مقاله پژوهشی: ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی

محسن آقایی[1]، علی معینی[2]، ابوذر عرب سرخی[3]، ایوب محمدیان[4] و علی اصغر زارعی[5]

تاریخ دریافت: ۱۳۹۷/۷/۸ **تاریخ پذیرش: ۱۳۹۷/۹/۲۰**

چکیده

توسعه زیرساخت‌های ارتباطی و اتصال شبکه‌های ناهمگون با گسترش هم‌زمان سرویس‌ها و خدمات مفید و متنوع در سطوح سازمانی، بخشی و ملی در کنار ساختار نامتعارف و درهم‌تنیده آنها باعث رشد آسیب‌پذیری‌ها و تهدیدات امنیتی در فضای سایبر شده است. تهدیدات سایبری با اثرگذاری در سطح ملی علیه برخی از این زیرساخت‌ها به عنوان زیرساخت‌های حیاتی، هزینه‌های زیاد و گاه غیرقابل جبرانی را به سازمان‌ها، جوامع و کشورها تحمیل می‌کند. اقدام اصلی در مواجهه با این موارد شناسایی تهدیدات فوق است. مطالعه و تحلیل این تهدیدات در قالب ارائه مدل مفهومی منطقی برای طبقه‌بندی آنها هدف اصلی این تحقیق است. دست‌یابی به این هدف مستلزم شناسایی طبقه‌بندی‌های تهدیدات سایبری، بررسی منطق و گونه‌شناسی آنها در سطح زیرساخت‌های حیاتی است. در این تحقیق با مطالعه تحقیقات انجام شده مرتبط، بررسی ادبیات موضوعی، شناسایی تهدیدات سایبری پرتکرار، اعتبارسنجی آنها از منابع معتبر و استخراج مفاهیم مشترک مربوط به شناسایی تهدیدات سایبری، ابعاد، مولفه‌ها و شاخص‌های طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی استخراج شدند. گردآوری داده‌ها با روش فراترکیب و اعتبارسنجی یافته‌ها با استفاده از ضریب کاپا انجام شد. نتایج در قالب مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی با ابعاد شش‌گانه: تهدیدات، عوامل تهدید، مشخصات تهدید، نگاه از دید نفوذگر، توصیف سیستم و منابع شناسایی تهدیدات، حاصل شد.

کلیدواژه‌ها: زیرساخت حیاتی، تهدیدات سایبری، دسته‌بندی تهدیدات، مدل مفهومی

---

۱. دانشجوی دکتری مدیریت سیستم‌ها دانشگاه تهران

۲. استاد و عضو هیات علمی دانشکده علوم مهندسی پردیس دانشکده‌های فنی دانشگاه تهران(نویسنده مسئول)

۳. استادیار و عضو هیات علمی پژوهشگاه ارتباطات و فناوری اطلاعات

٤. استادیار و عضو هیات علمی دانشکده مدیریت دانشگاه تهران

۵. استادیار و عضو هیات علمی دانشگاه امام حسین(ع)

مقدمه

امروزه عمده فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی وحاکمیتی کشورها در زیست بوم[1] فضای سایبر انجام می‌شود. توسعه اقتصادی و اجتماعی، افزایش سطح رفاه عمومی، ارتقاء توان دفاعی و امنیتی کشورها نیازمند برخورداری از زیرساخت‌های مناسب حمل‌ونقل، انرژی، آب، فناوری‌اطلاعات و ارتباطات، بانک‌داری، آموزش وپژوهش، پست، بهداشت و درمان، دفاعی و غیره است که در سند امنیت ملی سال ۲۰۱۸ ایالات متحده به تعداد ۱۷ مورد زیرساخت اشاره شده است(سند امنیت ملی ایالات متحده، بخش زیرساخت‌ها، ۲۰۱۸).

گسترش فراگیر زیرساخت‌های حیاتی همراه با ارائه سرویس‌ها و خدمات متنوع در فضای سایبر بستری برای توسعه و رفاه ایجاد نموده‌است. به عنوان نمونه بر اساس گزارش سال ۲۰۱۷ گارتنر[2]، سرمایه‌گذاری جهت توسعه حوزه زیرساخت ارتباطات از استقبال فراوانی برخوردار بوده است و بر اساس پیش‌بینی‌های این موسسه از حدود ۳۲۵۰ بیلیون دلار در سال ۲۰۱٦ به بیش از ٤۰۰۰ بیلیون دلار در سال ۲۰۲۲ خواهد رسید(گارتنر، ۲۰۱۷).

نامتعارف بودن ساختار، رشد سریع و نامتوازن این شبکه‌های ناهمگون به‌هم‌پیوسته، آسیب‌پذیری‌ها، تهدیدهای متنوع و حوادث خطرناک با دامنه اثر بالا، ایجاد ناامنی و بروز چالش و اختلال در زندگی شهروندی و حتی تهدید برای امنیت ملی کشورها را بدنبال دارد. برخی از این زیرساخت‌ها نقش حیاتی در منافع و خدمات سطح ملی دارند که با توجه به اهمیت آنها به عنوان زیرساخت‌های حیاتی شناخته می‌شوند و اختلال کوتاه‌مدت در عملکرد این زیرساخت‌ها آسیب‌های جدی در حوزه‌های پایداری، امنیت و ایمنی جامعه را بدنبال دارد و باید در برابر تهدیدات درونی و بیرونی محافظت شوند.

موسسه پست‌نوت[3] درسال ۲۰۱۷ اعلام نمود تهدید سایبری منجر به حمله درسال

1. Echosystem
2. WWW.GARTNER.COM
3. POSTNOTE (Cyber Security of UK Infrastructure)

۲۰۱۵ به زیرساخت توزیع نیروی برق کشور اوکراین و قطع برق ۲۲۵,۰۰۰ مشترک، آثار مخربی را تا چند ماه در پی داشته‌است(پست نوت، ۲۰۱۷). به گزارش موسسه سایبربان سرقت ۸۱ میلیون دلار از بانک‌های بنگلادش، سرقت ۵۰۰ میلیون حساب کاربری یاهو یا ۱۹ هزار ایمیل از کمیته ملی حزب دموکرات آمریکا در انتخابات سال ۲۰۱۶، از اقدامات تهدیدآمیز در زیرساخت‌های اقتصادی، امنیت ملی و. .. است(سایبربان، ۱۳۹۶). بر این اساس کارشناسان حوزه امنیت سایبری معتقدند که امنیت سایبری باید به شکل دغدغه در بدنه حاکمیت هر کشور نهادینه شود و در میان نهادهای حاکمیتی، فرهنگ‌سازی آن در نهادهای دولتی از اهمیت بالاتر برخوردار است(قوچانی،حسین‌پور،۱۳۹۶).

بر همین اساس در پی ابلاغ طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری از سوی مرکز مدیریت راهبردی افتای ریاست جمهوری اسلامی ایران، ۱۳۹۸، اعلام شد با توجه به مخاطرات نوظهور در عرصه فناوری اطلاعات و ارتباطات، طرح امن‌سازی زیرساخت‌های حیاتی در قبال حملات سایبری با بازنگری همه جانبه و با تحقیق، پژوهش، بررسی آسیب‌ها و توانمندی‌های سایبری و ارزیابی ظرفیت امنیت سایبری تدوین نهایی و ابلاغ شده است(جواهری، مرکز مدیریت راهبردی افتای ریاست جمهوری اسلامی ایران، ۱۳۹۸).

موارد فوق نشان از این واقعیت دارد که برای ارتقاء امنیت زیرساخت‌های حیاتی، درک، تحلیل و شناخت تهدیدات علیه این زیرساخت‌ها دارای اهمیت و باعث تداوم و استمرار ارائه خدمات در سطح ملی می‌شود. براین اساس شناسایی و روش درست اندیشیدن در مورد تهدیدات سایبری زیرساخت‌های حیاتی جهت جلوگیری از خطا در تشخیص و ارائه راه‌کارهای مواجهه با آنها، یعنی منطق[1] این گونه از تهدیدات، همچنین

---

۱. در فرهنگ معین منطق چنین معنی شده است: علمی که با به کار بستن اصول و قواعد آن می‌توان از فکر غلط یا استدلال نادرست پرهیز کرد. همچنین در پایگاه اطلاع‌رسانی حوزه به آدرس: چنین آمده است که: منطق « قانون صحیح فکر کردن است». یعنی قواعد و قوانین منطقی به منزله مقیاس و معیار و آلت سنجش است که هرگاه بخواهیم درباره برخی از موضوعات علمی یا فلسفی تفکر و استدلال کنیم باید استدلال خود را با آن مقیاس‌ها و معیارها بسنجیم و ارزیابی کنیم که بطور غلط نتیجه‌گیری نکنیم. در دانشنامه رشد نیز، منطق، راه و روش صحیح فکر کردن و درست اندیشیدن و نتیجه گیری کردن است.

