل اطلاعات در میان بازیگران است. شبکه‌ها ابزاری اساسی برای پیدایش و انتشار اطلاعات محسوب می‌شوند. به‌طور کلی تعاملاتی که موجب ارتباط واحدها در شبکه می‌شوند، نشان از تبادل اطلاعات در شبکه دارند (خواجه نائینی و همکاران، ۱۳۹٤).

تحلیلگران شبکه اجتماعی، از دو نوع ابزار ریاضی برای بازنمایی اطلاعات مربوط به الگوهای روابط میان کنشگرهای اجتماعی استفاده می‌کنند: ماتریس‌ها و گراف‌ها. یک گراف متشکل از رئوس یا کنشگرانی است که با یال به یکدیگر وصل شده‌اند که نشانگر وجود رابطه میان کنشگرها است. هر رابطه‌ای می‌تواند جهت‌دار یا غیرجهت‌دار باشد. روابط جهت‌دار با پیکان بازنمایی می‌شوند و روابط هم‌بند یا غیرجهت‌دار با خطوط. روابط جهت‌دار در صورتی که متقابل باشند با پیکان‌های دوسر نمایش داده می‌شوند. بازنمایی اطلاعات مربوط به روابط میان کنشگرها به‌وسیله گراف‌ها، یک روش سودمند و کارآمد برای توصیف روابط اجتماعی به حساب می‌آید. گراف‌ها اگر به درستی کشیده شوند، قادرند نکات و اطلاعات بسیار مهمی را در مورد کل ساختار شبکه به ما منتقل کنند. اطلاعاتی از قبیل اینکه آیا همه‌ی رئوس با هم در ارتباط هستند یا خیر؛ آیا درون شبکه کنشگرهایی وجود دارد که تعداد روابطشان از دیگر کنشگرها بیشتر باشد (هنمن و ریدل، ۲۰۰۵). نرم‌افزارهای متعددی برای رسم گراف‌های شبکه‌های اجتماعی تعریف شده‌اند. ازجمله پرکاربردترین این نرم‌افزارها می‌توان به یوسی نت[3]، گفی[4] و نودیکس‌ال[5] اشاره کرد.

1. Carlos.
2. Chakkingal.
3. UCINET.
4. Gephi.
5. NodeXL.

یک ویژگی بسیار مهم در شبکه، مرکزیت است. مرکزیت گره‌های شبکه با سه شاخص مرکزیت درجه‌ای (درجه)، مرکزیت نزدیکی و مرکزیت بینیّت (بینابینی) سنجیده می‌شود. مرکزیت درجه شاخصی است که تعداد پیوندهای واردشده یا خارج‌شده از هر گره را نشان می‌دهد (فریمن، ۱۹۷۹). دو شاخص اصلی مورد استفاده برای تحلیل داده‌ها در شبکه به دست آمده عبارت‌اند از: مرکزیت درجه و مرکزیت بینابینی. بالاتر بودن مرکزیت درجه برای یک بازیگر، به معنای برخوردار بودن از ارتباطات بیشتر در کل شبکه است و به تعبیری نشان از قدرتمند بودن یک بازیگر دارد. مرکزیت بینابینی یا شاخص بینیّت از دیگر شاخص‌های مرکزیت به شمار می‌رود. شاخص بینیّت به میزانی که یک گره در کوتاه‌ترین مسیر میان هر دو گره دیگر در شبکه قرار می‌گیرد دلالت دارد؛ بنابراین گره‌ای که بینیّت بیشتری دارد، در اتصالات شبکه تأثیرگذارتر است (عرفان‌منش و همکاران، ۱۳۹٤).

نرم‌افزار گفی

این ابزار نرم‌افزاری منبع باز[1] برای تحلیل و اکتشاف بصری شبکه‌ها است. بر اساس این تعریف که شبکه به‌عنوان مجموعه‌ای از موجودیت‌ها در قالب تجمیع نودها یا گره‌ها در نظر گرفته می‌شود و در این مجموعه، یال‌ها وسیله ارتباطات میان گره‌ها هستند، نرم‌افزارهای متنوعی برای بصری‌سازی، تجزیه‌وتحلیل شبکه‌ها وجود دارند و در این خصوص نرم‌افزار گفی به‌عنوان یکی از ابزارهای تحلیل در چنین محیط‌هایی است. کاربران گفی با بصری‌سازی در زمان واقعی و مستقر کردن گره‌ها در فضای دو یا سه‌بعدی و با استفاده از الگوریتم‌های خاص[2] تأثیر متقابل گره‌ها بر هم را ارائه می‌کنند. مطالعه همبستگی گره‌ها و ساختن شبکه با استفاده از الگوهای بصری است. در این نرم‌افزار هر نوع شبکه‌ای با خصوصیات فوق قابل تحلیل است.

