فصلنامهٔ امنیت پژوهی (علمی-پژوهشی)
سال نوزدهم: شماره ۶۹ – بهار ۱۳۹۹
صص: ۳۳ – ۵۸

Amniat Pajouhi: Security Research Quarterly
Vol.19, No.69, Spring 2020
P-P: 33 - 58

الگوی مفهومی ساختارشناسی تهدیدات سایبری مراکزداده

محسن آقایی[۱]
علی معینی[۲]
ابوذر عرب‌سرخی[۳]

چکیده

توسعه زیرساخت‌های ارتباطی و اتصال شبکه‌هایی با پیکربندی‌های ناهمگون باعث رشد آسیب‌پذیری‌ها و تهدیدات و کاهش امنیت سایبری شده است. مراکزداده به‌عنوان قلب تپنده زیرساخت‌های اطلاعاتی و ارتباطی از اهداف مهم تهدیدات سایبری زیرساخت‌های حیاتی به شمار می‌روند. شناسایی ساختار تهدیدات سایبری مراکزداده از اقدامات مهم برای ارتقاء امنیت سایبری و به‌عنوان هدف اصلی این تحقیق است. روش فراترکیب به‌عنوان روش کیفی نظام‌مند برای جمع‌آوری اطلاعات شناسایی طبقه‌بندی‌های تهدیدات سایبری این زیرساخت‌ها، گونه‌شناسی و تحلیل آن‌ها و شناسایی تهدیدات سایبری پرتکرار مورد استفاده محققین قرارگرفته است. اعتبارسنجی نتایج در دو مرحله با استفاده از روش کیفی گروه کانونی و روش کمی ضریب کاپا در مورد ۹ بُعد: فناوری، منشأ، ماهیت، انگیزه، دامنه بروز، آثار و پیامدها، دامنه اثرگذاری، شیوه تحقق و آسیب‌پذیری و ۳۶ مؤلفه تهدیدات سایبری مراکزداده انجام و نتایج در قالب الگوی مفهومی ارائه شده است.

کلمات کلیدی: الگوی طبقه‌بندی، زیرساخت حیاتی، تهدیدات سایبری، طبقه‌بندی تهدیدات، مرکز داده

۱. دانشجوی دکتری مدیریت سیستم‌ها دانشگاه تهران، *Aghaeemh@ut.ac.ir*
۲. استاد و عضو هیات علمی دانشکده علوم مهندسی پردیس دانشکده‌های فنی دانشگاه تهران *Moeini@ut.ac.ir*
۳. استادیار و عضو هیات علمی پژوهشگاه ارتباطات و فناوری اطلاعات(نویسنده مسئول) *Abouzar_arab@itrc.ac.ir*

مقدمه

در حال حاضر بیشتر فعالیت‌ها و تعاملات حوزه‌های اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشورها در فضای سایبر انجام می‌شود. توسعه و پیشرفت در بخش‌های اقتصادی و اجتماعی، رفاه عمومی، توانمندی دفاعی و امنیتی در کشورها نیازمند برخورداری از زیرساخت‌های مناسب است که در سند امنیت ملی ایالات‌متحده با عنوان ۱۷ زیرساخت حیاتی به آن‌ها اشاره شده است (سند امنیت ملی ایالات‌متحده، ۲۰۱۸، ۷). بنا بر گزارش سال ۲۰۱۷ موسسه گارتنر[1]، سرمایه‌گذاری توسعه زیرساخت‌های ارتباطی با استقبال فراوانی روبرو بوده است به‌طوری‌که بر اساس پیش‌بینی‌های این موسسه بازار این حوزه از حدود ۳۲۵۰ بیلیون دلار در سال ۲۰۱۶ به بیش از ۴۰۰۰ بیلیون دلار در سال ۲۰۲۲ خواهد رسید (گارتنر، ۲۰۱۷، ۲۷).

ساختار نامتعارف، رشد سریع و نامتوازن شبکه‌های ناهمگون به‌هم‌پیوسته، آسیب‌پذیری‌ها، تهدیدهای متنوع و حوادث خطرناک با دامنه اثر بالا به همراه ناامنی و بروز چالش و اختلال در زندگی شهروندی و حتی تهدید برای امنیت ملی کشورها را به دنبال داشته است. برخی از این زیرساخت‌ها با توجه به نقش حیاتی خود در ارائه خدمات به دیگر زیرساخت‌ها در سطح ملی به‌عنوان زیرساخت‌های حیاتی شناخته می‌شوند و اختلال کوتاه‌مدت در آن‌ها تأثیر جدی بر پایداری، امنیت ملی و ایمنی جامعه دارد. جوزف ساموئل نای[2] نویسنده کتاب آینده قدرت، تأکید دارد «لایه اطلاعاتی فضای سایبر، از بازده فزاینده نسبت به مقیاس برخوردار و عرصه آن برای پایش قانونی مشکل است. پس بهتر است از حوزه اطلاعاتی با هزینه‌های پائین، تهدید را علیه لایه فیزیکی با منابع کمیاب و گران اعمال نمود» (جوزف ساموئل نای،۲۰۱۰: ۲۲). بخش زیادی از تهاجم‌های سایبری گسترده انجام شده سال‌های اخیر علیه زیرساخت‌های حیاتی کشورها، زیرساخت‌های اطلاعاتی و ارتباطی حیاتی و نیز مراکزداده[3] بر اساس این رویکرد قابل بررسی است.

دوگان[4] و میچالکسی[5](۲۰۰۹)، اعلام نموده‌اند که تحلیل و گونه‌شناسی تهدیدات سایبری زیرساخت‌های حیاتی مؤلفه کلیدی امنیت آن‌ها و پیش‌بینی، پایش و رفع آثار این تهدیدات مستلزم درک آن‌ها است که با بهره‌گیری از الگوی مفهومی و طبقه‌بندی تهدیدات سایبری فضای سایبر تسریع می‌شود (دوگان و میچالسکی، ۲۰۰۹: ۱۲). این موارد بیانگر این واقعیت است که برای ارتقاء امنیت زیرساخت‌های حیاتی مثل مراکزداده –به‌عنوان قلب تپنده و زیربنای اصلی فناوری اطلاعات و ارتباطات نوین–، درک، تحلیل و شناخت تهدیدات علیه این زیرساخت‌ها دارای اهمیت زیادی است زیرا استمرار فعالیت آن‌ها باعث

1. *WWW.GARTNER.COM*
2. *Joseph Nye*
3. *Data Center-DC (Internet Data Center-IDC)*
4. *David P. Duggan*
5. *John T. Michalski*

تداوم ارائه خدمات ملی می‌شود. پس شناسایی ساختارمند تهدیدات سایبری مراکزداده و الگوسازی آن‌ها –ضمن ارتقاء دانش و آگاهی در این حوزه– عامل توسعه قدرت تصمیمات راهبردی جهت ارتقاء امنیت سایبری زیرساخت‌های حیاتی اطلاعاتی و ارتباطی است.

شناخت ساختارمند این تهدیدات مستلزم بررسی الگوهای مختلف دسته‌بندی‌ها، طبقه‌بندی‌ها و رتبه‌بندی‌های تهدیدات سایبری علیه زیرساخت‌های حیاتی است. شناخت عمیق تهدیدات سایبری علیه مراکزداده زمینه‌ساز ارائه الگوی شامل ابعاد و مؤلفه‌های اصلی و مهم جهت توسعه دانش، ارتقاء قدرت مواجهه و تصمیم‌گیری در مراحل مختلف وقوع تهدید در مراکزداده است.

تهدید و تهاجم سایبری علیه زیرساخت‌های حیاتی، عدم پایداری[۱] امنیتی را به دنبال دارد (سند راهبردی پدافند غیرعامل، ۱۳۹۴، ۴). اجرای برنامه‌های امنیت سایبری نهادها و سازمان‌ها برگرفته از راهبردها و سیاست‌های کلان، ارتقادهنده قدرت پیش‌بینی، مدیریت و مقابله با تهدیدات سایبری، کاهش‌دهنده پیامدهای مخرب بروز تهدیدها و تسهیلگر در بازسازی حوزه‌های آسیب‌دیده با کمترین هزینه است. کارشناسان امنیت سایبری معتقدند که امنیت سایبری باید به شکل دغدغه در بدنه حاکمیت هر کشور نهادینه شود و فرهنگ‌سازی آن در نهادهای دولتی از اهمیت بالاتری برخوردار است (قوچانی، حسین‌پور، ۱۳۹۶،۷). براین‌اساس ضرورت دارد اقدامات مناسب برای مواجهه فعال با تهدیدات سایبری زیرساخت‌های حیاتی بخصوص مراکزداده انجام شود.

مؤسسه پست‌نوت[۲] در سال ۲۰۱۷ اعلام نمود که آثار مخرب تهدید سایبری منجر به حمله در سال ۲۰۱۵ به مرکز داده زیرساخت توزیع نیروی برق کشور اوکراین و قطع برق ۲۲۵/۰۰۰ مشترک تا چند ماه ادامه داشت (پست نوت، ۲۰۱۷). همچنین به گزارش سایت آی‌تی‌ایران[۳] تهاجم سایبری فروردین‌ماه ۱۳۹۷ منجر به اختلال در فعالیت برخی از مراکزداده، سرویس‌دهنده‌ها و تعداد زیادی از سایت‌های جمهوری اسلامی ایران و برخی کشورها به‌طور هم‌زمان شد (سایت آی‌تی‌ایران، ۱۳۹۷). این رخداد به‌واسطه وجود ضعف امنیتی در برخی سوییچ‌های شبکه[۴] مراکزداده حادث شده است. به گزارش شرکت سانز[۵]، تغییرات زیاد معماری مراکزداده امروزی در شرکت‌های بزرگ، مراکزداده سنتی را ملزم به تجهیز زیرساخت‌هایی از ابر ترکیبی نموده است که به شکلی پویا مدیریت می‌شوند (سانز، ۲۰۱۵). این گستردگی فناوری، تهدیدات سایبری متنوع‌تر در حوزه رایانش ابری را به وجود می‌آورد.