طبقه‌بندی‌ها و موارد تاثیرگذار بر آنها می‌تواند ضمن ارتقاء دانش و آگاهی در این حوزه، عاملی برای توسعه قدرت تصمیم‌سازی و تصمیم‌گیری راهبردی باشد. به منظور شناسایی این منطق در قالب توصیفی که فهم اجزاء و ارتباط آنها را ارائه دهد، می‌توان اقدام به ارائه مدل مفهومی نمود(کاروالینهو، المیدا، فونسکا، گازاردی، ۲۰۱۷) تا ارتباط منطقی جنبه‌های مختلف در روند شناسایی تهدیدات سایبری زیرساخت‌های حیاتی مشخص شوند.

بیان مساله

تهدید و تهاجم سایبری علیه زیرساخت(بستر)های حیاتی عدم پایداری[1] امنیتی را بدنبال دارد. اجرای برنامه‌های امنیت سایبری نهادها و سازمان‌ها، برگرفته از راهبردها و سیاست‌های کلان تدوین شده، توان مجموعه را برای پیش‌بینی، مدیریت و مقابله با تهدیدات سایبری افزایش و پیامدهای مخرب بروز تهدیدها را کاهش می‌دهد و بازسازی حوزه‌های آسیب‌دیده را با کمترین هزینه میسر می‌سازد.

تهدیدات مهم سایبری دهه اخیر نشان می‌دهد حمله‌ها علیه زیرساخت‌های حیاتی بدلیل نوع و حوزه اثر در گروه تهدیداتی قرار می‌گیرند که مقابله با آنها تدابیر و راه‌کارهای خاصی در سطوح ملی می‌طلبد.(وظیفه‌دان، ۱۳۹۵) اعلام پانزده تهدید سایبری رتبه بالا در گزارش سال ۲۰۱۷ آژانس امنیت سایبری اروپا(انیسا[2]) گویای این موضوع است که نرخ رشد این گروه از تهدیدات سایبری دارای شتاب زیادی است(انیسا،۲۰۱۷).

تحلیل و گونه‌شناسی تهدیدات سایبری زیرساخت‌های حیاتی مولفه‌ای کلیدی در امنیت زیرساخت‌ها، برنامه‌های کاربردی و پایگاه‌های داده است. پیش‌بینی، کنترل و رفع آثار آنها مستلزم درک آنها است که با بهره‌گیری از مدل مفهومی شناسایی و طبقه‌بندی تهدیدات سایبری فضای سایبر تسریع می‌شود(دوگان‌ومیچالسکی،۲۰۰۹).

مدیریت و کاهش آثار بروز این تهدیدات، ارتقاء قدرت تصمیم‌سازی و تصمیم‌گیری و

---

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

۲. آژانس امنیت سایبری اتحادیه اروپا (انیسا) European Network and Information Security Agency (ENISA)

در نتیجه ایجاد و استمرار امنیت سایبری در سطح زیرساخت‌های حیاتی، نیازمند مدلی برای مواجهه با شرایط قبل از وقوع، در زمان وقوع و بعد از وقوع تهدیدات است و تعیین منطق طبقه‌بندی و سنجش اولویت این تهدیدات به عنوان پیش‌نیاز مدیریت امنیت و دست‌یابی به این مهم در قالب ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی به واسطه ارتقاء سطح نگرش و شناسایی فراگیر نسبت به بازه وسیع و تنوع زیاد تهدیدات سایبری به عنوان ویژگی خاص این مدل با کارکرد[1] در مقیاس گسترده زیرساخت‌های حیاتی، اهمیت زیادی دارد زیرا این مدل می‌تواند پیش‌نیاز و زمینه‌ساز درک تهدیدات سایبری این نوع از زیرساخت‌ها و اتخاذ تصمیمات راهبردی باشد.

در این تحقیق، قصد داریم تهدیدات سایبری علیه زیرساخت‌های حیاتی را با ارائه منطق طبقه‌بندی آنها به شرحی که برای صفت «منطقی» جهت مدل مفهومی ارائه شد، بازنمایی کنیم. بنابراین تمرکز بر گونه‌ای از تهدیدات سایبری بر اساس نوع، حوزه اثر و تاثیرگذاری بر بخش خاصی از سرمایه‌ها و دارایی‌ها است که مقوله پایداری امنیتی را خدشه‌دار می‌کنند و به عنوان تهدیدات سایبری زیرساخت‌های حیاتی شناخته می‌شوند. علیرغم وجود مدل‌های مختلفی که برای طبقه‌بندی تهدیدات سایبری در تحقیقات داخلی و خارجی ارائه شده‌اند مدل مفهومی به شرحی که مورد هدف این تحقیق است تا کنون برای طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی ارائه نشده است و تحقیق حاضر به واسطه خلاء دانشی موجود در این حوزه به دنبال ایجاد فرایندی است که بتواند تهدیدات سایبری مورد نظر این تحقیق را به شکلی مشخص طبقه‌بندی نماید. بنابر این سئوال اصلی تحقیق این است که: «مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی چیست»

---

۱. در فرهنگ فارسی عمید کارکرد، «اندازه و مقیاس کار انجام‌شده» معنی شده است.

اهمیت پژوهش

بررسی‌ها، نیازسنجی‌ها و همچنین پیش‌بینی محقق نشان‌دهنده موارد ذیل در اهمیت انجام این تحقیق است:

- ارتقاء سطح نگرش و شناسایی فراگیر نسبت به بازه وسیع و تنوع زیاد تهدیدات سایبری زیرساخت‌های حیاتی
- توسعه دانش بومی این حوزه به منظور ارتقاء وضعیت تامین امنیت سایبری زیرساخت‌های حیاتی
- شناخت منطقی اقدامات تهدیدآمیز سایبری علیه زیرساخت‌های حیاتی جهت مواجهه فعال

ضرورت پژوهش

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

- ضعف در پیش‌بینی و شناخت تهدیدات و افول قدرت مدیریت امنیت سایبری زیرساخت‌های حیاتی
- کاهش توانمندی در پاسخگویی به نیازهای امنیت سایبری زیرساخت‌های حیاتی و تحمیل هزینه‌های زیاد
- افزایش میزان خسارات اقدامات تهدیدآمیز سایبری در صورت نبود مدل مفهومی مقبول برای مواجهه فعال

نقشه راه تحقیق

نقشه راه کلی انجام این تحقیق جهت ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی چنین بوده است که ابتدا مفهوم‌شناسی متغیرها، پیشینه‌شناسی و بررسی ادبیات موضوعی بر اساس گردآوری داده‌ها به روش فراترکیب و سپس تعریف متغیرهای تحقیق به منظور ارائه تعریف محوری «تهدیدات سایبری زیرساخت‌های حیاتی» انجام شد و در مرحله بعد ابعاد، مولفه‌ها و شاخص‌ها استخراج شدند و مجموعه موارد استخراج شده با

بکارگیری ضریب کاپا مورد اعتبارسنجی قرار گرفتند. در نهایت و بر اساس تایید موارد استخراج شده مدل مفهومی مورد نظر، نتیجه گیری و پیشنهادها ارائه شدند.

اهداف

هدف از انجام این تحقیق ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی به شکلی است که با ارائه آن بتوان روند شناسایی این تهدیدها را در قالبی با قدرت شناسایی بیشتر و خطای کمتر مورد نظر قرار داد. بنابر این هدف اصلی و اهداف فرعی این تحقیق عبارتند از:

هدف اصلی: «ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی»

اهداف فرعی

- شناخت طبقه‌بندی‌های رایج در حوزه تهدیدات سایبری
- شناخت طبقه‌بندی‌های تهدیدات سایبری در سطح زیرساخت‌های حیاتی
- شناخت ابعاد، مولفه‌ها و شاخص‌های معرف تهدیدات سایبری و منطق طبقه‌بندی آنها

سئوالات

سئوال اصلی: مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی چه ابعاد، مولفه‌ها و شاخص‌هایی دارد؟

سئوالات فرعی

- طبقه‌بندی‌های مطرح تهدیدات سایبری دارای چه ابعاد، مولفه‌ها و شاخص‌هایی هستند؟
- طبقه‌بندی‌های مطرح تهدیدات سایبری زیرساخت‌های حیاتی چه ابعاد، مولفه‌ها و

شاخص‌هایی دارند؟

- منطق طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی چیست؟

مبانی نظری

مفهوم‌شناسی متغیرهای پژوهش

در استاندارد سیستم مدیریت امنیت اطلاعات، کلیّات و واژگان، «تهدید» به معنی «پتانسیل ایجاد حادثه ناخواسته، با احتمال واردشدن صدمه به یک سامانه یا سازمان»، تعریف شده است(مؤسسه بین‌المللی استاندارد، ۲۰۱٤). همچنین در سند راهبردی پدافند سایبری جمهوری اسلامی ایران، تهدید سایبری «عامل خارجی با قابلیت وارد نمودن ضربه فاجعه‌بار به امنیت، منافع و اقتصاد ملی، وجهه و روابط بین‌المللی، سلامت، ایمنی و اطمینان عمومی، باورهای دینی و ملی یا اداره امور کشور، از طریق تخریب یا ایجاد اختلال گسترده در عملکرد سرمایه‌های ملی سایبری کشور» تعریف شده است (سند راهبردی پدافند سایبری جمهوری اسلامی ایران،۱۳۹٤). در نتیجه تعریف عملیاتی «تهدید سایبری»، «رویداد یا واقعه‌ای با قابلیت واردنمودن ضربه به مأموریت‌ها، وظایف، تصویر یا اعتبار دستگاه متولی، سرمایه ملی سایبری یا کارکنان دستگاه به واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، انهدام، افشاء، تغییر اطلاعات و یا ممانعت از(ایجاد اختلال در) ارائه خدمت» است.

