فصلنامه امنیت ملی
سال نهم، شماره ۳۳، پاییز ۱۳۹۸
مقاله چهاردم از صفحه ۳۸۹ الی ٤٢٤

مقاله پژوهشی: ارائه مدل مفهومی ارزیابی تهدیدات تروریسم سایبری

حسین امیرلی[۱] و کامیار ثقفی[۲]

تاریخ دریافت: ۱۳۹۷/۰۳/۱۲ **تاریخ پذیرش: ۱۳۹۷/۰٦/۱۵**

چکیده

تروریسم سایبری یکی از تهدیدهای فضای سایبر می‌باشد که در سال‌های اخیر بسیاری از کشورها از جمله جمهوری اسلامی ایران با آن مواجه بوده است. در این مقاله پس از مطالعه پیشینه مرتبط با تروریسم و تروریسم سایبری، جایگاه آن در میان سایر تهدیدات فضای سایبری، ویژگی‌های تروریسم سایبری، هستی‌شناسی، بازیگران، اجزای آن، راهبردهای تروریسم سایبری، انواع حملات این نوع تروریسم تشریح و تعریف محقق ساخته در زمینه تروریسم سایبری بیان شده است، در ادامه روش‌های ارزیابی تهدید تروریسم سایبری بررسی و ضمن استخراج اجزا و عوامل مربوطه از ادبیات پژوهش، مدل مفهومی در این زمینه ارائه گردیده است. سپس با استفاده از روش گلوله برفی خبرگان حوزه‌های راهبردی فضای سایبر به تعداد ۳۱ نفر احصاء و با توسل به نظرات آن‌ها از طریق ابزار مصاحبه و پرسشنامه و نیز بهره‌گیری از نرم‌افزار SPSS,SMART PLS، مدل مفهومی پیشنهادی مورد آزمون قرار گرفته و مدل نهایی ترسیم شده است.

کلیدواژه‌ها: تروریسم، تروریسم سایبری، ارزیابی تهدیدات

۱. دانش‌آموخته دوره دکتری مدیریت راهبردی امنیت فضای سایبری- (نویسنده مسئول)- *h.amirli@chmail.ir*
۲. عضو هیئت علمی دانشگاه شاهد- *saghafi@shahed.ac.ir*

مقدمه

ویژگی‌های منحصربه‌فرد فضای سایبر سبب شده تبهکاران و مجرمین سنتی، این عرصه را برای پیاده‌سازی مقاصد و اهداف خود مناسب دیده و تلاش نمایند ضمن مهاجرت به فضای مزبور، از امکانات گسترده آن بهره‌برداری کنند؛ آنان به سبب چابکی با استفاده از منابع این فضا، سریع‌تر از دولت‌ها و شرکت‌های بزرگ قدرتمندتر می‌شوند و دامنه تهدیدات خود را گسترش می‌دهند. تروریسم سایبری یکی از تهدیدات سایبری است که از تلاقی پدیده تروریسم با فضای سایبر ایجاد می‌گردد؛ با افزایش وابستگی زیرساخت‌های حساس و حیاتی[1] کشورها به فضای سایبر مانند حمل و نقل، انرژی، شبکه بهداشت و سایر زیرساخت‌ها، جذابیت بیشتری برای این دسته از تبهکاران فراهم‌شده و آن‌ها به سهولت از اهرم‌های فشاری که این فضا در اختیارشان قرار می‌دهد به منظور پیشبرد اهداف ایدئولوژیک، سیاسی و اجتماعی و ... خود بهره‌برداری می‌نمایند؛ بنابراین ضرورت دارد این تهدید با اولویت بیشتری مورد پیگیری قرار گیرد.

یکی از زیرساخت‌های لازم برای مدیریت این‌گونه تهدیدات، ارزیابی تهدید می‌باشد که به شاخص‌ها و عوامل متعددی بستگی دارد که تاکنون به صورت جامع احصاء و در قالب مدل مفهومی ارائه نشده است؛ پژوهش حاضر گامی در جهت برنامه‌ریزی راهبردی برای رویارویی و مدیریت چنین تهدیدهای محسوب می‌شود؛ به عبارت دیگر با ارزیابی تهدیدهای تروریسم سایبری می‌توان آن‌ها را اولویت‌بندی نموده و برای مواجهه با آن‌ها، منابع به صورت هدفمند تخصیص یابد. غفلت از چنین تحقیقاتی می‌تواند به عدم هدفمندی در اختصاص منابع و هدررفت آن‌ها و در نتیجه شیوع تروریسم و کاهش امنیت و اعتماد عمومی به فضای سایبر برای تداوم کسب‌وکار و ترویج احساس ناامنی و در نهایت خدشه‌دار شدن امنیت ملی منجر شود. این پژوهش با هدف دستیابی به مدل مفهومی ارزیابی تهدید تروریسم سایبری و فرضیه «مدل مفهومی ارزیابی تهدید تروریسم سایبری از طریق احصاء احتمال تهدید تروریسم سایبری، دارایی‌های کلیدی، آسیب‌پذیری سامانه‌ها، قابل ارائه می‌باشد؟» برنامه‌ریزی شده است.

مبانی نظری:

در این بخش نخست کلیدواژه اصلی مبحث تبیین می‌گردد و در ادامه پیشینه‌های مرتبط با تروریسم و تروریسم سایبری جایگاه آن در میان سایر تهدیدات فضای سایبری تبیین شده، سپس

۱- Critical Infrastructure

ویژگی‌های تروریسم سایبری، هستی‌شناسی، بازیگران، اجزای آن، تروریسم از منظر عوامل ایجاد مخاطره، شاخص‌ها و راهبردهای تروریسم سایبری، انواع حملات آن‌ها، مدل‌های مختلف مفهومی از تروریسم تشریح و تعریف محقق ساخته از تروریسم سایبری بیان می‌شود؛ در ادامه روش‌های ارزیابی تهدید، در حوزه تهدیدات ناشی از تروریسم سایبری بررسی و با استخراج عوامل آن‌ها به صورت مدل مفهومی ارائه می‌گردد.

تروریسم سایبری[۱]: تروریسم سایبری عبارت است از اقدام عمدی هر فردی با استفاده از فناوری اطلاعات و ارتباطات به صورت غیرقانونی با روش‌هایی که انجام یا قصد عامدانه برای مرگ افراد یا آسیب مؤثر به اموال عمومی یا خصوصی، اقتصاد، محیط زیست و یا اختلال مؤثر در خدمات عمومی با هدف 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***)***.

ارزیابی مخاطرات[۲]: عبارت است از شناسایی دارایی‌های کلیدی کسب‌وکار، شناسایی تهدیدات، ارزیابی خسارتی که ممکن است از یک حمله موفق حادث شده باشد، شناسایی آسیب-پذیری‌های سامانه‌ها که ممکن است مورد بهره‌برداری حمله‌کننده قرار گیرد و حاصل‌ضرب آن‌ها پس از ارزیابی مخاطره امنیتی، اقدام برای کاهش مخاطره با پیاده‌سازی کنترل‌های مناسب و نظارت بر اثربخشی کنترل‌های اجرا شده صورت می‌پذیرد. (***NIST,*** ۲۰۰۸)

مفهوم شناسی ترور: در فرهنگ دهخدا آمده است: «ترور مأخوذ از زبان فرانسه و به معنی قتل سیاسی به‌وسیله اسلحه است و در فارسی متداول شده است. این کلمه در فرانسه به معنی وحشت و خوف آمده است و تروریست به شخصی اطلاق می‌شود که با اسلحه، مرتکب قتل سیاسی بشود. تروریسم در زبان فارسی به اصلی گفته می‌شود که در آن از قتل‌های سیاسی و ترور دفاع گردد» (دهخدا، ۱۳۴۳: ٦۳٦). در برخی از فرهنگ‌های فارسی نیز تروریسم، روش کسانی معرفی شده است که «آدم کشی و تهدید مردم و ایجاد خوف و وحشت را به هر طریق که باشد برای رسیدن به اهداف خود، لازم دانسته‌اند» (عمید، ۱۳۵۷: ٥٦۹).

تروریسم: ترور به معنای کشتار سیاسی به کار می‌رود و کسانی را که به کشتار سیاسی دست بزنند تروریگر (تروریست) می‌خوانند. (آشوری،۱۳۸۲: ۹۹-۹۸) تروریسم به معنای خشونت با

۱- cyber Terrorism
۲- Risk Management

انگیزه سیاسی از پیش طراحی شده علیه اهداف غیرنظامی است که گروه‌ها یا عواملی برای تحت تأثیر قرار دادن مخاطب آن را صورت می‌دهند.