1. OPEN SOURCE.
2. LAYOUT & MOVE.

تحلیل و بررسی

چنانچه قبلاً اشاره شد، معیار مورد نظر در سنجش تهدیدات حضور آن‌ها در هر یک از موقعیت‌ها در فرایند زنجیره مرگ در نظر گرفته می‌شود. تهدیدات سایبری مورد نظر در این پژوهش که از نتایج آماری مرکز امنیت سایبری اتحادیه اروپا (۲۰۱۷ و ۲۰۱۹) و نتایج گزارش پژوهشگاه ارتباطات و فناوری اطلاعات (۱۳۹۶) بر مبنای میزان حضور در بخش‌های مختلف فرایند زنجیره مرگ انتخاب شده‌اند، به شرح جدول ذیل می‌باشند. اطلاعات جدول ذیل نشان‌دهنده میزان حضور هر یک از تهدیدها در مراحل مشخص‌شده زنجیره مرگ سایبری است. میزان استفاده از هر تهدید در هر مرحله به‌عنوان معیاری برای اهمیت تهدیدها در نظر گرفته می‌شود. ضمناً مشابهت عنوان فازهای زنجیره مرگ سایبری بر اساس مطالعه گزارش «پژوهشگاه ارتباطات و فناوری اطلاعات» و گزارش «شرکت لاکهید مارتین» تنظیم شده است.

جدول (۳)- جایگاه هرکدام از تهدیدها در زنجیره مرگ

	شناسایی	ابزاریابی (تسلیحات)	آمادگی برای اقدام (نصب)	اجرای حمله (بهره‌برداری)	فعال‌سازی (تحویل)	فرمان و کنترل (دستور و کنترل)	اقدام بر مبنای هدف (اقدام برای هدف)
بدافزار			✓			✓	✓
حمله‌های مبتنی بر وب		✓		✓	✓		
حمله‌های برنامه‌های کاربردی وب	✓		✓	✓			
جلوگیری از سرویس	✓	✓				✓	✓
بات‌نت						✓	
فیشینگ	✓	✓			✓		
هرزنامه		✓			✓		
باج‌افزار			✓			✓	✓
تهدید داخلی	✓	✓	✓	✓	✓	✓	✓
دست‌کاری فیزیکی/ سرقت/ فقدان				✓			✓
کیت‌های بهره‌بردار		✓	✓	✓	✓		
نقض داده		✓	✓	✓	✓	✓	✓
سرقت هویت	✓	✓			✓		✓
نشت اطلاعات	✓	✓		✓	✓		✓
جاسوسی سایبری	✓	✓	✓	✓	✓	✓	✓

در این جدول مراحل سناریو حمله در زنجیره مرگ سایبری به‌عنوان هفت معیار برای به‌کارگیری تهدیدها شناسایی و مورد نظر قرار گرفته است. برای تعیین رتبه وزنی هر یک از تهدیدها بر اساس ضریب اهمیت معیارها بایستی ابتدا وزن و اهمیت هر معیار در نظر گرفته شود.

برای این منظور می‌بایست:

ـ در مرحله اول ضریب اهمیت معیارهای هفت‌گانه را تعیین نمود (نظرسنجی یا خبرگی).

ـ در مرحله دوم اقدامات بی‌مقیاس‌سازی انجام می‌شود.

ـ در مرحله سوم بر اساس ضریب اهمیت وزنی معیارها ماتریس وزن‌دار تشکیل می‌شود.

ـ در مرحله چهارم انتخاب گزینه برتر با جمع سطری ماتریس وزن‌ها انجام می‌شود.

ضرایب اهمیت معیارها

با توجه به اینکه در این گزارش میزان حضور هر یک از تهدیدها در مراحل زنجیره مرگ سایبری به‌عنوان محور ارزیابی در نظر گرفته می‌شود و بر اساس اقدامات چهارگانه فوق تعداد حضور هر تهدید در هر مرحله به‌عنوان اهمیت در نظر گرفته می‌شود؛ بنابراین برای هر یک از معیارهای هفت‌گانه بر اساس تعداد حضور تهدیدها به شرح زیر ضریب اهمیت را تعیین می‌کنیم.