دومین مفهوم کلیدی «زیرساخت حیاتی» است. در سال ۲۰۱۱، دولت انگلیس در گزارشی تحت عنوان «محافظت از زیرساخت‌های حیاتی در کشور بریتانیا» زیرساخت‌های ملی حیاتی کشور را قسمتی از زیربناهای کشور تلقی کرده است که تداوم فعالیت آنها برای کشور حیاتی و ازکارافتادگی، تاخیر 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). در سند راهبردی پدافند غیرعامل جمهوری اسلامی ایران،۱۳۹۱، مراکز حیاتی، مراکزی هستند که انهدام کل یا قسمتی از آنها، موجب

بروز بحران، آسیب و صدمات جدی و مخاطره آمیز در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری ملی شود(سند راهبردی پدافند غیرعامل جمهوری اسلامی ایران، ۱۳۹۱). بر این اساس تعریف عملیاتی این متغیر،«مجموعه عناصر به هم پیوسته در قالب سیستمی بزرگ با ابعاد فناورانه گسترده، ابعاد فیزیکی غیرقابل حرکت، ارائه دهنده خدمات اساسی و چارچوبی برای پشتیبانی از ساختارهای کلان است که اختلال یا تخریب آن بر مولفه‌های امنیت ملی اثرگذاری دارد»(شکل-۱).

شکل (۱)- نمونه‌ای اززیرساخت‌های حیاتی – توزیع انرژی که با استفاده از امکانات سایبری کنترل می‌شود.

در سال ۲۰۱۰، دیوید کلارک مدل چهارلایه‌ای فضای سایبر را معرفی نمود(شکل-۲). در این مدل فضای سایبر شامل: لایه‌های انسانی، اطلاعاتی، منطقی و فیزیکی است. هدف اصلی از ارائه این مدل، تفهیم نقاط کنترل فضای سایبر و اینترنت بوده است. در ارائه این مدل چنین در نظر گرفته شده است که مبانی فیزیکی فضای سایبر بسیار مهم هستند. فضای سایبر در سطح منطقی، مجموعه‌ای از سکوها[1]ی جدید برای نوآوری‌های جدید می‌باشد. لایه اطلاعات متضمن اطلاعات، ویدئو، موزیک، موارد تجاری، معاملاتی، کلان(فرا)داده[2]،

1 Platforms
2 meta-data

اطلاعات ایستا، پویا و غیره است. لایه بالایی یعنی لایه انسانی نه فقط شامل کاربران غیرفعال فضای سایبر، بلکه افراد دیگر با هر شکل وابستگی به این فضا مورد نظر هستند(کلارک، ۲۰۱۰).

در لایه زیرین این مدل زیرساخت‌های ارتباطی و اطلاعاتی قرار دارند که با توجه به میزان اهمیت و نقش‌آفرینی خود بخشی از زیرساخت‌های حیاتی هستند(محقق).

شکل (۲) – مدل چهارلایه‌ای از فضای سایبر(کلارک، ۲۰۱۰)

به عنوان سومین مفهوم کلیدی، برگرفته از مفاهیم اشاره‌شده، «تهدید سایبری زیرساخت حیاتی»، چنین مفهوم می‌شود: «رویداد، واقعه و یا اقدام احتمالی متخاصمین بالقوه و بالفعل بر اساس انگیزه با هدف اختلال در سیستم‌ها و مؤلفه‌های نرم‌افزاری و سخت‌افزاری، ضربه به ماموریت‌ها، وظایف، اعتبار سرمایه ملی سایبری یا کارکنان شبکه(زیرساخت حیاتی)، با استفاده از ابزارها، به واسطه سامانه اطلاعاتی با دسترسی غیرمجاز، انهدام، افشاء، تغییر اطلاعات و یا ممانعت از ارائه خدمت و روش خاص و اثرگذاری عملیاتی و اطلاعاتی، برگرفته از آسیب‌پذیری‌ها و ریسک‌های انسانی و سیستمی و ایجاد آثار مخاطره‌آمیز در امنیت ملی» است.

«طبقه‌بندی تهدیدات سایبری زیرساخت حیاتی»، به عنوان چهارمین مفهوم کلیدی این تحقیق است که طبقه‌بندی در فرهنگ فارسی عمید به مفهوم صف‌بندی می‌باشد و تعریف

عملیاتی آن در این تحقیق «تقسیم تهدیدات سایبری زیرساخت‌های حیاتی به گروه‌های منظم» در نظر گرفته می‌شود.

پیشینه و سابقه پژوهش

با توجه به اهمیت مفاهیم و مدل‌های مطرح در حوزه تهدیدات سایبری و بخصوص تهدیدات سایبری زیرساخت‌های حیاتی در سطح جهان، بررسی منابع برای تحلیل سوابق مربوطه، دسته‌بندی‌ها و مدل‌های ارائه‌شده مرتبط در منابع مختلف خارجی و داخلی انجام شد که خلاصه این نتایج در ادامه ارائه شده است.

مونا جوینی[1] و همکاران(۲۰۱٤) در مقاله‌ای[2]، با بررسی مدل‌های طبقه‌بندی تهدیدات سایبری سیستم‌های اطلاعاتی و تاکید بر مطالعه اثر کلاس تهدید به جای اثر یک تهدید و بررسی طبقه‌بندی‌های مختلف مخاطرات امنیتی، مدل ترکیبی طبقه‌بندی تهدیدات امنیت سایبری را بر اساس ارتباط تهدید با منبع، عامل، انگیزه، قصد و اثر و با هدف کمک به سازمان‌ها برای اجرای راهبردهای امنیت اطلاعات ارائه نموده‌اند(جوینی و همکاران، ۲۰۱٤).

در مقاله‌ای[3] دیگر، احمد بختیاری و زورانی اسماعیل[4](۲۰۱۲) با تمرکز بر سیستم اطلاعات سلامت به عنوان زیرساخت حیاتی و تغییرات تهدیدات سایبری، بیش از ۷۰ تهدید را بر اساس ۳۰ معیار مشترک شناسایی، رتبه‌بندی و طبقه‌بندی نموده‌اند تا در ارزیابی مخاطرات استفاده نمایند(اسماعیل، بختیاری، ۲۰۱۲).

همچنین کاجرلند[5](۲۰۱۵) با تحلیل حملات به سیستم‌های اسکادا[6] به عنوان بخش مهم در زیرساخت‌های حیاتی، مدلی را با تمرکز بر روش عملیات، اثر، عوامل و هدف تهدید

1. Mouna Jouini, Latifa Ben Arfa Rabai, Anis Ben Aissa
2. Classification of security threats in information systems
3. A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS
4. Ahmad Bakhtiyari Shahri, Zuraini Ismail
5. Kajerland
6. SCADA: Supervisory Control and Data Acquisition

برای طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی ارائه نموده است(کاجرلند،۲۰۱۵).

علی اسماعیلی و جلال ثناقربانی(۱۳۹۶) در مقاله‌ای[۱] با هدف سناریوپردازی آینده‌های محتمل و مطلوب تهدیدات سایبری، برخی ابعاد، مولفه‌ها و شاخص‌های تهدیدات سایبری زیرساخت‌های حیاتی را در کنار الگوی پایش این تهدیدات و شناسایی تهدیدات آینده برای جلوگیری از غافلگیری ارائه نموده‌اند(اسماعیلی،قربانی،۱۳۹۶).

لاندروس‌ای‌مگ‌لاراس و همکاران[۲](۲۰۱۸) در مقاله[۳] خود، با توجه به عملکرد سیستم‌های اسکادا، اینترنت اشیاء و پیش‌بینی ظهور تهدیدات نوین علیه زیرساخت‌های حیاتی، روش‌های امنیتی جدید و تشخیص سریع تهدیدات بدون بارگذاری اضافه بر سیستم‌ها را بررسی کرده‌اند و ابعاد جدید تهدیدات سایبری و رویکردهای مهاجمین در خصوص سیستم‌های اسکادا و کنترل صنعتی را ارائه نموده‌اند(مگ‌لاراس‌وهمکاران،۲۰۱۸).