با توجه به تنوع فراوان فضای وقایع تروریستی، هر گروه و یا عمل تروریستی متناسب با هر تعریف متعارف از تروریسم، معمولاً در جهات مختلف منحصر به فرد می‌باشد. با این حال، چند بعد عمومی وجود دارد که برای تشخیص برخی از تروریست‌ها، گروه‌های تروریستی و اقدامات تروریستی از سایر اقدامات به کار می‌رود. گروه‌های تروریستی خاص و اقدامات فردی تروریسم در هر یک از انواع دسته‌بندی بر اساس این ابعاد مشخص می‌شوند: آیا انگیزه‌های سیاسی وجود دارد یا نه؟ آیا اقدام تحت حاکمیت دولت عامل انجام شده یا نه؟ درجه ارتباط با سازمان‌های تروریستی چقدر می‌باشد؟ سازمان‌دهی و برنامه‌ریزی چگونه است؟ آیا از نظر مذهبی یا قومی توجیه دارد؟ آیا در درجه اول هدف مردم هستند و یا اهداف نمادین دارد؟ چه نوع مردمی را هدف قرار می‌دهد؟ هر مورد معمولاً می‌تواند به راحتی مشخص شود یا در ترکیب خاصی از این ابعاد که مناسبند قرار می‌گیرد. 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 طراحی شده برای تأثیرگذاری به دولت و یا سازمان‌های بین‌المللی یا ارعاب مردم و یا بخشی از جامعه و اجبار به منظور پیشبرد سیاسی، مذهبی، نژادی و یا علت ایدئولوژیک آن شامل موارد ذیل می‌باشد: 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)

تعاریف متعددی از تروریسم در منابع مختلف بیان شده که شباهت‌ها و تفاوت‌های زیادی بین آن‌ها مشاهده می‌شود. الکس اشمید[۱] برای دستیابی به یک تعریف واحد به تجزیه‌وتحلیل ۱۰۹ تعریف گوناگون از تروریسم پرداخته و عناصر مشترک (۲۲ عنصر) آن را استخراج نموده است که خشونت و زور با ۸۳/۵ درصد تکرار انگیزه سیاسی با ٦٥ درصد و وحشت با ٥۱ درصد بالاترین رتبه‌ها را به خود اختصاص داده‌اند (سمیعی اصفهانی، ۱۳۹٤).

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. همه تروریست‌ها

۱-Alex Schmidt

۱-Bruce Hoffman

به خشونت و تهدید به خشونت اقدام می‌کنند. تروریسم به‌طور خاص طراحی می‌شود تا اثرات روانی گسترده و فوری بر قربانی یا مفعول حملات داشته باشد. این به معنای القای ترس و در نتیجه ارعاب مخاطبان هدف که ممکن است رقیب قومی یا گروه مذهبی، یک کشور، دولت ملی، حزب سیاسی و یا افکار عمومی باشد. تروریسم طراحی شده برای ایجاد قدرت در جایی که قدرت حاکمیت ضعیف است. با تبلیغ ایجاد شده 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 می‌باشند (***Chuipka,*** ۲۰۱۷).

انواع تروریسم: محققان در ایالت متحده 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:

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 به زور را بدون اعلان جنگ به‌کار گیرند تا با ترساندن افراد به خواسته‌های سیاسی دست یابند. نمونه بارز این نوع از تروریسم، رژیم اشغالگر قدس می‌باشد.

۲. *تروریسم سایبر*: در ادامه بحث به‌طور کامل به آن پرداخته خواهد شد.

۳. *اکو تروریسم*[۲]: تروریسم هسته‌ای به روش‌های متفاوتی وجود دارد که ممکن است مواد هسته‌ای به منزله 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 به منظور تأثیرگذاری بر حکومت‌ها یا جلوگیری از تلاش‌های آن‌ها در متوقف ساختن تجارت دارو بود. در سال‌های اخیر نارکو تروریسم 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*[1]: حمله 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 در جهت 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 به وجود آورنده این پدیده شوم می‌باشد که عبارتند از: ۱- اینکه تروریسم عملی از پیش طراحی شده است ۲- این کنش دارای جهت‌گیری کلان است ۳- قربانیان بی‌دفاع بوده و وسیله‌ای هستند در رسیدن به هدف ٤- عوامل مرتکب ترور گروه‌های مخفی فروملی و یا بعضاً فراملی هستند (ناجی‌راد،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 مورد استفاده در عملیات تقسیم‌بندی شود مثلاً «تروریسم هسته‌ای» اشاره به استفاده از سلاح‌های هسته‌ای در فعالیت‌های تروریستی دارد یا «سایبرتروریسم» استفاده سیاسی از شبکه‌های کامپیوتری، داده‌ها و نرم‌افزارهای گروه‌های فراملیتی به منظور تهدید و یا ایجاد خشونت به منظور ارعاب مخاطبان گسترده می‌باشد. به همین ترتیب، باکر و ون زویدوویون[2] (۲۰۱٦) به «تروریسم شیمیایی»، «بیولوژیکی» و «رادیولوژیکی» اشاره می‌کنند که با دستگاه‌های خانگی ساخته شده‌اند (***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 منتشر گردیده که از آشفتگی زیادی برخوردار بوده است. به برخی از این تعاریف در ذیل اشاره و در خاتمه 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 به منظور ارعاب مردم و حاکمیت برای پیشبرد اهداف سیاسی و

۱-Bioterrorism

۲-Bakker and van Zuijdewijn

۱-Dorothy E. Denning

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 ذخیره شده در درون آن‌ها از طریق شبکه 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 نتیجه آن خشونت، تخریب یا اختلال در خدمات، با هدف ایجاد ترس از طریق ایجاد سردرگمی و عدم اطمینان در داخل یک جمعیت مشخص، به منظور تأثیرگذاری بر یک دولت یا جمعیت با یک برنامه خاص سیاسی، اجتماعی یا ایدئولوژیک می‌باشد» (***Lourdeau,*** ۲۰۰٤).

دولت هلند با استفاده از تعریف اتحادیه 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 با هدف 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 سیستم‌های اطلاعاتی و شبکه، یا دسترسی غیرمجاز مؤثر بر اطلاعات و کنترل‌های فرآیندهای 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 محیط زیست، یک مخاطره مؤثر بر سلامتی و ایمنی عمومی، نقض ثبات سیاسی و اجتماعی و انسجام یک ملت شود اطلاق می‌گردد. (***Akhgar,*** ۲۰۱٤:۱٦)

گروه مطالعاتی ایلا[۱] در سال ۲۰۱٦ با بررسی و تجمیع کلیه 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 به صورت غیرقانونی با روش-هایی که انجام یا قصد عامدانه برای مرگ افراد یا آسیب مؤثر به اموال عمومی یا خصوصی، اقتصاد، محیط زیست و یا اختلال مؤثر در خدمات عمومی با هدف ارعاب جمعیت غیرنظامی یا

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

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 حمله سایبری با بهره‌کشی یا استفاده از رایانه یا شبکه‌های ارتباطی برای ایجاد تخریب مؤثر به منظور 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 طراحی شده برای پیامدهای روانی گسترده و فوری بر هدف باشد؛ پنجم توسط سازمان با فرماندهی و یا ساختاری برای توطئه(بدون لباس و نشان شناخته شده) یا افراد و مجموعه‌ای از افراد با انگیزه با الهام از اهداف ایدئولوژیک یا مثالی از جنبش‌های تروریستی با راهبران آن بوده و در نهایت مرتکب یک گروه محلی یا نهاد غیردولتی باشد. ***(Chuipka,*** ۲۰۱۷***)***

هستی‌شناسی تروریسم سایبری: تبیین کلاس‌های موجود در تروریسم سایبری نخستین مرحله هستی‌شناسی است. مهم‌ترین کلاس‌های مطرح در تروریسم سایبری عبارتند از: بازیگران، وقایع سایبری، عینیت، انگیزه، تجارب، تأثیر و اهداف آن می‌باشد. بازیگران در این عرصه عبارتند از رقبای تجاری، هکرها، هکرکدهای اسکریپت، هکر ماهر، خودی، مدیر خودی، کارمند معمولی، یک گروه جنایی سازمان یافته، گروه معترض. تأثیر تروریسم سایبری در طیف بدون تأثیر، حداقل یعنی تأثیر قابل پوشش، تأثیر زیاد یعنی تأثیر غیرقابل پوشش و فاجعه اشاره دارد. انگیزه شامل زیر کلاس‌های جنائی، اخلاقی، اجتماعی، سیاسی، دینی، مالی، نظامی و تفریحی است. اهداف بدافزارها و حملات به منظور انهدام، ویرانی، تحمیل خواسته، مداخله، ارعاب، کشتن یا صدمه، اعتراض، تبلیغ، سرقت، وحشت یا با هدف پشتیبانی مانند پشتیبانی مالی، اطلاعاتی، لجستیکی، برنامه‌ریزی، تجدید قوا، خدمات اجتماعی یا آموزش می‌باشد. برخی از تجارب در زمینه تروریسم سایبری نشان می‌دهد روش‌هایی که در این عرصه مورد استفاده قرار می‌گیرد عبارتند از: روش‌های عدم استنادپذیری[۱] (پیش‌نویس پیام، رمزنگاری، پنهان نگاری مبتنی بر آی‌پی، گمنامی و پروکسی، پنهان نگاری) دستکاری داده‌ها (منع خدمات، آلودگی با کرم و ویروس و تروجان) جذب سرمایه (حراج، کازینو، سرقت کارت اعتباری، اهداء، مواد مخدر، فیشینگ) مهندسی اجتماعی (در حوزه