جدول (٤) – ضریب اهمیت معیارهای هفت‌گانه

ردیف	معیار	تعداد حضور تهدیدات در هر مرحله (حضور در معیار)	ضریب اهمیت
١	شناسایی	٧	٠/١
٢	ابزاریابی	١٠	٠/٢٥
٣	آمادگی برای اقدام	٨	٠/١
٤	اجرای حمله	٨	٠/١
٥	فعال‌سازی	١٠	٠/٢٥
٦	فرمان و کنترل	٧	٠/٥
٧	اقدام بر مبنای هدف	٩	٠/١٥

لازم به ذکر است که می‌توان ضریب اهمیت را بر اساس نظر خبرگان در قالب ارائه پرسشنامه یا اخذ نظر خبرگی نیز به دست آورد. در این گزارش با توجه به تعداد حضور تهدیدها در هر مرحله و منتج از منابع معتبر، ضریب اهمیت معیارها بر اساس نظر خبرگی پژوهشگر در نظر گرفته شده است. در ادامه ضریب اهمیت وزنی به شرح جدول زیر ارائه می‌شود.

جدول (۵) –ضریب اهمیت و نرمال‌سازی شده اطلاعات

	شناسایی	ابزاریابی (تسلیحات)	آمادگی برای اقدام (نصب)	اجرای حمله (بهره‌برداری)	فعال‌سازی (تحویل)	فرمان و کنترل (دستور و کنترل)	اقدام بر مبنای هدف (اقدام برای هدف)
وزن هر معیار	۰/۱	۰/۲۵	۰/۱	۰/۱	۰/۲۵	۰/۵	۰/۱۵
بدافزار	۰	۰	۱	۰	۰	۱	۱
حمله‌های مبتنی بر وب	۰	۱	۰	۱	۱	۰	۰
حمله‌های برنامه‌های کاربردی وب	۱	۰	۱	۱	۰	۰	۰
جلوگیری از سرویس	۱	۱	۰	۰	۰	۱	۱
بات‌نت	۰	۰	۰	۰	۰	۱	۰
فیشینگ	۱	۱	۰	۰	۱	۰	۰
هرزنامه	۰	۱	۰	۰	۱	۰	۰
باج‌افزار	۰	۰	۱	۰	۰	۱	۱
تهدید داخلی	۱	۱	۱	۱	۱	۱	۱
دست‌کاری فیزیکی/ سرقت/ فقدان	۰	۰	۰	۱	۰	۰	۱
کیت‌های بهره‌بردار	۰	۱	۱	۱	۱	۰	۰
نقض داده	۰	۱	۱	۱	۱	۱	۱
سرقت هویت	۱	۱	۰	۰	۱	۰	۱
نشت اطلاعات	۱	۱	۰	۱	۱	۰	۱
جاسوسی سایبری	۱	۱	۱	۱	۱	۱	۱

به دلیل شرایط خاص این جدول یعنی حضور اعداد ۰ و ۱، جدول بی‌مقیاس شده نیز دارای همین مقادیر است. بنابراین به محاسبه وزن ۱۵ گزینه یعنی تهدیدها می‌پردازیم.