پژوهشگران گروه «ارزیابی امنیتی شبکه‌ها و سامانه‌ها» در پژوهشکده امنیت ارتباطات و فناوری اطلاعات(۱۳۹۶)، در گزارش تحقیقاتی[٤]، ضمن شناسایی و صورت‌بندی پیشران‌های امنیتی در چهار مرحله: مفاهیم، پیشران‌های امنیتی سایبری، روندهای کلان امنیت سایبری و ملاحظات امنیتی، سه بعد: :نوع تهدید، عوامل تهدید و بردار حمله را در مورد تهدیدات سایبری مورد تاکید قرارداده‌اند(عرب‌سرخی و همکاران، ۱۳۹۶).

توماس‌ای‌جانسون[۵](۲۰۱۵) در کتاب حفاظت از زیرساخت‌های حیاتی[٦]، با نگاه به موارد قدرت‌ساز و آسیب‌پذیر زیرساخت‌های حیاتی کشور آمریکا ضمن 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 ارتقاء

---

۱. تبیین نسبت سناریوهای محتمل و مطلوب تهدیدات سایبری، فصل‌نامه امنیت ملی، دانشگاه علی دفاع ملی، ۱۳۹۷

2. Leandros A. Maglarasa, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag,Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, Tiago J. Cruz

3. Cyber Security on Critical Infrastructure

٤. تبیین ملاحظات امنیتی در حوزه ارتباطات و فناوری اطلاعات

5. Thomas A. Johnson

6. CYBERSECURITY, Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare

امنیت سایبری و شناخت تهدیدات داخلی سایبری معرفی نموده است(جانسون، ۲۰۱۵).

موسسه انیسا(۲۰۱۷) در گزارش سالیانه[1]، تهدیدات سایبری با فرکانس تکرار زیاد را مشخص، تشریح و رتبه‌بندی نموده است و بر موارد: تهدید، بردارحمله و عوامل‌تهدید به عنوان سه مولفه اصلی درحوزه سنجش تهدیدات توجه نموده است. این موارد در گزارش گروه ارزیابی امنیت شبکه و سامانه‌ها از پژوهشگاه ارتباطات و فناوری اطلاعات (۱۳۹٦) نیز تحلیل، بررسی و تایید شده‌اند(انیسا،۲۰۱۷)(جدول ۱).

جدول ۱- لیست تهدیدات سایبری

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

ادبیات مرتبط

مدل مفهومی: مدل‌سازی برای ارائه مدل مفهومی فعالیت توصیفی است که برخی جنبه‌های فیزیکی و اجتماعی پیرامون ما با هدف فهم اجزاء و ارتباط آنها را بدنبال دارد. این توصیف‌گری فعالیتی بنیادین در مهندسی سیستم‌های اطلاعاتی است. محصول اصلی این فعالیت مدل نظری(مفهومی) است.(کاروالینهو، المیدا، فونسکا، گازاردی، ۲۰۱۷) این مدل، حاوی منطق بنیادی و ساختار روابط بین مفاهیم مورد استفاده است. سیستم مدل سازی تهدید سعی در تحقق «تعیین میزان امنیت نرم‌افزار، شناسایی و رسیدگی به تهدیدات و آسیب‌پذیری‌های بالقوه و تعریف روند استدلال منطقی برای تعیین امنیت سیستم» دارد(بلیکی،۱۳۹۳:۲۳۱).

۱. پانزده تهدید و روند مرتبه بالا درسال ۲۰۱۷

یکی از روش‌های کشف، مطالعه و مدیریت تهدید، مدل‌سازی تهدیدات است. مدل‌سازی تهدید اجازه کشف تهدیدات بالقوه و بالتبع آسیب‌پذیری‌های ممکن را، پیش از حمله نفوذگر می‌دهد. در این خصوص، مدل ارائه شده شرکت مایکروسافت[1] دارای مراحل: «نگاه به سیستم از دید نفوذگر»، «توصیف سیستم» و «شناسایی تهدیدات» است.

روش‌شناسی تحقیق

نوع تحقیق

نظر به اینکه اجرای این تحقیق ارائه مدل مفهومی برای شناخت منطق طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی است و نتایج عملیاتی آن قدرت تصمیم‌سازی تصمیم‌سازان حوزه امنیت سایبری زیرساخت‌های حیاتی را افزایش می‌دهد، جنبه کاربردی دارد و با توجه به گسترش دانش در این حوزه، توسعه‌ای است. بنابراین تحقیق حاضر با توجه به هدف، از نوع توسعه‌ای- کاربردی است.

روش تحقیق

روش تحقیق مورد استفاده، با رویکرد آمیخته(کیفی و کمی) است. در بخش کیفی با مراجعه به مقالات، کتابها و گزارشات پژوهشی با استفاده از روش فراترکیب، ابعاد، مولفه‌ها و شاخص‌های مدل مفهومی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی استخراج و کنترل کیفی یافته‌ها انجام شد. بر اساس یافته‌ها مدل مفهومی اولیه شکل گرفت و پس از ارزیابی با روش ضریب کاپا، مدل مفهومی نهایی ارائه شد.

روش گردآوری داده‌ها و ابزار آن

داده‌های کیفی با روش فراترکیب جمع‌آوری شدند. فراترکیب، نوعی مطالعه کیفی است که اطلاعات و یافته‌های استخراج‌شده از مطالعات کیفی دیگر با موضوع مشابه و مرتبط را بررسی می‌کند. در نتیجه نمونه موردنظر از مطالعات کیفی منتخب و بر اساس ارتباط آن‌ها

1. Microsoft

با سؤال پژوهش ساخته می‌شود.(لیندگرین و دیگران[1]، ۲۰۰٤) در این پژوهش، از روش فراترکیب به‌منظور مقایسه، تفسیر، تبدیل و ترکیب چارچوب‌ها و مدل‌های مختلف ارائه شده در زمینه تهدیدات سایبری زیرساخت‌های حیاتی استفاده شده است.

معرفی روش فراترکیب

فرامطالعه[2]، یکی از روش‌های بررسی، ترکیب و تحلیل پژوهش‌های گذشته است. با تجزیه وتحلیل عمیق کارهای پژوهشی انجام‌شده در حوزه خاص و با توجه به نیازمندی تحقیق، بر چهار حوزه فراروش، فرانظری، فراتحلیل و فراترکیب دلالت دارد. فراتحلیل، مشهورترین حوزه فرامطالعه، بر مطالعات کمی پیشین تمرکز دارد. این روش اگر به‌صورت کیفی انجام شود و مفاهیم و نتایج مورد استفاده در مطالعات پیشین را با کدگذاری متداول پژوهش‌های کیفی مثل نظریه برخواسته از داده بررسی کند، فراترکیب نامیده می‌شود(سهرابی و همکاران، ۱۳۹۰)(شکل ۳).

فراترکیب مانند فراتحلیل، برای یکپارچه‌سازی چندین مطالعه و ایجاد یافته‌های جدید و تفسیر آن‌ها به کار می‌رود. بااین‌حال بر خلاف فراتحلیل که بر داده‌های کمی و رویکردهای آماری تأکید دارد، فراترکیب بر مطالعات کیفی و تفسیر و تحلیل عمیق آن‌ها به جهت فهم عمیق‌تر است. (نقی‌زاده و همکاران، ۱۳۹۳: ۳۱)

این پژوهش به دنبال تبیین رابطه بین تهدیدات سایبری زیرساخت‌های حیاتی و طبقه‌بندی آنها در قالب ارائه مدل مفهومی به گونه‌ای است که ضمن مشخص‌نمودن ویژگی‌های این گونه از تهدیدات و منطق طبقه‌بندی، بکارگیری آنها برای تصمیم‌سازان حوزه امنیت سایبر به سهولت انجام شود. در تحقیقات داخلی فعالیت‌های مرتبط و مفیدی انجام شده است لیکن به دلیل محدود بودن پژوهش‌ها در این مورد و نبود مطالعه‌ای با هدف بررسی توامان رابطه تهدیدات سایبری زیرساخت‌های حیاتی و طبقه‌بندی آنها در قالب ارائه مدل مفهومی، تلاش شد از طریق پایگاه‌های اطلاعاتی «ساینس‌دایرکت[3]»،

1. Lindgreen, Palmer and Vanhamm
2. Meta Study
3. ScienceDirect

«اسکوپوس[1] و ژورنال امنیت اطلاعات[2] با محوریت کلیدواژه‌های مرتبط به جستجو پرداخته شود و نتایج آن مورد بررسی و مطالعه قرار گیرد. در ادامه بر اساس مراحل ارائه شده در شکل(۳)، پژوهش انجام شد.

تجزیه و تحلیل یافته‌ها

۱. انتخاب هدف؛ در گام اول اجرای تحقیق با روش فراترکیب نیاز است تا هدف اصلی پژوهش آشکار شود. هدف اصلی این پژوهش، همان‌گونه که قبلاً اشاره شده است، «ارائه مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی» است.

