فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره ۲، بهار ۱۴۰۱
مقاله اول، از صفحات ۷-۴۴

مقاله پژوهشی:

ارائه مدل مفهومی مدیریت تهدیدات ناشی از تروریسم سایبری

حسین امیرلی[۱]، کامیار ثقفی[۲]

تاریخ دریافت: ۱۴۰۰/۰۳/۱۰ **تاریخ پذیرش: ۱۴۰۰/۰۹/۱۶**

چکیده

رشد روزافزون فضای سایبر و جذابیت‌های موجود در این فضا سبب شده، بخش قابل‌توجهی از فعالیت‌های روزمره شهروندان، کسب‌وکارها، تفریح و سرگرمی آن‌ها به فضای مزبور منتقل گردد؛ خصوصیات منحصربه‌فرد فضای سایبر، زمینه را برای فعالیت مجرمین و تبهکاران تسهیل نموده است؛ تروریسم سایبری یکی از این تهدیدات راهبردی است که در سال‌های اخیر بسیاری از کشورها ازجمله جمهوری اسلامی ایران با آن مواجه بوده است. اسناد راهبردی کشورهای پیشرو نیز حاکی از قرار گرفتن این تهدید در اولویت‌های نخست تهدیدات این کشورها است به‌طوری‌که منابع زیادی را برای رویارویی با آن اختصاص می‌دهند. در این مقاله پس از مطالعه پیشینه‌های مرتبط با تروریسم و تروریسم سایبری، جایگاه آن در میان سایر تهدیدات فضای سایبری تبیین شده و درنهایت تعریف محقق ساخته از تروریسم سایبری بیان گردیده و در ادامه مدیریت تهدیدات، روش‌های ارزیابی تهدید، رویکردهای مدیریتی تشریح و با بهره‌گیری از آن‌ها، مدل مفهومی ترسیم و با کسب نظرات خبرگان این حوزه مورد آزمون قرارگرفته و مدل نهایی ارائه‌شده است.

کلیدواژه‌ها: تروریسم، تروریسم سایبری، مدیریت تهدیدات

۱. دانشجوی مقطع دکتری دانشگاه عالی دفاع ملی (نویسنده مسئول)، *h.amirli@chmail.ir*
۲. عضو هیئت علمی دانشگاه شاهد.

مقدمه

رشد روزافزون فن‌آوری اطلاعات و امتزاج آن با سایر علوم بشری سبب ظهور فضای جدیدی به نام فضای سایبر گردیده است؛ با پیدایش آن، بسیاری از فعالیت‌های انسان اعم از فعالیت‌های اقتصادی، اجتماعی و سیاسی و... به این فضا منتقل یا در حال انتقال به آن می‌باشد؛ در این میان، تبهکاران و مجرمین سنتی نیز فضای نوین را برای پیاده‌سازی مقاصد خود، مناسب دیده و تلاش می‌نمایند، ضمن مهاجرت به فضای مزبور، از امکانات گستردهٔ آن بهره‌برداری کنند؛ آنان به سبب چابکی با استفاده از منابع این فضا، سریع‌تر از دولت‌ها و شرکت‌های بزرگ قدرتمندتر می‌شوند و دامنهٔ تهدیدات سایبری را گسترش می‌دهند. تروریسم سایبری یکی از تهدیدات سایبری است که با افزایش وابستگی زیرساخت‌های حساس و حیاتی[۱] کشورها به فضای سایبر (مانند حمل‌ونقل، انرژی، شبکهٔ بهداشت و غیره) جذابیت‌های بیشتری برای این دسته از تبهکاران فراهم‌شده و آن‌ها به سهولت از اهرم‌های فشاری که این فضا در اختیارشان قرار می‌دهد به‌منظور پیشبرد اهداف سیاسی و اجتماعی و... خود بهره‌برداری می‌نمایند. آسیب‌پذیری و صدمات ناشی از حملات تروریستی، در جوامعی که به شبکه‌های الکترونیکی وابستگی بیشتری دارند، بسیار وسیع‌تر است؛ این خطر به‌گونه‌ای است که یک مقام امنیتی امریکا گفته «با یک میلیارد دلار و بیست نفر متخصص و خبرهٔ رایانه می‌توان کل امریکا را فلج نمود»؛ یک تروریست هم می‌تواند به این توانایی دست یابد. روندشناسی تهدیدات سایبری در چند سال اخیر این واقعیت را نشان می‌دهد که احتمال وقوع برخی تهدیدات مانند جنگ سایبری در جهان بسیار ضعیف بوده و غیر از چند مورد نادر (که اغلب کشورها در آن اتفاق‌نظر ندارند) نمونهٔ واقعی آن تاکنون تحقق‌نیافته است ولی مصادیق تهدید تروریسم سایبری به‌وفور در کشورهای مختلف قابل‌مشاهده است؛ بنابراین ضرورت دارد این تهدید با اولویت بیشتری مورد پیگیری قرار گیرد. مسئله این تحقیق چگونگی کاهش دامنهٔ خسارت و پیامدهای تروریسم سایبری شکل‌گرفته است و بر این اساس تلاش می‌شود چگونگی بهبود تاب‌آوری[۲] در مقابل آن بهبود یابد و روشی را برای احصای

---

۱. Critical Infrastructure

۲. Resistance

آسیب‌پذیری کشور در حوزهٔ فضای سایبر و اولویت‌بندی آن برای اثربخشی اقدامات در قبال تهدید تروریسم سایبری ارائه شود. پژوهش حاضر باهدف «دستیابی به مدل مفهومی مدیریت تهدیدات ناشی از تروریسم سایبری» و به‌منظور پاسخگویی به این سؤال که «مدل مفهومی مدیریت تهدیدات ناشی از تروریسم سایبری چگونه است؟» و سؤالات فرعی «ابعاد و عوامل مدیریت تهدیدات ناشی از تروریسم سایبری کدام‌اند؟ اولویت‌بندی و ارزیابی تهدیدات تروریسم سایبری چگونه صورت می‌پذیرد؟ چگونه رویکرد مناسب مدیریتی برای رویارویی با تهدیدات تروریسم سایبری انتخاب می‌شود؟» برنامه‌ریزی‌شده است.

مبانی نظری

در این بخش، نخست کلیدواژهٔ اصلی مبحث تبیین می‌گردد و در ادامه پیشینه‌های مرتبط با تروریسم و تروریسم سایبری، تبیین جایگاه آن در میان سایر تهدیدات فضای سایبری تبیین شده و درنهایت تعریف محقق ساخته از تروریسم سایبری و روش ردیابی آن ارائه می‌شود؛ سپس مدیریت تهدیدات، روش‌های ارزیابی تهدید، بررسی و نحوهٔ کاربست آن‌ها در تهدیدات ناشی از تروریسم سایبری به‌صورت مدل مفهومی ترسیم می‌گردد.

تروریسم سایبری[۱]: تروریسم سایبری یک حملهٔ سایبری با بهره‌کشی یا استفاده از رایانه یا شبکه‌های ارتباطی برای ایجاد تخریب مؤثر به‌منظور ترس و ارعاب یک جامعه یا یک هدف ایدئولوژیک می‌باشد (Seissa and Yahaya, ۲۰۱۷).

مدیریت مخاطرات[۲]: عبارت است از شناسایی دارایی‌های کلیدی کسب‌وکار، شناسایی تهدیدات، ارزیابی خسارتی که ممکن است از یک حملهٔ موفق حادث‌شده باشد، شناسایی آسیب‌پذیری‌های سامانه‌ها که ممکن است مورد بهره‌برداری حمله‌کننده قرار گیرد و حاصل‌ضرب آن‌ها. پس از ارزیابی مخاطرهٔ امنیتی، اقدام برای کاهش مخاطره با پیاده‌سازی کنترل‌های مناسب و نظارت بر اثربخشی کنترل‌های اجراشده صورت می‌پذیرد (NIST, ۲۰۰۸)؛ در بسیاری از کشورها این

۱. cyber Terrorism

۲. Risk Management

نوع مدیریت اثربخش (مدیریت مخاطرات) در چالش‌های اقتصادی و مـالی، اجتمـاعی و فرهنگـی تحت عنوان مدیریت مخاطرات و در مسائل امنیتی و نظـامی بـا عنـوان مـدیریت تهدیـد مشـاهده می‌شود. در کشور امریکا در برابر انواع تهدیدات مانند طوفان، سیل و زلزله و همچنـین حفاظـت از تأسیسات و اماکن حساس و حیاتی از این شیوهٔ راهبردی استفاده می‌شود و متناسـب بـا تهدیـداتی احتمالی، روش‌ها، تجهیزات و فرایندهای حفـاظتی سـامان داده می‌شـود (Leson, ۲۰۰۵). در پـژوهش حاضر با توجـه بـه اسـتفاده از مـدیریت مخـاطرات در مسـائل امنیتـی یعنـی تروریسـم سـایبری، به‌طورکلی به آن مدیریت تهدید اطلاق خواهد شد.

مفهوم شناسی ترور

در فرهنگ دهخدا آمده است: «ترور مأخوذ از زبان فرانسه و به معنـی قتـل سیاسـی، به‌وسـیلهٔ اسلحه است و در فارسی متداول شده است؛ این کلمه در فرانسه به معنی وحشـت و خـوف آمـده است و تروریست به شخصی اطلاق می‌شود که با اسلحه، مرتکب قتل سیاسـی بشـود. تروریسـم در زبان فارسی، به اصلی گفته می‌شود که در آن از قتل‌های سیاسـی و تـرور دفـاع گـردد» (دهخـدا، ۱۳٤۳: ٦۳٦). در برخی از فرهنگ‌های فارسـی نیـز تروریسـم، روش کسـانی معرفی‌شـده اسـت کـه «آدم‌کشی و تهدید مردم و ایجاد خوف و وحشت را به هر طریق که باشد، برای رسیدن به اهـداف خود، لازم دانسته‌اند» (عمید، ۱۳۵۷: ٥٦۹).

تعریف تروریسم

با توجه به تنوع فراوان فضای وقایع تروریستی، هر گروه و یا عمل تروریستی متناسـب بـا هـر تعریف متعارف از تروریسم، معمولاً در جهات مختلف منحصربه‌فرد اسـت؛ بااین‌حـال، چنـد بعـد عمومی وجود دارد که برای تشخیص برخی از تروریست‌ها، گروه‌های تروریستی با توجه به تنـوع فراوان فضای وقایع تروریستی، هر گروه و یا عمل تروریستی متناسب بـا هـر تعریـف متعـارف از تروریسم، معمولاً در جهات مختلف منحصربه‌فرد می‌باشد؛ بااین‌حـال، چنـد بعـد عمـومی وجـود دارد که برای تشخیص برخی از تروریست‌ها، گروه‌های تروریستی و اقدامات تروریسـتی از سـایر اقدامات به کار می‌رود. گروه‌های تروریستی خاص و اقدامات فردی تروریسم در هر یـک از انـواع دسته‌بندی بر اساس این ابعاد مشخص می‌شوند: آیا انگیزه‌های سیاسی وجود دارد یا نه؟ آیـا اقـدام

تحت حاکمیت دولت عامل انجام‌شده یا نه؟ درجهٔ ارتباط با سازمان‌های تروریستی چقدر است؟ سازمان‌دهی و برنامه‌ریزی چگونه است؟ آیا ازنظر مذهبی یا قومی توجیه دارد؟ آیا در درجهٔ اول هدف، مردم هستند و یا اهداف نمادین دارد؟ چه نوع مردمی را هدف قرار می‌دهد؟ هر مورد معمولاً می‌تواند به‌راحتی مشخص شود یا در ترکیب خاصی از این ابعاد که مناسب‌اند قرار گیرد. تغییر رفتار در میان این دسته‌بندی‌های مختلف ممکن است در بسیاری از موارد، بیشتر از تغییر رفتار در یک دسته‌بندی خاص باشد (forest, ۲۰۰۹:۸). بر اساس قانون سال ۲۰۰۰ تروریسم بریتانیا، تروریسم استفاده یا تهدید با یک اقدام طراحی‌شده برای تأثیرگذاری به دولت و یا سازمان‌های بین‌المللی یا ارعاب مردم و یا بخشی از جامعه و اجبار به‌منظور پیشبرد سیاسی، مذهبی، نژادی و یا علت ایدئولوژیک آن شامل موارد ذیل است:

خشونت جدی علیه فرد، آسیب جدی به اموال، تهدید زندگی فرد، خطر جدی برای سلامت و ایمنی عمومی، دخالت جدی یا اختلال به سیستم الکترونیکی (uiijf, ۲۰۱٤:۱٤).