جدول (٦) – وزن تهدیدات در ارتباط با حضور در زنجیره مرگ سایبری

	شناسایی	ابزاریابی (تسلیحات)	آمادگی برای اقدام (نصب)	اجرای حمله (بهره‌برداری)	فعال‌سازی (تحویل)	فرمان و کنترل (دستور و کنترل)	اقدام بر مبنای هدف (اقدام برای هدف)	محاسبه وزن تهدیدات
وزن هر معیار	۰/۱	۰/۲۵	۰/۱	۰/۱	۰/۲۵	۰/۵	۰/۱۵	
بدافزار	۰	۰	۱	۰	۰	۱	۱	(۱*۰/۱۵)+(۱*۰/۵)+(۱)/ ۰/۷۵=(۱*۰)
حمله‌های مبتنی بر وب	۰	۱	۰	۱	۱	۰	۰	(۱*۰/۲۵)+(۱*۰/۱)+(۱*۰/۲۵) ۰/٦=(۱*۰/)
حمله‌های برنامه‌های کاربردی وب	۱	۰	۱	۱	۰	۰	۰	(۱*۰/۱)+(۱*۰/۱)+(۱*۰/۱) ۰/۳=(۱*)
جلوگیری از سرویس	۱	۱	۰	۰	۰	۱	۱	(۱*۰/۱۵)+(۱*۰/۵)+(۱*۰/۲۵) ۱=(۱*۰/۱)+(۱*۰/)
بات‌نت	۰	۰	۰	۰	۰	۱	۰	۰/۵= (۱*۰/۵)
فیشینگ	۱	۱	۰	۰	۱	۰	۰	(۱*۰/۲۵)+(۱*۰/۲۵)+(۱*۰/۱) ۰/٦=(۱*۰/)
هرزنامه	۰	۱	۰	۰	۱	۰	۰	(۱*۰/۲۵)+(۱*۰/۲۵) ۰/۵=
باج‌افزار	۰	۰	۱	۰	۰	۱	۱	(۱*۰/۱۵)+(۱*۰/۵)+(۱)/ ۰/۷۵=(۱*۰)
تهدید داخلی	۱	۱	۱	۱	۱	۱	۱	(۱*۰/۱۵)+(۱*۰/۵)+(۲۵ +(۱*۰/۱)+(۱*۰/ (۱*۰/۱)+(۱*۰/۲۵)+(۱)/ ۱/٤۵=(۱*۰)
دست‌کاری فیزیکی/ سرقت/ فقدان	۰	۰	۰	۱	۰	۰	۱	+(۱*۰/۱۵) (۱*۰/۱)=۰/۲۵
کیت‌های بهره‌بردار	۰	۱	۱	۱	۱	۰	۰	(۱*۰/۲۵)+(۱*۰/۱)+(۱)/ ۰/۷= (۱*۰/۲۵)+(۱*۰)
نقض داده	۰	۱	۱	۱	۱	۱	۱	(۱*۰/۱۵)+(۱*۰/۵)+(۲۵ +(۱*۰/۱)+(۱*۰/ =((۱*۰/۲۵)+(۱*۰/۱)) ۱/۳۵

	شناسایی	ابزاریابی (تسلیحات)	آمادگی برای اقدام (نصب)	اجرای حمله (بهره‌برداری)	فعال‌سازی (تحویل)	فرمان و کنترل (دستور و کنترل)	اقدام بر مبنای هدف (اقدام برای هدف)	محاسبه وزن تهدیدات
سرقت هویت	۱	۱	۰	۰	۱	۰	۱	(۰/۱۵*۱)+(۰/۲۵*۱)+(۰/۲۵*۱)+(۰/۱*۱) =۰/۷۵
نشت اطلاعات	۱	۱	۰	۱	۱	۰	۱	(۰/۱۵*۱)+(۰/۲۵*۱)+(۱ /۰*۱)+(۰/۲۵*۱) +(۰/۱*۱) = ۰/۸۵
جاسوسی سایبری	۱	۱	۱	۱	۱	۱	۱	(۰/۱۵*۱)+(۰/۵*۱)+(۲۵ /۰*۱)+(۰/۱*۱)+ (۰/۱*۱)+(۰/۲۵*۱)+(۱/ ۰*۱)= ۱/٤۵

بر اساس نتایج به‌دست‌آمده از جدول فوق و برای تعیین رتبه وزنی تهدیدات سایبری جدول (۷) در قالب جدول اوزان گزینه‌ها و برای تعیین مقادیر وزنی رتبه‌بندی‌شده ارائه می‌شود.

جدول (۷) – اوزان گزینه‌ها (تهدیدات)

اوزان	مقادیر	حداکثرها
W1	۰/۷۵	Max5
W2	۰/٦	Max7
W3	۰/۳	Max9
W4	۱	Max3
W5	۰/۵	Max8
W6	۰/٦	Max7
W7	۰/۵	Max8
W8	۰/۷۵	Max5
W9	۱/٤۵	Max1
W10	۰/۲۵	Max10
W11	۰/۷	Max6
W12	۱/۳۵	Max2
W13	۰/۷۵	Max5
W14	۰/۸۵	Max4
W15	۱/٤۵	Max1

