فصلنامه پژوهش‌های حفاظتی-امنیتی
دانشگاه جامع امام حسین(علیه‌السلام)
سال دوازدهم شماره ۴۶ تابستان ۱۴۰۲

الگوی فرایندی تولید هشدار در اقدامات تروریستی

● حسین حسینی جیردهی ●
دانشیار مدیریت بحران دانشکده علوم اجتماعی ، دانشگاه جامع امام حسین علیه السلام ، تهران ، ایران
● حسین عربیان ●
دانش آموخته دکتری مطالعات منطقهای دانشگاه جامع امام حسین علیه السلام ، تهران ، ایران
● غلامعلی زوارزاده ●
استادیار دانشگاه جامع امام حسین علیه السلام ، تهران ، ایران

تاریخ دریافت: ۱۴۰۲/۰۴/۱۴ تاریخ پذیرش: ۱۴۰۲/۰۶/۱۴

چکیده

هشداردهی در اقدامات تروریستی با هدف جلوگیری از ظهور و بروز خطر تروریستی صورت می گیرد. این هشدار به دلیل هوشمندی بازیگران آن همواره از حساسیت بالایی برخوردار بوده و موفقیت و شکست در آن بر امنیت ملی کشور اثری مستقیم دارد. از این منظر توجه به طراحی الگوی فرایند تولید هشدار که به تمامی فرایندهای تولید هشدار توجه داشته و بتواند از حجم مشکلات و چالش های این حوزه بکاهد ضرورتی قابل توجه است.

در این راستا، پژوهش حاضر با رویکردی کاربردی و با هدف ارائه الگوی فرایندی تولید هشدار اقدامات تروریستی طراحی شده است. با توجه به سوال پژوهش از راهبرد پژوهشی سنتز پژوهی با بهره گیری از روش های گرد آوری کتابخانه ای-اسنادی استفاده شده است. داده های کیفی حاصل از گردآوری به روش تحلیل محتوای کیفی مورد تجزیه و تحلیل قرار گرفته و در نهایت الگوی بدست آمده توسط شش خبره مرتبط با موضوع اعتبار سنجی شده است.

یافته ها و نتایج پژوهش نشان می‌دهد که الگوی طراحی شده الگویی پویا، فرایندی، مبتنی بر احتمالات،کیفی و مفهومی است که گام‌بندی‌های اصلی آن عبارتند از: شناسایی نشانه های ظهور اقدامات تروریستی؛ رصد نشانه ها ؛پردازش داده‌ها و تحلیل نشانه‌ها در رسیدن به خلق معنا.

کلید واژه‌ها: تروریسم، هشداردهی، پایش و پویش محیطی، نشانه‌شناسی، تحلیل نشانه‌ها

مقدمه و بیان مسئله

مبارزه با اقدامات تروریستی از وجوه مختلفی برخوردار است. یکی از مهم‌ترین وجوه مبارزه با تروریسم رویکرد اطلاعاتی است. این رویکرد یکی از مهم‌ترین رویکردهای مطرح در بین رویکردهای دیپلماتیک، حقوق بشری، کیفری - غیرکیفری و نظامی در مبارزه با تروریسم محسوب می‌شود. این رویکرد که عمدتاً از سوی سازمان‌های اطلاعاتی و امنیتی دنبال می‌شود درصدد است با بهره‌گیری از شیوه‌ها و تاکتیک‌های اطلاعاتی از جمله جمع‌آوری، تحلیل، تخمین، هشدار، نفوذ، جریان‌سازی و غیره، اولاً مانع شکل‌گیری گروه‌های تکفیری و جمع شدن افراد دور همدیگر برای تکوین این گروه‌ها شده و ثانیاً در صورت شکل‌گیری این گروه‌ها، مانع به نتیجه رسیدن و تصمیم‌گیری آن‌ها برای انجام حمله تروریستی به اهداف و مقاصد خودی شود (پور سعید،۱۳۹۷:۲۷۸).