بروس هافمن[۱] تعریفی از تروریسم ارائه نمود که شامل شاخص‌های این پدیده می‌باشد «ایجاد و بهره‌برداری از خشونت یا تهدید به خشونت» برای دستیابی به تغییرات سیاسی. همهٔ تروریست‌ها به خشونت و تهدید به خشونت اقدام می‌کنند. تروریسم به‌طور خاص طراحی می‌شود تا آثار روانی گسترده و فوری بر قربانی یا مفعول حملات داشته باشد؛ این به معنای القای ترس و درنتیجه، ارعاب مخاطبان هدف که ممکن است رقیب قومی یا گروه مذهبی، یک کشور، دولت ملی، حزب سیاسی و یا افکار عمومی باشد. تروریسم برای ایجاد قدرت درجایی که قدرت حاکمیت ضعیف می‌باشد طراحی‌شده است. با تبلیغ ایجادشده توسط خشونت، تروریست‌ها به دنبال به دست آوردن اهرم، نفوذ و قدرت هستند؛ در غیر این صورت آن‌ها فاقد تأثیرگذاری در تغییرات سیاسی در مقیاس منطقه‌ای و بین‌المللی هستند (Chuipka, ۲۰۱۷).

۱. Bruce Hoffman

انواع تروریسم

محققان در ایالات‌متحده در دهۀ ۷۰، در پی دهه‌ای که به همراه رشد و پیشرفت‌های گروه‌های سیاسی تروریستی داخلی و بین‌المللی بود، انواع متفاوتی از تروریسم را از هم تفکیک کردند که عبارت‌اند از:

۱. ***تروریسم دولتی***[۱]: بسیاری از تعاریف تروریسم، آن را به عاملان غیردولتی محدود می‌کند اما می‌توان به این بحث پرداخت که دولت‌ها می‌توانند تروریست باشند و در عمل نیز چنین بوده‌اند. دولت‌ها این امکان را دارند که زور یا تهدید را بدون اعلان‌جنگ به‌کارگیرند تا با ترساندن افراد به خواسته‌های سیاسی دست یابند. نمونۀ بارز این نوع از تروریسم، رژیم اشغالگر قدس است؛

۲. ***تروریسم سایبری***: در ادامۀ بحث به‌طور کامل به آن پرداخته خواهد شد؛

۳. ***اکو تروریسم***[۲]: تروریسم هسته‌ای به روش‌های متفاوتی وجود دارد که ممکن است مواد هسته‌ای به‌منزلۀ روشی تروریستی به کار گرفته شوند؛ این امر شامل حمله به تأسیسات هسته‌ای، خریداری سلاح‌های هسته‌ای، ساخت آن‌ها یا یافتن راه‌هایی برای آزادسازی مواد رادیواکتیو است؛

٤. ***نارکوتروریسم***[۳]: نارکوتروریسم از زمان شکل‌گیری در سال ۱۹۸۳ تاکنون معنای گوناگونی داشته است؛ نخستین معنای آن اعمال خشونت قاچاقچیان دارو به‌منظور تأثیرگذاری بر حکومت‌ها یا جلوگیری از تلاش‌های آن‌ها در متوقف ساختن تجارت دارو بود. در سال‌های اخیر نارکوتروریسم به موفقیت‌هایی اشاره دارد که گروه‌های تروریستی از قاچاق دارو برای تأمین مالی دیگر فعالیت‌هایشان بهره می‌گیرند؛

---

۱. State Terrorism

۲. Eco-Terrorism

۳. Narcoterrorism

۵. ***بیوتروریسم***[۱]: حملهٔ بیوتروریسم، آزادسازی عمدی ویروس‌ها و باکتری‌ها یا دیگر عوامل میکروبی است که برای ایجاد بیماری یا مرگ انسان‌ها، حیوانات یا گیاهان به کار می‌رود؛ این عوامل معمولاً در طبیعت یافت می‌شوند اما این امکان است که برای افزایش قدرت بیماری‌زایی‌شان، مقاوم‌سازی آن‌ها به داروهای متداول یا افزایش قدرت انتشارشان در محیط، آن‌ها را تغییر دهند (جلالی، ۱۳۸۹).

شناخت انواع تروریسم نیازمند شناخت عناصر اساسی به‌وجودآورندهٔ این پدیدهٔ شوم می‌باشد که عبارت‌اند از:

۱- اینکه تروریسم عملی از پیش طراحی‌شده است؛ ۲- این کنش دارای جهت‌گیری کلان است؛ ۳-قربانیان بی‌دفاع بوده و وسیله‌ای هستند دررسیدن به هدف؛ ٤- عوامل مرتکب ترور گروه‌های مخفی فرو ملی و یا بعضاً فراملی هستند (ناجی راد،۱۳۸۷:٤۳). با درک صحیح از سه عنصر اول می‌توان اشکال مختلف تروریست را این‌گونه بیان نمود: تروریسم مذهبی، تروریسم دولتی، تروریسم هسته‌ای، تروریسم ملی‌گرا، تروریسم سایبری، تروریسم فرهنگی (همان،۷۸).

الرحمن (۲۰۰۷) استدلال می‌کند که تروریسم نیز می‌تواند از طریق ابزار مورداستفاده در عملیات تقسیم‌بندی شود؛ مثلاً «تروریسم هسته‌ای» اشاره به استفاده از سلاح‌های هسته‌ای در فعالیت‌های تروریستی دارد یا «سایبر تروریسم»، استفادهٔ سیاسی از شبکه‌های رایانه‌ای، داده‌ها و نرم‌افزارهای گروه‌های فراملیتی به‌منظور تهدید و یا ایجاد خشونت به‌منظور «ارعاب مخاطبان گسترده» می‌باشد؛ به همین ترتیب، باکر و ون زویدوویون[۲] (۲۰۱٦) به «تروریسم شیمیایی»، «بیولوژیکی» و «رادیولوژیکی» اشاره می‌کنند که با دستگاه‌های خانگی ساخته‌شده‌اند (Bester, ۲۰۱۹).

تروریسم سایبری

در دهه‌های اخیر بسیاری از رشته‌های علوم برای پژوهش در این حوزه وارد شدند و به همین دلیل طیف گسترده‌ای از تعاریف مابین سال‌های ۱۹۹۷ تا ۲۰۰۱ در مورد تروریسم سایبری

---

۱. Bioterrorism

۲. Bakker and van Zuijdewijn

منتشرشده که از آشفتگی زیادی برخوردار بوده است؛ به برخی از این تعاریف در ذیل اشاره و در خاتمهٔ مبحث، به تعریف محقق ساخته از تروریسم سایبری می‌پردازیم:

دنینگ[1] در سال ۲۰۰۱ تروریسم سایبری را چنین تعریف می‌نماید: «حملات غیرقانونی و تهدید علیه رایانه‌ها، شبکه و اطلاعات به‌منظور ارعاب مردم و حاکمیت برای پیشبرد اهداف سیاسی و اجتماعی می‌باشد» (Denning, ۲۰۰۱) .در ویکی‌پدیا تروریسم سایبری چنین تعریف می‌شود: «اقدامات برنامه‌ریزی‌شده و هدفمند با اغراض سیاسی و غیرشخصی که علیه رایانه‌ها و امکانات و برنامه‌های ذخیره‌شده در درون آن‌ها از طریق شبکهٔ جهانی صورت می‌گیرد و هدف از چنین اقدامی، نابودی یا وارد آوردن آسیب‌های جدی به آن‌هاست». در پلیس فدرال ایالات‌متحده (FBI) تروریسم سایبری: «یک اقدام جنایی با استفاده از رایانه و قابلیت‌های ارتباطات راه دور که نتیجهٔ آن خشونت، تخریب یا اختلال در خدمات، باهدف ایجاد ترس از طریق ایجاد سردرگمی و عدم اطمینان در داخل یک جمعیت مشخص، به‌منظور تأثیرگذاری بر یک دولت یا جمعیت با یک برنامهٔ خاص سیاسی، اجتماعی یا ایدئولوژیک است» (Lourdeau, ۲۰۰٤). دولت هلند با استفاده از تعریف اتحادیهٔ اروپا، تعریف خود را تغییر داده و به شرح ذیل منتشر نمود: «تهدید، آماده‌سازی و انجام اعمال خشونت‌آمیز با دلایل ایدئولوژیک به افراد یا خسارت زدن به اموال برای اخلال در جامعه باهدف تغییر اجتماعی و ارعاب در عموم مردم و تأثیر بر تصمیمات سیاسی اطلاق می‌گردد» (NCTb, ۲۰۱٤)؛ تعریف دیگر، آماده‌سازی، تهدید یا استفاده از یک اقدام طراحی‌شده برای دستیابی به یک تغییر اجتماعی، با ایجاد ترس و وحشت در بین مردم برای تأثیرگذاری در تصمیم سیاسی دولت یا سازمان‌های بین‌المللی به‌منظور پیشبرد اهداف سیاسی، مذهبی، نژادی و عقیدتی از طریق تأثیرگذاری بر تمامیت و محرمانگی و دسترس‌پذیری اطلاعات و سامانه‌های اطلاعاتی و شبکه، یا دسترسی غیرمجاز مؤثر بر اطلاعات و کنترل‌های فرایندهای فیزیکی مبتنی بر فن‌آوری ارتباطات که منجر به رنج و آسیب‌های جدی یا مرگ افراد، آسیب‌های مؤثر به اموال، ضرر اقتصادی مؤثر، نقض مؤثر در محیط‌زیست، یک مخاطرهٔ مؤثر بر سلامتی و ایمنی عمومی، نقض ثبات سیاسی و اجتماعی و انسجام یک ملت شود اطلاق می‌گردد (Akhgar, ۲۰۱٤:۱٦).

---

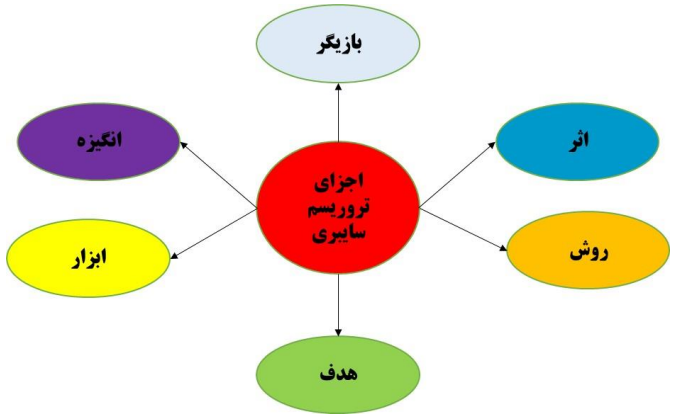
۱. Dorothy E. Denning

گروه مطالعاتی ایلا[۱] در سال ۲۰۱۶ با بررسی و تجمیع کلیهٔ تعاریف موجود تلاش نموده‌اند نواقص تعاریف قبلی را مرتفع و تعریف جامع‌تری ارائه نمایند: «تروریسم سایبری عبارت است از اقدام عمدی هر فردی با استفاده از فناوری اطلاعات و ارتباطات به‌صورت غیرقانونی با روش‌هایی که انجام یا قصد عامدانه برای مرگ افراد یا آسیب مؤثر به اموال عمومی یا خصوصی، اقتصاد، محیط‌زیست و یا اختلال مؤثر در خدمات عمومی باهدف ارعاب جمعیت غیرنظامی یا مجبور کردن دولت، جمعیت غیرنظامی یا سازمان بین‌المللی به انجام یا اجتناب یک عمل خاص را فراهم نماید اطلاق می‌شود» (P.Fidler and etal, ۲۰۱۶) برابر تعریف ناتو: تروریسم سایبری یک حملهٔ سایبری با بهره‌کشی یا استفاده از رایانه یا شبکه‌های ارتباطی برای ایجاد تخریب مؤثر به‌منظور ترس و ارعاب یک جامعه با یک هدف ایدئولوژیک می‌باشد».(SEissa and Yahaya, ۲۰۱۷) به استناد تعریف بورس هافمن از تروریسم می‌توان یک مجموعه شاخص‌هایی را به تروریسم سایبری اختصاص داد؛ نخست اینکه از طریق فضای سایبر انجام شود؛ دوم اینکه دارای اهداف و انگیزه‌های ایدئولوژیک و سیاسی باشد؛ سوم با خشونت و یا تهدید به خشونت همراه باشد؛ چهارم طراحی‌شده برای پیامدهای روانی گسترده و فوری بر هدف باشد؛ پنجم توسط سازمان با فرماندهی و یا ساختاری برای توطئه (بدون لباس و نشان شناخته‌شده) یا افراد و مجموعه‌ای از افراد باانگیزه با الهام از اهداف ایدئولوژیک یا مثالی از جنبش‌های تروریستی با راهبران آن بوده و درنهایت مرتکب یک گروه محلی یا نهاد غیردولتی باشد (Chuipka, ۲۰۱۷).