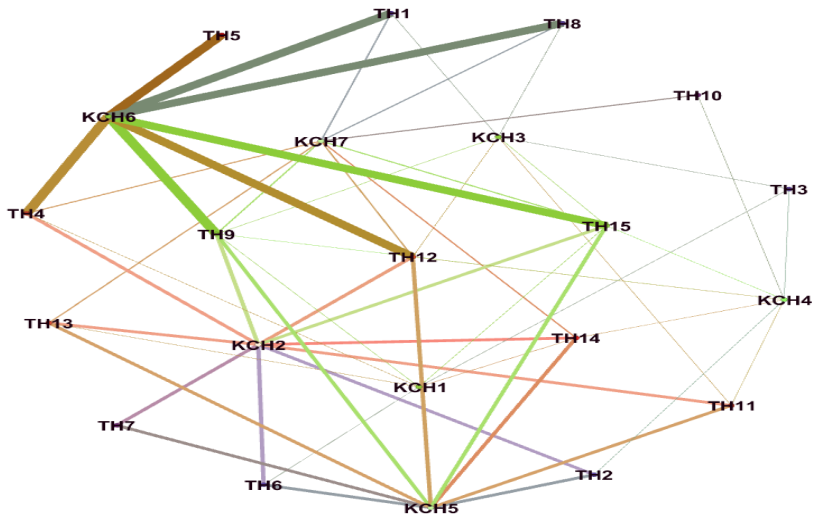
در ادامه و بر مبنای نیازمندی به رتبه‌بندی گزینه‌ها بر اساس عدد وزنی اختصاص‌یافته جدول رتبه‌بندی تهدیدات سایبری جدول (۸) ارائه می‌شود.

جدول (۸) – رتبه‌بندی گزینه‌ها به ترتیب (تهدیدات)

ردیف	نام تهدید	وزن	رتبه
۱	تهدید داخلی	۱/٤٥	۱
۲	جاسوسی سایبری	۱/٤٥	۱
۳	نقض داده	۱/۳٥	۲
٤	جلوگیری از سرویس	۱	۳
٥	نشت اطلاعات	۰/۸٥	٤
٦	بدافزار	۰/۷٥	٥
۷	باج‌افزار	۰/۷٥	٥
۸	سرقت هویت	۰/۷٥	٥
۹	کیت‌های بهره‌بردار	۰/۷	٦
۱۰	حمله‌های مبتنی بر وب	۰/٦	۷
۱۱	فیشینگ	۰/٦	۷
۱۲	بات‌نت	۰/٥	۸
۱۳	هرزنامه	۰/٥	۸
۱٤	حمله‌های برنامه‌های کاربردی وب	۰/۳	۹
۱٥	دست‌کاری فیزیکی/ سرقت/ فقدان	۰/۲٥	۱۰

نتایج

ارائه نتایج به‌منظور تبیین ارتباط تهدیدات سایبری در یک سناریو حمله مثل زنجیره مرگ راه‌کاری است برای پاسخ‌گویی بخشی از نیازمندی مراکز امنیت سایبری برای رهگیری حملات سایبری و برنامه‌ریزی برای کسب تجربه از مخاطرات قبلی که بر اساس موارد قبلی شرح داده شده؛ نتایج در قالب خروجی نرم‌افزار گفی ارائه می‌شود. در شکل زیر؛ تهدیدهای سایبری مورد نظر در این پژوهش بر اساس وزن، رتبه و اولویت به‌دست‌آمده به‌عنوان ورودی نرم‌افزار گفی مورد تحلیل قرار گرفتند و شکل ارتباطی آن‌ها مشخص شده است.



شکل (۲)- ارتباط تهدیدات سایبری بر اساس وزن و رتبه به‌دست‌آمده از روش وزن‌دهی ساده

بدیهی است این ارتباط که دارای اولویت وزنی تهدیدات مورد نظر، منتج از روش وزن‌دهی ساده است، گویای این موضوع مهم است که این تهدیدات به چه ترتیب در یک سناریو حمله نقش‌آفرینی می‌کنند. به این ترتیب تا حد زیادی اقدامات بر ضد مهاجمان قابل برنامه‌ریزی خواهد بود. در این نرم‌افزار اطلاعات دیگری نظیر «توزیع مرکزیت بینابینی»، «نزدیکی توزیع مرکزی»، «نزدیکی هارمونیک توزیع مرکزیت» و «توزیع غیرعادی» نیز برای اجزاء مجموعه مورد نظر- در این پژوهش، تهدیدات سایبری- قابل ارائه است.

بالاترین درجه مرکزیت ورودی[1] متعلق به تهدید داخلی و پس از آن جاسوسی سایبری است و به این معنی است که دیگر بازیگران فعال در گراف ارتباط تهدیدات و زنجیره مرگ، بیشترین ارتباط را با فرمان و کنترل برقرار می‌کنند؛ به عبارت دیگر قدرتمندترین تهدیدات، تهدید داخلی هستند. فهرست قدرتمندترین تهدیدات، از حیث روابط موجود در شبکه گراف فوق، به ترتیب درجه مرکزیت داخلی در جدول (۹) آورده شده است.