۲. مشخص کردن سؤالات پژوهش، واژه‌های کلیدی و منابع جستجو؛ در این گام، برای تکمیل سؤال‌های پژوهش، موارد زیر بررسی و پاسخ داده شد:

- چه چیزی: شناسایی رابطه تهدیدات سایبری زیرساخت‌های حیاتی و طبقه‌بندی آنها موردمطالعه قرار گرفت؛
- جامعه موردمطالعه: پایگاه‌های اطلاعاتی «ساینس‌دایرکت[3]»، «اسکوپوس[4] و ژورنال امنیت اطلاعات[5]
- بازه زمانی: در منابع داخلی محدوده زمانی از ۱۳۹۱ الی ۱۳۹۸ و برای منابع خارجی از ۲۰۱۲ تا ۲۰۱۸ می‌باشد؛
- چگونگی روش: با روش تحلیل اسناد، داده‌های کیفی تحلیل شدند؛
- واژه‌های کلیدی: برخی از مهم‌ترین واژگان کلیدی مورد استفاده در جستجو شامل موارد زیر هستند(جدول ۲).

۳. بررسی و جستجوی انتخابی مقالات و منابع مرتبط: در آغاز فرآیند جستجو، تناسب مقالات دریافتی با سؤال پژوهش مشخص می‌شود. به این منظور، مجموعه

1. Scopus
2. Journal of Information Security (JIS)
3. ScienceDirect
4. Scopus
5. Journal of Information Security (JIS)

مطالعات منتخب در چندین مرحله بازبینی و در هر مرحله بازبینی، مقالات بر اساس عوامل مختلفی از جمله میزان ارتباط با موضوع تحقیق بررسی شدند و مواردی که دارای ارتباط کمتری بودند، از فرآیند فراترکیب در مراحل مختلف کنار گذاشته شدند.

٤. استخراج مفاهیم و کدهای مرتبط با موضوع پژوهش: در تمامی مراحل فراترکیب، پژوهشگر به‌طور پیوسته مقالات منتخب و نهایی شده را به‌منظور دستیابی به یافته‌های درون محتوایی مجزایی که در آن‌ها مطالعه‌های اولیه و اصلی انجام می‌شود، چندین بار مرور می‌کند. در این مرحله، محتوای مقالات و منابع استخراج‌شده به طور دقیق بررسی شد و کدهایی که ارتباط با واژه‌های کلیدی داشتند، انتخاب و بر اساس آن‌ها مفاهیم و مقوله‌ها شکل گرفت. در روند روش فراترکیب برای جستجوی مقالات تعداد ۹۵ مقاله گردآوری شد که پس از بررسی چکیده‌ها، بررسی محتوا و در نهایت سنجش ارتباط مستقیم با هدف محقق تعداد ۱۲ مورد مورد تایید قرار گرفت.

٥. استخراج مقوله‌ها(ترکیب یافته‌های کیفی)؛ با هدف ایجاد تفسیر یکپارچه و جدید از یافته‌ها پس از شناخت مفاهیم، طبقه‌بندی آن‌ها در قالبی مناسب برای ارائه بهترین توصیف انجام شد.

٦. تبیین ارتباط میان مفاهیم، مقوله‌ها و مضامین؛ این ارتباط در مدل مفهومی ارائه می‌شود.

جدول(۲) : نمونه‌ای از واحدهایی معنایی و کدهای استخراج‌شده

موضوع ارائه شده در مقاله	منبع	مفاهیم مستخرجه
در مدل‌سازی تهدیدات مایکروسافت، جریان داده و دنبال‌کردن پردازش‌های کلیدی روی داده در هر مرحله شناسایی و روند پردازش تهدیدات مشخص می‌شود..	مدل‌سازی‌تهدیدات سایبری، مجله شبکه و امنیت، شماره ۲۷۵، ۱۳۹۵، Achile	مراحل شناسایی و بررسی شامل: «نگاه به سیستم از دید نفوذگر»، «توصیف سیستم» و «شناسایی تهدیدات».
با رویکرد فناوری حملات، مدل سه بعدی متعامد	طبقه‌بندی تهدیدات امنیتی در سیستم‌های اطلاعاتی، ۲۰۱٤ Mouna Jouinia, , Latifa Ben Arfa Rabaia, Anis Ben Aissab	ابعاد مدل: انگیزه، بومی‌سازی[1]، عامل تهدید
با رویکرد فناوری حملات، مدل ترکیبی طبقه‌بندی تهدید		ابعاد مدل: فرکانس‌تهدید، محدوده فعالیت[2]، منبع تهدید
با رویکرد فناوری حملات، مدل هرمی طبقه‌بندی تهدیدات امنیتی		ابعاد مدل: آگاهی[3]، حساسیت منطقه، اتلاف[4]
با رویکرد توجه به اثر تهدید، مدل استرایدِ[5]		ابعاد مدل: اهداف، مقاصد حملات
با رویکرد توجه به اثر تهدید، مدل ایزو		ابعاد مدل: خرابی، تغییر، سرقت، حذف، افشاء اطلاعات، وقفه خدمات
با رویکرد توجه به اثر تهدید، مدل چندبعدی (هیبریدی)		ابعاد مدل: منبع، عامل، انگیزه، هدف، ااثر
شناسایی بعد منبع تهدید	مدل درختی شناسایی تهدیدات به عنوان اولین بخش از ارزیابی مخاطره در سیستم‌های اطلاعات سلامت، ۲۰۱۲-	مولفه‌های: انسانی، غیرانسانی، فنی، عملیاتی، محیطی
مدل سازمانی طبقه‌بندی تهدیدات سایبری		ابعاد: افشای‌تصادفی،کنجکاوی‌افراد داخلی، نقض اطلاعات توسط افراد خودی و خارجی،تهاجم فیزیکی و نفوذ غیرمجاز

۱. محلی سازی تهدید منعکس کننده تهدیدات داخلی یا خارجی است.

۲. نشان دهنده دامنه اثر تهدید مانند امنیت فیزیکی است امنیت پرسنل، امنیت ارتباطات و داده و امنیت عملیاتی.

۳. میزان آگاهی مهاجم در مورد سخت افزار، نرم افزار، کارمندان و دانش کاربران سیستم

٤. میزان زیان‌های قابل رخداد در سیستم یا سازمان (حریم خصوصی، صداقت. ..)

۵. روش طبقه بندی تهدیدات سایبری مایکروسافت(STRIDE)، شامل: جعل هویت، سوء استفاده از داده، انکار، افشاء اطلاعات، منع سرویس و افزایش سطح دسترسی STRIDE: Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service and Elevation of privilege.

موضوع ارائه شده در مقاله	منبع	مفاهیم مستخرجه
طبقه‌بندی ویتمن[1] (با رویکرد اولویت سنجی و رتبه‌بندی)	Ahmad Bakhtiyari Shahri, Zuraini Ismail	ابعاد: حملات نرم‌افزاری هدفمند، خطاهای نرم‌افزاری فنی، خطاهای انسانی، جاسوسی و.
طبقه‌بندی کوتز[2]		ابعاد: تهدیدات‌هویت، تهدیدات-دسترسی و تهدیدات افشاء
بررسی تولید و بکارگیری استاکس‌نت؛ تاثیر بر عملکرد سیستم‌های کنترلی برای دستگاه‌های کنترل‌کننده قابل برنامه‌ریزی	امنیت سایبری زیرساخت‌های حیاتی (۲۰۱۸) Leandros A. Maglaras Ki-Hyung Kim Helge Janicke Mohamed Amine Ferrag	بعد رفتاری تهدیدات: پدیده بی‌ثباتی در رفتار سیستم‌ها
فعالیت‌ها، نشان داده‌اند نیمی از تهدیدات، انسانی و در داخل سیستم است.		بعد عامل تهدید: انسان به عنوان سهم زیاد تهدیدات
هم‌افزایی سیستم‌های‌کنترل‌صنعتی، اینترنت اشیاءوتهدیدات جدید		بعد نوع تهدید: ترکیب ناشناخته از تهدیدات سایبری

۷. نظر به بررسی پیشینه‌ها و جهت تجمیع اطلاعات برای تدوین ابعاد، مولفه و شاخص‌های مرتبط با طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی، بر اساس اطلاعات مستخرجه از منابع فوق، نظرسازمان‌ها، نهادها و منابع علمی امنیت سایبری در خصوص تهدیدات سایبری مهم با محوریت رتبه‌بندی تهدیدات از گزارش سال ۲۰۱۷ انیسا و برخی منابع دیگر با توجه به لزوم اعتبارسنجی اطلاعات در (جدول ۳) ارائه شده‌است.

1. M. E. Whitman, “Enemy at the Gate: Threats to Information Security,”
2. D. Kotz, “A Threat Taxonomy for mHealth Privacy,” Proceedings of the 3rd International Conference on Com- munication Systems and Networks of the IEEE COMS- NETS, Bangalore, 4-8 January 2011, pp. 1-6.