اجزای تروریسم سایبری

اجزای تروریسم سایبری در شکل (۱) توصیف نموده است:

۱. ILA, Study Group on Cybersecurity, Terrorism, and International Law, http://www.ila-hq.org/en/studygroups/index.cfm/cid/۱۰۵۰.



شکل (۱): اجزای تروریسم سایبری

در این شکل بازیگر می‌تواند به‌عنوان یک مشارکت‌کننده در هرگونه اقدام یا فرایند باشد؛ که به هر شخص، گروه یا سازمان اشاره می‌کند. انگیزه به هر دلیلی از اقدام یا رفتار در یک روش خاص اشاره دارد؛ آن می‌تواند هر مفهوم، ایدئولوژی یا انتقام باشد. ابزار، وسیله‌ای برای انجام اقدام خاص مانند سلاح و جنگ‌افزار شبکه است. هدف به شخص، سازمان، دولت، جامعه، اشیا اطلاق می‌شود. روش، یک رویهٔ خاص برای انجام یا نزدیک شدن به برخی چیزهاست. روش به هر اقدام یا عمل که مربوط به تروریسم سایبری است، اشاره می‌کند. تأثیر به‌عنوان یک اثر مشخص‌شده یا نفوذ تعریف می‌شود و می‌تواند در چهار دستهٔ فیزیکی، روان‌شناسی، اجتماعی و اقتصادی طبقه‌بندی‌شده باشد. هر خشونت و تهدید که بر روی هدف انجام شود می‌تواند به‌عنوان تأثیر در نظر گرفته شود (Salleh and etal ۲۰۱۶). با یک نگاه اجمالی در تعاریف تروریسم سایبری و مطالب بیان‌شده، می‌توان کلیدواژه‌های اصلی آن را استخراج نمود؛ این کلیدواژه‌ها عبارت‌اند از:

هدف (نیروهای نظامی، حاکمیت سایبری و زیرساخت‌های فیزیکی، زیرساخت‌های حیاتی ملی، هویت ملی و اجتماعی، هویت و صنعت بخش خصوصی)، انگیزه (انگیزهٔ اجتماعی، دینی مذهبی، سیاسی و ایدئولوژیک)، ابزار و وسیله (رایانه و فناوری‌های ارتباطی و شبکه‌ها)، تأثیر (خشونت، انهدام و اختلال خدمات، فیزیکی، خسارت عملیاتی و اطلاعاتی و صدمه به اشخاص و گروه‌ها)، قصد و نیت (منفعت سیاسی، اجتماعی، نظامی و مزیت ایدئولوژیک) (Al Mazari and etal, ۲۰۱۶).

تروریسم سایبری از منظر هدف

همان‌طوری که قبلاً نیز بیان شد، تروریسم سایبری درصدد ایجاد رعب و وحشت برای دستیابی به اهداف موردنظر است. تروریسم سایبری را بر اساس اهداف آن می‌توان طبقه‌بندی کرد:

۱. ***حملات تروریسم سایبری علیه نیروهای نظامی:*** این نوع از حملات تروریسم سایبری ممکن است در اشکال مختلف مانند حملهٔ انکار سرویس، جاسوسی و جنگ علیه طیف وسیعی از تأسیسات، وظایف، عملیات و خدمات و قابلیت‌های نظامی انجام شود؛

۲. ***تروریسم سایبری علیه دولت سایبری و زیرساخت‌های فیزیکی:*** این نوع از حملهٔ تروریستی، تسهیلات و زیرساخت‌های دولتی را مورد هدف قرار می‌دهد؛ مانند حملاتی که در کشور گرجستان علیه دولت الکترونیک شکل گرفت؛

۳. ***تروریسم سایبری علیه زیرساخت‌های ملی حیاتی:*** حملات تروریسم سایبری ممکن است طیف گسترده‌ای از زیرساخت‌های ملی و حیاتی مانند زیرساخت‌های مالی مهم سازمان‌ها، سدها، دستگاه‌های تصفیهٔ آب، سامانه‌های مخابراتی، امکانات پستی، مؤسسات آموزشی، سامانه‌های حمل‌ونقل، ارائه‌دهندگان خدمات بهداشتی، خدمات رسانه، اورژانس، خدمات و امکانات انرژی را مورد هدف قرار دهد؛

٤. ***تروریسم سایبری علیه هویت ملی و اجتماعی:*** سازمان‌ها و ملت‌ها برای توسعهٔ محیط موردنظر برای عملیات مؤثر و بدون اشتباه تلاش می‌نمایند. یکی از اهداف تروریست‌ها تلاش برای نابودی شهرت و اعتبار یک سازمان یا ملت است؛ مانند دیفیس کردن سایت اینترنتی سازمان و پخش شایعات در آن؛

۵. ***تروریسم سایبری علیه موجودیت‌ها و صنایع خصوصی:*** سازمان‌های تجاری میلیون‌ها دلار بابت حملات تروریسم سایبری از دست می‌دهند؛ مانند بدافزار باران تایتان (SEissa and et al., **۲۰۱۷)**.

تروریسم سایبری از منظر الگوهای مجرمانه

بر اساس تحقیقات مؤسسه (SANS)[۱]، الگوهای مجرمانهٔ تروریسم سایبری به حمله، تخریب، قطع سرویس، نشر اکاذیب و بدشکل کردن وب‌سایت‌ها تقسیم می‌شود. حمله و تهاجم خیلی معمولی است و به‌صورت گسترده انجام می‌شود و برای نفوذ به سامانه‌ها و شبکه‌ها به‌منظور دستیابی یا دست‌کاری اطلاعات صورت می‌پذیرد. تخریب باهدف ایجاد مزاحمت برای سامانه‌های رایانه‌ای و شبکه‌ها به‌منظور واردکردن آسیب شدید به عملیات سازمانی است. قطع خدمات یا انکار سرویس باهدف اخلال در معاملات جاری از طریق روانه نمودن سیل بسته‌های داده، به سمت سرور انجام می‌شود. نشر اکاذیب شامل انتشار اطلاعات مخرب در مورد قربانی باهدف خدشه‌دار کردن شهرت قربانی است. بدشکل کردن وب‌سایت‌ها نیز به‌منظور تغییر محتویات، تعبیهٔ پیام نامطلوب و هدایت کاربر به وب‌سایت‌های با محتوای نامطلوب و با مقاصد تبلیغاتی است (Al Mazari et al., ۲۰۱٦).

تروریسم سایبری از منظر ایجاد عوامل مخاطره

۱. مخاطرات امنیت ملی: زیرساخت‌های بسیاری از کشورها بر اساس فن‌آوری سایبری، مانند سخت‌افزار و نرم‌افزار رایانه‌ای و شبکه‌های ارتباطی پایه‌گذاری شده است؛ لذا این زیرساخت‌ها با حملات و تهدیدات سایبری مواجه هستند. انهدام فیزیکی و مجازی و یا قطعی هریک از این خدمات ممکن است، زندگی ملت مشخصی را به‌صورت مستقیم و غیرمستقیم تهدید نماید؛

۲. ***مخاطرات مالی:*** مخاطرات مالی حملات سایبری به اشخاص و سازمان‌ها محدود نمی‌شود و آن‌ها در سطح ملی نیز گسترش می‌یابند؛ گرچه هدف این حملات ساختارهای سازمانی و دولتی است ولی آن‌ها به‌صورت معنی‌دار بر اقتصاد یک کشور از طریق اختلال و قطع خدمات اثرگذار هستند؛ این خدمات عبارت‌اند از شکست در ارائهٔ محصولات و خدمات در مقابل نیازهای بازار و درنتیجه چالش‌های روانی، فیزیکی و اقتصادی ملی؛

۳. ***مخاطرات فرهنگی و اجتماعی:*** بسیاری از حملات سایبری سبب ایجاد خسارت به تصویر و اعتبار یک سازمان، شخص، جامعه یا فرهنگ می‌شوند. بدشکل کردن وب‌سایت‌ها و

---

۱ - System Administration, Networking, and Security Institute

انتشار اکاذیب علیه یک سازمان یا شخص از طریق ایمیل، وب‌سایت یا شبکه‌های اجتماعی سبب از بین رفتن اشتهار قربانی می‌شود و در کل این نوع حملهٔ سایبری نباید دست‌کم گرفته شود. یکی دیگر از مخاطرات اجتماعی از دست دادن محرمانگی و عدم حفاظت از اطلاعات و افشای غیرمجاز آن برای دشمنان است. از دست دادن محرمانگی یکی از موارد از دست دادن اعتبار اجتماعی است. از دست دادن تمامیت و محرمانگی در یک نظام معیوب منجر به پیامدهایی مانند عدم دقت اجتماعی، اشتباه در تصمیم‌گیری و تقلب می‌شود.

٤. ***مخاطرات اختلال عملیاتی:*** تروریسم سایبری به دارایی‌های غیر فیزیکی مانند اقتصاد محدود نمی‌شود بلکه به زیرساخت‌های فیزیکی که عملیات و فراهم‌سازی خدمات را انجام می‌دهند، گسترش می‌یابد. یک حملهٔ موفق ممکن است اختلال جدی در سامانهٔ ترافیک راه‌آهن که به جابه‌جایی مردم، وسایل و کالاها مربوط می‌شود، ایجاد نماید. اختلال در حمل‌ونقل اثر منفی بر موقعیت تجاری یک کشور خواهد گذاشت. حملات سایبری بر منابع انرژی و سامانه‌های ارتباطی نیز اثر مشابهی بر جای می‌گذارد.

۵. ***مخاطرهٔ انهدام فیزیکی:*** ممکن است انهدام فیزیکی یکی از نتایج حملات سایبری بوده و به‌صورت یک موضوع کلیدی از اهداف اصلی دشمن باشد. انهدام فیزیکی یک توانمندی از طریق بهره‌گیری از فن‌آوری اطلاعات و ارتباطات به‌منظور ایجاد خسارت در اموال، ابزارها یا هر دارایی فیزیکی دیگر است. زیرساخت‌های ملی مانند بیمارستان‌ها، نیروگاه‌های برق، سامانه‌های آب و حمل‌ونقل می‌تواند موضوع این تهدید باشد که از طریق سامانه‌های اسکادا کنترل می‌شوند (Al Mazari and etal., ۲۰۱٦).

شاخصه‌های موردنیاز برای بررسی شبکه‌های تروریستی

شناخت شبکه‌های تروریستی به‌عنوان یک نظام ضروری است؛ با این شیوه، درک بهتری از فرهنگ، انگیزه، مدل عملیات و سازمان‌یافتگی شبکه‌های تروریستی حاصل می‌شود. در ادامه به پنج نوع متغیر حالت ناشی از رویکرد شبکه‌ای پرداخته می‌شود: ***سطح سازمانی تروریست‌ها*** – *طرح مدیریتی آن*: تا چه حد یک تروریست یا گروهی از آن‌ها در یک شبکه سازماندهی می‌شوند؟ و به چه چیزی شباهت دارند؟ ***سطح توصیفی***– *روایتی که گفته می‌شود*: چرا عضو

شبکهٔ خاص فرض شده‌اند؟ چرا آن‌ها به این فرم باقی‌مانده‌اند؟ ***سطح دکترین***- *روش‌ها و نقاط قوت مشترک:* چه دکترینی برای به کار بردن بهتر شبکهٔ سازمان وجود دارد؟ ***سطح فن‌آوری***- ***سامانه‌های اطلاعاتی:*** چه الگو و ظرفیتی برای جریان اطلاعات و ارتباطات درون شبکه وجود دارد؟ چه فن‌آوری‌هایی آن را پشتیبانی می‌کند؟ ***سطح اجتماعی***- *وابستگی‌های شخصی، اطمینان، وفاداری و اعتماد*: یک شبکه با عملکرد کامل بستگی دارد به اینکه چقدر خوب است و از چه روشی اعضای شناخته‌شده را به یکدیگر پیوند می‌دهد؛ این پنج متغیر برای بررسی شبکه‌های تروریستی جامع و فراگیر هستند و با متغیرهای دیگر مانند *سطح بودجه* که از گروه‌های تروریستی پشتیبانی می‌کند *و سطح پیچیدگی* که گروه با آن می‌تواند برای توسعهٔ اقدامات خاص و قابلیت‌ها و مقاصد خود اقدام نماید تکمیل می‌شوند (Y.HAIMES, ۲۰۰۹).