مدیریت و کاهش آثار بروز تهدیدات، ارتقاء قدرت تصمیم‌سازی و تصمیم‌گیری و درنتیجه ایجاد و استمرار امنیت سایبری زیرساخت‌های حیاتی اطلاعاتی و ارتباطی با محوریت "مراکزداده" نیازمند شناسایی

---

۱. اصل پایداری از اصول پدافند غیرعامل است. (سند راهبردی پدافند سایبری جمهوری اسلامی ایران، ۱۳۹٤)

2. POSTNOTE (Cyber Security of UK Infrastructure)

3. https://itiran.com

4. CISCO Network Switch

5. SANS, The State of Dynamic Data Center and Cloud Security in the Modern Enterprise, 2015

تهدیدات سایبری علیه این زیرساخت‌ها در ابعاد مختلف برای مواجهه فعال و خردمندانه در شرایط قبل از وقوع، در زمان وقوع و بعد از وقوع تهدیدات است. به‌کارگیری الگوی مفهومی خاص تهدیدات سایبری مراکزداده به‌عنوان پیش‌نیاز اقدامات مدیریت امنیت سایبری مطرح است. دست‌یابی به این مهم –در قالب ارائه الگوی مفهومی تهدیدات سایبری مراکزداده– اهمیت زیادی در ارتقاء سطح نگرش و شناسایی فراگیر این تهدیدات و نیز ارتقاء قدرت تصمیم‌گیری برای حفظ و گسترش امنیت سایبری این زیرساخت‌های حیاتی دارد.

در این تحقیق تمرکز بر گونه‌ای از تهدیدات سایبری است که بر اساس نوع، حوزه اثر و تأثیرگذاری بر پایداری امنیتی بخش خاصی از سرمایه‌ها و دارایی‌های مراکزداده مؤثر هستند و به‌عنوان تهدیدات سایبری مراکزداده شناخته می‌شوند. علیرغم وجود الگوهای مختلف طبقه‌بندی تهدیدات سایبری در تحقیقات داخلی و خارجی الگو خاص مورد هدف این تحقیق تاکنون برای طبقه‌بندی تهدیدات سایبری چنین زیرساخت‌هایی ارائه نشده است و جمع‌آوری منابع مرتبط نیز به شکلی نظام‌مند انجام شده است. براین‌اساس به‌واسطه خلأ دانشی این حوزه مسئله اصلی تحقیق این است که: "الگوی مفهومی ساختار تهدیدات سایبری مراکزداده چیست؟"

بررسی‌ها، نیازسنجی‌ها و پیش‌بینی محقق نشان‌دهنده دلایل اهمیت انجام این تحقیق به شرح ذیل است:

- ✓ ارتقاء سطح شناخت تهدیدات سایبری زیرساخت‌های حیاتی اطلاعاتی و ارتباطی
- ✓ شناخت ساختار اقدامات تهدیدآمیز سایبری علیه مراکزداده جهت مواجهه فعال با آن‌ها
- ✓ ارتقاء قدرت تصمیم‌سازی و تصمیم‌گیری به‌منظور مدیریت امنیت در مراکزداده

و بررسی‌های اولیه نشان می‌دهد پیامدهای عدم انجام این تحقیق به شرح زیر هستند:

- ✓ افزایش میزان خسارات اقدامات تهدیدآمیز سایبری علیه زیرساخت‌های حیاتی
- ✓ ضعف در شناسایی تهدیدات مراکزداده و افول قدرت مدیریت امنیت سایبری در سطح این زیرساخت‌ها
- ✓ افول قدرت و توانمندی در مواجهه فعال نسبت به تهدیدات سایبری مراکزداده در گذر از وضعیت سنتی به جدید

نقشه راه کلی انجام این تحقیق جهت شناخت ساختار و ارائه الگوی مفهومی تهدیدات سایبری مراکزداده چنین بوده است که ابتدا مفهوم‌شناسی متغیرها، پیشینه‌شناسی و بررسی ادبیات موضوعی با گردآوری داده‌ها با روش فراترکیب انجام می‌شود. این روش برای شناسایی تهدیدات سایبری زیرساخت‌های حیاتی اطلاعاتی و ارتباطی کاربرد دارد. دراین‌راستا ضمن شناسایی و تعریف متغیرهای تحقیق، تعریف محوری "تهدیدات سایبری مراکزداده" ارائه شد. سپس ابعاد و مؤلفه‌های شناسایی و تحلیل تهدید استخراج و

در قالب الگوی مفهومی ارائه شدند. این نتایج با شاخص ضریب کاپا مورد اعتبارسنجی قرار گرفتند. در بخش انتهایی و بر اساس تأیید مفاد مندرج در الگوی مفهومی شناخت تهدیدات سایبری مراکزداده، پاسخ به سؤالات تحقیق انجام و پیشنهادهایی ارائه شده است.

هدف این تحقیق ارائه الگو شناخت ساختار تهدیدات سایبری مراکزداده به شکلی است که با ارائه آن بتوان روند شناسایی این تهدیدها را در قالبی ساختاریافته (با قدرت شناسایی بیشتر و خطای کمتر) مورد توجه قرار داد. بنابراین هدف اصلی این تحقیق عبارت است از: "ساختارشناسی تهدیدات سایبری مراکزداده در قالب ارائه الگوی مفهومی" که بر این اساس اهداف فرعی به شرح ادامه پی‌گیری می‌شوند.

- ✓ شناخت تهدیدات سایبری رایج علیه زیرساخت‌های حیاتی اطلاعاتی و ارتباطی
- ✓ شناخت طبقه‌بندی‌های تهدیدات سایبری در سطح زیرساخت‌های حیاتی اطلاعاتی و ارتباطی
- ✓ شناخت ابعاد و مؤلفه‌های تهدیدات سایبری مراکزداده

بر این اساس سؤال اصلی تحقیق عبارت است از اینکه: الگوی مفهومی برای ساختارشناسی تهدیدات سایبری مراکزداده چیست؟ و سؤالات فرعی عبارتند از اینکه

- ✓ تهدیدات سایبری رایج علیه زیرساخت‌های حیاتی کدامند؟
- ✓ طبقه‌بندی‌های مطرح تهدیدات سایبری زیرساخت‌های حیاتی اطلاعاتی و ارتباطی کدامند؟
- ✓ تهدیدات سایبری علیه مراکزداده نوین دارای چه ابعاد و مؤلفه‌هایی هستند؟

روش‌شناسی تحقیق

نظر به ارائه الگوی مفهومی تهدیدات سایبری مراکزداده و نتایج عملیاتی آن که افزایش قدرت تصمیم‌سازی در حوزه امنیت سایبری زیرساخت‌های حیاتی (اطلاعاتی و ارتباطی) 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 فراترکیب نسبت به مراجعه به مقالات، کتاب‌ها، اسناد راهبردی و گزارش‌های پژوهشی اقدام و با بررسی نتایج و تفسیر آن‌ها، ابعاد، مؤلفه‌ها و شاخص‌های الگو ساختاری تهدیدات سایبری مراکزداده استخراج گردید. پایش کیفی یافته‌ها و ارزیابی آن‌ها با روش ضریب کاپا و با استفاده از فرمول و بر اساس استاندارد انجام شد.

در این تحقیق داده‌های کیفی با روش فراترکیب جمع‌آوری شده‌اند. این روش معرف مطالعه کیفی است که اطلاعات و یافته‌های استخراج‌شده از مطالعات کیفی دیگر با موضوع مشابه و مرتبط را بررسی می‌کند. سپس نمونه موردنظر از مطالعات کیفی انتخاب و بر اساس ارتباط آن‌ها با سؤال پژوهش گزاره‌های جدید

ساخته می‌شود (لیندگرین و دیگران[1]، ۲۰۰۴: ۱۱). در این تحقیق از روش فراترکیب جهت مقایسه، تفسیر، تبدیل و ترکیب چارچوب‌ها و الگوهای ارائه‌شده تهدیدات سایبری مراکزداده استفاده شده است. در معرفی روش فراترکیب باید گفت که فراترکیب (مانند فراتحلیل) برای یکپارچه‌سازی چندین مطالعه و ایجاد یافته‌های جدید و تفسیر آن‌ها به‌کار می‌رود. بااین‌حال برخلاف فراتحلیل که بر داده‌های کمی و رویکردهای آماری تأکید دارد، فراترکیب بر مطالعات کیفی و تفسیر و تحلیل عمیق آن‌ها به جهت فهم عمیق‌تر توجه دارد (نقی‌زاده و همکاران، ۱۳۹۳: ۸).

پیشینه و سابقه پژوهش

احمد بختیاری و زورانی اسماعیل[2](۲۰۱۲) با تمرکز بر سامانه اطلاعات سلامت –به‌عنوان زیرساخت حیاتی– و با در نظر داشتن تغییر تهدیدات سایبری، بیش از ۷۰ تهدید را بر اساس ۳۰ معیار مشترک شناسایی، رتبه‌بندی و طبقه‌بندی نموده‌اند تا در ارزیابی مخاطرات از آن‌ها استفاده نمایند (بختیاری، زورانی، ۲۰۱۲، ۶).

در مقاله‌ای دیگر، مونا جوینی[3] و همکاران (۲۰۱۴)، به بررسی الگوهای طبقه‌بندی تهدیدات سایبری سامانه‌های اطلاعاتی پرداخته‌اند. آن‌ها بر مطالعه اثر کلاس تهدید به‌جای اثر یک تهدید و بررسی طبقه‌بندی‌های مختلف مخاطرات امنیتی تأکید داشته و الگوی ترکیبی طبقه‌بندی تهدیدات امنیت سایبری را بر اساس ارتباط تهدید با منبع، عامل، انگیزه، قصد و اثر (با هدف کمک به سازمان‌ها برای اجرای راهبردهای امنیت اطلاعات) ارائه نموده‌اند (جوینی، ۲۰۱۴، ۱۵).

همچنین کاجرلند[4](۲۰۱۵) با تحلیل حملات به سامانه‌های اسکادا[5]، الگویی را با تمرکز بر روش عملیات، اثر، عوامل و هدف تهدید برای طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی ارائه نموده است (کاجرلند، ۲۰۱۵، ۱۴).

محققان مؤسسه انای‌اس‌تی[6] با تألیف مقاله‌ای در سال ۲۰۱۶ نسبت به بررسی الگوسازی تهدیدات برای زیرساخت‌های مراکزداده ابری با محوریت سطح حمله، درخت حمله و نمودار حمله اقدام نموده‌اند (الحبشی و همکاران، ۲۰۱۶،۶).

از طرفی گزارش سال ۲۰۱۵ مؤسسه سانز بیانگر موارد خاص تهدیدات امنیتی در سطح مراکزداده و ساختارهای ابری است. ۵۰ درصد تهدیدات فوق مربوط به نرم‌افزارهای مخرب و نقص برنامه‌های کاربردی است (سانز، ۲۰۱۵). بر اساس گزارش سال ۲۰۱۹ این مؤسسه، تهدیدات فیزیکی نیز از تهدیدات مهم مراکزداده است (همان، ۲۰۱۹).