۱-Anti Forenzic

برنامه کاربردی، وبلاگ، فروم، بازی، موزیک، وب‌سایت‌ها) بدشکل کردن وب (با تزریق کد در آن) بهره‌برداری از اطلاعات موجود در وب (بیوگرافی، دانش‌نامه‌ها، راهنماها، گاه‌نامه‌ها، اشعار، اظهارات، ویدئو). اهداف شامل دولت یا اهداف حیاتی، اشخاص و سازمان‌ها می‌باشد. برای طبقه-بندی وقایع سایبری شرایط ذیل باید احراز گردد:۱. تأثیر حملات تروریستی باید زیاد یا به صورت فاجعه باشد به عبارت دیگر کم یا فاقد تأثیر نباشد.۲. به صورت فعال حمله دستکاری داده‌ها یا بدشکل کردن وب انجام شده باشد.۳. انگیزه سیاسی دینی یا اجتماعی در بین باشد.٤. هدف باید سازمان، دولت یا هدف حیاتی باشد.***(Veerasamy and etal,*** ۲۰۱٦)

در مقاله دیگری اجزای تروریسم سایبری بازیگران، انگیزه، ابزار، هدف، روش مورد استفاده، اثر بیان شده است. بازیگر می‌تواند به عنوان یک مشارکت‌کننده در هرگونه اقدام یا فرآیند باشد. آن 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، اشیاء اطلاق می‌شود. روش یک رویه خاص برای انجام یا نزدیک شدن به برخی چیزهاست. روش به هر اقدام یا عمل که مربوط به تروریسم سایبری است اشاره می‌کند. تأثیر به عنوان یک اثر مشخص شده یا نفوذ تعریف می‌شود و می‌تواند در چهار دسته فیزیکی، روانشناسی، اجتماعی و اقتصادی طبقه-بندی شده باشد. هر خشونت و تهدید که بر روی هدف انجام شود می‌تواند به عنوان تأثیر در نظر گرفته شود ***(Salleh and etal*** ۲۰۱٦).

با یک نگاه اجمالی در تعاریف تروریسم سایبری و مطالب بیان شده، می‌توان کلیدواژه‌های اصلی آن را استخراج نمود. این کلیدواژه‌ها عبارتند از هدف (نیروهای نظامی، حاکمیت سایبری و زیرساخت‌های فیزیکی، زیرساخت‌های حیاتی ملی، هویت ملی و اجتماعی، هویت و صنعت بخش خصوصی)، انگیزه (انگیزه 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,*** ۲۰۱٦).

تروریسم سایبری از منظر هدف: همان‌طوری که قبلاً نیز بیان گردید؛ تروریسم سایبری درصدد ایجاد رعب و وحشت برای دستیابی به اهداف مورد نظر می‌باشد. تروریسم سایبری را بر اساس اهداف آن می‌توان طبقه‌بندی کرد:

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

۲. *تروریسم سایبری بر علیه دولت سایبری و زیرساخت‌های فیزیکی:* این نوع از حمله تروریستی تسهیلات و زیرساخت‌های دولتی را مورد هدف قرار می‌دهد مانند حملاتی که در کشور گرجستان بر 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، سیستم‌های تصفیه 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 توسعه محیط مورد نظر برای عملیات مؤثر و بدون اشتباه تلاش می‌نمایند. یکی از اهداف تروریست‌ها تلاش برای نابودی شهرت و اعتبار یک سازمان یا ملت می‌باشد؛ 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)*** برخی از خصوصیاتی که برای تروریسم سایبری برشمرده شد با ویژگی‌های برخی از تهدیدات سایبری مشترک می‌باشد. مانند:۱. هکتیویسم[۱] : ترکیبی از اعتراض سیاسی با هک رایانه‌ها می‌باشد. ۲. جنگ سایبری[۲]: اقدام یک دولت بر علیه رایانه‌ها و شبکه‌های دولت دیگر با هدف ایراد خسارت یا انهدام. ۳. جرم سایبری[۳]: استفاده از رایانه یا به کاربردن هر ابزار

۱-Hacktivism
۲-Cyberwarfare
۳-Cybercrime

الکترونیکی از طریق سامانه‌های اطلاعاتی برای تسهیل رفتار غیرقانونی می‌باشد.٤. جاسوسی سایبری[۱]: جاسوسی سایبری شامل به دست آوردن اسرار و اطلاعات طبقه‌بندی شده بدون اجازه افراد، شرکت‌ها، دولت‌ها، برای کسب مزیت سیاسی، اقتصادی، نظامی با استفاده غیرقانونی از اینترنت، شبکه، رایانه‌ها که می‌تواند به واسطه شکستن قفل یا بدافزاری مانند تروجان یا جاسوس-افزار باشد.۵. بازیگران هرج‌ومرج[۲]: این بازیگران لزوماً اهداف و انگیزه سیاسی ندارند و ممکن است جلوگیری، خرید یا مذاکره با آنان مشکل باشد.٦.اوباشی‌گری[۳]: اوباش‌ها به واقعیت یک اشتباه محدود می‌نگرند و لزوماً به وابستگی‌هایی که از اقدام آن‌ها تأثیر می‌پذیرد فکر نمی‌کنند که آیا آن‌ها فنی، سیاسی و یا شخصی هستند.۷. رگلاتور[٤]: رگلاتور ممکن است از وابستگی‌های متقابل بازی در فضای سایبر آگاهی نداشته باشد. اقدامات آن‌ها هنگامی‌که خوب به نظر می‌رسد می‌تواند عواقب ناخواسته و اثرات آبشاری داشته باشد که قابل پیش‌بینی نبوده است. برای درک وجه تمایز این تهدیدات با تروریسم سایبر، اشتراک و افتراق آن‌ها در شاخص‌های یاد شده در جدول ذیل گردآوری شده است: ***(Chuipka,*** ۲۰۱۷***)***

جدول (۱): تروریسم سایبری در مقابل سایر تهدیدات

شاخص های تروریسم سایبری	هکتیویسم	جنگ سایبری	جرم سایبری	جاسوسی سایبری	بازیگران هرج و مرجی	اوباشی گری	تروریسم سایبری
اجرا از طریق فضای سایبر	✓	✓	✓	✓	✓	✓	✓
اهداف و انگیزه ها سیاسی و ایدئولوژیک	✓	✓	–	–	×	✓	✓
خشونت یا تهدید به خشونت	–	–	×	×	–	×	✓
طراحی شده برای پیامدهای روانی گسترده و فوری بر هدف	×	–	×	×	–	×	✓
هدایت شده هم به وسیله یک سازمان زنجیری فرماندهی و توطئه (بدون لباس و نشان مشخص) یا افراد و یا مجموعه ای از افراد، با انگیزه و الهام از اهداف ایدئولوژیک یا مثالی از جنبش تروریستی و رهبران آن	–	×	–	–	×	–	✓
ارتکاب به وسیله یک گروه محلی یا نهاد غیر دولتی	✓	×	–	–	✓	✓	✓

۱-Cyber Espionage
۲-Chaotic Actors
۳-Vigilantes
٤- Regulators

تروریسم سایبری از منظر الگوها مجرمانه: بر اساس تحقیقات مؤسسه (***SANS***)[1] الگوهای مجرمانه تروریسم سایبری به: حمله، تخریب، قطع سرویس، نشر اکاذیب و بدشکل کردن وب‌سایت‌ها تقسیم می‌گردد. حمله و تهاجم خیلی معمولی است و به صورت گسترده انجام می‌شود و برای نفوذ به سامانه‌ها و شبکه‌ها به منظور دستیابی یا دستکاری اطلاعات صورت می‌پذیرد. تخریب با هدف ایجاد مزاحمت برای سامانه‌های رایانه‌ای و شبکه‌ها به‌منظور وارد کردن آسیب شدید به عملیات سازمانی می‌باشد. قطع خدمات یا انکار سرویس با هدف 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 با هدف خدشه‌دار کردن شهرت قربانی است. بدشکل کردن وب‌سایت‌ها نیز به‌منظور تغییر محتویات، تعبیه پیام نامطلوب و هدایت کاربر به وب سایت‌های با محتوای نامطلوب و با مقاصد تبلیغاتی است ***(Al Mazari et al., ۲۰۱۶)***.