راهبردهای تروریست‌های سایبری

ارعاب: تروریست‌ها با استفاده از تهدید و ارعاب تلاش می‌کنند مردم را متقاعد سازند که آن‌ها به‌اندازهٔ کافی برای مجازات نافرمانی، قدرتمند هستند و دولت نیز بیش‌ازاندازه ضعیف است.

تحریک: این راهبرد حریف را به دادن پاسخ تروریست‌ها با یک خشونت بی‌رویه وادار می‌نماید تا جمعیتی را تحریک نموده و به حمایت از تروریست‌ها حرکت نمایند.

تباه کردن: حملهٔ تباه‌کنندگان، تلاش برای متقاعد ساختن حریف به میانه‌روی با تروریست‌های ضعیف و غیرقابل‌اعتماد به‌منظور دستیابی به توافق صلح است.

روی دست کسی بلند شدن: گروه‌هایی که از خشونت استفاده می‌کنند، می‌خواهند عموم مردم را به اینکه تروریست‌ها عزم بیشتری از رقبا برای نبرد با دشمنان دارند و درنتیجه درخور حمایت هستند، متقاعد کنند.

فرسایشی: در راهبرد فرسایشی تروریست‌ها به دنبال متقاعد کردن حریف هستند به اینکه تروریست‌ها به‌اندازهٔ کافی قوی برای تحمیل هزینه‌های قابل‌توجه هستند، اگر دشمن آن‌ها به یک سیاست مشخصی ادامه دهد (Chuipka, ۲۰۱۷). پس از بررسی ادبیان نظری پیرامون تروریسم سایبری، از جمع‌بندی آن‌ها تعریف محقق ساخته از تروریسم ارائه می‌شود:

تعریف محقق ساخته از تروریسم سایبری

هرگونه تهدید یا اقدام طراحی‌شدهٔ غیرقانونی، آگاهانه و عمدی افراد، گروه‌ها، بازیگران دولتی و غیردولتی برای ایجاد رعب و وحشت در جامعه از طریق فضای سایبر با نقض مؤلفه‌های اساسی امنیت یعنی تمامیت، محرمانگی، دسترس‌پذیری و تأثیرگذاری بر تصمیم سیاسی دولت یا سازمان‌های بین‌المللی، صنایع خصوصی، زیرساخت‌های حیاتی، حساس، مهم، کنترل‌های فرایندهای فیزیکی مبتنی بر فضای سایبر، به‌منظور پیشبرد اهداف نظامی، سیاسی، مذهبی، نژادی و ایدئولوژیک و فردی یا هر هدف خاص دیگر که منجر به مواردی مانند خشونت، رنج و آسیب مؤثر جسمی و روحی، نقض ثبات سیاسی، هویت ملی و ارزش‌های اساسی جامعه، آسیب مؤثر بر اموال، سلامت و ایمنی عمومی، اقتصاد، محیط‌زیست شود، تروریسم سایبری اطلاق می‌گردد.

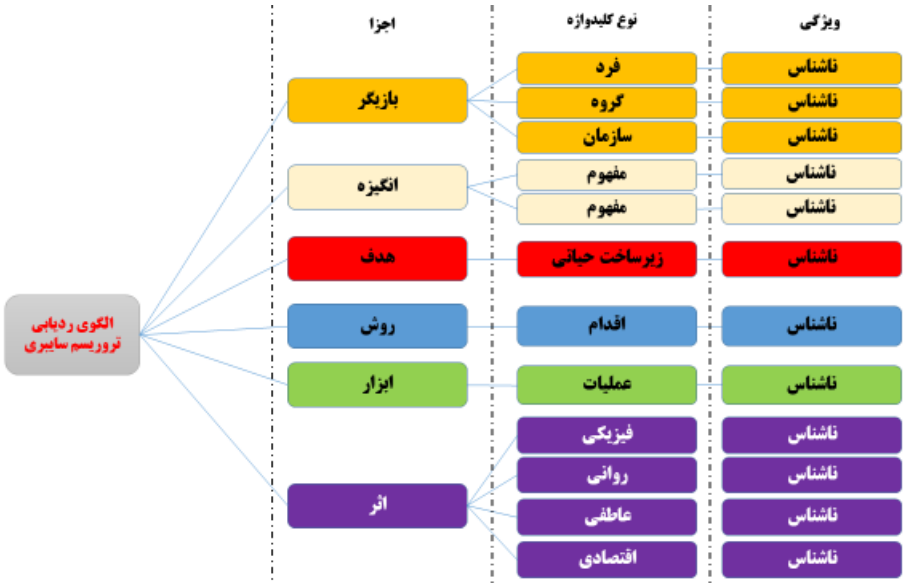
ردیابی تروریسم سایبری

روش ردیابی یکی از شیوه‌های ردگیری فعالیت تروریست‌ها بر مبنای جمع‌آوری اطلاعات آن‌ها از فضای سایبر و داده‌کاوی است. در فن ردیابی سه مرحله وجود دارد و برای کشف فعالیت‌های تروریسم سایبری بر اساس اجزای تروریسم سایبری (بازیگران، اثر، روش، هدف، ابزار و انگیزه) به شرح ذیل اقدام می‌شود:

مرحلهٔ اول ردیابی استخراج و طبقه‌بندی: یعنی روش جستجو کلمه و روش‌های جستجوی وب برای استخراج استفاده می‌شود. ردیابی برای تدوین الگوی ردیابی و کشف آثار استفاده می‌شود. ردیابی هر کلمهٔ کلیدی مورداستفاده توسط تروریست یا URL می‌تواند باشد؛ در این مرحله، ردیاب‌ها طبقه‌بندی می‌شوند؛ گروه، سازمان، مفهوم، ایدئولوژی، زیرساخت حیاتی، عمل، عملیات، روانی، عاطفی و اقتصادی است. فرایند طبقه‌بندی کلمات کلیدی به نوع کلمات کلیدی بر اساس معنی کلمه بستگی دارد.

مرحلهٔ دوم ردیابی مراجع و پیوند: هدف اصلی این فرایند در این مرحله به دست آوردن آثار کامل از فعالیت‌های تروریسم سایبری است؛ بنابراین، پس از ردیابی طبقه‌بندی‌شده در مرحلهٔ اول، ارتباط بین ردیاب‌ها به‌منظور شناسایی روابط برقرار می‌شود. ارجاع متقابل نیز برای شناسایی رابطه بین صفات و اجزای تروریسم سایبری انجام می‌شود.

مرحلهٔ سوم ارزیابی ردیابی: در این مرحله، ردیابی‌هایی که در مرحلهٔ دوم مرتبط شده‌اند مورد بهره‌برداری قرارگرفته و برای شناسایی فعالیت‌های تروریسم سایبری از الگوی ردیابی استفاده می‌شود. برای هر نوع از کلمهٔ کلیدی شناسایی‌شده در وب‌سایت با نقشه‌برداری، اجزای تروریسم سایبری شامل بازیگر، انگیزه، ابزار، روش، هدف و تأثیر وجود خواهد داشت؛ روند نقشه‌برداری در شکل نشان داده‌شده است (Salleh, ۲۰۱٦).



شکل (۲) الگوی ردیابی تروریسم سایبری

مدیریت تهدیدات

در بسیاری از کشورها از شیوه‌های مدیریتی برای رویارویی با چالش‌های اقتصادی و مالی، اجتماعی فرهنگی تحت عنوان مدیریت مخاطرات و در مسائل امنیتی و نظامی با عنوان مدیریت تهدید مشاهده می‌گردد که ارزیابی تهدید یا مخاطره بخش عمدهٔ آن است (Leson, ۲۰۰۵). هرچند ریسک و تهدید بخشی از یک منطق هستند که سطح مشخصی از عدم اطمینان آن‌ها مجزا می‌نماید و بر همین اساس هم در مکتب امنیتی مبتنی بر تهدید کپنهاگ، مخاطره از تهدید جداشده است؛ این در حالی است که مکتب مدیریت پاریس هر دو (تهدید و خطر) را پوشش می‌دهد (Munk, ۲۰۱۵:۲۱۱). با توجه به اینکه پژوهش حاضر در حوزهٔ مسائل امنیتی قرار دارد،

بنابراین در این تحقیق به آن مدیریت تهدید اطلاق می‌شود که بخش عمدهٔ آن ارزیابی تهدید خواهد بود.

ارزیابی تهدید

اجزای ضروری که در ارزیابی تهدیدات به کار می‌روند عبارت‌اند از (Leson, ۲۰۰۵):

شناسایی زیرساخت‌های حیاتی و دارایی‌های کلیدی[۱]: زیرساخت‌های حیاتی و دارایی‌های کلیدی، زیرساخت‌هایی هستند که سلامت، امنیت عمومی، حاکمیت، امنیت اقتصادی و ملی، حفظ اعتماد عمومی مرتبط می‌شوند؛

ارزیابی میزان حساسیت و حیاتی بودن آن‌ها[۲]: تلاش نظام‌مند برای شناسایی و ارزیابی دارایی‌های مهم و یا حیاتی در یک حوزه است. ارزیابی حساسیت به برنامه‌ریزان برای تعیین اهمیت نسبی دارایی، اولویت‌بندی و تخصیص منابع به دارایی‌های حیاتی کمک می‌کند. از یک شاخص پنج‌گانه برای تخمین میزان تأثیر از دست دادن زندگی و مال، وقفه در خدمات یا استفاده از دارایی‌ها یا کسب منفعت توسط دشمن استفاده می‌نماید؛

ارزیابی تهدید[۳]: تلاش نظام‌مند برای شناسایی و ارزیابی تهدیدات مانند تهدیدات تروریستی موجود و بالقوه برای دارایی هدف است. اطلاعات ضروری برای جمع‌آوری و تجزیه‌وتحلیل و ارزیابی تهدید شامل:

الف – نوع دشمن مانند تروریست، دستهٔ دشمن مثل دشمن خارجی یا داخلی، تروریست یا جنایتکار؛ ب– اهداف دشمن مانند سرقت، خرابکاری، شمار دشمنان مورد انتظار برای هر دسته، مانند بمب‌گذار انتحاری، تروریست‌ها و باندها، اهداف گزینشی دشمن مثل زیرساخت‌های حیاتی، ساختمان‌های دولتی و غیره؛ ج– نوع فعالیت‌های برنامه‌ریزی موردنیاز برای اجرای هدف مانند عکس و نظارت پلیس یا الگوهای گشت‌زنی، به‌احتمال‌زیاد یا «بدترین حالت» زمان حملهٔ دشمن هنگام شلوغی یا شب؛ د– طیفی از تاکتیک‌های دشمن مانند مخفی‌کاری و فریب؛ ه–

---

۱. Criticality Assessment: Evaluating Assets

۲. Calculating Criticality

۳. Threat Assessment

قابلیت‌های دشمن مانند دانش و انگیزه است. سطوح تهدید بر اساس درجه و میزان ترکیب عوامل ذیل ارائه می‌شود (این سطوح به‌صورت نمونه برای گروه‌های تروریستی تبیین شده است):

۱. موجودیت: یعنی گروه تروریستی وجود داشته باشد و یا قادر به کسب دسترسی محلی باشد؛ ۲. قابلیت: با توانایی یک گروه تروریستی به انجام یک حمله ارزیابی می‌شود؛ ۳. قصد و نیت: شواهدی از فعالیت گروه تروریستی، ازجمله قصد اظهار و ارزیابی‌شده برای هدایت فعالیت تروریستی؛ ٤. تاریخچه: فعالیت تروریستی انجام‌شده درگذشته؛ ۵. هدف قرار دادن: اطلاعات معتبر کنونی و یا فعالیتی به‌منظور آماده‌سازی برای مجموعه عملیات اطلاعاتی تروریستی خاص توسط یک گروه مظنون، تهیهٔ دستگاه‌های مخرب یا اقدامات دیگر؛ ٦. محیط امنیتی: وضعیت سیاسی و امنیتی حوزه که تحت تأثیر عناصر تروریستی قرارگرفته‌اند را نشان می‌دهد؛ برای اندازه‌گیری تهدید نیز از شاخص‌های کمی شدهٔ بحرانی، بالا، متوسط، پایین و ناچیز استفاده می‌شود.