1. *Lindgreen, Palmer and Vanhamm*
2. *Zuraini Ismail*
3. *Mouna Jouini, Latifa Ben Arfa Rabai, Anis Ben Aissa*
4. *Kajerland*
5. *SCADA: Supervisory Control and Data Acquisition*
6. *NIST, National Institute of Standards and technology*

پنج تهدید مهم امنیت سایبری مراکزداده نیز از سوی شرکت امنیتی اینفوسک[1] در سال ۲۰۱۴ اعلام شده‌اند که عبارتند از: حملات منبع سرویس توزیع شده، حملات برنامه‌های وب، بهره‌برداری از ساختار سرویس نام دامنه، مشکلات مربوط به ارتباط اس‌اس آل و ضعف در تشخیص هویت و حملات بروت‌فورث. البته پایشگرهای مستقر در قلب مرکز داده می‌توانند این حملات را متوقف کرده، ترافیک رمزگذاری‌شده را بازرسی و تفتیش نمایند و از دسترسی غیرمجاز به برنامه‌ها جلوگیری کنند (اینفوسک، ۲۰۱۴).

موسسه اِنیسا (۲۰۱۷) در گزارش سالیانه خود تهدیدات سایبری با فرکانس تکرار زیاد را مشخص، تشریح و رتبه‌بندی نموده است (انیسا،۲۰۱۷). این تهدیدات و نظرات مؤسسات و نهادهای امنیت سایبری در ادامه ارائه شده‌اند. موارد یادشده در گزارش پژوهشگاه ارتباطات و فناوری اطلاعات –پژوهشکده امنیت ارتباطات و فناوری اطلاعات– گروه ارزیابی امنیت شبکه و سامانه‌ها (۱۳۹۶) نیز تحلیل، بررسی و تأیید شده‌اند. این نتایج در قالب جدول (۱) ارائه شده است.

جدول (۱)– لیست تهدیدات سایبری و نظرات مؤسسات و نهادهای امنیت سایبری

تهدیدات سایبری	سازمان‌ها، نهادها و منابع علمی امنیت سایبری												
	Symantecc	Kaspersky	McAfee	ENISA	Esset	Cisco	Accenture	iDefense	NTT Security	Data Gravity	NOPSEC	Check Point[2]	Trend Micro[3]
بدافزار	▣	▣	▣	▣	▣	▣			▣	▣	▣		▣
حملات مبتنی بر وب	▣			▣									
برنامه‌های کاربردی وب	▣			▣									
جلوگیری از سرویس	▣	▣		▣		▣	▣	▣			▣		▣
بات‌نت				▣		▣						▣	
فیشینگ	▣	▣		▣		▣	▣	▣			▣		▣
هرزنامه	▣	▣		▣		▣							
باج‌افزار	▣	▣	▣	▣	▣						▣	▣	
تهدیدهای داخلی				▣		▣							
دست‌کاری فیزیکی/ آسیب/ سرقت/ فقدان	▣			▣									

1. InfoSec

۲. Check Point شرکت فعال رژیم اشغالگر قدس در حوزه امنیت سایبری، ارائه‌کننده محصولات امنیتی سایبری حفاظت از شبکه‌ها و زیرساخت‌های حیاتی، گزارش سال ۲۰۱۸

۳. Trend Micro شرکت فعال آمریکایی در حوزه اطلاع‌رسانی امنیت سایبری، گزارش سال ۲۰۱۵

تهدیدات سایبری	سازمان‌ها، نهادها و منابع علمی امنیت سایبری													
	Symantecc	*Kaspersky*	*McAfee*	*ENISA*	*Esset*	*Cisco*	*Accenture*	*iDefense*	*NTT Security*	*Data Gravity*	*NOPSEC*	*Check Point*[2]	*Trend Micro*[3]
کیت‌های بهره‌بردار	▣	▣		▣	▣	▣							
نقض‌داده				▣									
سرقت هویت	▣			▣									
نشت اطلاعات		▣		▣									
جاسوسی سایبری			▣	▣	▣	▣	▣	▣					
فریب معکوس							▣	▣					
رمز ارزها							▣	▣				▣	
نشانه‌گذاری کاذب									▣				
اینترنت اشیاء											▣	▣	
مهندسی اجتماعی											▣		
خطای انسانی											▣		
هکتیویسم													▣

علی اسماعیلی و جلال ثنا قربانی (۱۳۹۶) در تحقیق خود به برنامه‌سازی پیرامون آینده‌های محتمل و مطلوب تهدیدات سایبری، ابعاد، مؤلفه‌ها و شاخص‌های تهدیدات سایبری مهم زیرساخت‌های حیاتی پرداخته‌اند. آن‌ها الگوی پایش تهدیدات و شناسایی تهدیدات آینده را جهت جلوگیری از غافلگیری ارائه نموده‌اند (اسماعیلی، ثنا قربانی، ۱۳۹۶، ۱۲).

پژوهشگران پژوهشکده امنیت ارتباطات و فناوری اطلاعات (۱۳۹۵) در گزارشی به بررسی اجزاء مرکز داده پرداخته‌اند. براین‌اساس مرکز داده از چهار جزء فیزیکی، پردازشی و محاسباتی، ارتباطی و ذخیره‌سازی تشکیل شده است (قرایی، ۱۳۹۵، ۳۳).

استانداردهای امنیتی بر پایه مخاطرات، تهدیدها و حملات خاص مراکزداده تعیین و بر اساس آن الزامات امنیتی فیزیکی، عملیاتی و پردازشی، ارتباطی و شبکه، ذخیره‌سازی اطلاعات، معماری امنیتی و تجهیزات امنیتی و الزامات پدافندی شناسایی شده‌اند (همان، ۱۲). بدیهی است بخشی از تهدیدات معطوف به اجزاء ذکرشده هستند. در این خصوص گروهی دیگر از پژوهشگران آن پژوهشکده –در گزارش

تحقیقاتی[1]. ضمن شناسایی و صورت‌بندی پیشران‌های امنیتی به بررسی سه بعد نوع تهدید، عوامل تهدید و بردار حمله در مورد تهدیدات سایبری تأکید نموده‌اند (عرب‌سرخی و همکاران، ۱۳۹۶، ۴۵).

در سند راهبردی پدافند سایبری (جدول ۲)، تهدیدات سایبری در چهار سطح فردی، اجتماعی، امنیت ملی و بین‌المللی و اطلاعات بر اساس منشأ، هدف، کارکرد مقابله و سطوح اقدام صورت‌بندی شده است (سند راهبردی پدافند سایبری، ۱۳۹۴، ۲۲).

جدول (۲)– سطح‌بندی تهدیدات سایبری (سند راهبردی پدافندی سایبری کشور، ۱۳۹۴)

سطح تهدید	منشأ تهدید	سطح امنیت	هدف تهدید	کارکرد مقابله	سطوح اقدام
سطح فردی	فرد هکر	امنیت فردی	رایانه فرد	ایمنی	تاکتیکی
سطح اجتماعی	گروه هکری	امنیت اجتماعی	شبکه‌های کارکردی	امنیت	عملیاتی
سطح امنیت ملی	دولت هکر	امنیت ملی	زیرساخت‌های حیاتی	دفاع	استراتژیک
سطح بین‌المللی	ترکیبی	امنیت بین‌المللی	زیرساخت‌های بین‌المللی	تهاجم	فراملی و بین‌المللی

مفاهیم و مبانی نظری

مفهوم شناسی متغیرهای پژوهش

"تهدید سایبری" در واژه‌نامه امنیت سایبری مشترک ایالات‌متحده و روسیه (۲۰۱۴) به‌عنوان "خطری با قابلیت برقراری ارتباط با آسیب‌پذیری سایبری برای فعال نمودن آن" تعریف شده است (واژه‌نامه امنیت سایبری مشترک ایالات‌متحده و روسیه: ۲۰۱۴، ۳۸). این مفهوم در سند راهبردی پدافند سایبری جمهوری اسلامی ایران چنین آمده است:"هر رویداد یا واقعه با قابلیت واردنمودن ضربه به مأموریت‌ها، وظایف، تصویر دستگاه متولی، سرمایه ملی سایبری یا پرسنل دستگاه به‌واسطه سامانه اطلاعاتی، دسترسی غیرمجاز، تخریب (انهدام)، افشاء، تغییر اطلاعات و یا ممانعت از (ایجاد اختلال در) ارائه خدمت معرف تهدید سایبری است" (سند راهبردی پدافند سایبری جمهوری اسلامی ایران، ۱۳۹۴، ۲۴). نظر به موارد ارائه‌شده، تعریف عملیاتی این متغیر "رویداد یا واقعه‌ای با قابلیت واردنمودن ضربه به اهداف، عملکرد و کارکنان مرتبط با سرمایه ملی سایبری، با به‌کارگیری آسیب‌پذیری موجود از طریق دسترسی غیرمجاز، انهدام، افشاء، تغییر اطلاعات و یا ممانعت از ارائه خدمت" است.

مفهوم کلیدی دیگر "زیرساخت‌های حیاتی" است که دولت انگلیس (۲۰۱۱) در گزارشی تحت عنوان "محافظت از زیرساخت‌های حیاتی در کشور بریتانیا" به آن اشاره کرده است. زیرساخت‌های ملی حیاتی

۱. تبیین ملاحظات امنیتی در حوزه ارتباطات و فناوری اطلاعات

کشور قسمتی از زیربناهای کشور تلقی شده‌اند که تداوم فعالیت آن‌ها برای کشور حیاتی و ازکارافتادگی، تأخیر طولانی در خدمات‌رسانی، قطع خدمات و یا خدمات‌رسانی ناصحیح آن‌ها ضمن پیامدهای سنگین برای دولت و جامعه موجب لطمات جدی به بدنه اقتصادی و اجتماعی می‌شود (راهبرد امنیت سایبری انگلستان،۲۰۱۱، ۱۱). در سند راهبردی پدافند غیرعامل جمهوری اسلامی ایران (۱۳۹۱)، مراکز حیاتی معرف مراکزی هستند که انهدام کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات جدی و مخاطره‌آمیز در نظام سیاسی، هدایت، پایش و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری ملی شود (سند راهبردی پدافند غیرعامل جمهوری اسلامی ایران، ۱۳۹۱، ۷). پس زیرساخت حیاتی چنین تعریف می‌شود: **"مجموعه عناصر به‌هم‌پیوسته** در قالب زیربناهایی با ابعاد فناورانه گسترده، ارائه‌دهنده خدمات حیاتی برای ایمنی عمومی، پایداری اقتصادی، امنیت ملی، پایداری بین‌المللی، تاب‌آوری و چارچوبی برای پشتیبانی از ساختارهای کلان که انهدام کل یا قسمتی از آن‌ها، سبب بحران، آسیب و صدمات جدی و مخاطره‌آمیز در نظام سیاسی، هدایت، پایش و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری ملی شود".