تروریسم سایبری از منظر ایجاد عوامل مخاطره: تروریسم از این منظر شامل:

۱. مخاطرات امنیت ملی: زیرساخت‌های بسیاری از کشورها بر روی فناوری سایبری مانند سخت‌افزار و نرم‌افزار رایانه‌ای و شبکه‌های ارتباطی پایه‌گذاری شده است؛ بنابراین این زیرساخت‌ها با حملات و تهدیدات سایبری مواجه می‌باشند. انهدام فیزیکی و مجازی و یا قطعی هریک از این خدمات ممکن است زندگی ملت مشخصی را به صورت 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 به صورت معنی‌دار بر اقتصاد یک کشور از طریق اختلال و قطع خدمات اثرگذار می‌باشند. این خدمات عبارتند از شکست در ارائه محصولات و خدمات در مقابل نیازهای بازار و در نتیجه 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 انتشار اکاذیب بر علیه یک سازمان یا شخص از طریق ایمیل، وب‌سایت یا شبکه‌های اجتماعی سبب از بین رفتن اشتهار قربانی می‌گردد و در کل این نوع حمله سایبری نباید دست کم گرفته شود. یکی دیگر از مخاطرات اجتماعی از دست دادن محرمانگی و عدم حفاظت از اطلاعات و افشای

۱- System Administration, Networking, and Security Institute

غیرمجاز آن برای دشمنان می‌باشد. از دست دادن محرمانگی یکی از موارد از دست دادن اعتبار اجتماعی است. از دست دادن تمامیت و محرمانگی در یک سیستم معیوب منجر به پیامدهایی مانند عدم دقت اجتماعی، اشتباه در تصمیم‌گیری و تقلب می‌گردد.

٤. *مخاطرات اختلال عملیاتی:* تروریسم سایبری به دارایی‌های غیرفیزیکی مانند اقتصاد محدود نمی‌شود، بلکه به زیرساخت‌های فیزیکی که عملیات و فراهم‌سازی خدمات را انجام می‌دهند گسترش می‌یابد. یک حمله موفق ممکن است اختلال جدی در سامانه ترافیک راه‌آهن که به جابجایی 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. *مخاطره انهدام فیزیکی:* ممکن است انهدام فیزیکی یکی از نتایج حملات سایبری بوده و به صورت یک موضوع کلیدی از اهداف اصلی دشمن باشد. انهدام فیزیکی یک توانمندی از طریق بهره‌گیری از فناوری اطلاعات و ارتباطات به منظور ایجاد خسارت در اموال، ابزارها یا هر دارایی فیزیکی دیگر می‌باشد. 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 مورد نیاز برای بررسی شبکه‌های تروریستی: شناخت شبکه‌های تروریستی به عنوان یک سیستم ضروری است. با این شیوه درک بهتری از فرهنگ، انگیزه، مدل عملیات و سازمان‌یافتگی شبکه‌های تروریستی حاصل می‌گردد. در ادامه به پنج نوع متغیر حالت که ناشی از رویکرد سیستمی است می‌پردازیم: *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 شبکه خاص فرض شده‌اند؟ چرا آن‌ها به این فرم باقی مانده‌اند؟ *سطح دکترین- روش‌ها و نقاط قوت مشترک:* چه دکترینی برای به کار بردن بهتر شبکه سازمان وجود دارد؟ *سطح فناوری- سیستم‌های اطلاعاتی:* چه الگو و ظرفیتی برای جریان اطلاعات و ارتباطات درون شبکه وجود دارد؟ چه فناوری‌هایی 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 اعضاء شناخته شده 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 توسعه اقدامات خاص و قابلیت‌ها و مقاصد خود اقدام نماید تکمیل می‌شوند (***Y.HAIMES,*** ۲۰۰۹).

در ادامه مبحث برای شفافیت موضوع، یک مورد از حملات سایبری در جهان را با شاخص-های مزبور بررسی می‌نماییم:

ویروس استاکس‌نت: به عقیده کارشناسان استاکس‌نت اولین سلاح سایبری شناخته شده است که برای هدف قرار دادن سامانه‌های کنترل صنعتی حیاتی ایجاد شده است. نسخه‌های قبلی این ویروس از سال ۲۰۰۷ منتشر شده بود. این ویروس یکصدهزار رایانه را در سراسر جهان آلوده کرده بود که ۵۰ تا ٦۰ درصد آن‌ها در کشور ایران قرار داشتند. برخلاف بدافزارهای مخرب دیگر استاکس‌نت از شرایط خاصی برخوردار بود و ساختار پیچیده آن نشان می‌دهد که منابع و زمان زیادی برای آن صرف شده بود و اطلاعات عمیق برای استقرار آن نیاز بوده است. هدف ویروس استاکس‌نت به تأخیر انداختن برنامه هسته‌ای ایران در نطنز و اخلال در روند غنی‌سازی سانتریفیوژها بوده است. نگاهی به کدهای این بدافزار نشان می‌دهد این کدها به زبان‌های مختلف و برای سوءاستفاده از آسیب‌پذیری «روز صفر» برنامه‌ریزی شده بود. آقای کیم زتر[1] سلاح سایبری را چنین توصیف می‌کند: مانند سلاح‌ها متعارف، بیشتر سلاح‌های سایبری از دو بخش تشکیل می‌یابند. موشک یا بخش تحویل که مسئولیت گسترش بدافزار و نصب آن بر روی ماشین‌ها می‌باشد و محموله آن‌که حمله واقعی را شکل می‌دهد؛ مانند سرقت داده‌ها یا کارهای دیگری بر روی ماشین آلوده. استاکس‌نت نیز از این ویژگی برخوردار بوده است. در جدول ذیل استاکس‌نت با شاخص‌های تروریسم سایبری مورد بررسی قرار گرفته است: ***(Chuipka,*** ۲۰۱۷)

۱-Kim Zetter

جدول (۲): مطالعه موردی استاکس‌نت

شاخص های تروریسم سایبری	ویروس استاکس نت	جنگ سایبری	تروریسم سایبری
اجرا از طریق فضای سایبر	✓	✓	✓
اهداف و انگیزه ها سیاسی و ایدئولوژیک	✓	✓	✓
خشونت یا تهدید به خشونت	✓	–	✓
طراحی شده برای پیامدهای روانی گسترده و فوری بر هدف	✓	–	✓
هدایت شده هم به وسیله یک سازمان زنجیری فرماندهی و توطئه (بدون لباس و نشان مشخص) یا افراد و یا مجموعه ای از افراد، با انگیزه و الهام از اهداف ایدئولوژیک یا مثالی از جنبش تروریستی و رهبران آن	×	×	✓
ارتکاب به وسیله یک گروه محلی یا نهاد غیر دولتی	×	×	✓

راهبردهای تروریست‌های سایبری:

ارعاب: تروریست‌ها با استفاده از تهدید و ارعاب تلاش می‌کنند مردم را متقاعد سازند که آن‌ها به‌اندازه کافی برای مجازات نافرمانی، قدرتمند هستند و دولت نیز بیش از اندازه 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: حمله تباه‌کنندگان، تلاش برای متقاعد ساختن حریف به میانه‌روی با تروریست‌های ضعیف و غیرقابل اعتماد به منظور دستیابی به توافق صلح می‌باشد.

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 به اندازه کافی قوی برای تحمیل هزینه‌های قابل‌توجه می‌باشند اگر دشمن آن‌ها به یک سیاست مشخصی ادامه دهد.***(Chuipka,*** ۲۰۱۷***)***

پس از بررسی ادبیات نظری پیرامون تروریسم سایبری، از جمع‌بندی آن‌ها تعریف محقق ساخته از تروریسم ارائه می‌شود:

هرگونه تهدید یا اقدام طراحی شده 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 فرآیندهای فیزیکی مبتنی بر فضای سایبر، به منظور 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، محیط زیست شود تروریسم سایبری اطلاق می‌گردد.

ارزیابی 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 عمده آن می‌باشد (***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 جدا شده 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 حوزه مسائل امنیتی قرار دارد، بنابراین در این تحقیق به آن ارزیابی تهدید اطلاق می‌نماییم.

اجزای ضروری که در ارزیابی تهدیدات به کار می‌روند عبارتند 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 مانند بخش کشاورزی، بانکداری و امور مالی، مواد شیمیایی و ضایعات خطرناک، صنایع دفاعی پایه، انرژی، خدمات ضروری، غذا، دولت، ارتباطات و اطلاعات، حمل‌ونقل، خدمات پستی، سلامت عمومی، آب و دارایی‌های کلیدی مانند آثار ملی، نیروگاه هسته‌ای، سدها، امکانات دولتی و دارایی‌های تجاری.