ارزیابی آسیب‌پذیری[۱]: عبارت است از شناسایی نقطه‌ضعف در ساختارهای فیزیکی، سامانه‌های حفاظت کارکنان، فرایندها و یا مناطق دیگر که ممکن است توسط تروریست‌ها مورداستفاده قرار گیرد. فاکتورهایی که برای اندازه‌گیری آسیب‌پذیری مورداستفاده قرار می‌گیرند عبارت‌اند از:

۱. **محل سکونت**: موقعیت جغرافیایی اهداف بالقوه یا امکانات، مسیرهای ورود و خروج، موقعیت تأسیسات یا اهداف مربوط به مناطق همگانی، مسیرهای حمل‌ونقل یا مناطقی که به‌راحتی شکننده هستند؛

۲. **دسترسی**: چگونگی دسترسی به تأسیسات یا هدف دیگر توسط دشمن؛

۳. **کفایت**: کفایت از امکانات ذخیره‌سازی، حفاظت و ممانعت از دسترسی به دارایی‌های باارزش و یا حساس مانند مواد خطرناک، سلاح‌ها، وسایل نقلیه یا تجهیزات سنگین و مواد

۱. Vulnerability Assessment

منفجره یا موادی که برخی از اشخاص و یا سازمان‌های فرصت‌طلب می‌توانند به‌عمد برای ایراد صدمه استفاده نمایند؛

٤. **در دسترس بودن:** در دسترس بودن تجهیزات، کفایت نیروها واکنشی و به‌طورکلی اقدامات امنیتی فیزیکی.

محاسبهٔ تهدید: کلیهٔ ارزیابی‌های قبلی برای تکمیل و به تصویر کشیدن تهدید یک دارایی یا گروهی از دارایی‌ها ترکیب می‌نماید:

۱. حساسیت یا میزان حیاتی بودن دارایی: دربارهٔ اینکه اگر یک دارایی شناسایی‌شده از بین برود یا از یک رویداد خاص خسارت یا آسیب ببیند چه تأثیر احتمالی خواهد داشت، سؤال می‌کند؛

۲. احتمال تهدید: دربارهٔ اینکه چقدر احتمال دارد دشمن به دارایی شناسایی‌شده حمله نماید، سؤال می‌کند؛

۳. **آسیب‌پذیری:** دربارهٔ اینکه دشمن از چه آسیب‌پذیری‌هایی احتمالاً برای هدف قرار دادن دارایی استفاده خواهد کرد، سؤال می‌کند؛ فرمول ارزیابی تهدید = دارایی‌های کلیدی*آسیب‌پذیری*احتمال وقوع خلاصه می‌شود.

ارزیابی تهدیدات در سازمان پدافند غیرعامل کشور

در این سازمان با رویکردهای گوناگون به ارزیابی تهدیدات که مهم‌ترین بخش مدیریت تهدیدات است پرداخته و درنهایت تلاش شده یک چارچوب و مدل بومی در این رابطه ارائه شود؛ برخی از الگوهایی که در این رابطه موردمطالعه قرارگرفته‌اند عبارت‌اند از:

۱. روش ارزیابی تهدیدات توسط آژانس مدیریت شرایط اضطراری فدرال[۱]؛ ۲. مدل رمکپ[۲]؛ ۳. روش میز؛ ٤. روش ارزیابی مخاطره و تهدید توسط مؤسسهٔ ملی دادگستری امریکا؛ ۵. چارچوب ارزیابی تهدیدات در سازمان پدافند غیرعامل (سازمان پدافند غیرعامل, ۱۳۹۱).

---

۱ - Fema

۲ -RAMCP: Risk Analysis and Management for Critical Asset Protection

روش (OWASP)

رویکرد استانداردی توسط OWASP[۱] برای ارزیابی مخاطره عرضه‌شده است در این روش «تهدید= احتمال * اثر» می‌باشد:

مرحلهٔ اول: شناسایی تهدید- در اولین گام برای شناسایی یک خطر امنیتی، نیاز است تا نرخ‌گذاری صورت پذیرد. آزمون‌کنندهٔ نخست به جمع‌آوری اطلاعات دربارهٔ عامل حمله می‌پردازد که شامل حمله‌ای است که از یک آسیب‌پذیری استفاده می‌کند و به‌طور موفق بر کسب‌وکار تأثیر می‌گذارد؛ به‌طورکلی بهتر است بدترین گزینه که بیشترین خطر را دارد انتخاب شود.

مرحلهٔ دوم: عوامل تخمین احتمال- هنگامی‌که آزمون‌کننده خطر احتمالی را شناسایی کرد، می‌خواهد بداند چقدر جدی است؛ بنابراین احتمال را باید ارزیابی کند؛ لازم نیست این برآورد خیلی دقیق باشد و به‌طورکلی با طیف کم، متوسط و زیاد سنجیده می‌شود.

برخی از عوامل وجود دارد که به سنجش احتمال کمک می‌کند؛ اولین عامل، عامل تهدید است؛ هدف، تخمین احتمال یک حملهٔ موفق از یک گروه مهاجمین می‌باشد. توجه داشته باشید که عوامل تهدید چندگانه‌ای ممکن است وجود داشته باشد که می‌تواند از آسیب‌پذیری خاص بهره‌برداری نماید؛ بنابراین بهتر است بدترین احتمال استفاده شود.

ویژگی‌های عامل تهدید: اولین مجموعه، ویژگی‌های عامل تهدید است. هدف تخمین احتمال یک حملهٔ موفق به‌وسیلهٔ گروهی از عوامل تهدید می‌باشد. بدترین حالت برای عامل تهدید در نظر گرفته می‌شود:

---

۱ - The Open Web Application Security Poroject

جدول (۱): خصوصیات عامل تهدید

ردیف	ویژگی	توصیف
۱	سطح مهارت	عوامل تهدید چقدر از مهارت فنی برخوردار هستند؟ مهارت نفوذ امنیتی(۹) مهارت برنامه‌نویسی و شبکه(۶) کاربر پیشرفته رایانه(۵) برخی از مهارت های فنی(۳) بدون مهارت فنی(۱)
۲	انگیزه	عوامل تهدید برای پیدا کردن و بهره‌برداری از آسیب‌پذیری چقدر انگیزه دارند؟ کم و بدون پاداش(۱) امکان پاداش(۴) پاداش بالا(۹)
۳	فرصت	برای این گروه از عوامل تهدید به منظور پیدا کردن و بهره‌برداری از آسیب‌پذیری چه منابع و فرصتهای وجود دارد؟ دسترسی کامل و منابع گرانبها مورد نیاز است(۰) دسترسی یا منابع ویژه مورد نیاز است(۴) برخی از دسترسیها و منابع مورد نیاز است(۷) دسترسی و منابع نیاز نیست(۹)
۴	اندازه	گروه عوامل تهدید چقدر بزرگ هستند؟ توسعه دهندگان(۲) مدیران سیستم(۲) کابران اینترانت(۴) شرکاء(۵) کلبران احراز هویت شده(۶) کاربران گمنام در اینترنت(۹)

ویژگی‌های آسیب‌پذیری: سری بعدی از خصوصیات مربوط به آسیب‌پذیری‌هاست؛ هدف تخمین احتمال کشف و بهره‌کشی از یک آسیب‌پذیری با فرض انتخاب عامل تهدید ذکرشدهٔ بالا می‌باشد.

جدول (۲): خصوصیات آسیب‌پذیری

ردیف	ویژگی آسیب پذیری	توصیف
۱	کشف آسان	چقدر عوامل تهدید به سهولت آسیب پذیری را کشف مینماید؟ به طور مشخص ناممکن(۱) مشکل(۳) آسان(۷) با ابزار های خودکار در دسترس است(۹)
۲	سهولت در بهره برداری	به درستی چقدر بهره برداری از این آسیب پذیری برای گروه تهدید آسان است؟ به صورت تئوریک یا نظری(۱) مشکل(۳) آسان(۵) با ابزارهای خودکار(۹)
۳	آگاهی	عوامل تهدید چقدر این آسیب پذیری را میشناسند؟ ناشناخته(۱) مخفی(۴) آشکار(۶) دانش عمومی(۹)
۴	تشخیص نفوذ	چقدر احتمال دارد که بهره کشی و سوء استفاده تشخیص داده شود؟ با برنامه کاربردی فعال(۱) با بررسی لاگ ها(۳) لاگ بدون بررسی(۸) بدون لاگ(۹)

مرحله سوم: عوامل تخمین اثر– با توجه به تأثیر یک حملهٔ موفقیت‌آمیز مهم است بدانیم دو نوع اثر وجود دارد؛ اول «تأثیر فنی» بر روی برنامه‌های کاربردی، داده‌های مورداستفاده و توابع آن را فراهم می‌نماید؛ دیگر «کسب‌وکار سازمان»؛ هر عامل گزینه ۰ تا ۹ را به خود اختصاص می‌دهد.

جدول (۳): عوامل تأثیر فنی

عوامل تأثیر منفی		
ردیف	ویژگی آسیب‌پذیری	توصیف
۱	از دست دادن محرمانگی	چقدر داده می‌تواند افشاء شود و حساسیت آن‌ها چقدر است؟ افشای حداقل داده‌ها و غیر حساس‌اند؟(۲) حداقل اطلاعات حیاتی افشاشده (٦) داده‌های غیر حساس گسترده افشاشده (٦) داده‌های حیاتی افشاشده (۷) تمام داده‌های افشاشده (۹)
۲	از دست دادن تمامیت	چقدر اطلاعات خراب‌شده و چقدر آسیب‌دیده است؟ حداقل اطلاعات کمی تخریب‌شده (۱) حداقل اطلاعات به‌طورجدی خراب‌شده (۳) اطلاعات با شدت کمی خراب‌شده (۵) اطلاعات به‌طورجدی خراب‌شده (۷) تمام داده‌ها کاملاً خراب‌شده (۹)
۳	از دست دادن دسترس‌پذیری	چقدر خدمات می‌تواند ازدست‌رفته باشد و چقدر حیاتی هستند؟ حداقل خدمات ثانویه قطع‌شده (۱) حداقل خدمات اولیه قطع‌شده (۵) خدمات ثانویه فراوانی قطع‌شده (۵) خدمات اولیه گسترده قطع‌شده (۷) تمام خدمات به‌طور کامل از بین رفته‌اند (۹)
٤	از دست رفتن حسابرسی و انتساب	آیا اقدامات عوامل تهدید قابل‌ردیابی و انتساب به یک فرد است؟ کاملاً قابل‌ردیابی (۱) احتمالاً قابل‌ردیابی (۷) کاملاً ناشناس (۹)

عوامل کسب‌وکاری اثر: تأثیر کسب‌وکاری بر تأثیر فنی اثرگذار است اما نیاز به درک عمیق ازآنچه برای سازمان مهم است، می‌باشد. ویژگی‌های زیر برای بسیاری از کسب‌وکارها مشترک است اما این منطقه حتی خصوصیات مربوط به عامل تهدید، آسیب‌پذیری و اثر فنی برای سازمان منحصربه‌فردتر است.

جدول (٤): عوامل تأثیر تجاری

عوامل تجاری اثر		
ردیف	ویژگی آسیب‌پذیری	توصیف
۱	خسارت مالی	چقدر خسارت مالی از این بهره‌کشی حاصل‌شده است؟ کمتر از هزینه رفع آسیب‌پذیری (۱) اثر جزئی بر سود سالانه (۳) اثر معنی‌دار بر سود سالانه (۷) ورشکستگی (۹)
۲	خسارت بر اعتبار	آیا سوءاستفاده منجر به آسیب رسیدن به اعتبار و درنتیجه خسارت به کسب‌وکار شده است؟ حداقل خسارت (۱) از دست دادن حساب کاربری اصلی (٤) از دست دادن حسن نیت (۵) خسارت به نام تجاری (۹)
۳	عدم انطباق	چقدر در معرض عدم انطباق قرار می‌گیرد؟ نقض جزئی (۲) نقض روشن (۵) نقض بالا (۹)
٤	نقض حریم خصوصی	چقدر اطلاعات شخصی قابل‌شناسایی افشاء شده است؟ یک فرد (۳) صدها نفر (۵) هزاران نفر (۷) میلیون‌ها نفر (۹)

مرحلهٔ چهارم: تعیین شدت تهدید– در این مرحله، تخمین احتمال و اثر برای شدت تهدید صورت می‌گیرد که شامل گزینه‌های پایین، متوسط و بالا است.

مرحلهٔ پنجم: تصمیم برای رفع تهدید– بعدازاینکه تهدیدات طبقه‌بندی شدند، یک فهرست اولویتی ازآنچه باید برطرف شود وجود دارد؛ به‌عنوان یک قاعدهٔ کلی، ابتدا باید شدیدترین خطرات را تعیین کرد.

مرحلهٔ ششم: سفارشی‌سازی مدل– داشتن چارچوب قابل تنظیم برای سازگاری با کسب کار حیاتی است. مدل تنظیم‌شده به‌احتمال‌زیاد نتایج بهتری مطابق با درک افراد دربارهٔ خطر جدی ارائه می‌نماید؛ بنابراین می‌توان زمان زیادی را برای تحقیق در این مدل صرف نمود و خصوصیات، عوامل سفارشی و وزن هریک از عوامل را تغییر داد ("OWASP Risk Rating Methodology - OWASP," n.d.)