همچنین در واژه‌نامه امنیت سایبری مشترک ایالات‌متحده و روسیه (۲۰۱۴)، "زیرساخت سایبری حیاتی" معرف زیرساخت سایبری است که برای خدمات ایمنی عمومی، پایداری اقتصادی، امنیت ملی، پایداری بین‌المللی و تاب‌آوری و استقرار مجدد فضای سایبر حیاتی نقش اساسی دارد. در این سند فناوری اطلاعات و ارتباطات و فضای سایبر در ساختار ذیل (با عنوان چارچوب هشت‌بعدی) نمایش داده می‌شود (واژه‌نامه امنیت سایبری مشترک ایالات‌متحده و روسیه: ۲۰۱۴، ۲۱).

جدول (۳)– چارچوب هشت‌بعدی زیرساخت فناوری اطلاعات و ارتباطات

منابع انسانی	ظرفیت	نرم‌افزار	نیرو (برق)
خط‌مشی	شبکه‌ها	سخت‌افزار	محیط

در کتاب راهنمای مرکز مشارکتی نخبگان دفاع سایبری ناتو (۲۰۱۲) برای سه مفهوم زیرساخت، زیرساخت حیاتی و زیرساخت اطلاعاتی و ارتباطی حیاتی چنین آمده است که: زیرساخت یا ستون فقرات معرف عوامل ساختاری به‌هم‌پیوسته‌ای هستند که به‌مثابه تکیه‌گاه برای یک سازه عمل می‌نمایند و ضربه به این عوامل، موجب گسیختگی سازه خواهد شد (مرکز مشارکتی نخبگان دفاع سایبری ناتو، ۲۰۱۲، ۱۵).

از سال‌ها پیش زیرساخت‌های برق، انرژی، آب، سلامت، پولی و مالی، آموزش و پژوهش، حمل‌ونقل، زیرساخت ارتباطات و فناوری اطلاعات و سایر زیرساخت‌ها به‌عنوان زیرساخت‌های حیاتی مطرح بوده‌اند (همان، ۲۵). براین‌اساس "زیرساخت‌های حیاتی" معرف زیرساخت‌هایی هستند که نقش حیاتی در توسعه

اقتصادی و اجتماعی، افزایش سطح رفاه عمومی، ارتقاء توان دفاعی و امنیتی و تأمین نیازمندی‌های ضروری هر کشور دارند و اختلال حتی کوتاه‌مدت در عملکرد آن‌ها تأثیر فاجعه‌باری بر امنیت ملی، اقتصاد ملی، سلامت و ایمنی و اطمینان عمومی و اداره امور کشور دارد.

در سال ۲۰۱۰ دیوید کلارک الگوی چهار لایه‌ای فضای سایبر را معرفی نمود (شکل-۱). این الگو دربرگیرنده لایه‌های انسانی، اطلاعاتی، منطقی و فیزیکی است. در این الگو ضمن تفهیم نقاط پایش فضای سایبر و اینترنت بر بعد فیزیکی فضای سایبر به‌عنوان لایه‌ای بسیار مهم تمرکز شده که زیرساخت‌های اطلاعاتی و ارتباطی را در برمی‌گرفت. در این الگو لایه منطقی شامل مجموعه‌ای از سکوهای[1] جدید، لایه اطلاعات متضمن اطلاعات، ویدئو، کلان‌داده، اطلاعات ایستا، پویا و لایه انسانی دربرگیرنده کاربران غیرفعال فضای سایبر و افرادی با هر شکل وابستگی به این فضا هستند (کلارک، ۲۰۱۰، ۱۰).

شکل (۱) – الگوی چهار لایه‌ای فضای سایبر (کلارک، ۲۰۱۰)

همچنین الگوی ارائه شده از سوی مرکز ملی فضای مجازی معرف الگوی شش لایه‌ای فضای سایبر است که در مراجع داخلی به‌عنوان الگوی مرجع انتخاب شده است (مرکز ملی فضای مجازی، ۱۳۹۶). این الگو در قالب شکل (۲) به تصویر کشیده شده است.

مدیریت و مقررات (حکمرانی)	کاربر	امنیت
	محتوا	
	خدمات	
	بستر (زیرساخت)	

شکل (۲) – الگوی شش لایه‌ای فضای سایبر (شورای عالی فضای مجازی، ۱۳۹۶)

با توجه به موارد فوق، تعریف عملیاتی "زیرساخت اطلاعاتی و ارتباطی حیاتی" چنین در نظر گرفته می‌شود: "زیرساخت اطلاعاتی و ارتباطی که برای ایجاد و استمرار خدمات حیاتی جهت ایمنی عمومی، پایداری اقتصادی، امنیت ملی، پایداری بین‌المللی و استقرار و تاب‌آوری فضای سایبر حیاتی –با به‌کارگیری

1. *Platforms*

امکانات سخت‌افزاری، نرم‌افزاری، شبکه‌ای و ارتباطی به‌منظور دستیابی مطلوب به اطلاعات-، نقش اساسی را ایفا می‌کند." از انواع مهم این زیرساخت‌ها می‌توان به "مراکزداده" اشاره نمود که بررسی تهدیدات سایبری علیه آن‌ها موردنظر این تحقیق است.

"تهدید سایبری زیرساخت‌های حیاتی اطلاعاتی و ارتباطی" نیز چنین تعریف می‌شود: "رویداد، واقعه و یا اقدام احتمالی متخاصمین بالقوه و بالفعل بر اساس انگیزه با هدف اختلال در سامانه‌ها و مؤلفه‌های نرم‌افزاری و سخت‌افزاری، ضربه به مأموریت‌ها، وظایف، اعتبار زیرساخت‌های اطلاعاتی و ارتباطی حیاتی یا کارکنان آن، با استفاده از ابزارها، به‌واسطه سامانه اطلاعاتی با دسترسی غیرمجاز، انهدام، افشاء، تغییر اطلاعات و یا ممانعت از ارائه خدمت و روش خاص با اثرگذاری عملیاتی و اطلاعاتی، برگرفته از آسیب‌پذیری‌ها، خطرهای انسانی، سامانه‌ای و ایجاد آثار مخاطره‌آمیز در سطح امنیت ملی است."

با توجه به تمرکز تحقیق بر "مراکزداده" به‌عنوان زیرساخت‌های حیاتی اطلاعاتی و ارتباطی و بررسی وضعیت تهدیدهای سایبری علیه آن‌ها، در این بخش مفهوم مذکور واکاوی می‌شود. در مقاله ارائه‌شده از سوی نپ[1] (۲۰۱۴) مرکز داده به‌عنوان مخزن مرکزی برای ذخیره‌سازی، مدیریت و پخش داده به‌منظور پشتیبانی از یک اقدام اقتصادی یا یک سازمان تعریف شده است (نپ، ۲۰۱۴، ۸). امروزه ایجاد این زیرساخت‌ها برای حفظ و نگهداری اطلاعات و در راستای میزبانی از سرویس‌های الکترونیکی (نظیر آموزش از راه دور، دولت الکترونیکی، اینترنت ملی و...) در هر کشور ضروری و منطقی است. مرکز داده معرف مجموعه سرویس‌دهنده‌ها، زیرساخت‌های ارتباطی و برنامه‌های کاربردی برای ارائه سرویس، نگهداری و پشتیبانی اطلاعات شبکه -با سرعت و امنیت بالا- است. برخی از مراکزداده بزرگ فعال در شرکت‌هایی همچون گوگل، آمازون، یاهو و مایکروسافت با استفاده از فناوری‌های جدید مثل رایانش ابری[2]، سامانه‌های هوشمند[3]، کلان‌داده‌ها[4] و داده‌کاوی با سرعت بالا[5] خدمات بهتر، پرسرعت و شبانه‌روزی را ارائه می‌کنند.

در سند تدوین ملاحظات پدافند غیرعامل در طراحی و ساخت مراکزداده (۱۳۸۷) چنین آمده است:"مرکز داده مکانی است با امنیت فیزیکی و الکترونیکی بالا، برخوردار از پهنای باند ارتباطی وسیع، متصل به شبکه‌های رایانه‌ای ملی و جهانی، با خدمات تمام‌وقت و در دسترس، دارای انواع تجهیزات سخت‌افزاری (رایانه‌ها، کلیدها، مودم‌ها و مسیریاب‌ها...) و نرم‌افزارهای (پایگاه داده، سرویس‌دهنده‌ها، سامانه عامل و ...) پیشرفته، برخوردار از پشتیبانی و نگهداری حرفه‌ای همراه با ارائه انواع خدمات مرتبط با اطلاعات و داده‌ها (از قبیل خدمات ذخیره، نگهداری و بازیابی داده‌ها، میزبانی خدمات اینترنتی[6]،

1. *Kenneth J. Knapp*
2. *Cloud Computing*
3. *Smart SYSTEMS*
4. *Big DATA*
5. *High speed DATA Mining*
6. *ISP*

میزبانی خدمات کاربردی، میزبانی برون‌سپاری خدمات و ...) برای کلیه اشخاص حقوقی و حقیقی دولتی و غیردولتی" (تدوین ملاحظات پدافند غیرعامل در طراحی و ساخت مراکزداده، ۱۳۸۷). به‌عبارت‌دیگر مراکزداده مجموعه‌ای عظیم از سامانه‌های سخت‌افزاری و نرم‌افزاری هستند که با داشتن تأسیسات کاملاً مجهز و پیشرفته و با تعداد زیادی پرسنل مجرب و متخصص در حوزه‌های متنوع مشغول به کار هستند (همان). همچنین در پروژه تحقیقاتی انجام شده در پژوهشکده امنیت پژوهشگاه فناوری اطلاعات و ارتباطات (۱۳۹۴) مرکز داده معرف مکانی با سامانه‌های کامپیوتری و تجهیزات جانبی مربوطه مانند سامانه‌های ذخیره‌سازی و ارتباطی تعریف شده است (قرایی، ۱۳۹۴، ۱۲).

شرکت سرور ایران[1]، مرکزداده را مجموعه سرویس‌گرها، زیرساخت‌های ارتباطی/ امنیتی و تجهیزات الکترونیکی برای ارائه، نگهداری و پشتیبانی از سرویس‌های تحت شبکه (اینترنت/ اینترانت/ اکسترانت) معرفی کرده است. این مراکز به انواع سازمانی، تجاری و دانشگاهی، خصوصی، فراهم‌کننده‌های سرویس، مراکزداده اینترنتی و فراسازمانی و محلی تقسیم می‌شوند.