ارزیابی میزان حساسیت و حیاتی بودن آن‌ها[۲]: تلاش سیستماتیک برای شناسایی و ارزیابی دارایی‌های مهم و یا حیاتی در یک حوزه است. ارزیابی حساسیت به برنامه‌ریزان برای تعیین

۱-Criticality Assessment: Evaluating Assets
۲-Calculating Criticality

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. در این رابطه طیف مورد استفاده شامل بسیار زیاد، زیاد، متوسط، کم و ناچیز می‌باشد.

ارزیابی تهدید[1]: تلاش سیستماتیک برای شناسایی و ارزیابی تهدیدات مانند تهدیدات تروریستی موجود و بالقوه برای دارایی هدف می‌باشد. با توجه به مشکلات موجود در ارزیابی دقیق، قابلیت، مقاصد و تاکتیک‌های تروریست‌ها، ارزیابی تهدید ممکن است تنها اطلاعات کلی در مورد مخاطرات بالقوه را در بربگیرد. اطلاعات ضروری برای جمع‌آوری و تجزیه‌وتحلیل و ارزیابی تهدید شامل:

الف – نوع دشمن مانند تروریست، دسته 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 مورد نیاز برای اجرای هدف مانند عکس و نظارت پلیس یا الگوهای گشت‌زنی، به احتمال زیاد یا «بدترین حالت» زمان حمله دشمن هنگام شلوغی یا شب. د– طیفی از تاکتیک‌های دشمن مانند مخفی‌کاری و فریب. ه– قابلیت‌های دشمن مانند دانش و انگیزه می‌باشد. سطوح تهدید بر اساس درجه و میزان ترکیب عوامل ذیل ارائه می‌گردد: (این سطوح به صورت نمونه برای گروه‌های تروریستی تبیین گردیده 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 می‌گردد.

۳. قصد و نیت: شواهدی از فعالیت گروه تروریستی، از جمله قصد اظهار و ارزیابی شده برای هدایت فعالیت تروریستی.

٤. تاریخچه: فعالیت تروریستی انجام شده در گذشته.

۱-Threat Assessment

۵. هدف قرار دادن: اطلاعات معتبر کنونی و یا فعالیتی به منظور آماده‌سازی برای مجموعه عملیات اطلاعاتی تروریستی خاص توسط یک گروه مظنون، تهیه دستگاه‌های مخرب یا اقدامات دیگر.

٦. محیط امنیتی: وضعیت سیاسی و امنیتی حوزه که تحت تأثیر عناصر تروریستی قرار گرفته‌اند را نشان می‌دهد. برای اندازه‌گیری تهدید نیز از شاخص‌های کمی شده بحرانی، بالا، متوسط، پایین و ناچیز استفاده می‌شود.

ارزیابی آسیب‌پذیری[1]: عبارت است از شناسایی نقطه‌ضعف در ساختارهای فیزیکی، سیستم-های حفاظت کارکنان، فرآیندها و یا مناطق دیگر که ممکن است توسط تروریست‌ها مورد استفاده قرار گیرد. فاکتورهایی که برای اندازه‌گیری آسیب‌پذیری مورد استفاده قرار می‌گیرند عبارتند 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 به راحتی 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 منفجره یا موادی که برخی از اشخاص و یا سازمان‌های فرصت‌طلب می‌توانند به عمد برای ایراد صدمه استفاده نمایند.٤. در دسترس بودن: در دسترس بودن تجهیزات، کفایت نیروها واکنشی و به‌طور کلی اقدامات امنیتی فیزیکی.

محاسبه تهدید: کلیه ارزیابی‌های قبلی (حساسیت، تهدید، آسیب‌پذیری) برای تکمیل و به تصویر کشیدن مخاطره یک دارایی یا گروهی از دارایی‌ها ترکیب می‌نماید ۱. حساسیت یا میزان حیاتی بودن: درباره اینکه اگر یک دارایی شناسایی شده از بین برود یا از یک رویداد خاص خسارت یا آسیب ببیند چه تاثیر احتمالی خواهد داشت سؤال می‌کند.۲. احتمال تهدید: درباره این‌که چقدر احتمال دارد دشمن به دارایی شناسایی شده حمله نماید سؤال می‌کند.۳. آسیب‌پذیری: درباره اینکه دشمن از چه آسیب‌پذیری‌هایی احتمالاً برای هدف قرار دادن دارایی استفاده خواهد کرد سؤال می‌کند. فرمول ارزیابی تهدید در فرمول:

تهدید= دارایی‌های کلیدی*آسیب‌پذیری*احتمال وقوع خلاصه می‌شود.

۱-Vulnerability Assessment

ارزیابی تهدیدات در سازمان پدافند غیرعامل کشور: در این سازمان با رویکردهای گوناگون به ارزیابی تهدیدات که مهم‌ترین بخش مدیریت تهدیدات می‌باشد پرداخته شده و در نهایت تلاش گردیده یک چارچوب و مدل بومی در این رابطه ارائه شود. برخی از الگوهایی که در این رابطه مورد مطالعه قرار گرفته‌اند عبارتند 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 مؤسسه ملی دادگستری آمریکا
۵. چارچوب ارزیابی تهدیدات در سازمان پدافند غیرعامل (سازمان پدافند غیرعامل، ۱۳۹۱).

روش (***OWASP***): رویکرد استانداردی توسط***OWASP*** [۳] برای ارزیابی مخاطره عرضه شده است در این روش: تهدید= احتمال * اثر می‌باشد: ***("OWASP Risk Rating Methodology - OWASP," n.d.)***

مرحله اول: شناسایی تهدید- در اولین گام برای شناسایی یک خطر امنیتی، نیاز است تا نرخ-گذاری صورت پذیرد. آزمون‌کننده نخست به جمع‌آوری اطلاعات درباره عامل حمله می‌پردازد که شامل حمله‌ای است که از یک آسیب‌پذیری استفاده می‌کند و به‌طور موفق بر کسب‌وکار تأثیر می-گذارد، به‌طور کلی بهتر است بدترین گزینه که بیشترین خطر را دارد انتخاب شود.

مرحله دوم: عوامل تخمین احتمال- هنگامی‌که آزمون کننده خطر احتمالی را شناسایی کرد می‌خواهد بداند چقدر جدی است؛ بنابراین احتمال را بایستی ارزیابی کند. لازم نیست این برآورد خیلی دقیق باشد و به‌طور کلی 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 حمله 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 سناریو استفاده گردد. به‌طور مثال یک فرد داخلی ممکن است یک مهاجم مؤثرتری از یک

۱-Fema
۲-RAMCP: Risk Analysis and Management for Critical Asset Protection
۳-The Open Web Application Security Poroject

بیگانه باشد که به تعدادی از عوامل بستگی دارد. هر مجموعه دارای گزینه‌هایی است که از صفرتا نه نمره‌دهی می‌شود.

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

جدول (۳): 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) کاربران اینترانت(۴) شرکاء(۵) کاربران 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 ذکر شده بالا می‌باشد.

جدول (٤): 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 ابزارهای 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)

گام سوم: عوامل تخمین اثر- با توجه به تأثیر یک حمله موفقیت‌آمیز مهم است بدانیم دو نوع اثر وجود دارد، اول «تأثیر فنی» بر روی برنامه‌های کاربردی، داده‌های مورد استفاده و توابع آن را فراهم می‌نماید. دیگر «کسب‌وکار سازمان». هر عامل گزینه‌های صفر تا نه را به خود اختصاص می‌دهد.

جدول (۵): عوامل تأثیر فنی

عوامل تاثیر فنی		
ردیف	ویژگی آسیب پذیری	توصیف
۱	از دست دادن محرمانگی	چقدر داده می تواند افشاء شود و حساسیت آنها چقدر است؟ افشای حداقل داده ها و غیرحساسند (۲) حداقل اطلاعات حیاتی افشا شده (۶)، داده های غیرحساس گسترده افشا شده (۶)، داده های حیاتی افشا شده (۷)، تمام داده های افشا شده (۹)
۲	از دست دادن تمامیت	چقدر اطلاعات خراب شده و چقدر آسیب دیده است؟ حداقل اطلاعات کمی تخریب شده (۱)، حداقل اطلاعات به طور جدی خراب شده (۳)، اطلاعات با شدت کمی خراب شده (۵)، اطلاعات به طور جدی خراب شده (۷)، تمام داده ها کاملا خراب شده (۹)
۳	از دست دادن دسترس پذیری	چقدر خدمات می تواند از دست رفته باشد و چقدر حیاتی هستند ؟ حداقل خدمات ثانویه قطع شده (۱)، حداقل خدمات اولیه قطع شده (۵)، خدمات ثانویه فراوانی قطع شده (۵)، خدمات اولیه گسترده قطع شده (۷)، تمام خدمات به طور کامل از بین رفته اند (۹)
۴	از دست رفتن حسابرسی و انتساب	آیا اقدامات عوامل تهدید قابل ردیابی و انتساب به یک فرد است؟ کاملا قابل ردیابی (۱)، احتمالا قابل ردیابی (۷)، کاملا ناشناس (۹)

عوامل کسب‌وکاری اثر: تأثیر کسب‌وکاری بر تأثیر فنی اثرگذار می‌باشد، اما نیاز به درک عمیق از آنچه برای سازمان مهم است می‌باشد. ویژگی‌های زیر برای بسیاری از کسب وکارها مشترک است؛ اما این منطقه حتی خصوصیات مربوط به عامل تهدید، آسیب‌پذیری و اثر فنی برای سازمان منحصر به فردتر است.