1. Indegree.

جدول (۹). فهرست تهدیدات کلیدی بر اساس بیشترین درجه مرکزیت داخلی

تهدیدات	درجه مرکزیت داخلی
تهدید داخلی	٦٣
جاسوسی سایبری	٥٩
نقض داده	٥٥
جلوگیری از سرویس	٤٩

در شبکه‌های حاوی روابط جهت‌دار، کنشگرهایی که مرکزیت درجه بیرونی[1] بالایی دارند، اغلب کنشگرهای بانفوذی هستند. نتایج به‌دست‌آمده نشان می‌دهد بانفوذترین تهدیدات در زنجیره مرگ به ترتیب تهدید داخلی، جاسوسی سایبری، نقض داده و جلوگیری از سرویس هستند. به بیان دیگر این تهدیدات بیش از بقیه تهدیدات دارای تأثیر در زنجیره مرگ بوده و الزام به ارتباط با دیگر تهدیدات دارند. تفاوت عدد مرکزیت داخلی میان تهدید داخلی و جاسوسی سایبری قابل توجه است. تفاوت در مدل کارکردی این تهدیدات می‌تواند یکی از دلایل فاصله موجود در درجه مرکزیت آن‌ها باشد.

جدول (۱۰). فهرست تهدیدات کلیدی با بیشترین مرکزیت بینابینی

تهدیدات	مقدار مرکزیت بینابینی
تهدید داخلی	٣٣
جاسوسی سایبری	٣٠.٥
نقض داده	٢٩
جلوگیری از سرویس	٢٥
نشت اطلاعات	٢١.٥
بدافزار	٢٠

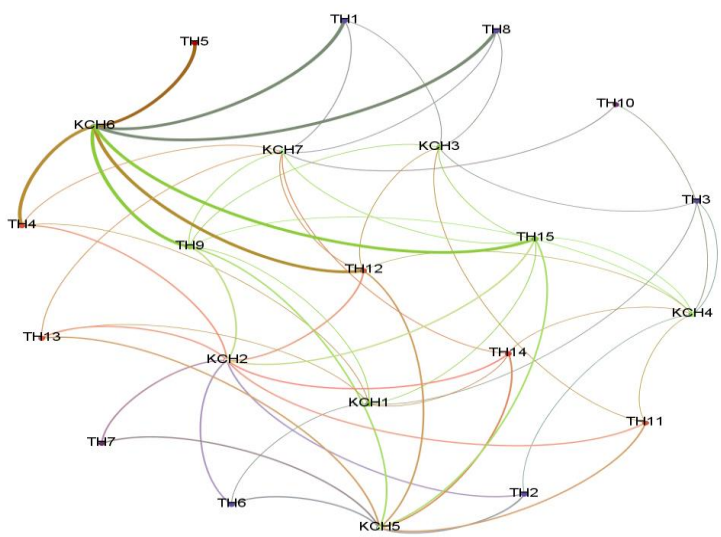
1. Outdegree.

بازیگران دارای نقش بینابینی

شاخص بینیّت[1] یا مرکزیت بینابینی به میزانی که یک گره در کوتاه‌ترین مسیر میان هر دو گره دیگر در شبکه قرار می‌گیرد دلالت دارد. هرچه مرکزیت بینابینی یک بازیگر بیشتر باشد قدرت واسطه‌گری و پل زنندگی آن بیشتر است و می‌توان گفت بازیگری که بینابینی بیشتری دارد، در اتصالات شبکه تأثیرگذارتر است. در شبکه ترسیم‌شده در این پژوهش، بیشترین مرکزیت بینابینی به تهدید داخلی، جاسوسی سایبری تعلق دارد. تهدیدات دارای بیشترین نقش واسطه‌گری در زنجیره مرگ به همراه عدد بینابینی آن‌ها در جدول (۳) آورده شده است.

تهدیدات اثرگذار در شبکه

تهدیدات کلیدی زنجیره مرگ در بخش اصلی فرمان و کنترل جای دارند. جهت دستیابی به تصویری کلی‌تر از روابط موجود میان تهدیدات اصلی زنجیره مرگ، در شکل (۳) که به‌وسیله نرم‌افزار گفی ترسیم شده است، روابط تهدیدات اصلی زنجیره مرگ با اختصاص رنگ‌های جداگانه به هر بخش نمایش داده شده است.



شکل ۳. روابط میان تهدیدات و نقش آن‌ها در زنجیره مرگ (خروجی نرم‌افزار «گفی»)

1. Betweenness.

محاسبه مقدار درجه مرکزیت برای تهدیدات اصلی نیز محاسبه شده است. نتایج نشان می‌دهد پس از فرمان و کنترل که بیشترین درجه مرکزیت را در بین دیگر بخش‌های زنجیره مرگ دارند، فعال‌سازی بیشترین اهمیت و تأثیرگذاری را در زنجیره مرگ دارد.