یکی از مهم‌ترین وظایف سازمان‌های اطلاعاتی و امنیتی در مبارزه با تروریسم، هشداردهی است. هشداردهی نه تنها خود سازمان‌های اطلاعاتی بلکه سایر سازمان‌های امنیتی، حفاظتی و انتظامی را نیز درگیر مأموریت می‌کند. اگر سازمان‌های اطلاعاتی و امنیتی نتوانند در تولید به هنگام هشدارها به‌درستی عمل نمایند مجبور خواهند بود به بحران‌ها به‌صورت واکنشی پاسخ دهند. پاسخ واکنشی نتیجه‌ای جز غافلگیری در برابر تهدیدات و شکست جامعه اطلاعاتی از مأموریت‌های محوله نخواهد داشت.

از این‌رو می‌توان گفت هشداردهی نه تنها خروجی بسیاری از فرایندهای اطلاعاتی بلکه اصلی‌ترین فرآورده دستگاه‌های اطلاعاتی محسوب می‌شود. این فرآورده منحصربه‌فرد با سازوکار مشخص و با هدف اعلام‌خطر علیه منافع ملی و امنیت ملی کشور قبل از وقوع حادثه عمل می‌کند. در تعریفی جامع‌تر می‌توان هشداردهی را «فرایند شناخت هوشمندانه و اعلام به هنگام علائم و نشانه‌های ضعیف ناشی از احتمال ظهور تدریجی پدیده مخاطره‌آمیز یا قریب‌الوقوع بودن رخدادهای پرخطر برای مراجع ذی‌نفع (منافع نظام سیاسی یا سرمایه‌های نهادی و انسانی) دانست که باهدف پیش‌آگاهی متقاعدکننده برای واکنش پیشگیرانه تصمیم‌گیران و جلوگیری از غافلگیری منجر به شکست اطلاعاتی - امنیتی صورت می‌گیرد» (مزینانی،۱۳۹۷:۸۸).

با این تعریف رسیدن به هشداردهی نیازمند نظام هشداردهی منسجمی است که در آن به گام‌های مهمی چون تولید هشدار، انتقال هشدار، به باور رساندن هشدار نزد مشتری، سیاست‌گذاری پیش از وقوع و در نهایت آماده‌باش به‌صورت مبسوط پرداخته شود. پرداختن به هر یک از مراحل یادشده نیازمند پژوهش‌های متعددی است که محدودیت‌های پژوهشی اجازه پرداختن به همه آن‌ها را در چارچوب مقاله‌ای واحد نمی‌دهد.

از سوی دیگر بررسی‌های میدانی نشان می‌دهد که عمده پیامدها در نظام هشداردهی به مرحله تولید هشدار برمی‌گردد. ازجمله این پیامدها می‌توان به «تعدد و تکثر هشدارهای ارائه‌شده» و «نبود تاریخ انقضایی برای هشدارها» اشاره داشت که در کنار «کمبود نیروی انسانی در حوزه‌های عملیاتی» باعث می‌گردد یگان‌های عملیاتی با هر هشداری به نیروهای خود فشاری مضاعف آورده و توان بالای عملکردی را از آن‌ها مطالبه کنند که این عامل به فرسودگی نیروهای امنیتی و حفاظتی منجر می‌گردد.

از پیامدهای دیگر تولید هشدار ناکارآمد می‌توان به کاهش باور فرماندهان به هشدارهای اقدامات تروریستی و بی‌اعتبار شدن هشدارهای صادر از سوی سازمان‌های اطلاعاتی اشاره داشت. همچنین در هشدارهای داده‌شده، احتمال نزدیکی یا دوری تهدید تروریستی به‌درستی مشخص نشده است و بیشتر نگاه صفر و یکی به هشدار وجود دارد و کمتر به احتمال بروز تهدید و سطح‌بندی آن توجه شده است. گذشته از این موارد، در هشدارهای داده‌شده نه توجهی به ارائه راهکارهای متناسب با نوع تهدید شده و نه از مجاری ثابتی اعلام می‌گردد به‌گونه‌ای که سازمان‌های متعددی با مجاری متنوعی هشدارها را به سازمان‌های امنیتی منتقل می‌کنند.