جدول (٦): عوامل تأثیر تجاری

عوامل تجاری اثر		
ردیف	ویژگی آسیب پذیری	توصیف
۱	خسارت مالی	چقدر خسارت مالی از این بهره کشی حاصل شده است؟ کمتر از هزینه رفع آسیب پذیری(۱) قدر جزئی بر سود سالانه(۳) اثر معنی دار بر سود سالانه(۷) ورشکستگی(۹)
۲	خسارت بر اعتبار	آیا سوء استفاده منجر به آسیب رسیدن به اعتبار و در نتیجه خسارت به کسب و کار شده است؟ حداقل خسارت(۱)از دست دادن حساب کاربری اصلی(۴) 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)
۴	نقض حریم خصوصی	چقدر اطلاعات شخصی قابل شناسایی افشاء شده است؟ یک فرد(۳) صدها نفر(۵) هزاران نفر(۷) ملیون ها نفر(۹)

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

مرحله پنجم: تصمیم برای رفع تهدید- بعد از اینکه تهدیدات طبقه‌بندی شدند، یک لیست اولویتی از آنچه باید برطرف شود؛ وجود دارد. به عنوان یک قاعده کلی، ابتدا باید شدیدترین خطرات را تعیین کرد.

مرحله ششم: سفارشی سازی مدل - داشتن چارچوب قابل تنظیم برای سازوکاری با کسب کار حیاتی است. مدل تنظیم شده به احتمال زیاد نتایج بهتری مطابق با درک افراد درباره 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.

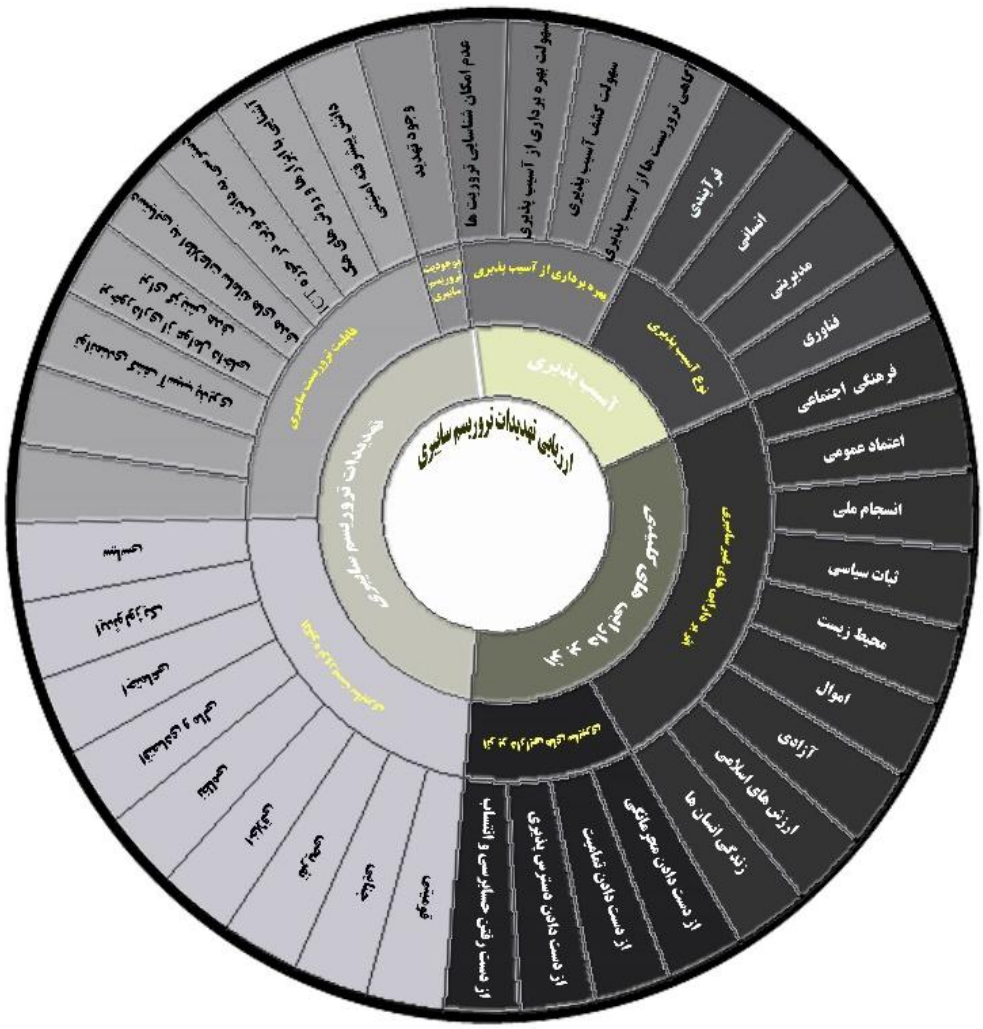
جمع‌بندی ارزیابی تهدید: در بخش قبلی روش‌های مختلف ارزیابی تهدید، عوامل مؤثر در این فرآیند و به‌طور اخص در ارزیابی تهدیدات تروریسم سایبری مورد بررسی قرار گرفت. تقریباً کلیه روش‌های ارزیابی از زمینه یکسانی برخوردار می‌باشند و در همه آن‌ها از الف- احتمال وقوع تهدید تروریسم سایبری ب- بهره‌برداری از آسیب‌پذیری‌های 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 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 غیرسایبری روش مناسب‌تری برای ارزیابی تهدید تروریسم سایبری محسوب می‌گردد بنابراین معادله مورد استفاده از این روش به شرح ذیل ارائه می‌شود:

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

مدل مفهومی پیشنهادی: پس از احصاء ابعاد و عوامل ارزیابی تهدیدات تروریسم سایبری می‌توان مدل مفهومی ذیل را برای پژوهش پیشنهاد نمود:

شکل (۱): مدل مفهومی ارزیابی تهدیدات تروریسم سایبری



روش تحقیق:

در این تحقیق، از روش موردی زمینه‌ای استفاده گردیده است، یعنی پژوهشگر پس از مطالعه موقعیت قبلی تروریسم و ارزیابی این تهدید در فضای حقیقی به بررسی آن در موقعیت جدید

یعنی فضای سایبر می‌پردازد این فرآیند، مراحل پژوهش موردی زمینه‌ای است.

جامعه آماری مورد نظر در این تحقیق متناسب با روش مورد استفاده شامل خبرگانی می‌باشد که مسلط به مسائل راهبردی فضای سایبر بوده و در حوزه تروریسم و تروریسم سایبری صاحب‌نظر باشند، بنابراین تعداد آنان در کشور بسیار محدود بوده و با بهره‌گیری از روش هدفمند گلوله برفی[۱] تعداد آن‌ها را احصاء 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 ۳۱ نفر رسید.