جمع‌بندی مبحث ارزیابی تهدید

در بخش قبلی روش‌های مختلف ارزیابی تهدید، عوامل مؤثر در این فرایند و به‌طور اخص در ارزیابی تهدیدهای تروریسم سایبری موردبررسی قرار گرفت؛ تقریباً کلیهٔ روش‌های ارزیابی از زمینهٔ یکسانی برخوردار هستند و در همهٔ آن‌ها از: الف– احتمال وقوع تهدید تروریسم سایبری؛ ب– بهره‌برداری از آسیب‌پذیری‌های موجود در سامانه‌ها؛ ج– اثر تهدید بر دارایی‌های کلیدی برای ارزیابی تهدید بهره‌برداری شده است. با توجه تعریف محقق ساخته از تروریسم سایبری و هدایت این تهدید از طریق فضای سایبر (رایا/رایانه‌ای) با نقض مؤلفه‌های اساسی امنیت شامل محرمانگی، دسترس‌پذیری و تمامیت داده‌ها و پیامدهای حاصل از آن در فضای سایبری و فضای حقیقی به نظر می‌رسد رویکرد OWASP ضمن پرداختن به دارایی‌های سایبری و دارایی‌های غیر سایبری روش مناسب‌تری برای ارزیابی تهدید تروریسم سایبری محسوب می‌شود؛ بنابراین معادلهٔ مورداستفاده از این روش به شرح ذیل ارائه می‌شود:

ارزیابی تهدید = احتمال وقوع تهدید* آسیب‌پذیری* اثر تهدید بر دارایی‌های سایبری و غیر سایبری

راهبردهای مدیریتی تهدید

می‌دانیم که امنیت یک مقولهٔ نسبی می‌باشد؛ این امر سبب شده است مدیریت تهدید در این فضا نیز همانند سایر قلمروها فیزیکی مدنظر متخصصین و مدیران باشد. تهدیدات امنیتی بر اساس میزان ارزشمندی سرمایه‌ها و شدت صدمات محتمل بر آن‌ها، وابسته به‌احتمال بهره‌برداری منابع تهدید از آسیب‌پذیری‌های شبکه هستند که در سه سطح با تأثیر کم، متوسط و زیاد ارزیابی می‌شوند. تلاش در راستای مدیریت تهدیدات امنیتی تا باقی نماندن آن‌ها با تأثیر زیاد، متمرکز می‌باشد. روش و چگونگی برخورد با تهدید متفاوت است؛ به‌طورکلی چهار گزینه در این نوع مدیریت وجود دارد: پرهیز از خطر[۱]، نگه‌داشتن خطر[۲]، کاهش خطر[۳] و انتقال خطر[٤].

حالت اول، پرهیز از خطر در صورتی اتفاق می‌افتد که هیچ‌گونه وابستگی به سامانه‌ها، شبکه‌های ارتباطی و وب‌سایت‌های اینترنتی وجود نداشته باشد. در شرایط فعلی بسیاری از معاملات و تجارت از این طریق انجام می‌شود و تقریباً غیرممکن است؛ حالت دوم، یا همراهی با خطر وضع حال شرکت‌های مجهز به تصمیم هوشمند هستند که اقدام به تجزیه‌وتحلیل خطر کرده و از این طریق، خطرات داخلی را شناخته و مدیریت خطر را آزمایش می‌کنند؛ شرکتی این روش را انتخاب می‌کند که ازلحاظ مالی استفاده از گزینه‌های دیگر برایش مقدور نباشد؛ حالت سوم، کاهش میزان خطر، فرایند و روش مدیریتی می‌باشد؛ این حالت وابستگی کامل به میزان سرمایه‌ها و تجهیزات به‌کاررفته برای شناسایی تهدیدها دارد تا به دنبال آن نسبت به ادامه یا توسعهٔ فرایندهای امنیتی بتوان تصمیم‌گیری کرد؛ مورد چهارم انتقال خطر، با حضور شرکت‌های بیمه همراه است که شرکت بیمه‌گر، بیمه شونده را در مقابل حوادث غیرقابل‌پیش‌بینی ازلحاظ مالی با توجه به قرارداد فی‌مابین حمایت می‌کند. معمولاً شرکت‌ها از ترکیب این چند گزینه بهره می‌برند، به این صورت که درصدی از خطر را می‌پذیرند، درصدی از آن را کاهش می‌دهند و مابقی را بیمه می‌کنند؛ به‌عنوان‌مثال شرکتی، دارای وب‌سایت قابل‌دسترسی از طریق اینترنت است و کنترل‌های امنیتی را بر روی آن پیاده می‌کند اما همچنان به خاطر وجود خطرات، از معاملات از

---

۱. Avoiding The Risk

۲. Retaining The Risk

۳. Mitigating The Risk

٤. Transferring The Risk

طریق اینترنت خودداری می‌کند. مسئلهٔ مدیریت خطر در غالب ارگان‌ها موردپذیرش و تأکید است. خبرگان علم رایانه همواره درحال‌توسعهٔ فن‌آوری‌هایی به‌منظور حل مشکلات امنیتی اینترنت هستند اما برقراری امنیت مطلق و کامل، غیرممکن است و این ایده که امنیت به‌طور طبیعی در حد «خوب کافی» باشد کفایت می‌کند و درصدی از خطرات که قابل کاهش نیست را با راهکار انتقالی به محصولات بیمه‌ای واگذار می‌کنند (قوامی و همکاران، ۱۳۸۸).

هنگامی‌که تهدیدات شناسایی و ارزیابی می‌شوند، سازمان باید راهبرد مناسب را برای به حداقل رساندن تهدید انتخاب کند؛ راهبردهای مورداستفاده عبارت‌اند از:

اجتناب از تهدیدات و حملات: با از بین بردن منبع خطر یا جلوگیری از قرار گرفتن دارایی در معرض خطر؛ معمولاً زمانی استفاده می‌شود که دارایی خاص وجود دارد؛ به‌عنوان‌مثال، عدم اتصال به اینترنت؛

کاهش تهدید: با بهره‌گیری از فن‌آوری‌های مناسب و ابزار (مانند فایروال، سامانه‌های آنتی‌ویروس و غیره) و یا اتخاذ مناسب سیاست‌های امنیتی (مانند کلمهٔ عبور، کنترل دسترسی، مسدود کردن پورت و غیره)؛

انتقال تهدید: با خدمات امنیتی برون‌سپاری یا خرید بیمه؛

پذیرش تهدید[1]: زمانی استفاده می‌شود که هزینهٔ تدابیر امنیتی یا بیمه با هزینهٔ تهدید برابر باشد (NIST,۲۰۰۲).

مدیریت تهدیدات تروریسم سایبری

برای بهره‌برداری از روش‌های مزبور در حوزهٔ فضای سایبر و تروریسم سایبری باید به چند نکتهٔ کلیدی توجه داشت:

۱- فضای سایبر، زیرساخت سایر زیرساخت‌های دیگر مانند آب، برق، حمل‌ونقل و غیره محسوب می‌شود؛ بنابراین دارایی‌های حیاتی کشور نیز متأثر از زیرساخت‌های سایبری بوده و در ارزیابی دارایی‌ها نه‌تنها دارایی‌های سایبری بلکه دارایی‌های زیرساخت‌های موجود در فضای سایبر و دارایی‌های غیر سایبری نیز موردتوجه قرار می‌گیرند؛ بنابراین دارایی‌ها در این فضا از دو

---

۱. Acceptance

منظر تحت تأثیر قرار می‌گیرند؛ اولی اثر فنی است که بـر دارایـی‌هـای سـایبری تأثیرگـذار اسـت و دومی تأثیر عامل تهدید بر دارایی‌های غیر سایبری می‌باشد؛

۲- آسیب‌پذیری‌ها در حوزهٔ سایبر که تروریست‌ها از آن بـرای دسـتیابی مقاصـد خـود بهـره‌برداری می‌نمایند، بسیار متفاوت از فضای حقیقی است و شاخص‌هـای فضـای حقیقـی عمـلاً در فضای سایبر فاقد کارایی لازم است و شـاخص‌هـای جدیـدی موردنیـاز می‌باشـد کـه در ادبیـات موضوع به آن‌ها پرداخته‌شده است؛

۳- ارزیابی تهدیدات، نیازمند کسب یک پیش‌زمینهٔ اطلاعاتی از تروریست‌هـا و بـه‌عبارت‌دیگر اشراف اطلاعاتی سایبری بر تروریسم است؛ بنابراین فعالیت آن‌ها برابر الگوی ردیابی که صـفحات قبل به آن پرداخته شد، به‌صورت مداوم در فضای سایبر مورد رصد و پایش قرارگرفته و بـا بهـره‌گیری از فنون فارنزیک و داده‌کاوی، داده‌های مرتبط جمع‌آوری، کلیـدواژه‌هـای مـرتبط بـا اجـزای تروریسم سایبری استخراج و کلاستر شده و با ارزش‌گذاری آن‌ها در الگـوی موصـوف، اطلاعـات ذی‌قیمتی پیرامون این اجزا گردآوری و امکان پیش‌بینی تحرکات تروریسـم بـا بهـره‌گیـری از یـک رویکرد آینده‌پژوهانه فراهم می‌شود؛ بنابراین احتمـال وقـوع تهدیـد به‌صـورت بهینه‌شـده بـرآورد می‌شود؛

٤- رویکرد مدیریتی یا گزینش راهبردهای مدیریتی نکتـهٔ دیگـری اسـت کـه پـس از ارزیـابی تهدید موردتوجه قرار می‌گیرد. راهکارهای متنـوعی بـرای ارتقـای امنیـت سـایبری در حوزه‌هـای قانونی، فن‌آوری، سیاست‌گذاری و... تدوین‌شده است ولی راهبردهای مدیریتی یـک بسـتهٔ جـامع مدیریتی هستند که کلیهٔ ایـن تـدابیر و راهکارهـا را دربرداشـته و می‌توانـد بـرای همـهٔ حوزه‌هـای تهدید، اعم از بخش خصوصی و دولتی و حتی زیرسـاخت‌های حیـاتی و حسـاس نسـخهٔ امنیتـی ارائه نمایند؛ این راهبردها از قابلیت ترکیب شدن نیز برخوردار هستند؛ یعنی وقتی «راهبـرد کـاهش» درصدد فراهم‌سازی سـازوکارهای امنیتـی بـا اسـتفاده از تـدابیر فنـی و سیاسـت‌گذاری می‌باشـد، می‌توان به‌صورت موقت یا دائمی با استفاده از «راهبرد اجتناب» از تهدیدات دوری نمود؛ این بسـتهٔ جامع حتی راهکارهایی ساده و کارآمد برای بخـش خصوصـی پیشـنهاد می‌نمایـد؛ یعنـی بـا یـک

مکانیسم ساده مانند بیمهٔ سایبری می‌توان تهدیداتی را که هزینهٔ گزافی به سازمان تحمیل می‌کند به حوزهٔ دیگری منتقل نمود.

در این بخش بر آنیم تا با تکیه‌بر ادبیات موضوع و گردآوری اجزای اصلی تروریسم سایبری برای بهره‌برداری در الگوی ردیابی به‌منظور پیش‌بینی فعالیت‌های تروریسم سایبری و همچنین احصای علل و عوامل اصلی ارزیابی تهدید تروریسم و قرار دادن آن‌ها در معادله (ارزیابی تهدید تروریسم سایبری= اثر تهدید* احتمال تهدید) و اضافه کردن رویکردهای مدیریتی به آن مدل مفهومی پژوهش را ترسیم نماییم.