جدول(۳)- تهدیدات سایبری و نظرات سازمان‌ها، نهادها و منابع علمی 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[1]	Trend Micro[2]
بدافزار	✓	✓	✓	✓	✓	✓			✓	✓	✓		✓
حملات مبتنی بر وب	✓			✓									
برنامه‌های کاربردی وب	✓			✓									
جلوگیری از سرویس	✓	✓		✓		✓	✓	✓			✓		✓
بات‌نت				✓		✓						✓	
فیشینگ	✓	✓		✓		✓	✓	✓			✓		✓
هرزنامه	✓	✓		✓		✓							
باج‌افزار	✓	✓	✓	✓	✓						✓	✓	
تهدیدهای داخلی				✓		✓							
دستکاری‌فیزیکی/ آسیب/ سرقت/ فقدان	✓			✓									
کیت‌های بهره‌بردار	✓	✓		✓	✓	✓							
نقض داده				✓									
سرقت هویت	✓			✓									
نشت اطلاعات		✓		✓									
جاسوسی سایبری			✓	✓	✓	✓	✓	✓					
فریب معکوس							✓	✓					
رمز ارزها							✓	✓				✓	
نشانه‌گذاری کاذب									✓				
اینترنت اشیاء											✓	✓	
مهندسی اجتماعی											✓		
خطای انسانی											✓		
هکتیویسم													✓

۱. شرکت فعال اسراییلی در زمینه اقدامات امنیت سایبری، ارائه‌کننده محصولات امنیتی سایبری حفاظت از شبکه‌ها و زیرساخت‌های حیاتی، گزارش سال ۲۰۱۸

۲. شرکت فعال آمریکایی در حوزه اطلاع‌رسانی امنیت سایبری، گزارش سال ۲۰۱۵

با توجه به اطلاعات فوق که اعتبارسنجی آنها براساس اسناد مربوط به سازمان‌ها، نهادها و منابع علمی امنیت سایبری ارائه شد، بر مبنای نظر محقق، کلیدواژه‌هایی بر اساس معیارهای مشترک در همه طبقه‌بندی‌ها و دسته‌بندی‌های ارائه‌شده، مشخص و تعریف شده‌اند که به عنوان «راهنمای مفاهیم مشترک» و یا «مشخصات تهدید» جهت بکارگیری در تکمیل مدل مفهومی نهایی مورد استفاده قرار گرفته‌اند. این مفاهیم در قالب شاخص‌های مرجع تهدیدات سایبری برای تجمیع اطلاعات بر اساس اخذ نظر از اسناد معتبرعلمی ملی و بین‌المللی بررسی و نتایج در(جدول٤) به منظور اعتبارسنجی ارائه شده‌اند که عبارتند از:

۱. هدف تهدیدات: نقطه انتهایی شامل: شبکه، سیستم، مؤلفه‌های نرم‌افزاری و سخت‌افزاری مورد توجه تهدیدکننده برای ابهام مدافعان در شناسایی اهداف حملات بعدی مثل: سیستم عامل، شبکه، کاربر و...

۲. منشاء/ تهدیدگران: اقدام‌کنندگان و مواردی که به عنوان فاعلیت عمل تهدید موردنظر می‌باشند.

۳. روش: روند یا سناریوی دسترسی مهاجم به سیستم بر اساس آسیب‌پذیری‌ها و بااستفاده از ابزارها است.

٤. آثار: شامل تاثیر عملیاتی: امکان دستیابی به منابع و داده‌های حساس برای مهاجمان و فراهم شدن اطلاعات سطح بالای کارشناسان و کاربران سیستم برای آنها. مثل: سوء استفاده از منابع، مسلط شدن بر کاربر و. .. و تاثیر اطلاعاتی: یک حمله علیه یک سیستم هدف می‌تواند به طرق مختلف روی اطلاعات حساس تأثیر گذارد. آثار مختلف حملات سایبری روی اطلاعات عبارتند از: دستکاری، وقفه، تخریب و. ..

۵. ابزار: کلیه نرم‌افزارها و وسایل مورد استفاده تهدیدکننده برای اقدامات تهدیدآمیز مثل: ویروس، بدافزارو. ..

٦. آسیب‌پذیری: کلیه نقایص موجود در طراحی، بکارگیری، امور فنی و مدیریتی سیستم که زمینه را برای اجرای تهدید و حمله مهیا می‌سازد. مثل: پیکربندی نادرست، عیوب

هسته، خطاهای طراحی، سرریز بافر، اعتبارسنجی ناکافی ورودی، پیوندهای نمادین، حمله توصیف‌گر فایل و. ..

۷. ریسک (مخاطره) شامل: ریسک انسانی: اقدامات و اعمال خطای افراد که موجب بروز تهدید می‌شود و ریسک سیستمی: خرابی سیستم‌ها و بکارگیری اشتباه فناوری که زمینه‌ساز بروز تهدید می‌شود.

۸. وقایع خارجی: موارد خارج از کنترل که می‌تواند شرایط بروز تهدید را فراهم نماید.

۹. انگیزه : انواع انگیزه‌های مالی، روانی، ایجاد تغییرات بیشتر، متفرق سازی و. ..

۱۰. نوع اقدام : اقدامات تهدیدکننده برای تهدیدات فعال و غیرفعال شامل: شنود، فریب، تغییر اطلاعات و. ....

۱۱. سطح تهدید: تاثر گذاری در سطوح منطقه‌ای، ملی و بین‌المللی

۱۲. فرکانس تکرار: تعداد تکرار یک تهدید در بازه زمانی مشخص

۱۳. شدت تهدید: میزان تاثیرگذاری بر هدف و مرتبط با میزان تحقق هدف از سوی تهدیدکننده و میزان خسارت بوجودآمده از سوی تهدیدشونده

جدول(٤) – تجمیع اطلاعات طبقه‌بندی‌های معتبر برای بررسی میزان اعتبار مفاهیم مشترک یا مشخصات تهدید، استخراج شده از مطالعه منابع

اسناد	رویکردها	مفاهیم مشترک در تحلیل تهدیدات سایبری											
		هدف تهدیدات	منشاء/ تهدیدگران	روش	آثار		ابزار	آسیب پذیری	ریسک		وقایع خارجی	انگیزه	اقدام/ عملیات
					تاثیر عملیاتی	تاثیر اطلاعاتی			ریسک انسانی	ریسک سیستمی			
سند افتا	اقدامات تهدیدآمیز												●
کنگره‌آمریکا	عوامل، گروه‌ها و منشاء		●										●
AVOIDIT[1]	شناسایی جزییات، دفاع و حمله	●		●	●	●							
CERT	انگیزه محور	●	●		●	●						●	●
Hansman & Hunt	پوشش‌حملات کامپیوتر و شبکه	●			●	●	●	●					●
VERDICT[2]	توجه به حمله و آسیب‌پذیری							●					
Howard[3]	پیشامد پایه	●			●	●	●	●					●
کارنگی ملون آپا[4]	ریسکهای امنیتی سایبری‌عملیاتی								●	●	●		
F-Secure	نرم‌افزار پایه						●						●
STRIDE[5]	مدل‌سازی تهدیدات سایبری												●
سیمانتک[6]	نقاط‌انتهایی[7]	●					●	●					●
کاسپر سکی[8]	//	●					●						●

1. Attack Vector, Operational Impact, Defense, Information Impact, and Target (AVOIDIT)
2. Validation Exposure Randomness Deallocation Improper Conditions Taxonomy (VERDICT)- Lough

۳. طبقه‌بندی حملات بر اساس پیشامدها. در این طبقه‌بندی برای حمله، سیستم هدف و نیز نتیجه حاصل از حمله تعیین می‌شود .حمله شاامل پنج مرحله است. ابزارها، آسیب‌پذیری، عملیات، هدف و نتیجه غیرمجاز.

4. CMU

۵. کلاهبرداری کردن از هویت کاربران، دستکاری داده‌ها، انکار، افشای اطلاعات، تکذیب سرویس و افزایش سطح دسترسی.

٦. شرکت سیمانتک(Symantec) بزرگترین شرکت تولیدکننده نرم‌افزارهای امنیتی به‌حساب می‌آید. این شرکت در سال ۱۹۸۲ توسط گری هِندریکس با کمک «بنیاد ملی علوم آمریکا» تأسیس شد.

۷. نقاط انتهایی شامل ابزارها، سیستم‌های سخت‌افزاری، نرم‌افزارها و هرگونه وسیله ارتباطی و بعضاً کاربران داخلی سازمان که در ارتباطات و انتقال اطلاعات دخیل هستند.

۸. کاسپرسکی(Kaspersky) شرکت روسی فعال در زمینه امنیت سایبری با محصول‌هایی مثل ضدویروس کاسپرسکی و دارای گروه فعال بین‌المللی در بیش از ۲۰۰ کشور در سراسر جهان.

اسناد	رویکردها	مفاهیم مشترک در تحلیل تهدیدات سایبری										
		هدف تهدیدات	مشاء/ تهدیدگران	روش	آثار		ابزار	آسیب پذیری	ریسک		وقایع خارجی	انگیزه	اقدام/ عملیات
					تاثیر عملیاتی	تاثیر اطلاعاتی			ریسک انسانی	ریسک سیستمی			
مَک‌آفی[1]	//	●					●	●					●
انیسا	//	●					●			●			●
ایسِت[2]	//	●					●	●	●			●	●
سیسکو	//	●					●						
سیسکو	شبکه[3]	●					●	●	●			●	●
انیسا	شبکه	●					●					●	●

۸. ارائه یافته‌ها؛ یافته‌های حاصل از مراحل قبل در قالب ابعاد، مولفه‌ها و شاخص‌ها از منابع ذیل، بر اساس هدف اصلی مقاله یعنی مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی ارائه می‌شود.