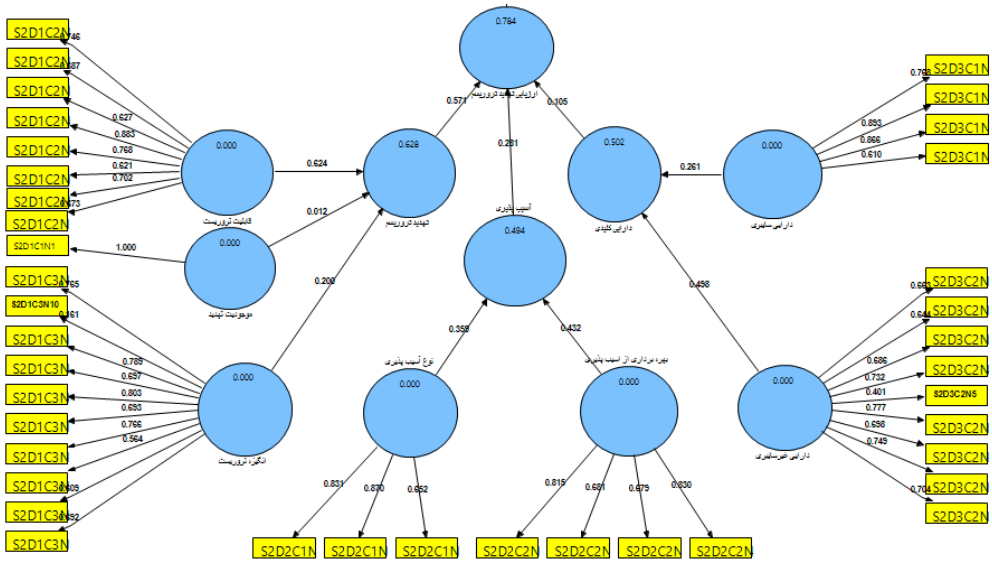
در این پژوهش تلاش شده است برای گردآوری اطلاعات از روش:۱- کتابخانه‌ای شامل کتابخانه علمی و تخصصی، سایت‌های معتبر اینترنتی ۲- روش میدانی: شامل مصاحبه با خبرگان و تنظیم پرسشنامه استفاده شود.

تجزیه وتحلیل داده‌ها و یافته‌های تحقیق:

در این پژوهش پس از جمع‌آوری پرسشنامه‌ها، داده‌های حاصل از آن نخست در نرم‌افزار *SPSS* وارد شده و برای تجزیه وتحلیل توصیفی جامعه آماری، این نرم‌افزار مورد استفاده قرار گرفته است. سپس برای دستیابی به بار عاملی، چیدمان سازه‌های اصلی شامل ابعاد و عوامل استخراج شده 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 مرحله بعدی روایی همگرا با استفاده از ضرایب *AVE* سازه‌ها و روایی واگرا با استفاده از روش فورنل و لارکر مورد بررسی قرار گرفته است. در مراحل بعدی برازش مدل ساختاری با بهره‌گیری از ضرایب معناداری *Z* و همچنین ضریب تعیین *R۲* و معیار *Q۲* احراز و سپس برازش کلی مدل *GOF* محاسبه و با پاسخ به سؤال پژوهش، مدل نهایی نیز ترسیم شده است.

پایایی (بارهای عاملی): همان‌طور که در شکل (۲) مشاهده می‌شود عوامل ***S۲D۱C۳N۱۰*** و ***S۲D۳C۲N۵*** دارای بار عاملی کمتر از ۰/٤ یا ۰/٤ می‌باشند بنابراین از مدل انعکاسی حذف شدند بقیه عوامل از بار عاملی قابل قبولی برخوردار هستند.

۱-Snowball Sampling



شکل (۲): مدل‌های اندازه‌گیری ارزیابی تهدید

آلفای کرونباخ: همان‌طور که در جدول (۷) مشاهده می‌شود، آلفای کرونباخ مدل‌های انعکاسی بیشتر از ۰.۷ است که حکایت از پایا بودن حوزه ارزیابی تهدید دارد.

جدول (۷): آلفای کرونباخ ارزیابی تهدید

	Cronbachs Alpha
ارزیابی تهدیدات تروریسم سایبری	0.863922
تهدید تروریسم	0.738140
موجودیت تهدید	0.904217
قابلیت تهدید	0.8809979
انگیزه تروریست	0.766361
آسیب پذیری	0.735383
نوع آسیب پذیری	0.797553
بهره برداری از آسیب پذیری	0.8594423
دارایی های کلیدی	0.754111
دارایی های سایبری	0.7128849
دارایی های غیر سایبری	0.7007375

پایایی ترکیبی (مشترک): همان‌طور که در جدول (۸) مشاهده می‌شود، پایایی ترکیبی (مشترک) بیشتر از ۰.٦ است که حکایت از پایایی مناسب مدل دارد.

جدول (۸): پایایی ترکیبی ارزیابی تهدید

	Composite Reliability
ارزیابی تهدیدات تروریسم سایبری	0.893588
تهدید تروریسم	0.883363
موجودیت تهدید	0.939775
قابلیت تهدید	0.902093
انگیزه تروریست	0.839798
آسیب پذیری	0.840598
نوع آسیب پذیری	0.868311
بهره برداری از آسیب پذیری	0.889157
دارایی های کلیدی	0.890369
دارایی های سایبری	0.838890
دارایی های غیرسایبری	0.839714

روایی: روایی همگرا همان‌طور که در جدول (۹) مشاهده می‌شود، مقادیر سازه‌های این حوزه نیز بیشتر از ۰.۵ است که حکایت از روایی همگرای مناسب مدل دارد.

جدول (۹): روایی همگرا ارزیابی تهدید تروریسم سایبری

AVE	
0.515244	ارزیابی تهدیدات تروریسم سایبری
0.791188	تهدید تروریسم
0.838793	موجودیت تهدید
0.509077	قابلیت تهدید
0.569395	انگیزه تروریست
0.651487	آسیب پذیری
0.627034	نوع آسیب پذیری
0.501556	بهره برداری از آسیب پذیری
0.802415	دارایی های کلیدی
0.636602	دارایی های سایبری
0.623987	دارایی های غیرسایبری

روایی واگرا: همان‌طور که در ماتریس فورنل و لارکر مدل جدول (۱۰) مشاهده می‌گردد، 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 قابل قبول بودن روایی واگرای متغیرهای حوزه ارزیابی تهدید تروریسم سایبری می‌باشد.

جدول (۱۰): 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

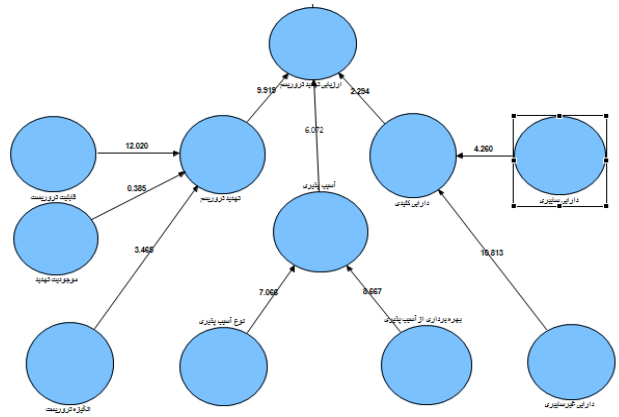
بررسی برازش مدل ساختاری: این برازش با استفاده از محاسبات بوت استرپینگ (خود راه‌اندازی) نرم‌افزار به منظور ارزیابی روابط بین متغیرهای پنهان (دایره‌ها) در سه معیار ۱- ضرایب معناداری ***z*** (مقادیر ***t-values***) ۲- معیار ***R***۲[۱] (ضریب تعیین) ۳- معیار ***Q***۲[۲] صورت گیرد.

ضرایب معناداری ***z*** *(مقادیر* ***t-values****)*: مقادیر عددی ضرایب معناداری ***z*** (مقادیر لینک‌های متصل به دایره‌ها) در این بعد برابر شکل (۳) 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 می‌گردد معناداری سایر روابط در جدول زیر نشان داده شده است.

۱- R Squares

۲- Stone-Geisser Criterion

شکل (۳): گزارش بوت استرپینگ ارزیابی تهدید



معیار ***R*** ۲ *(ضریب تعیین)*: نشان دهنده میزان تأثیر یک متغیر برون‌زا بر یک متغیر درون‌زا است. در جدول (۱۱) برازش بر اساس ***R***۲ گزارش شده که از متوسط تا قوی ارزیابی گردیده است.

جدول (۱۱): ضریب تعیین (R۲)

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

معیار ***Q***۲: نشان‌دهنده قدرت پیش‌بینی مدل است. مقادیر بالای صفر نشان می‌دهند که مقادیر مشاهده شده خوب بازسازی شده‌اند و مدل توانایی پیش‌بینی دارد. با توجه به جدول (۱۲)، برازش مدل ارزیابی تهدید مناسب می‌باشد.

جدول (۱۲): معیار Q۲

	SSO	SSE	Q^2 (=1-SSE/SSO)	نتیجه
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

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 به عنوان مقادیر ضعیف، متوسط و قوی برای ***GOF*** ارائه شده است، به این معنی که مثلاً در صورت محاسبه 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»[1] و میانگین «ضریب تعیین» از جدول (۱۳) حاصل می‌گردد.