بنابراین تعریف عملیاتی"مرکز داده" چنین است: "مجموعه‌ای عظیم از سامانه‌های سخت‌افزاری و نرم‌افزاری مستقر در تأسیسات کاملاً مجهز و پیشرفته با تعداد مناسب پرسنل مجرب و متخصص برای خدمات: میزبانی وب، پروتکل انتقال فایل، محیط گپ، خدمات نام دامنه، پست الکترونیک، انباشت موقت، دسترسی باند پهن که دسترسی به آن از طریق شبکه‌های رایانه‌ای، شبکه خصوصی مجازی و خدمات کاربردی فناوری اطلاعات با در نظر داشتن الزامات مدیریتی و امنیتی به وجود می‌آید". بنابراین"تهدید سایبری مرکز داده"معرف"رویداد، واقعه یا اقدام احتمالی متخاصمین بالقوه و بالفعل بر اساس انگیزه با هدف اختلال در مؤلفه‌های نرم‌افزاری و سخت‌افزاری، مأموریت‌ها، وظایف و اعتبار مرکز داده با استفاده از ابزارها و دسترسی غیرمجاز، انهدام، افشاء، تغییر اطلاعات و ممانعت از ارائه خدمت با روش و اثرگذاری عملیاتی و اطلاعاتی و استفاده از آسیب‌پذیری‌ها و تأثیر بر امنیت ملی کشور" است. "الگو" نیز ابزار کمکی ارائه و تجسم روابط مابین متغیرها و عوامل مهم مسئله تحقیق است (منصوریان، ۱۳۹۲،۱۲).

تجزیه‌وتحلیل یافته‌ها

در گام اول اجرای تحقیق با روش فراترکیب باید هدف اصلی پژوهش آشکار شود. هدف این پژوهش «تبیین رابطه بین تهدیدات سایبری مراکزداده و ساختار آن‌ها» است. همچنین مشخص کردن سؤالات پژوهش، واژه‌های کلیدی و منابع جستجو که در ادامه مورد بررسی قرار می‌گیرند.

- چه چیزی: شناسایی رابطه تهدیدات سایبری زیرساخت‌های حیاتی و طبقه‌بندی آن‌ها موردمطالعه

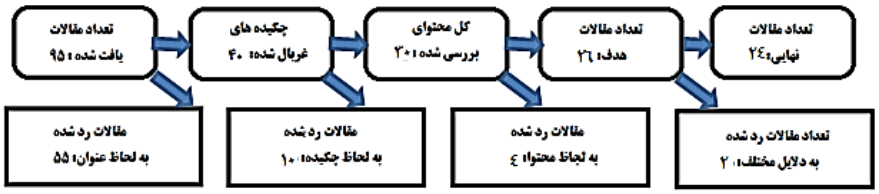
1. www.serveriran.net

قرار گرفت؛

- جامعه مطالعه: پایگاه‌های اطلاعاتی ساینس‌دایرکت، اسکوپوس، ژورنال امنیت اطلاعات، پایگاه‌های داده گوگل و مرکز اسناد و منابع علمی کتابخانه مرکزی دانشگاه تهران؛
- محدوده زمانی: با توجه به مستندات قابل‌دسترس محدوده زمانی منابع خارجی از سال ۲۰۱۲ تا ۲۰۱۸ است؛
- چگونگی روش: با روش تحلیل اسناد، داده‌های کیفی تحلیل شدند؛
- واژه‌های کلیدی: برخی از مهم‌ترین واژگان کلیدی مورد استفاده در جستجو عبارتند از: دسته‌بندی تهدیدات سایبری، تهدیدات سایبری زیرساخت‌های حیاتی، تهدیدات سایبری علیه مراکزداده، تهدیدات نوین سایبری علیه مراکزداده، الگوسازی تهدیدات سایبری زیرساخت‌های حیاتی، تهدیدات سامانه‌های اطلاعاتی و ابعاد تهدیدات سایبری زیرساخت‌های حیاتی.

به‌منظور بررسی و جستجوی انتخابی مقالات و منابع مرتبط، ابتدا به بررسی تناسب مقالات دریافتی با سؤال پژوهش و بازبینی مجموعه مطالعات منتخب در چندین مرحله و بر اساس ارتباط با موضوع تحقیق و موارد دیگر اقدام و سپس برخی منابع و مقالات از فرآیند بررسی و تحلیل فراترکیب جدا شدند. این روند در قالب شکل (۳) ارائه شده است.

برای استخراج مفاهیم و کُدهای مرتبط با موضوع پژوهش، در تمامی مراحل فراترکیب، به‌طور پیوسته مقالات منتخب جهت دستیابی به یافته‌های درون محتوایی مجزا (شامل مطالعه‌های اولیه و اصلی) چندین بار مرور شدند. در این فرایند محتوای منابع مستخرجه بررسی، کُدهای مرتبط انتخاب و مفاهیم و مقوله‌ها شکل گرفتند.



شکل (۳) – روند استخراج مقالات

پس از بررسی تناسب مقالات با پارامترهای مطالعه، کیفیت روش شناختی مطالعات ارزیابی می‌شوند. برخی مقالات به دلیل عدم اعتماد به یافته‌ها حذف و برای ارزیابی کیفیت مطالعات اولیه از روش CASP استفاده شد. با استفاده از ۱۰ سؤال مفهومی تحقیق کیفی طبق جدول (۴) و با تمرکز بر ۱۰ عامل، کل منابع جمع‌آوری، ارزیابی و رتبه‌بندی شدند. با در نظر گرفتن حداکثر ۵ امتیاز برای هر عامل و در کل ۵۰ امتیاز برای هر مقاله محقق نسبت به تعیین سطح امتیاز برای هر یک از منابع (مقالات)

اقدام نمود. در این تحقیق سطوح طبقه‌بندی در فرایند امتیازدهی به شرح ادامه در نظر گرفته‌شده است [عالی: ۵۰ – ۴۱ (E)، خیلی خوب: ۴۰ – ۳۱ (VG)، خوب: ۳۰ – ۲۱ (G)، متوسط: ۲۰ – ۱۱ (F)، ضعیف: ۱۰ – ۰ (P).]

جدول (۴)– امتیازات داده‌شده به مقالات نهایی پذیرفته‌شده

معیار مقاله	اهداف تحقیق	منطق روش	طرح تحقیق	نمونه برداری	جمع آوری داده‌ها	انعکاس پذیری	ملاحظات اخلاقی	دقت تجزیه و تحلیل	بیان روشن یافته‌ها	ارزش تحقیق	جمع
۱	٤	٤	٤	۳	٤	۲	۳	٤	۳	٤	۳۵
۲	۳	٤	۳	۳	۳	۳	٤	٤	۳	٤	۳٤
۳	٤	۳	٤	٤	۳	٤	۳	۳	۳	۳	۳٤
٤	٤	٤	۳	۳	۳	٤	٤	۳	٤	٤	۳۲
۵	٤	۳	٤	۳	۲	۲	٤	۳	۳	۳	۳۱
۶	٤	٤	٤	۳	۳	۳	٤	٤	٤	٤	۳۷
۷	٤	۳	٤	۳	٤	٤	۳	٤	٤	۳	۳۶
۸	٤	٤	٤	۳	٤	۳	٤	۳	۵	۳	۳۷
۹	٤	٤	۳	٤	۳	٤	۳	٤	۵	٤	۳۸
۱۰	٤	٤	٤	۲	۲	۳	٤	٤	٤	۳	۳٤
۱۱	٤	۳	٤	۳	٤	۳	۳	٤	۳	٤	۳۵
۱۲	٤	۳	٤	۳	٤	٤	۳	٤	۳	٤	۳۶
۱۳	٤	۲	۳	۳	۳	۳	٤	۳	٤	۳	۳۲
۱٤	٤	۳	٤	٤	۳	۳	٤	۳	۵	۳	۳۶
۱۵	٤	۳	۳	٤	٤	٤	٤	۳	٤	۳	۳۷
۱۶	٤	۳	۳	٤	۳	٤	٤	٤	٤	٤	۳۷
۱۷	٤	٤	۵	۳	۳	٤	٤	٤	٤	۳	۳۸
۱۸	٤	٤	٤	٤	۳	۳	٤	٤	۳	٤	۳۷
۱۹	٤	٤	۳	٤	۳	٤	٤	٤	۳	٤	۳۷
۲۰	٤	۳	۳	۳	٤	٤	۳	۳	٤	۳	۳٤
۲۱	٤	۳	۳	۳	۳	۳	٤	۳	٤	۳	۳۳
۲۲	٤	۳	٤	٤	۳	۳	٤	٤	۵	۳	۳۷
۲۳	٤	۳	٤	۳	۳	۳	٤	۲	۳	۳	۳۲
۲٤	۳	۳	٤	٤	۳	٤	۳	٤	٤	۳	۳۵

امتیاز منابع در حوزه تهدیدات امنیتی سایبری شبکه‌های عمومی، زیرساخت‌های حیاتی، زیرساخت‌های حیاتی اطلاعاتی و ارتباطی و مرکزداده به میزان حداقل ۳۱ و حداکثر ۳۸ بوده است. برای ترکیب یافته‌های کیفی، استخراج مقوله‌ها و ایجاد تفسیر یکپارچه و جدید از یافته‌ها، با شناخت مفاهیم، سازماندهی آن‌ها در قالب طبقه‌بندی مناسب برای بهترین توصیف انجام می‌شود. طبقه‌بندی مقوله‌ها و مؤلفه‌های مستخرج از منابع در قالب جدول (۵) ارائه شده است.