۸-۱. توجه به مدل فضای سایبروتهدیدات لایه بستر(زیرساخت)

۸-۲. منطق دسته‌بندی شرکت مایکروسافت و موارد گزارش انیسا سال(۲۰۱۷)

۸-۳. موارد استخراج شده از منابع حاصل از روش فراترکیب در فالب مقالات، کتاب‌ها و گزارش‌های پژوهشی

۸-٤. موارد ارائه شده در جدول تجمیع اطلاعات طبقه‌بندی‌ها و دسته‌بندی‌های معتبر برای تکمیل مدل مفهومی

۸-۵. استفاده از مفاهیم مشترک و جدول شاخص‌های مرجع تهدیدات سایبری

---

۱. مَک‌آفی(McAfee) شرکتی امنیتی فعال در حوزه امنیت رایانه‌ای که در سال ۱۹۸۷ توسط جان دیوید مَک‌آفی در شهر کالیفرنیا آغاز به کار کرد.

۲. ایسِت (Esset) موسسه امنیتی در حوزه فناوری‌اطلاعات است که. شروع فعالیت آن به سال ۱۹۸۷ باز می‌گردد.

۳. بررسی و ارزیابی تهدیدها و حمله‌های سایبری از سطح بالاتر (شبکه) هم امکان‌پذیر است به‌عنوان‌مثال، سازمان‌هایی –نظیر سیسکو و اِنیسا و...– مجموعه تهدیدها و حمله‌های سایبری را در سطح شبکه جمع‌آوری و ارزیابی می‌کنند.

جدول (۵)- ابعاد، مولفه‌ها و شاخص‌ها

ردیف	ابعاد	مولفه‌ها	شاخص‌ها
۱	توصیف سیستم	نیازمندی‌ها	- منابع خارجی - خط‌مشی امنیتی مدل‌سازی‌شده
		فرضیات	- جزییات طراحی - جزییات پیاده‌سازی
		سناریو استفاده	- آشکارنمودن آسیب‌پذیری‌ها - کوچکی حوزه بررسی سیستم - معتبرسازی مدل‌سازی تهدید - تشخیص راه‌های حمله
		اسناد امنیتی	- داخلی: اطلاعات و ویژگی‌های امنیتی سیستم و روش طراحی - خارجی:اطلاعات آگاه‌سازی کاربر از امنیت سیستم
۲	نگاه نفوذگر	تعیین دارایی‌ها	شناسایی، ارزش‌گذاری، وزن‌دهی، میزان دسترسی
		شناسایی ورودی‌ها و خروجی ها	رصد، پویش، پایش
		تعیین سطح اعتماد	حق دسترسی یک هویت خارجی به: دارایی‌ها، داده و تاثیر آن بر سیستم
۳	منابع شناسایی تهدیدات	بانک‌های اطلاعاتی	پایگاه‌های مقالات، گزارش‌های معتبر
		شرکت‌ها	شرکت‌های حوزه امنیت اطلاعات
		مجامع علمی	دانشگاهی، تشکل‌های سایبری، انجمن‌های علمی
٤	تهدیدات	تهدیدات پر تکرار	پانزده تهدید پرتکرار تشکیل دهنده بردار حمله
		بردارهای حمله	- نقض‌داده(جمع‌آوری‌اطلاعات، بهره‌برداری از آسیب‌پذیری، ارائه بدافزار، جمع‌آوری اطلاعات، کنترل از راه دور، انتقال غیر مجاز داده، اخاذی) - منع سرویس(شناسایی، جستجو، بهره‌برداری، انتشار، اجرا از راه دور، ارسال درخواست جعلی) - هدف‌مند(شناسایی و جمع‌آوری اطلاعات، ایجاد برنامه عملی خاص، محاصره دفاع شبکه‌های خارجی، نفوذ به شکاف‌های هوایی[1] وحمله‌های زنجیره‌ای، نصب بدافزارهای دیگر) - باج‌افزار
٥	مشخصات تهدید	برنامه	هدف، منشاء، انگیزه
		شرایط وقوع	بستر مخاطره، وقایع خارجی
		سطح	منطقه‌ای، ملی، بین‌المللی
		اجرای تهدید	ابزار، روش، نوع اقدام
		نتایج	آثار، شدت، تکرار
٦	عوامل تهدید	انسانی	انگیزه‌ها، سطوح توانایی‌و آمادگی، قدرت تاثیر،دانش، هوش، اطلاعات، اجتناب از شناسایی، استفاده از ابزار، غفلت، خطا
		غیرانسانی	برنامه‌ها، شرایط، موقعیت‌ها

1. Airgaps

در جدول قبل، مولفه انسانی بعد عوامل تهدید شامل: مجرمان سایبری، کارمندان داخلی[1]، جاسوس‌های سایبری[2]، هکتیویسم، متخلفان سایبری[3]، مبارزان سایبری[4]، تروریست‌های سایبری[5] و اسکریپت‌ها[6]. و مولفه غیرانسانی شامل:ربات‌ها، شرایط ناخواسته و غیرقابل کنترل و یا هر عامل غیرانسانی اجرای تهدید است.

۹. کنترل کیفیت: برای حفظ کیفیت مطالعه، از شاخص کاپا استفاده شده است. بدین طریق که شخص دیگری از خبرگان حوزه مطالعه حاضر، بدون اطلاع از نحوه ادغام کدها و مفاهیم ایجاد شده توسط پژوهشگر اقدام به طبقه بندی کدها در مفاهیم نمود. در ادامه مفاهیم ارائه شده توسط پژوهشگر (٦ مفهوم اصلی – ابعاد)با مفاهیم ارائه شده توسط این فرد مقایسه شد. در نهایت با توجه به تعداد مفاهیم ایجاد شده مشابه و متفاوت، شاخص کاپا محاسبه شد(جدول ٦).

جدول (٦) : پایایی روش فراترکیب

		نظر محقق		
		بله	خیر	مجموع
نظر خبره دیگر	بله	٤A=	١B=	٥
	خیر	١C=	٠D=	١
	مجموع	٥	١	٦N=

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

با توجه به مقدار شاخص کاپا برابر با ۰/٦۷ وضعیت شاخص در سطح توافق معتبر قرار گرفت.

1. Insiders
2. Cyber-spies
3. Cyber-offenders
4. Cyber-fighters
5. Cyber-terrorists
6. Script-kiddies

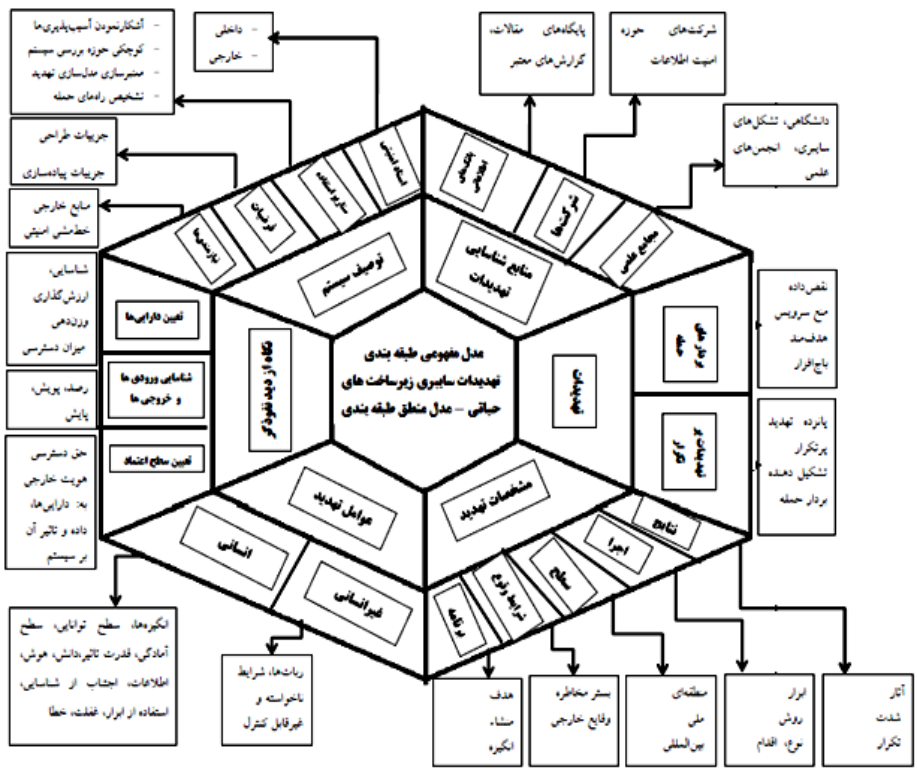
جدول (۷) : وضعیت شاخص کاپا (جنسن و آلن، ۱۹۹۶)

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

$$\text{توافقات شانسی} = \frac{A+B}{N} \times \frac{A+C}{N} \times \frac{C+D}{N} \times \frac{B+D}{N} = \frac{5}{6} \times \frac{5}{6} \times \frac{1}{6} \times \frac{1}{6} = 0.0192$$

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

نظر به اعتبار میزان بدست‌آمده عدد K بر اساس استاندارد اشاره‌شده در (جدول ۷)، موارد مستخرجه در قالب مدل مفهومی به شکل زیرارائه می‌شود(شکل ٤).