جدول (۱۳): ضریب تعیین و متوسط واریانس

	ضریب تعیین R2	متوسط واریانس استخراج شده
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
میانگین	0/609	0/675

$$GOF = \sqrt{\overline{\text{Communality}} \times \overline{R^2}} = \sqrt{.65 \times .602} = .641$$

همان‌طور که مشاهده می‌شود، مقدار برازش کلی مدل معادل ۰.۶۴۱ م و چون از ۰.۳۶ بیشتر است، برازش مدل قوی ارزیابی گردیده و با استفاده از نتایج حاصل می‌توان، به بررسی فرضیه

۱-Communality: این عنوان به صورت مشخص در نسخه ۲ نرم افزار وجود دارد ولی در نسخه ۳ نرم‌افزار از مقدار AVE استفاده می‌شود.

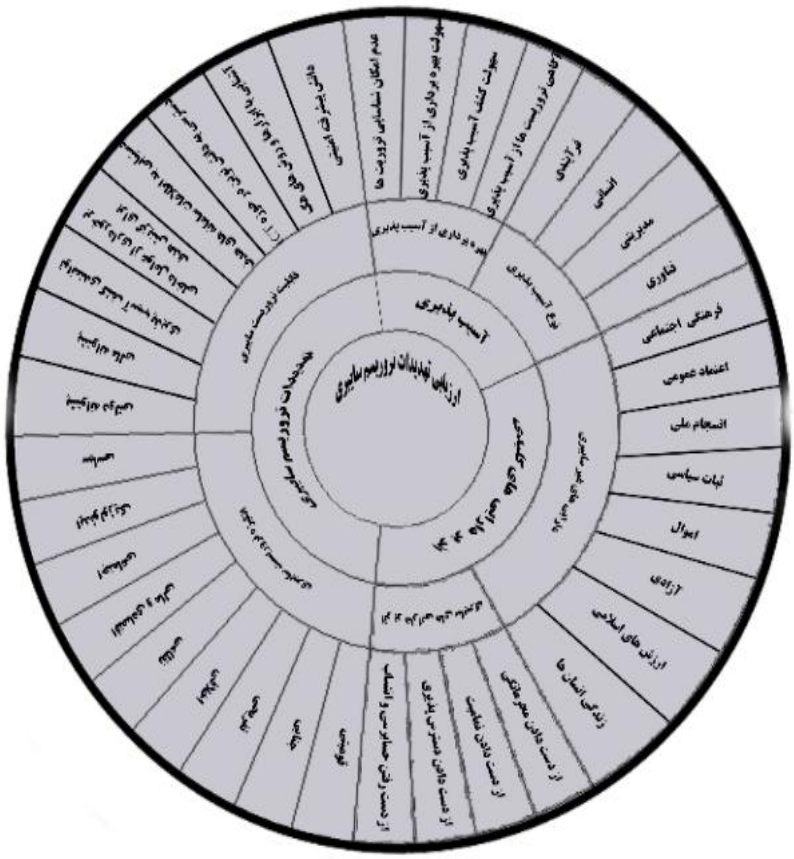
پژوهش پرداخت. برای این منظور، مقادیر ضرایب مسیرها، ضرایب **Z** در جدول زیر گردآوری و بر اساس آن مورد بررسی قرار گرفته و نهایتاً تأیید یا رد می‌شود:

جدول(۱٤) آزمون فرضیه

روابط	ضریب مسیر	ضرایب z	تأیید یا رد	سطح معناداری
ارزیابی تهدید تروریسم سایبری ⟵ احتمال تهدید تروریسم	۰/۵۷۵	۱۰.۲۳۱	**تأیید**	۰/۹۹
ارزیابی تهدید تروریسم سایبری ⟵ آسیب‌پذیری	۰/۲۸۰	٦.۲۱۱	**تأیید**	۰/۹۹
ارزیابی تهدید تروریسم سایبری ⟵ دارایی کلیدی	۰/۱۰۵	۲.۲۵۱	**تأیید**	۰/۹۵

نتیجه‌گیری:

برابر جدول (۱٤) ضریب معنی‌داری بیشتر از ۱.٦٤ و بیشتر از ۱.۹٦ و بیشتر از ۲.۵۸ باشد حکایت از صحت رابطه بین عوامل در سطح معناداری ۹۰٪ و ۹۵٪ و ۹۹٪ خواهد داشت. طبق یافته‌های حاصل از تجزیه و تحلیل داده‌ها، سه عامل یعنی «احتمال تهدید تروریسم سایبری، آسیب‌پذیری و دارایی‌های سایبری و غیرسایبری» ارزیابی تهدید تروریسم سایبری در سطح معناداری ۹۹٪ و ۹۹٪ و ۹۵٪ مؤثر می‌باشند و با محاسبه آن‌ها می‌توان تهدید تروریسم سایبری را ارزیابی نمود بنابراین فرضیه پژوهش نیز مورد تأیید قرار می‌گیرد و با حذف عوامل «موجودیت»، «عصر جدید» و «محیط زیست» مدل نهایی با اندک تغییراتی به شرح ذیل ترسیم و ارائه گردیده است.



شکل (٤): مدل نهایی ارزیابی تهدید تروریسم سایبری

پیشنهاد:

- با مدل ارائه شده تهدیدات تروریسم سایبری مورد ارزیابی و اولویت‌بندی قرار گیرد. این فرآیند مسیر اقدام مؤثر را برای مقابله با این پدیده هموار می‌نماید.
- ارزیابی تهدیدات مهم‌ترین فرآیند مدیریت تهدیدات می‌باشد؛ بنابراین با تلفیق ارزیابی تهدید و راهبردهای مدیریتی به صورت اثربخش تهدیدات حوزه تروریسم سایبری مدیریت شود.

پیشنهاد برای تحقیقات آتی:

پیشنهاد می‌شود بر اساس مدل مفهومی ارائه شده سامانه‌ای برای ارزیابی مستمر تهدیدات تروریسم سایبری طراحی شود.

منابع:

- آشوری، داریوش، (۱۳۸۲)، ***دانش‌نامه سیاسی***، تهران: انتشارات مروارید.
- بیات، غلامرضا، (۱۳۹۲)، ***نقش بسیج در پدافند سایبری و تأثیر آن بر امنیت ملی جمهوری اسلامی ایران***، تهران: فصلنامه راهبردی بسیج، شماره ۵۸.
- جعفری، مجتبی، (۱۳۹۲)، ***تهدیدات امنیتی سایبرتروریسم***، مشهد: ششمین کنگره انجمن ژئوپلیتیک ایران (پدافند غیرعامل).
- جلالی، غلامرضا، (۱۳۸۹)، ***روش و مدل برآورد تهدیدات و پدافند غیرعامل***، تهران: انتشارات دانشگاه امام حسین (ع).
- خلیلی، سیاوش، (۱۳۹۱)، ***روش‌های پژوهش آمیخته***، چاپ دوم، تهران: مؤسسه انتشارات یادواره کتاب.
- سمیعی‌اصفهانی، علیرضا؛ سالکی، عبدالکریم، (۱۳۹٤)، ***ترور، تروریسم و تروریسم دولتی***، مجله سیاسی، اقتصادی، شماره 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 نحوه بررسی و ارزیابی آن‌ها***، تهران: سازمان پدافند غیرعامل کشور.
- عبدالله خانی، علی، (۱۳۸٦)، ***تهدیدات امنیت ملی***، تهران: انتشارات بین‌المللی ابرار معاصر تهران.
- عمید، حسن، (۱۳۳۲)، ***فرهنگ فارسی عمید***، تهران، چاپ میلاد نور، چاپ اول قطع جیبی سال ۱۳۸۹.
- قرارگاه پدافند سایبری کشور، (۱۳۹٤)، ***سند راهبردی پدافند سایبری کشور***، تهران: قرارگاه پدافند سایبری.
- معین، محمد، (۱۳٦۳)، ***فرهنگ معین***، چاپ ششم، تهران: امیرکبیر.
- ناجی‌راد، محمدعلی، (۱۳۸۷)، ***جهانی‌شدن تروریسم***، چاپ اول، تهران: انتشارات وزارت امور خارجه.
- ویکی پدیای فارسی؛ http://fa.wikipedia.org

- 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.
- 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.
- Salleh, N. M. Selamat, S. R. Yusof, R. Sahib, S. (۲۰۱٦), Discovering Cyber Terrorism Using Trace Pattern. International Journal of Network Security.
- 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. (۲۰۱٦), Study Group on Cybersecurity, Terrorism, and International Law, INTERNATIONAL LAW ASSOCIATION, http://www.ila-hq.org/en/studygroups/
- index.cfm/cid/۱۰۵۰.
- SEissa, Israa. Ibrahim, Jamaludin. Yahaya, Nor-Zaiasron. (۲۰۱۷), Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review, International Journal of Science and Research, ISSN (Online): ۲۳۱۹-۷۰٦٤.
- Veerasamy, namosha, Grobler, M. Sloms, B. V. (۲۰۱٦), Building an Ontology for Cyberterrorism.https://www.researchgate.net