نتیجه‌گیری

بر اساس موارد تحلیل‌شده در این پژوهش، می‌توان نتیجه‌گیری نمود که تحلیل و بررسی تهدیدات سایبری در فرایندی ادامه‌دار بایستی به‌عنوان یکی از فعالیت‌های دائمی و دارای برنامه منسجم در حوزه امنیت سایبری سازمان‌ها باشد. در این پژوهش هدف این بوده است که صرف هزینه برای مقابله با تهدیدات سایبری به نحوی منطقی انجام شود تا سازمان‌ها بتوانند در حوزه امنیت شبکه‌ها و زیرساخت‌های حیاتی بهره‌ور عمل کنند.

نتایج این پژوهش نشان می‌دهد اولویت‌سنجی تهدیدات برای نقش‌آفرینی در سناریوهایی که به‌عنوان نمونه، سناریو «زنجیره مرگ» مورد مطالعه قرار گرفت و از طرفی ارتباط تهدیدات سایبری با یکدیگر در سناریوهای تدوین‌شده توسط مهاجمان که از ابعاد مختلف مورد بررسی قرار گرفت، در مراکز عملیات امنیت[1] قابل استفاده است و حتی اطلاعات تحلیل‌شده از این طریق می‌تواند در پایگاه دانش مخاطرات سازمان ثبت و نگهداری شود تا در آینده بتواند در زمان رخدادهای مشابه اقدامات از پیش برنامه‌ریزی‌شده را انجام داد.

بخش دیگری از نتایج این پژوهش نشان‌دهنده این واقعیت است که همگام با توسعه فناوری‌های مختلف، در حال حاضر، اقداماتی که سهواً یا عمداً در محدوده داخلی سازمان‌ها و برگرفته از آسیب‌پذیری‌های موجود در حوزه‌های انسانی و سیستمی و به شکل تهدیدات منتج به رخدادهای سایبری به وجود می‌آیند نشان از این موضوع مهم دارند که عوامل داخلی بیشترین تأثیر در افول امنیت سایبری در مجموعه‌ها را دارند. این واقعیت گویای صریح بر توجه به برنامه‌ریزی و هدف‌گذاری در حوزه شناسایی آسیب‌پذیری‌های سایبری در کلیه بخش‌ها به‌خصوص زیرساخت‌های حیاتی دارد.

1. Security Operation Center (S.O.C).

پیشنهادها

در این خصوص پیشنهاد می‌شود جنبه‌های عملیاتی و اجرایی این پژوهش برای مراکز عملیات امنیت سایبری، مراکز امداد رایانه‌ای[1] و کلیه بخش‌های فعال امنیت سایبری سازمان‌ها مورد توجه قرار گیرد. به عبارتی پیشنهادهای پژوهشگران عبارت‌اند از:

۱. تعمق و توسعه به‌کارگیری روش‌های شناسایی و تحلیل حملات سایبری بر ضد اهداف و سرمایه‌های سازمانی.

۲. برنامه‌ریزی در مورد شناسایی و کالبدشکافی تهدیدات سایبری و نوع عملکرد آن‌ها با به‌کارگیری شیوه به کار گرفته‌شده در این پژوهش.

۳. استفاده آموزشی از این روش برای دانشجویان و کارشناسان برای توسعه جنبه‌های عملیاتی آن.

همچنین پیشنهادهای پژوهشی در ارتباط با گسترش دامنه اقدامات انجام شده و استمرار آن‌ها در این پژوهش می‌تواند شامل موارد زیر باشد:

۱. بررسی نقش‌آفرینی تهدیدات سایبری با استفاده از گزارش‌های ارائه‌دهنده رتبه‌های تهدیدات پرتکرار در سناریوهای دیگر تهاجمات سایبری.

۲. تطبیق نتایج این پژوهش با پژوهش‌های مشابه برای به دست آوردن رفتار حملات سایبری.

۳. اجرای پژوهش‌های مشابه بر اساس میزان نقش‌آفرینی تهدیدات سایبری مشهور در سناریوهای حملات شناخته‌شده.