بُعد/مقوله	مؤلفه/مفاهیم مستخرجه (کد طبیعی)	منابع
فناوری تهدید	اقدامات بروز تهدید - سازو کار پشتیبانی تهدید - دانش تهدیدگر	مونا جوینی و لطیف بن عرفا (۲۰۱٤)؛ زورانی اسماعیل و احمد بختیاری شهری (۲۰۱۲)؛ کاجرلند (۲۰۱۵)؛ مگ‌لاراس و یونگ (۲۰۱۸)؛ علی اسماعیلی و جلال ثناقربانی (۱۳۹۶)؛ وزارت دفاع انگلستان، الفبای سایبر[1](۲۰۱۶؛ کیوان اسماعیلی (۱۳۹۷)، ابوذر عرب‌سرخی، فاطمه شبانی، اسما ایوازه، امین چاردولی، پروژه تحقیقاتی (۱۳۹۶)، سازمان پدافند غیرعامل، سند فرادستی (۱۳۹٤).
ریشه تهدید	انسان‌ها - دولت‌ها - سازمان‌های تروریستی - صنایع و کسب‌وکارها - عوامل محیطی- فناوری‌های نوظهور	زورانی اسماعیل، احمد بختیاری شهری (۲۰۱۲)؛ کاجرلند (۲۰۱۵)؛ مگ لاراس و یونگ (۲۰۱۸)؛ سازمان پدافند غیرعامل، سند فرادستی (۱۳۹٤)؛ وزارت دفاع انگلستان، کتاب الفبای سایبر (۲۰۱۶).
نوع تهدید	عمدی —غیرعمدی- نیمه عمدی	مونا جوینی و لطیف بن عرفا (۲۰۱٤)؛ زورانی اسماعیل و احمد بختیاری شهری (۲۰۱۲)؛ کیوان اسماعیلی (۱۳۹۷)؛ وزارت دفاع انگلستان، کتاب الفبای سایبر (۲۰۱۶).
علت تهدید	اقتصادی —سیاسی — امنیتی- دفاعی —فناورانه -اجتماعی	علی اسماعیلی و جلال ثناقربانی (۱۳۹۶)؛ سازمان پدافند غیرعامل، سند فرادستی (۱۳۹٤)؛ وزارت دفاع انگلستان کتاب الفبای سایبر (۲۰۱۶).
حوزه تهدید	انسانی - زیرساخت ارتباطی - زیرساخت داده‌ای - زیرساخت فیزیکی - زیرساخت‌های حیاتی	کاجرلند (۲۰۱۵)؛ احمد مکرم (۲۰۱٤)؛ محسن خواجوی و غلامرضا جلالی (۱۳۹۲)؛ سازمان پدافند غیرعامل، سند فرادستی (۱۳۹٤)؛ سازمان فناوری اطلاعات ایران، گزارش فنی الزامات امنیتی مرکز داده (۱۳۹۲)؛ حسین قرایی گرکانی پروژه تحقیقاتی الزامات پدافندی و امنیتی مراکزداده (۱۳۹۵)؛ وزارت دفاع انگلستان کتاب الفبای سایبر (۲۰۱۶).

1. *Cyber Primer, Concepts and Doctrine Centre*

بُعد/مقوله	مؤلفه/مفاهیم مستخرجه (کد طبیعی)	منابع
نتایج	داده و اطلاعات —خدمات - سازمان —زیرساخت - انسان	مونا جوینی و لطیف بن عرفا (۲۰۱٤)؛ کاجرلند (۲۰۱۵)؛ مگ لاراس و یونگ (۲۰۱۸)؛ وزارت دفاع انگلستان کتاب الفبای سایبر (۲۰۱۶).
حوزه اثر تهدید	محدوده، زیرساخت و میزان اثر تهدید	کاجرلند (۲۰۱۵)؛ نواف الحبشی و لینگو وانگ (۲۰۱۷)؛ محسن خواجوی و غلامرضا جلالی (۱۳۹۲)؛ علی اسماعیلی و جلال ثناقربانی (۱۳۹۶)؛ سازمان پدافند غیرعامل، سند فرادستی (۱۳۹٤).
روش تهدید	اجرای تهدید - بردار حمله - زمان‌بندی تهدید	کاجرلند (۲۰۱۵)؛ نواف الحبشی و لینگو وانگ (۲۰۱۷)؛ شیشیر کی سی (۲۰۱۸)؛ سازمان پدافند غیرعامل، سند فرادستی (۱۳۹٤)؛ ابوذر عرب‌سرخی، فاطمه شبانی، اسما ایوازه، امین چاردولی، پروژه تحقیقاتی (۱۳۹۶)، وزارت دفاع انگلستان کتاب الفبای سایبر (۲۰۱۶).
نوع آسیب‌پذیری	آسیب‌پذیری برنامه وب - آسیب‌پذیری سخت‌افزار و شبکه - آسیب‌پذیری نرم‌افزاری - آسیب‌پذیری انسانی	محسن خواجوی و غلامرضا جلالی (۱۳۹۲)؛ کیوان اسماعیلی (۱۳۹۷).

جدول (۵)- نمونه‌ای از واحدهایی معنایی و کدهای استخراج‌شده

پایش کیفیت (مرحله اول- گروه کانونی): جهت بررسی میزان اعتبار استنباط محققین در مورد واحدهای معنایی و کدهای استخراج‌شده که زمینه‌ساز ایجاد الگوی مفهومی است و همچنین برای تعمیق کیفی تحقیق، اعتبارسنجی کیفی موارد جدول فوق با استفاده از روش گروه کانونی در دو مرحله انجام شده است. ویلکینسون[1](۲۰۰۴) در این خصوص چنین بیان می‌کند که در این شیوه با حضور افراد در بحث گروهی غیررسمی (با چندین بحث (درباره یک موضوع یا مجموعه‌ای از موضوع‌ها انجام می‌شود (ویلکینسون، ۲۰۰۴، ۱۴). حسینی (۱۳۹۴) نیز بیان می‌کند که داده‌های کیفی به‌گونه‌ای فراهم می‌شود که به درک بیشتر محقق از ادراکات، احساسات و برداشت‌ها درباره مسائل مختلف کمک کند (حسینی، ۱۳۹۴، ۱۰). بنا بر نظر گلدمن[2](۱۹۶۲)، ازآنجاکه هدف تحقیق با گروه کانونی پرسیدن درباره «چرایی» است تا چه «تعدادی»، یعنی هدف، بیشتر تولید فرضیه‌ها است تا اثبات معرف بودن آن‌ها، پس مورد تردید قرار گرفتن پایایی اهمیت چندانی ندارد و ازآنجاکه بافت‌های موقعیتی و شرایط پیرامون، نقش مهمی در شکل‌گیری واکنش‌های افراد گروه ایفا می‌کنند، نمی‌توان مانند پژوهش‌های کمّی

1. wilkinson
2. Goldman

پایایی را مورد بررسی قرار داد (گلدمن، ۱۹۶۲، ۱۹). برنامه‌ریزی، هدایت و اجرای روش در تحقیق حاضر به شرح ادامه است.

ده نفر از متخصصان با محوریت اشتراک تخصص و تجربه در مورد مراکزداده و امنیت این زیرساخت برای حضور در جلسه و به‌منظور ارزیابی و اعتبارسنجی ابعاد و مؤلفه‌های اجزاء الگوی ساختاری تهدیدات سایبری مرکز داده با مشخصات ذیل به‌عنوان اعضاء گروه کانونی انتخاب شدند.

جدول (۶)– مشخصات اعضاء جلسه گروه کانونی

ردیف	ویژگی (دکتری، دانشجوی دکتری، کارشناس ارشد و کارشناس)	تعداد	درصد از کل جامعه
۱	اعضاء هیئت‌علمی آشنا به حوزه پژوهش	۲ نفر	%۲۰
۲	کارشناس فنی آشنا به حوزه پژوهش	٤ نفر	%٤۰
۳	مدیران عملیاتی آشنا به حوزه پژوهش	۳ نفر	%۳۰
۵	مدیران راهبردی و میانی آشنا به حوزه پژوهش	۱ نفر	%۱۰
	تعداد کل	۱۰	%۱۰۰

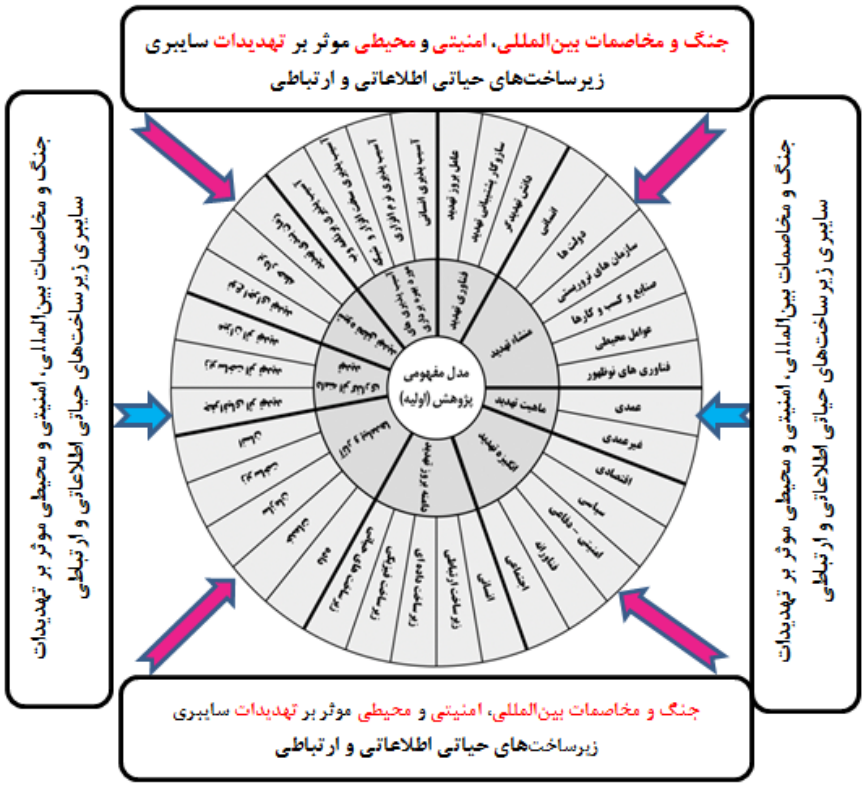
ابتدا با ارائه فرمی مشخصات کلی از اعضاء گروه اخذ گردید و برگزاری جلسه گروه کانونی بر اساس تمرکز بر اخذ نظرات اعضاء در مورد ۹ بعد در مرحله اول و ۳۶ مورد مؤلفه در مرحله دوم به این نحو انجام شد که ابتدا طرح سؤالات به شکل تشریحی و مکتوب و با ارائه حضوری انجام شد و روند پاسخگویی به‌صورت شنیداری و یادداشت انجام و نتایج ذیل بر اساس تحلیل‌های متنی، یادداشتی و حافظه‌ای ثبت شد و به‌صورت تحلیل منطقی به‌جای قیاسی و روش مقایسه ثابت اقدامات تحلیلی توسط محققین انجام شد و جهت تأیید به نماینده گروه کانونی تحویل و تأیید نهایی از ایشان دریافت شد. با توجه به توضیحات ارائه‌شده ۸ بعد به دلیل ماهیت و مفاهیم مرتبط تغییر یافت که تغییرات موردنظر به دلیل تمرکز اکثریت اعمال شد. همچنین به دلیل ماهیت مؤلفه‌ها، ۱۰ مورد از ۳۶ مورد مؤلفه نیز بر اساس نظر اکثریت تغییر یافت.