مدل مفهومی پژوهش

پس از احصای ابعاد مدیریت تهدیدات تروریسم سایبری شامل شناسایی و اشراف اطلاعاتی سایبری (فاز شناسایی)، ارزیابی تهدیدات تروریسم سایبری (فاز تحلیل و ارزیابی) و رویکرد مدیریتی (فاز اولویت‌بندی و عملیات) می‌توان مدل مفهومی ذیل را برای پژوهش ارائه نمود:

شکل (۳): مدل مفهومی مدیریت تهدیدات تروریسم سایبری

روش‌شناسی پژوهش

در این تحقیق، از روش موردی زمینه‌ای استفاده‌شده است؛ یعنی پژوهشگر پس از مطالعهٔ موقعیت قبلی تروریسم و ارزیابی این تهدید در فضای حقیقی به بررسی آن در موقعیت جدید یعنی فضای سایبر می‌پردازد؛ این فرایند، مراحل پژوهش موردی زمینه‌ای است. قلمروی زمانی پژوهش پنج سال و قلمروی مکانی آن فضای سایبر جمهوری اسلامی ایران می‌باشد که منطبق بر فضای سایبر جهانی است. جامعهٔ آماری موردنظر در این تحقیق متناسب با روش مورداستفاده شامل خبرگانی می‌باشد که مسلط به مسائل راهبردی فضای سایبر بوده و در حوزهٔ تروریسم و تروریسم سایبری صاحب‌نظر باشند؛ بنابراین تعداد آنان در کشور بسیار محدود بوده و با بهره‌گیری از روش هدفمند گلولهٔ برفی[۱] تعداد آن‌ها احصا شده است؛ با این روش، ابتدا تعداد ده نفر از خبرگانی که دارای حداقل پانزده سال سابقه در این حوزه بودند شناسایی و با هدایت آن‌ها سایر خبرگان به تعداد سی‌ویک نفر رسید؛ در این پژوهش تلاش شده است برای گردآوری اطلاعات از روش: ۱- کتابخانه‌ای شامل کتابخانهٔ علمی و تخصصی و سایت‌های معتبر اینترنتی؛ ۲- روش میدانی: شامل مصاحبه با خبرگان و تنظیم پرسشنامه استفاده شود.

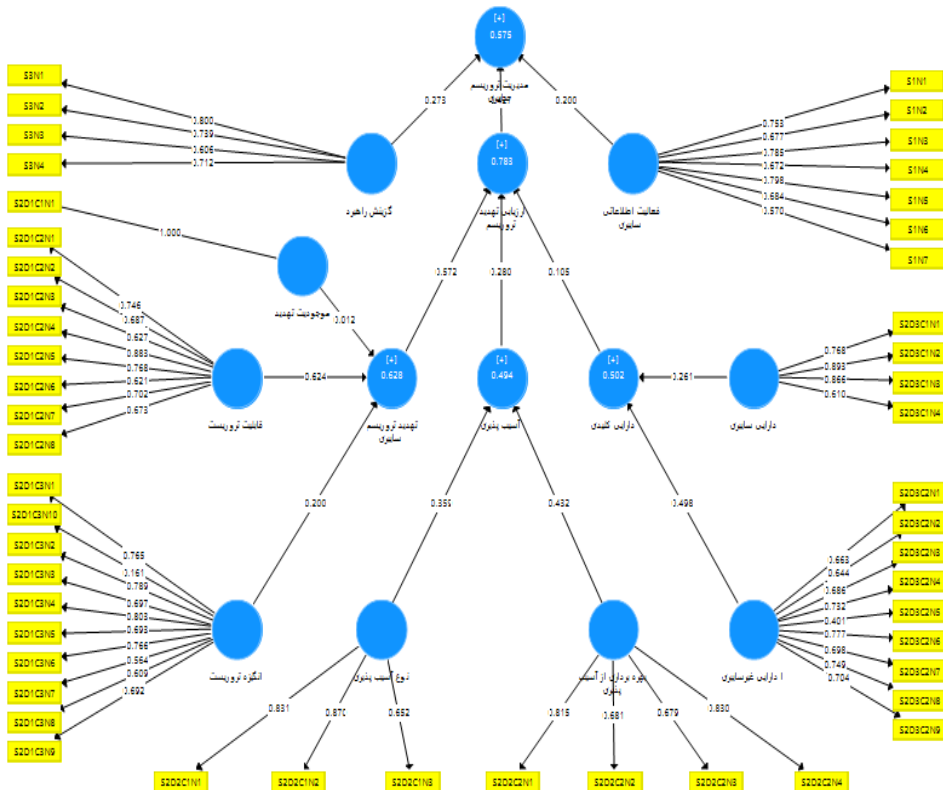
تجزیه‌وتحلیل داده‌ها و یافته‌های تحقیق

پس از جمع‌آوری پرسشنامه‌ها، داده‌های حاصل از آن نخست در نرم‌افزار SPSS واردشده و برای تجزیه‌وتحلیل توصیفی جامعهٔ آماری، این نرم‌افزار مورداستفاده قرارگرفته است؛ سپس برای دستیابی به بار عاملی، چیدمان سازه‌های اصلی شامل ابعاد و عوامل استخراج‌شده از ادبیات نظری، در نرم‌افزار SMART PLS صورت گرفته است؛ در این نرم‌افزار نخست برای بررسی برازش مدل، ابتدا پایایی مدل با بهره‌گیری از ضرایب بار عاملی، آلفای کرونباخ و پایای ترکیبی آن محاسبه و در مرحلهٔ بعدی روایی همگرا با استفاده از ضرایب AVE سازه‌ها و روایی واگرا با استفاده از روش فورنل و لارکر موردبررسی قرارگرفته است؛ در مراحل بعدی برازش مدل ساختاری با بهره‌گیری از ضرایب معناداری Z و همچنین ضریب تعیین R^2 و معیار Q^2 احراز و

۱. Snowball Sampling

سپس برازش کلی مدل GOF محاسبه و با پاسخ به سؤالات پژوهش، مدل نهـایی نیـز ترسیم‌شـده است.

پایایی (بارهای عاملی): همان‌طور که در شـکل (٤) مشـاهده می‌شـود، عوامـل S۲D۱C۳N۱۰ و S۲D۳C۲N۵ دارای بار عاملی کمتر از ۰/٤ یا ۰/٤ هستند؛ بنابراین از مدل انعکاسی حـذف شـدند، بقیهٔ عوامل از بار عاملی قابل‌قبولی برخوردار هستند.



شکل (٤): مدل‌های اندازه‌گیری مدیریت تهدید

آلفای کرونبـاخ: همان‌طور که در جدول (۵) مشاهده می‌شود، آلفای کرونبـاخ مـدل‌هـای انعکاسـی بیشتر از ۰.۷ است که حکایت از پایا بودن حوزهٔ مدیریت تهدید تروریسم دارد.

جدول (۵): آلفای کرونباخ مدیریت تهدید تروریسم

	آلفای کرونباخ	پایایی ترکیبی	متوسط واریانس استخراج شده
مدیریت تروریسم سایبری	0/713	0/838	0/635
شناسایی و اشراف	0/836	0/875	0/503
ارزیابی تهدیدات تروریسم سایبری	0/904	0/94	0/839
تهدید تروریسم	0/735	0/849	0/651
موجودیت تهدید	1	1	1
قابلیت تهدید	0/863	0/894	0/515
انگیزه تروریست	0/881	0/902	0/509
آسیب پذیری	0/738	0/883	0/791
نوع آسیب پذیری	0/701	0/831	0/624
بهره برداری از آسیب پذیری	0/766	0/84	0/569
دارایی های کلیدی	0/754	0/89	0/802
دارایی های سایبری	0/797	0/868	0/627
دارایی های غیرسایبری	0/859	0/889	0/502
رویکرد مدیریتی(گزینش راهبرد)	0/71	0/808	0/515

پایایی ترکیبی (مشترک): همان‌طور که در جدول (۵) مشاهده می‌شود، پایایی ترکیبی (مشترک) بیشتر از ۰.٦ است که حکایت از پایایی مناسب مدل دارد.

روایی: روایی همگرا همان‌طور که در جدول (۵) مشاهده می‌شود، مقادیر سازه‌های این حوزه نیز بیشتر از ۰.۵ است که حکایت از روایی همگرای مناسب مدل دارد.

روایی واگرا: همان‌طور که در ماتریس فورنل و لارکر مدل جدول (٦) مشاهده می‌شود، جذر AVE هر متغیر (قطر جدول) از ضرایب همبستگی آن متغیر با متغیرهای دیگر (مقادیر زیر همان مقدار در ستون) بیشتر شده است که این مطلب حاکی از قابل‌قبول بودن روایی واگرای متغیرهای حوزهٔ مدیریت تهدید تروریسم سایبری می‌باشد.

جدول (٦): ماتریس فورنل و لارکر

	TM	s2	s2d1	s2d1c1	s2d1c2	s2d1c3	s2d2	s2d2c1	s2d2c2	s2d3	s2d3c1	s2d3c2
TM	0/797											
s2	0/667	0/916										
s2d1	0/634	0/863	0/807									
s2d1c1	0/196	0/388	0/446	1/000								
s2d1c2	0/731	0/799	0/781	0/530	0/718							
s2d1c3	0/524	0/567	0/674	0/531	0/752	0/713						
s2d2	0/585	0/777	0/762	0/398	0/837	0/644	0/889					
s2d2c1	0/633	0/540	0/588	0/347	0/652	0/473	0/608	0/790				
s2d2c2	0/631	0/559	0/713	0/200	0/643	0/544	0/639	0/575	0/755			
s2d3	0/678	0/689	0/736	0/352	0/710	0/513	0/584	0/596	0/744	0/896		
s2d3c1	0/618	0/550	0/640	0/386	0/713	0/506	0/677	0/689	0/730	0/616	0/792	
s2d3c2	0/618	0/741	0/750	0/422	0/721	0/623	0/572	0/644	0/613	0/691	0/710	0/708

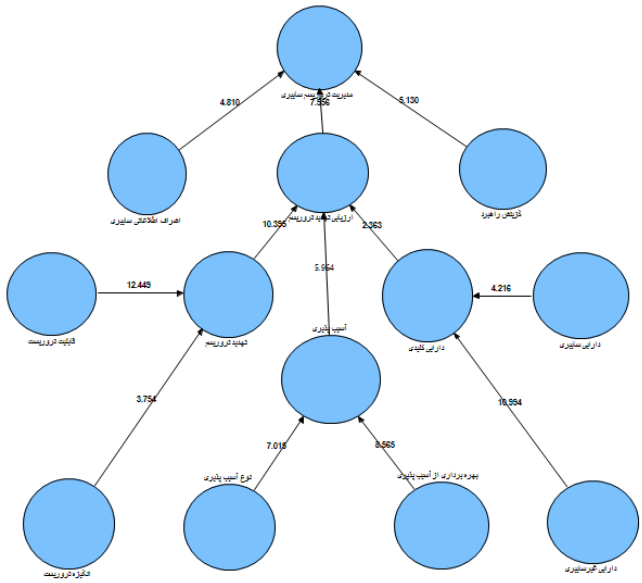
بررسی برازش مدل ساختاری

این برازش با استفاده از محاسبات بوت استرپینگ (خود راه‌اندازی) نرم‌افزار به‌منظور ارزیابی روابط بین متغیرهای پنهان (دایره‌ها) در سه معیار: ۱- ضرایب معناداری z (مقادیر t-values)؛ ۲- معیار R۲[۱] (ضریب تعیین)؛ ۳- معیار Q۲[۲] صورت گیرد.

ضرایب معناداری z (مقادیر t-values): مقادیر عددی ضرایب معناداری z (مقادیر لینک‌های متصل به دایره‌ها) در این بعد برابر شکل (۵) فقط روابط بین موجودیت و تهدید تروریسم سایبری با مقدار ۰/۳۵۸ از ۱.٦٤ کمتر و از معناداری برخوردار نیست؛ بنابراین این عوامل از مدل حذف می‌شود، معناداری سایر روابط در جدول زیر نشان داده‌شده است.

۱. R Squares

۲. Stone-Geisser Criterion



شکل (۵): گزارش بوت استرپینگ مدیریت تهدید تروریسم

معیار R۲ (ضریب تعیین): نشان‌دهندهٔ میزان تأثیر یک متغیر برون‌زا بر یک متغیر درون‌زا است؛ در جدول (۷) برازش بر اساس R۲ گزارش‌شده که از متوسط تا قوی ارزیابی‌شده است.

جدول (۷): ضریب تعیین (R۲)

متغیرپنهان	ضریب تعیین R2	نتیجه
مدیریت تروریسم سایبری	.576	برازش متوسط
ارزیابی تهدیدات تروریسم سایبری	.781	برازش قوی
تهدید تروریسم	.652	برازش متوسط
آسیب پذیری	.493	برازش متوسط
دارایی های کلیدی	.509	برازش متوسط

معیار Q۲: نشان‌دهندهٔ قدرت پیش‌بینی مدل است؛ مقادیر بالای صفر نشان می‌دهند که مقادیر مشاهده‌شده خوب بازسازی‌شده‌اند و مدل توانایی پیش‌بینی دارد. با توجه به جدول (۸)، برازش مدل مدیریت تهدید تروریسم مناسب است.