1. Computer Emergency Response Team (CERT).

فهرست منابع و مآخذ

الف. منابع فارسی

- سند راهبردی پدافند سایبری (۱۳۹٤)، سازمان پدافند غیرعامل.
- نای، جوزف (۲۰۱۰)، آینده قدرت، ترجمه احمد عزیزی، نشر نی.
- آقایی، محسن و همکاران (۱۳۹۸)، ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی، فصل‌نامه امنیت ملی، شماره ۳۲.
- واژه‌نامه امنیت سایبری مشترک ایالات متحده و روسیه، (۲۰۱٤)، انستیتو امنیت اطلاعات مسکو و دانشگاه شرق-غرب ایالات متحده.
- کریمی، فتانه و میرافضل، سید مرتضی (۱۳۹۸)، طیف گراف‌های ابرستاره و گراف‌های یالی آنها، نشریه: پژوهش‌های نوین در ریاضی (علوم پایه دانشگاه آزاد اسلامی)، شماره: آذر و دی ۱۳۹۸، دوره ۵، شماره ۲۱، صفحه ۱۲۵ تا صفحه ۱۳۲.
- حائریان اردکانی، علی؛ کوشا، حمیدرضا و میرسعیدی، فاطمه (۱۳۹۵)، مجله: پژوهش‌های مدیریت راهبردی، بهار ۱۳۹۵، شماره ٦۰، علمی-پژوهشی صفحه- ۳۷ تا ٦۲.
- عرب‌سرخی، ابوذر؛ شبانی، فاطمه؛ ایوازه، اسما و چاردولی، امین (۱۳۹٦)، تدوین نقشه راه امنیت در حوزه ارتباطات و فناوری اطلاعات؛ پژوهشگاه ارتباطات و فناوری اطلاعات-پژوهشکده امنیت ارتباطات و فناوری اطلاعات-گروه ارزیابی امنیت شبکه و سامانه‌ها.
- آقایی، محسن و همکاران (۱۳۹۹)، الگوی مفهومی ساختارشناسی تهدیدات سایبری مراکز داده، فصلنامه امنیت پژوهی دانشگاه فارابی، بهار ۱۳۹۹، شماره ٦۹، علمی-پژوهشی (وزارت علوم) ISC/ ۲٦ صفحه از ۳۳ تا ۵۸.
- نویدی، فاطمه؛ میرطاهری، سیده لیلا و حسن‌زاده محمد (۱۳۹٦)، روش‌های تحلیل داده و پیوندها در شبکه‌های اجتماعی، نشریه: تعامل انسان و اطلاعات، دوره ٤، شماره ۲، صفحه ۵۸ تا ۷۰.
- خواجه نایینی، علی؛ اشتریان، کیومرث؛ محمدی کنگرانی، حنانه و پوردیبا، غنچه (۱۳۹٤)، مطالعه و بررسی شبکه تبادل اطلاعات میان بازیگران حوزه نانو فناوری در ایران، پژوهش‌های مدیریت در ایران، پاییز ۱۳۹٤، دوره ۱۹، شماره ۳، صفحه ۱۰۷ تا صفحه ۱۳۳.
- عرفان‌منش، محمدامین؛ گرایی، احسان و بصیریان جهرمی، رضا (۱۳۹٤)، بررسی عملکرد ده‌ساله و تحلیل جرگه دانشگاه‌ها و مؤسسات پژوهشی در حوزه اطلاع‌سنجی کشور، فصلنامه علمی-پژوهشی پژوهشگاه علوم و فناوری اطلاعات ایران، دوره ۳۱، شماره ۲، صفحه ۳۲۵ تا صفحه ۳٤۷.

ب. منابع انگلیسی

- David P. Duggan, John T. Michalski, “A Threat Analysis Framework as Applied to Critical Infrastructures in the Energy Sector “,Sandia National Laboratories, September 2007
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- https://www.varonis.com/blog/cyber-kill-chain
- https://www.sciencedirect.com/topics/computer-science/cyber-kill-chain
- https://www.sans.org/blog/applying-security-awareness-to-the-cyber-kill-chain
- https://www.exabeam.com/information-security/cyber-kill-chain
- Thomas A. Johnson, “Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare”, Webster University, St. Louis, Missouri, USA, 2015
- ENISA Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends
- ENISA Threat Landscape Report 2019, 15 Top Cyber-Threats and Trends
- Leandros A. Maglaras, Ki-Hyung Kim, Helge Janickea, Mohamed Amine Ferragc,Stylianos Rallis, Pavlina Fragkoue, Athanasios Maglarasf, Tiago J. Cruz: Cyber security of critical infrastructures, ScienceDirect, 2018
- Patrick Mallory,: What types of attack scenarios can you simulate in a cyber range?, INFOSEC, 2021