جدول (۷)– نتایج تغییرات اعمال‌شده بر اساس نظرات اعضاء گروه کانونی

بُعد/مقوله	مؤلفه/مفاهیم مستخرجه (کد طبیعی)
فناوری تهدید	عامل بروز تهدید - سازوکار پشتیبانی تهدید - دانش تهدیدگر
منشأ تهدید	انسانی - دولت‌ها - سازمان‌های تروریستی - صنایع و کسب‌وکارها - عوامل محیطی- فناوری‌های نوظهور
ماهیت تهدید	عمدی - غیرعمدی
انگیزه تهدید	اقتصادی –سیاسی –امنیتی/ دفاعی –فناورانه - اجتماعی

بُعد/مقوله	مؤلفه/مفاهیم مستخرجه (کد طبیعی)
دامنه بروز تهدید	انسانی - زیرساخت ارتباطی - زیرساخت داده‌ای - زیرساخت فیزیکی - زیرساخت‌های حیاتی
آثار و پیامدها	داده —خدمات - سازمان —زیرساخت - انسان
دامنه اثر گذاری تهدید	جغرافیای اثر تهدید - زیرساخت اثر تهدید - میزان اثر تهدید
شیوه تحقق تهدید	نوع اجرای تهدید - بردار حمله - زمان‌بندی تهدید
آسیب‌پذیری‌ها	آسیب‌پذیری برنامه وب - آسیب‌پذیری سخت‌افزار و شبکه - آسیب‌پذیری نرم‌افزاری - آسیب‌پذیری انسانی

بر اساس اعمال نظرات منتج از برگزاری دومرحله‌ای گروه کانونی، الگوی مفهومی در قالب شکل (۴) ارائه شده است.



شکل (۴) – الگوی مفهومی منتج از یافته‌های تحقیق

ابعاد ارائه‌شده در الگوی مفهومی فوق در قالب جدول (۸) تعریف شده‌اند. این تعاریف برگرفته از نتایج

مطالعات جداول (۵)، (۷) و بررسی‌های محقق به‌عنوان تعاریف پیشنهادی و عملیاتی در این تحقیق به‌کاررفته است.

جدول (۸) – تعاریف موردنظر برای ابعاد معرفی‌شده در الگوی مفهومی

ردیف	بعد	تعریف‌پیشنهادی
۱	فناوری	مجموعه روش‌ها، دانش و مهارت ساخت ابزار سخت یا نرم به شکلی ساده و پیچیده که بتواند اقدامات تهدیدآمیز علیه هدف را محقق نماید.
۲	منشأ	سرآغاز و محل اولیه تفکر، طراحی و اقدامات مربوط به عاملیت تهدید سایبری از مواضع داخلی و خارجی که با روش‌ها و ابزارها به‌عنوان فاعلیت و منشأ عمل تهدید با هویت انسانی و غیرانسانی (محیط و فناوری) اقدام به طراحی و اجرای تهدید سایبری می‌کند.
۳	ماهیت	موجبات و دست‌مایه ایجاد ریشه‌های تهدید سایبری به شکل داخلی یا خارجی و ساختاری یا غیرساختاری در زمینه انسانی، سازمانی و یا سامانه‌ای و تعیین‌کننده خصوصیت و وجه ممیزه تهدید سایبری و موجب تفکیک آن از دیگر پدیده‌های موجود (آسیب‌پذیری و ....) در فضای سایبر
٤	انگیزه	دلیل، سبب و علت اصلی تحریک عامل تهدید در جهت اغراض و انگیزه‌های شخصی، سیاسی، اقتصادی فرهنگی، امنیتی و ... برای اقدام به تهدید علیه هدف مشخص.
۵	دامنه بروز	حوزه‌های زیرساختی هدف در جغرافیای فضای سایبر، موردنظر تهدیدگر به‌عنوان مقصد اصلی از طراحی و اجرای تهدید که قابل تعریف برای مواردی همچون شبکه عمومی اطلاعات، سامانه، مؤلفه نرم‌افزاری و سخت‌افزاری، زیرساخت‌های حیاتی (اطلاعاتی و ارتباطی) و مراکزداده است.
۶	آثار و پیامدها	نتایج حاصل از تحقق تهدید سایبری (در دو شکل عملیاتی و غیرعملیاتی و یا برگشت‌پذیر و برگشت‌ناپذیر) که عواقب آن می‌تواند قابل‌ترمیم و یا غیرقابل‌ترمیم باشد.
۷	دامنه اثرگذاری	جغرافیای تهدید که متضمن محدوده کلی اثرگذاری، میزان و نوع زیرساخت حیاتی موردنظر برای تحقق تهدید در سطوح شهری، استانی و ملی می‌شود.
۸	شیوه تحقق	قاعده، هنجار یا اسلوبی که به‌عنوان سبک اصلی تهدیدکننده سایبری برای اقدامات تهدیدآمیز در قالب روند یا سناریوی تهدید با استفاده از آسیب‌پذیری‌ها و ابزارهای اجرای تهدید سایبری در اشکال سخت‌افزاری، نرم‌افزاری، شبکه‌ای و انسانی توسط تهدیدگر و مورد کاربری عملیاتی در صحنه عمل
۹	آسیب‌پذیری	نقایص موجود در سامانه که به لحاظ طراحی، پیکربندی و ساخت به وجود می‌آید و شناسایی آن‌ها به‌عنوان عاملی اولیه و تحریک‌کننده برای تهدیدگر است که در زیرساختی مثل مرکز داده در حوزه‌های برنامه‌های وب، سخت‌افزار و نرم‌افزار و شبکه و کاربران قابل‌توجه است.

پایش کیفیت (مرحله دوم- ضریب کاپا): نظر به اینکه روند جمع‌آوری داده‌ها به شکلی نظام‌مند انجام

شده است و دقت در این فرایند بر میزان اعتبار اجزاء به‌دست‌آمده در الگوی مفهومی کمک می‌کند ضرورت ایجاب می‌نماید که ترکیب اجزاء در قالب الگوی مفهومی نیز اعتبارسنجی شود. براین‌اساس جهت حفظ کیفیت مطالعه، از شاخص کاپا استفاده شده است. در این روش شخص دیگری از خبرگان حوزه مطالعه، بدون اطلاع از نحوه ادغام کُدها و مفاهیم توسط پژوهشگر، اقدام به طبقه‌بندی کُدها در مفاهیم نمود. مفاهیم ارائه‌شده توسط پژوهشگر (۹ مفهوم اصلی-ابعاد) با مفاهیم ارائه‌شده توسط این فرد مقایسه و درنهایت با توجه به تعداد مفاهیم ایجادشده مشابه و متفاوت، شاخص کاپا محاسبه شد (جدول ۸).

جدول (۹) –پایایی روش فراترکیب

		نظر محقق		
		خیر	بله	مجموع
نظر خبره دیگر	بله	B=2	A= 6	8
	خیر	D=0	C=1	1
	مجموع	1	6	N=9

$$\text{توافقات مشاهده شده} = \frac{A+D}{N} = 0.67$$

جدول (۱۰) – وضعیت شاخص کاپا (جنسن و آلن، ۱۹۹۶)

وضعیت توافق	وضعیت توافق	مقدار عددی شاخص	مقدار عددی شاخص
ضعیف	بی‌اهمیت	کمتر از ۰	۰-۰/۲۰
متوسط	مناسب	۰/۲۱-۰/۴۰	۰/۴۱-۰/۶۰
معتبر	عالی	۰/۶۱-۰/۸۰	۰/۸۱-۱

$$\text{توافقات شانسی} = \frac{A+B}{N} \times \frac{A+C}{N} \times \frac{C+D}{N} \times \frac{B+D}{N} = \frac{8}{9} \times \frac{7}{9} \times \frac{1}{9} \times \frac{2}{9} = 0.0170$$

K=۰/۶۶=(توافقات شانسی -۱)/(توافقات شانسی – توافقات مشاهده‌شده)

نظر به اعتبار میزان به‌دست‌آمده عدد K -بر اساس استاندارد اشاره‌شده در جدول (۹)– موارد مستخرجه در قالب ابعاد و مؤلفه‌های تهدیدات سایبری مراکزداده (جدول ۶) صحیح است.

جمع‌بندی و پیشنهادها

با در نظر گرفتن مرکز داده به‌عنوان بخشی از زیرساخت‌های حیاتی اطلاعاتی و ارتباطی و توجه به ساختار مرکز داده به‌عنوان اهداف خاص تهدیدات هدفمند سایبری، نتایج تحقیق حاضر نشان می‌دهد ارائه الگوی شناسایی تهدیدات سایبری مراکزداده ارائه‌گر رهنمودی برای تشخیص راه‌کارهای مواجهه با تهدیدات این حوزه است. این مواجهه در مرحله قبل از رخداد سایبری می‌تواند به شکل ارزیابی، در زمان وقوع به‌عنوان ابزار پایشی و در زمان پس از وقوع به‌عنوان سنجه‌ای برای تصمیم‌گیری پیرامون اقدامات تاب‌آوری این‌گونه از زیرساخت‌ها مطرح شود. در این راستا محقق ضمن تحلیل انواع تهدیدات سایبری پرتکرار، نسبت به تدوین ساختار تهدیدات سایبری مرکزداده در قالب یک الگوی مفهومی اقدام نموده است. این امر مستلزم توجه به خط‌مشی‌ها و الزامات اسناد فرادستی امنیتی کشور، اطلاعات ارائه‌شده توسط مراجع تخصصی داخلی و خارجی و نیز تحلیل مشخصه‌ها و ویژگی‌های کلیدی در تشخیص و وارسی این دسته از تهدیدات سایبری است. بر اساس مجموعه موارد فوق، الگوی مفهومی ساختارشناسی تهدیدات سایبری متشکل از ۹ مقوله فناوری تهدید، منشأ تهدید، ماهیت تهدید، انگیزه تهدید، دامنه بروز تهدید، آثار و پیامدها، دامنه اثرگذاری تهدید، شیوه تحقق تهدید و آسیب‌پذیری‌ها طراحی و تدوین گردید. هر یک از این مقوله‌ها دربرگیرنده مجموعه مؤلفه‌هایی هستند که به‌صورت موردی یا جمعی به تبیین ویژگی‌های تهدیدات سایبری مراکزداده می‌پردازند. علاوه بر این که جمع‌آوری ادبیات این تحقیق به شکلی نظام‌مند بوده است، الگوی مفهومی ارائه شده نیز از منظر جامعیت، مانعیت و نحوه سازماندهی مقوله‌ها و مؤلفه‌ها دارای نوآوری است که می‌توان از آن به‌عنوان یک توانمندساز در حوزه‌های زیر استفاده نمود:

- تشخیص موقعیت تهدید برای تصمیم‌سازی سریع و کارا برای مراکزداده
- توسعه شناخت ساختار تهدیدات سایبری مراکزداده و سازماندهی مؤثرتر اقدامات و راهبردهای امنیتی از طریق درک ماهیت، منشأ پیامدها و سایر مشخصه‌های این دسته از تهدیدات سایبری