شکل (٤) – مدل مفهومی منطقی طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی

جمع‌بندی و پیشنهادها

منطق طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی با درنظرگرفتن نگاه سیستم از دیدگاه نفوذگر، توصیف سیستم، منابع شناسایی تهدیدات و ارتباط محورهایی همچون نوع تهدید، عوامل تهدید و مشخصات تهدید در قالب ابعاد منطق طبقه‌بندی با استفاده از مفاهیم مشترک استخراج شده از طبقه‌بندی‌های معتبر امنیتی ارائه‌شده و همچنین تحقیقات انجام شده در قالب مقالات و پژوهش‌های انجام شده، می‌تواند ارائه‌دهنده قالبی برای ایجاد طبقه‌بندی‌هایی خاص جهت تهدیدات سایبری زیرساخت‌های حیاتی باشد. بر این مبنا در موارد ذیل می‌توان با استفاده از نتایج تحقیق حاضر، پژوهش‌هایی مرتبط را به انجام رساند.

۱. تطبیق مدل مفهومی ارائه شده برای استفاده در طبقه‌بندی تهدیدات سایبری زیرساخت‌های حیاتی خاص مثل زیرساخت‌های ارتباطی و اطلاعاتی
۲. بررسی تهدیدات خاص مراکز داده در حوزه زیرساخت‌های ارتباطی و ارائه الگویی جهت طبقه‌بندی این تهدیدات بر اساس مدل مفهومی ارائه شده
۳. ارائه چارچوب مفهومی طبقه‌بندی تهدیدات سایبری مراکز داده با در نظرداشتن تمهیدات پدافندغیرعامل

فهرست منابع و مآخذ

الف. منابع فارسی

۱. سند راهبردی پدافند غیرعامل جمهوری اسلامی ایران، ۱۳۹۱
۲. سند راهبردی پدافند سایبری(۱۳۹٤)، سازمان پدافند غیرعامل
۳. سیاهکلی، محمد.(۱۳۹٤). طرح تحقیقاتی: الگوی تکالیف و مسئولیت سازمان‌ها در قبال امنیت فضای سایبر
٤. محمدی، علی(۱۳۹۲)؛ دسته‌بندی تهدیدات سایبری(با رویکرد طراحی نظام رصد تهدیدات سایبری)، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی
۵. خالقی، محمود؛(۱۳۹۱) ماموریت‌ها، ساختار تشکیلات و شرح وظایف قرارگاه پدافند سایبری کشور، مرکز پدافند سایبری کشور
٦. پورنقدی، بهزاد؛(۱۳۹۱) پدافندغیرعامل و بررسی تهدیدات نظم و امنیت در فضای سایبری
۷. عبدا...خانی، علی؛(۱۳۸۵) حفاظت از زیرساخت‌های حیاتی اطلاعاتی
۸. دبیرخانه شورای عالی امنیت فضای تبادل اطلاعات،(۱۳۸٤) سند راهبردی امنیت فضای تبادل اطلاعات کشور
۹. صلاحی، احمد؛(۱۳۹۳) حفاظت از زیرساخت‌های ملی در مقابل حملات سایبری،
۱۰. بلیکی، نوومن،(۱۳۹۳) طراحی پژوهش‌های اجتماعی ترجمه حسن چاووشیان، تهران، نشر نی
۱۱. سایت اینترنتی http://www.dadehara.com
۱۲. معاونت پژوهش و تولید علم دانشکده اطلاعات،(۱۳۹٤)حفاظت سایبری از زیرساخت‌های حیاتی
۱۳. سازمان فناوری اطلاعات،(۱۳۹۰) نظام دفاع سایبری، فصل ششم
۱٤. مجله شبکه و امنیت(۱۳۹۵)، شماره ۲۷۵
۱۵. اسماعیلی، علی؛ ثنا قربانی، جلال؛(۱۳۹۷) تبیین نسبت سناریوهای محتمل و مطلوب تهدیدات سایبری جمهوری اسلامی ایران، فصلنامه علمی – پژوهشی، امنیت ملی
۱٦. افتخاری، اصغر؛ (۱۳۹۲)برآورد تهدید-رویکردی نظام‌واره
۱۷. قوچانی خراسانی، محمدمهدی، حسین‌پور، داود؛(۱۳۹٦)، حاکمیت شبکه‌ای در نهادهای پژوهشی امنیت سایبری، دانشکده مدیریت و حسابداری دانشگاه علامه طباطبایی، فرایند مدیریت توسعه، دوره ۳۰، شماره ۱، ص ۸۰-۵۱،
۱۸. وظیفه‌دان، سارا؛(۱۳۹۵)، انواع تهدیدات در فضای سایبری و راهکارهای مقابله با آن، کنفرانس ملی پدافند غیرعامل در قلمرو فضای سایبر
۱۹. مشهدی، حسن، امینی ورکی، سعید؛ (۱۳۹٤)، تدوین و ارائه الگوی ارزیابی تهدیدات، آسیب پذیری و تحلیل خطرپذیری زیرساخت‌های حیاتی با تأ کید بر پدافند غیرعامل
۲۰. عرب‌سرخی، ابوذر؛ شبانی، فاطمه، ایوازه، اسما، چاردولی، امین؛(۱۳۹٦)؛ تدوین نقشه‌راه امنیت در حوزه ارتباطات و فناوری اطلاعات؛ پژوهشگاه ارتباطات و فناوری اطلاعات-پژوهشکده امنیت ارتباطات و فناوری اطلاعات-گروه ارزیابی امنیت شبکه و سامانه‌ها
۲۱. پایگاه اطلاع‌رسانی حوزه به آدرس https://hawzah.net/fa/Book/View/45217/14818/

ب. منابع لاتین

1. 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
2. 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
3. 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.
4. Thomas A. Johnson,"CyberSecurity,Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare" Webster University, St. Louis, Missouri, USA, 2015
5. "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.
6. ISO/IEC 27000, "Information technology - Security techniques - information security management systems – overview and vocabulary", 2014
7. U.S Department of Homeland Security, "National Cyber Incident Response Plan", September 2010
8. U.S. Office of Homeland Security, "The National Strategy for Homeland Security", July 16, 2002, p.30.
9. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cyber security", February 12, 2014
10. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity", January 10, 2017
11. HTTP://www.mio.gov.uk-134
12. Carvaliho, V.A. Almeida,J.P.A, Fonseca, C.M, & Guizzardi,G.(2017), Multi-level ontology based conceptual modeling Data & Knowledge Enginnering.
13. USGAO, United States Faces Challenges in Addressing Global Cybersecurity and Governance, United States Government Accountability Office, July 2010.
14. S.Hansman and R. Hunt, "A Taxonomy of Network and Computer Attacks," Computer and Security,2005
15. J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM ،CCR, April 2004
16. F. Lough, "A Taxonomy of Computer Attacks with Applications to Wireless Networks,"" Ph.D. Thesis,Virginia Polytechnic Institute and State University, 2001
17. J.D. Howard and T. Longstaff, "A Common Language for Computer Security Incidents" Technical report, Sandia National Laboratories, 1998
18. Thomas A. Johnson, "Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare", Webster University, St. Louis, Missouri, USA, 2015
19. www.techrepublic.com, 2017
20. www.infosecurity-magazine.com, 2017

21. ENISA Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends
22. www.nopsec.com, report of Cyber Attack, 2017
23. www.checkpoint.com, Security Report, 2018
24. Source:Check Point H2 2017 Global Threat Intelligence Trends Report, https://research.checkpoint.com/
25. h2-2017-global-threat-intelligence-trends-report
26. TREND Micro, Report on Cybersecurity and Critical Infrastructure in the Americas, 2015
27. https://www.gartner.com/technology/research/it-spending-forecast/
28. https://ec.europa.eu/digital-single-market/en/news/comprehensive-approach-evolving-cyber-threats,accessed November 2017.
29. The Department of Homeland Security, Critical Infrastructure Sectors, Last Published Date: August 22, 2018
30. POSTNOTE, Cyber Security of UK Infrastructure, Number 554 May 2017
31. David P. Duggan, John T. Michalski, "A Threat Analysis Framework as Applied to Critical Infrastructures in the Energy Sector ",Sandia National Laboratories, September 2007
32. 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
33. 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
34. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cyber security", February 12, 2014
35. UK Cabinet Office, "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world", November 2011
36. David Clark, Characterizing cyberspace: past, present and future, MIT CSAIL, 2010