جدول (۸): معیار Q۲

	SSO	SSE	Q^2 (=1-SSE/SSO)	نتیجه
TM	23/259	15/876	0/317	برازش متوسط
s1	25/134	18/523	0/263	برازش مناسب
s2	16/642	9/152	0/450	برازش مناسب
s2d1	17/710	10/858	0/387	برازش مناسب
s2d1c1	5/555		1/000	برازش مناسب
s2d1c2	46/480	24/994	0/462	برازش مناسب
s2d1c3	52/742	28/327	0/463	برازش مناسب
s2d2	7/710	2/967	0/615	برازش مناسب
s2d2c1	15/026	8/434	0/439	برازش مناسب
s2d2c2	14/505	7/530	0/481	برازش مناسب
s2d3	7/329	3/672	0/499	برازش مناسب
s2d3c1	11/192	6/397	0/428	برازش مناسب
s2d3c2	33/396	17/706	0/470	برازش مناسب
s3	13/798	9/665	0/300	برازش مناسب

بررسی برازش مدل کلی: معیار GOF

عددی که برای این معیار به دست می‌آید، بین صفر و یک می‌باشد. سه مقدار ۰.۰۱ و ۰.۲۵ و ۰.۳۶ به‌عنوان مقادیر ضعیف، متوسط و قوی برای GOF ارائه‌شده است، به این معنی که مثلاً در صورت محاسبهٔ مقدار ۰.۰۱ و نزدیک آن به‌عنوان GOF در یک مدل، می‌توان نتیجه گرفت که برازش کلی آن مدل در حد ضعیفی است و باید به اصلاح روابط بین سازه‌های مدل پرداخت؛ این مقدار از جذر، حاصل‌ضرب میانگین ستون «متوسط مشترک»[۱] و میانگین «ضریب تعیین» از جدول (۹) حاصل می‌شود.

جدول (۹): ضریب تعیین و متوسط واریانس

۱. Communality: مشخصاً در نسخهٔ ۲ نرم‌افزار وجود دارد ولی در نسخهٔ ۳ نرم‌افزار از مقدار AVE استفاده می‌شود.

ابعاد و عوامل	ضریب تعیین R2	متوسط واریانس استخراج شده
مدیریت تروریسم سایبری	0/575	0/635
شناسایی و اشراف		0/503
ارزیابی تهدیدات تروریسم سایبری	0/781	0/839
تهدید تروریسم	0/652	0/651
موجودیت تهدید		1/000
قابلیت تهدید		0/515
انگیزه تروریست		0/509
آسیب پذیری	0/493	0/791
نوع آسیب پذیری		0/624
بهره برداری از آسیب پذیری		0/569
دارایی های کلیدی	0/509	0/802
دارایی های سایبری		0/627
دارایی های غیرسایبری		0/502
رویکرد مدیریتی		0/515
میانگین	0/602	0/65

$$GOF = \sqrt{\overline{\text{Communality}} \times \overline{R^2}} = \sqrt{.65 \times .602} = .625$$

همان‌طور که مشاهده می‌شود، مقدار برازش کلی مدل معادل ۰.۶۲۵ به‌دست‌آمده است و چون از ۰.۳۶ بیشتر است، برازش مدل قوی ارزیابی‌شده و با استفاده از نتایج حاصل می‌توان، به بررسی سؤالات پژوهش پرداخت؛ برای آزمودن آن‌ها، می‌توان از آزمون معناداری T استفاده نمود. مقادیر ضریب مسیر (بار عاملی) و ضریب معناداری استخراج و در جدول ذیل درج گردید.

روابط	ضریب مسیر	ضرایب Z	تأیید یا رد	سطح معناداری
مدیریت تروریسم سایبری → شناسایی و اشراف	۰/۲۰۰	٤.۹۲۹	تائید	۰/۹۹
مدیریت تروریسم سایبری → رویکرد مدیریتی	۰/۲۷۳	۵.۱۷۰	تائید	۰/۹۹
مدیریت تروریسم سایبری → ارزیابی تهدید تروریسم	۰/۷۸۳	۷.۳۸۷	تائید	۰/۹۹

همان‌طور که در جدول یادشدهٔ بالا مشاهده می‌شود به تمام سؤالات فرعی پاسخ‌داده‌شده است؛ بنابراین می‌توان نتیجه گرفت که ضمن پاسخ به سؤال اصلی، مدل نهایی با حذف عوامل مرتبهٔ اول

«عصر جدید» و «محیط‌زیست» به ترتیب از عامل مرتبهٔ دوم انگیزه و دارایی‌های غیر سایبری مورد تأیید قرار می‌گیرد.

پیشنهاد

این مدل از قابلیت لازم برای تبدیل‌شدن به یک سامانهٔ یکپارچه و هوشمند برای مدیریت مستمر تحرکات تروریسم سایبری برخوردار است؛ اقدام لازم در این زمینه صورت پذیرد.

با بازنگری در عوامل مدل موصوف، قابلیت لازم برای کارکرد آن در کل حوزهٔ تروریسم فراهم می‌شود؛ پژوهشی در این زمینه، کارسازی شود.

فهرست منابع و مآخذ

الف- منابع فارسی

- آشوری، داریوش (۱۳۸۲)، دانشنامهٔ سیاسی، تهران: مروارید.
- بیات، غلامرضا (۱۳۹۲)، نقش بسیج در پدافند سایبری و تأثیر آن بر امنیت ملی ج.ا.ا، فصلنامهٔ راهبردی بسیج، ش ۵۸، تهران.
- جعفری، مجتبی (۱۳۹۲)، تهدیدات امنیتی سایبر تروریسم، ششمین کنگرهٔ انجمن ژئوپلیتیک ایران (پدافند غیرعامل)، مشهد.
- جلالی، غلامرضا (۱۳۸۹)، روش و مدل برآورد تهدیدات و پدافند غیرعامل، تهران: انتشارات دانشگاه امام حسین (ع).
- خلیلی، سیاوش (۱۳۹۱)، روش‌های پژوهش آمیخته، چ ۲، تهران: نشر مؤسسهٔ انتشارات یادوارهٔ کتاب.
- سمیعی اصفهانی، علی‌رضا و سالکی، عبدالکریم (۱۳۹٤)، ترور، تروریسم و تروریسم دولتی، مجلهٔ سیاسی و اقتصادی، ش ۲۹۹.
- شورای عالی افتا (۱۳۸٤)، مجموعه مستندات سند راهبردی امنیت فضای تبادل اطلاعات کشور، تهران.
- دهخدا، علی‌اکبر (۱۳۷۷)، فرهنگ لغات دهخدا، تهران: امیرکبیر.
- سازمان پدافند غیرعامل کشور (۱۳۹۱)، انواع تهدیدات و نحوهٔ بررسی و ارزیابی آن‌ها، تهران: نشر سازمان پدافند غیرعامل کشور.
- عبدالله خانی، علی (۱۳۸٦)، تهدیدات امنیت ملی، تهران: انتشارات بین‌المللی ابرار معاصر تهران.
- عمید، حسن (۱۳۸۹)، فرهنگ فارسی عمید، تهران، چ ۱.
- قرارگاه پدافند سایبری کشور (۱۳۹٤)، سند راهبردی پدافند سایبری کشور، تهران: قرارگاه پدافند سایبری.
- قوامی، ندا؛ کلانتری، رضا و رحیمی، مینا (۱۳۸۸)، تبیین نقش بیمهٔ امنیت فضای تبادل اطلاعات در مدیریت مخاطرات، پژوهشکدهٔ امنیت مرکز تحقیقات مخابرات ایران، تهران.
- معین، محمد (۱۳٦۳)، فرهنگ معین، چ ٦، تهران: امیرکبیر.
- ناجی راد، محمدعلی (۱۳۸۷)، جهانی‌شدن تروریسم، چ ۱، تهران: انتشارات وزارت امور خارجه.
- ویکی‌پدیای فارسی: **http://fa.wikipedia.org**.

ب- منابع لاتین

- Akhgar, Babak., Staniforth Andrew., Bosco, M.Francesca., (۲۰۱٤), Cyber Crime and Cyber Terrorism Investigator's Handbook, Elsevier, **http://www.sciencedirect.com.**
- Akhgar, B., Choraś, M., Brewster, B., Bosco, F., Vermeersch, E., Luda, V., … Wells, D., (۲۰۱٦), Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism. Combatting Cybercrime and Cyberterrorism Springer, Cham.
- Albahar, M., (۲۰۱۷), Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. Science And Engineering Ethics. **https://doi.org/۱۰,۱۰۰۷/s۱۱۹٤۸-۰۱٦-۹۸٦٤-۰**
- Al Mazari, A., Anjarin, A. H., Habib, S. A., Nyakwende, E., (۲۰۱٦), Cyber Terrorism Taxonomies: Definition,Targets, Patterns, Risk Factors, and Mitigation Strategies. International Journal of Cyber Warfare and Terrorism (IJCWT), ٦(۱), ۱–۱۲.
- Bester, P.C., (۲۰۱۹), Emerging challenges in terrorism and counterterrorism: A national security perspective. Paper presented on ۱۷ January ۲۰۱۹ at the, The Hague University of Applied Sciences, Faculty of Public Managament, Law and Safety, The Hague.
- Chuipka, A., (۲۰۱۷), The Strategies of Cyberterrorism: Is Cyberterrorism an effective means to Achieving the Goals of Terrorists. **http://۱۳۷,۱۲۲,۱٤,٤٤/handle/۱۰۳۹۳/۳٥٦۹٥**
- Denning, D.E., (۲۰۰۱), Is Cyber Terror Next? Social Science Research Council, W, DC, USA.
- Forest, Brian., (۲۰۰۹), Terrorism, Crime, and Public Policy, UK, Cambridge University Press.
- Haimes,Y.Yacov., (۲۰۰۹), Risk Modeling, Assessment, and Management, Third Edition, John Wiley and Sons, Inc.
- L. Edwards, Frances, Steinhäusler, Friedrich., (۲۰۰۷), NATO AND TERRORISM On Scene: New Challenges for First Responders and Civil Protection, U.S.A, San José State University Department of Political Science,Division of Physics and Biophysics,Salzburg, Austria University of Salzburg San José, CA, U.S.A.
- Leson, (۲۰۰٥), Assessing and / Managing the Terrorism Threat, U.S. Department of JusticeOffice of Justice Programs,Washington, DC ۲۰٥۳۱.
- Lourdeau, K., (۲۰۰٤), Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security, February ۲٤, ۲۰۰٤, Senate, Washington, DC, USA. http://www.fbi.gov/news/ testimony/hearing-on-cyber-terrorism.
- Luiijf, Eric., (۲۰۱٥), Definitions of Cyber Terrorism. **http://www.sciencedirect.com.**
- Munk, Tine Højsgaard., (۲۰۱٥)., cyber security in european region: Anticipatory Governance and Practices, University of Manchester, USA.
- NCTB., (۲۰۱٤), What is Terrorism? National Coordinator for Counterterrorism, Den Haag, the Netherlands.**http://english.nctb.nl/themes_en/Counterterrorism /what_is_terrorism, (۲۳,۰۲,۱٤).**
- NIST., (۲۰۰۸), Framework for Improving Critical Infrastructure Cybersecurity, **http://csrc.nist.gov**
- NIST., (۲۰۱٤), Framework for Improving Critical Infrastructure Cybersecurity version ۱,۰. **http://csrc.nist.gov**

- OWASP Risk Rating Methodology-OWASP **https://www.owasp.org/index.php /OWASP_Risk_Rating_Methodology#Approach.**
- P. Fidler, David, Buchan, Russell, Crawford, Emily, Adhihetty, TJ, Harrison Dinniss, Heather, Ducheine, Paul, Eichensehr, Kristen, Housen-Couriel, Deborah, Ivanov, Eduard,Kim, Sung-Won, Nasu, Hitoshi, K. Nkusi, Fred, Ellen O'Connell, Mary, Sobrinho de Morais Neto Arnaldo, Tsagourias, Nicholas, Ziolkowski, Katharina., (٢٠١٦), Study Group on Cybersecurity, Terrorism, and International Law, INTERNATIONAL LAW ASSOCIATION, http://www.ila-hq.org/en/studygroups/ index.cfm/cid/١٠٥٠.
- Salleh, N. M., Selamat, S. R., Yusof, R., Sahib, S., (٢٠١٦), Discovering Cyber Terrorism Using Trace Pattern. International Journal of Network Security.
- SEissa, Israa., Ibrahim, Jamaludin., Yahaya, Nor-Zaiasron., (٢٠١٧), Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review, International Journal of Science and Research, ISSN (Online): ٢٣١٩-٧٠٦٤.
- Veerasamy, namosha, Grobler, M., Sloms, B. V., (٢٠١٦), Building an Ontology for Cyberterrorism.**https://www.researchgate.net**