به نظر می‌رسد با استفاده از نتایج تحقیق حاضر بتوان پژوهش‌هایی با عناوین ذیل برای توسعه کاربری‌های تهدیدشناسی سایبری زیرساخت‌های حیاتی انجام داد:

- ✓ ارائه الگوی تهدیدات سایبری مراکزداده تجهیز شده به فناوری‌های نوظهور به‌نحوی‌که ارتباط بین اجزاء ارائه شده در الگوی مفهومی تحقیق حاضر را به شکلی عملیاتی ارائه نماید.
- ✓ بررسی تهدیدات سایبری امنیتی زیرساخت‌های حیاتی اطلاعاتی و ارتباطی از منظر پدافند غیرعامل با رویکرد رتبه‌بندی تهدیدات سایبری بر اساس اثر وزنی آن‌ها در میزان تأثیر بر سرمایه‌های سایبری
- ✓ ارائه چارچوب مفهومی طبقه‌بندی تهدیدات سایبری امنیتی مراکزداده حیاتی از منظر پدافند غیرعامل

منابع فارسی:

- **فرهنگ فارسی عمید**
- اسماعیلی، علی؛ ثنا قربانی، جلال؛ (۱۳۹۷) **تبیین نسبت سناریوهای محتمل و مطلوب تهدیدات سایبری جمهوری اسلامی ایران**، فصلنامه علمی – پژوهشی، امنیت ملی
- افتخاری، اصغر؛ (۱۳۹۲) **برآورد تهدید–رویکردی نظام‌واره**
- بلیکی، نوومن، (۱۳۹۳) **طراحی پژوهش‌های اجتماعی** ترجمه حسن چاووشیان، تهران، نشر نی
- پورنقدی، بهزاد؛ (۱۳۹۱) **پدافند غیرعامل و بررسی تهدیدات نظم و امنیت در فضای سایبری**
- جایگاه شبکه ملی اطلاعات در الگوی مفهومی لایه‌ای فضای مجازی (۱۳۹۶)، **شورای عالی فضای مجازی**، مرکز ملی فضای مجازی
- جوزف اس. نای، ترجمه دکتر رضامراد صحرایی، (۱۳۹۰)، **آینده قدرت**، تهران
- خالقی، محمود؛ (۱۳۹۱) **مأموریت‌ها، ساختار تشکیلات و شرح وظایف قرارگاه پدافند سایبری کشور**، مرکز پدافند سایبری کشور
- دبیرخانه شورای عالی امنیت فضای تبادل اطلاعات، (۱۳۸۴) **سند راهبردی امنیت فضای تبادل اطلاعات کشور**
- سازمان فناوری اطلاعات، (۱۳۹۰) **نظام دفاع سایبری**، فصل ششم
- سایت اینترنتی *http://www.dadehara.com*
- سایت اینترنتی آی تی ایران
- سایت اینترنتی شرکت سرور ایران *HTTP://www.serveriran.net*
- سند راهبردی پدافند سایبری (۱۳۹۰)، **سازمان پدافند غیرعامل**
- صلاحی، احمد؛ (۱۳۹۳) **حفاظت از زیرساخت‌های ملی در مقابل حملات سایبری**،
- عبدالله‌خانی، علی؛ (۱۳۸۵) **حفاظت از زیرساخت‌های حیاتی اطلاعاتی**
- عرب‌سرخی، ابوذر؛ شبانی، فاطمه، ایوازه، اسما، چاردولی، امین؛ (۱۳۹۶)؛ **تدوین نقشه راه امنیت حوزه ارتباطات و فناوری اطلاعات**؛ پژوهشگاه ارتباطات و فناوری اطلاعات–پژوهشکده امنیت ارتباطات و فناوری اطلاعات–گروه ارزیابی امنیت شبکه و سامانه‌ها
- قوچانی خراسانی، محمدمهدی، حسین‌پور، داود؛ (۱۳۹۶)، **حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری**، دانشکده مدیریت و حسابداری دانشگاه علامه طباطبایی، فرایند مدیریت توسعه، دوره ۳۰، شماره ۱، ص ۸۰–۵۱،
- **لغت‌نامه دهخدا**
- مجله **شبکه و امنیت**(۱۳۹۵) , شماره ۲۷۵
- محمدی، علی (۱۳۹۲)؛ **دسته‌بندی تهدیدات سایبری (با رویکرد طراحی نظام رصد تهدیدات سایبری)**، دانشگاه و

پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

- محمودزاده، محمود؛ اسدی، فرخنده؛ (۱۳۸٤)، **زیرساخت‌های فناوری اطلاعات و ارتباطات و اشتغال بخش خدمات ایران**، فصل‌نامه اقتصاد و تجارت نوین، شماره ۳، صفحات ۹۵-۱۱۸
- مشهدی، حسن، امینی ورکی، سعید؛ (۱۳۹٤)، **تدوین و ارائه الگوی ارزیابی تهدیدات، آسیب‌پذیری و تحلیل خطرپذیری زیرساخت‌های حیاتی با تأکید بر پدافند غیرعامل**
- معاونت پژوهش و تولید علم دانشکده اطلاعات، (۱۳۹٤) **حفاظت سایبری از زیرساخت‌های حیاتی**
- منصوریان، یزدان؛ (۱۳۹۳)، **روش تحقیق در علم اطلاعات و دانش‌شناسی**. انتشارات سمت، تهران
- وظیفه‌دان، سارا؛ (۱۳۹۵)، **انواع تهدیدات فضای سایبری و راه‌کارهای مقابله**، کنفرانس ملی پدافند غیرعامل در قلمرو فضای سایبر
- حسینی، مریم (۱۳۹٤)، **معرفی روش گروه کانونی و کاربرد آن در تحقیقات**، مرکز پژوهش و سنجش افکار، اداره کل پژوهش و سنجش سازمان صداوسیمای جمهوری اسلامی ایران

English Resources:

- *Mouna Jouini, Latifa Ben Arfa Rabai, Anis Ben Aissa, (2014),* ***Classification of security threats in information systems****, 5th International Conference on Ambient Systems, Networks and Technologies,Computer Science32(489 – 496), ScienceDirect, ELSEVIER*
- *Ahmad Bakhtiyari Shahri, Zuraini Ismail, (2012),* ***A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS,*** *Journal of Information Security, 2012, 3, 169-176*
- *D. Kotz,* ***"A Threat Taxonomy for Health Privacy,"*** *Proceedings of the 3rd International Conference on Communication Systems and Networks of the IEEE COMS- NETS, Bangalore, 4-8 January 2011, pp.1-6.*
- *Thomas A. Johnson,* ***"CyberSecurity,Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare"*** *Webster University, St. Louis, Missouri, USA, 2015*
- *"***Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems***" by NIST of United States of America. Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege.*
- *ISO/IEC 27000, "***Information technology - Security techniques - information security management systems – overview and vocabulary***", 2014*
- *U.S Department of Homeland Security, "***National Cyber Incident Response Plan***", September 2010*
- *U.S. Office of Homeland Security, "***The National Strategy for Homeland Security***", July*

16, 2002, p.30.

- National Institute of Standards and Technology, **"Framework for Improving Critical Infrastructure Cyber security"**, February 12, 2014
- National Institute of Standards and Technology, "**Framework for Improving Critical Infrastructure Cybersecurity**", January 10, 2017
- HTTP://www.mio.gov.uk-134
- Carvaliho, V.A. Almeida,J.P.A, Fonseca, C.M, & Guizzardi,G. (2017), **Multi-level ontology based conceptual modeling Data & Knowledge Enginnering**.
- USGAO, **United States Faces Challenges in Addressing Global Cybersecurity and Governance**, United States Government Accountability Office, July 2010.
- S.Hansman and R. Hunt, "**A Taxonomy of Network and Computer Attacks,**" Computer and Security,2005
- J. Mirkovic and P. Reiher, "**A Taxonomy of DDoS Attack and DDoS Defense Mechanisms,**" ACM,CCR, April 2004
- F. Lough, "**A Taxonomy of Computer Attacks with Applications to Wireless Networks,**"" Ph.D. Thesis,Virginia Polytechnic Institute and State University, 2001
- J.D. Howard and T. Longstaff, "**A Common Language for Computer Security Incidents**" Technical report, Sandia National Laboratories, 1998
- Thomas A. Johnson, "**Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare**", Webster University, St. Louis, Missouri, USA, 2015
- www.techrepublic.com, 2017
- www.infosecurity-magazine.com, 2017
- ENISA Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends
- www.nopsec.com, report of Cyber Attack, 2017
- www.checkpoint.com, Security Report, 2018
- Source:CheckPoint 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/
- h2-2017-global-threat-intelligence-trends-report
- TREND Micro, **Report on Cybersecurity and Critical Infrastructure in the Americas**, 2015
- https://www.gartner.com/technology/research/it-spending-forecast/
- https://ec.europa.eu/digital-single-market/en/news/comprehensive-approach-evolving-cyber-threats,accessed November 2017.
- The Department of Homeland Security, **Critical Infrastructure Sectors**, Last Published Date: August 22, 2018

- POSTNOTE, **Cyber Security of UK Infrastructure**, Number 554 May 2017
- David P. Duggan, John T. Michalski, "***A Threat Analysis Framework as Applied to Critical Infrastructures in the Energy Sector*** ",Sandia National Laboratories, September 2007
- Lindgreen, A., Palmer, R., and Vanhamme, J. "**Contemporary marketing practice: theoretical propositions and practical implications**", Marketing Intelligence and Planning, Vol. 22 No. 6, pp. 673-692. (ISSN 0263-4503), 2004
- 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
- www.dadehara.com
- https://itiran.com/2018/04/07/حمله-اینترنتی-به-مراکز-داده-ایران/
- Eastwest Institute and the Information Security Institute of Moscow State University, "**Russia-U.S. Bilateral on cybersecurity - critical terminology foundations**", Issue I, April 2011
- www.OECD.org/site/ictworkshops/33958011.pdf
- SANS, The State of Dynamic Data Center and Cloud Security in the Modern Enterprise, A SANS Survey, Dave Shackleford, October 2015
- Infosec, The Top 5 Data Center Threats You Need to Know, 18 Nov 2014
- Timothy Morrow, Carnegi Mellon University, Software Engineering Institute,. https://www.sei.cmu.edu/, 2018
- Kenneth J. Knapp, The University of Tampa, **Data Center Security: *Analysis of Two Audit Reports***, Researchgate, 2014
- Wilkinson.s, Focus group research. In D.Silverman (ed.), ***Qualitative research: Theory, method, and practice*** (pp. 177-199). Thousand oaks, CA: Sage, 2004
- Goldman, A.E., **The group depth interview**. Journal of Marketing, 26, 61-68., 1962
- Top 10 Data Center Industry Trends for 2019, Report Review 2019