مهم‌تر اینکه ترس از هزینه‌های بالای شکست اطلاعاتی که در پی وقوع اقدامات تروریستی ممکن است گریبان سازمان‌های اطلاعاتی را بگیرد، منجر شده سازمان‌های اطلاعاتی عمدتاً به‌سوی کلی‌گویی و گرد گویی در هشداردهی حرکت کنند. در چنین شرایطی هشدار تولیدشده اگرچه درست است، اما عمدتاً کلی است یا اینکه مطالب ارائه‌شده به‌گونه‌ای است که نقیض ندارد. تولید چنین هشدارهایی سبب شده عملاً هشدارهای داده‌شده کارآمدی کمتری برای سازمان‌های امنیتی داشته باشد. چنین وضعیتی نظام هشداردهی را درگیر چرخه‌ای معیوب کرده که سرمنشأ آن را می‌توان در تولید هشدار ناکارآمد دانست. نتیجه چنین چرخه‌ای تحمیل هزینه‌های سنگین به سازمان‌های اطلاعاتی و امنیتی و در نهایت اقتدار و امنیت کشور خواهد بود.

پیامدهای ذکرشده عمدتاً از گام نخست چرخه هشدار ایجاد می‌گردند که این امر باعث می‌گردد تولید هشدار نسبت به سایر گام‌ها از اولویت توجه بیشتری برخوردار باشد. در این گام علاوه بر شناخت نشانه‌ها و رصد محیطی آن‌ها، تحلیل نشانه‌ها نیز از اهمیت بالایی برخوردار است. چراکه گستردگی حجم داده‌های دریافتی، عدم قطعیت‌ها و لحظه‌ای و سیال بودن داده‌ها باعث می‌گردد تفکیک نشانه‌های دروغ و فریب از نشانه‌های اصلی، دچار مشکل شده و درنهایت معنا بخشی به

اطلاعات برای رسیدن به هشدار با چالش جدی مواجه شود. از این چالش به‌عنوان تفکیک سیگنال از سروصدا (نویز) نیز یاد می‌شود (ولستیتر،۱۹۶۲:۶۰).

بررسی ادبیات حرفه‌ای و دانشگاهی نیز تأیید می‌کنند که اگرچه در گذشته داشتن اطلاعات به‌تنهایی می‌توانست دست برتری را به سازمان اطلاعاتی دهد و داشتن اطلاعات به معنای پیروزی در جنگ اطلاعاتی محسوب می‌شد اما اکنون دیگر داشتن اطلاعات به‌تنهایی کفایت نمی‌کند. بلکه چگونگی بهره‌گیری از انبوه اطلاعات است که دست برتری را به سازمان‌های اطلاعاتی می‌دهد (موشراش،۱۳۹۷:۳). بر این اساس شناخت نشانه‌ها و علائم ضعیف، رصد و دیدبانی آن‌ها و درنهایت معنا بخشی به اطلاعات در میان انبوه داده‌های آشکار و پنهان از اهمیت اساسی در رسیدن به تولید هشدار برخوردار است.

لذا با توجه به اهمیت گام تولید هشدار و دغدغه‌مندی نگارندگان برای رفع چالش‌های مسیر تولید هشدار، این پژوهش درصدد ترسیم الگوی تولید هشدار اقدامات تروریستی بوده و در نظر دارد به این سؤال پاسخ دهد که الگوی تولید هشدار اقدامات تروریستی از چه فرایندی برخوردار است؟

مبانی نظری

تروریسم

تعارف مختلفی از تروریسم وجود دارد که هر یک با رویکرد خاصی به این پدیده نگریسته‌اند. به عنوان مثال در تعاریف لیست محور به جای توجه به اهداف تروریستی، شیوه‌های ستیز مورد تأکید قرار می‌گیرد. بر این اساس هر اقدامی همچون هواپیماربایی، گروگان‌گیری یا حمله به دیپلمات‌ها بدون توجه به انگیزه آن عملیات تروریستی نامیده می‌شود (لفری و فری لیچ،۱۳۹۹:۲۰۱). نوع دیگری از تعاریف لیست محور بر روی بازیگر تروریستی تمرکز می‌کنند و فهرستی از سازمان‌های تروریستی را بر همین مبنا معرفی می‌کنند. در این مورد ممکن است اعمال صورت گرفته به سادگی عملی مانند: توزیع برگه‌های تبلیغاتی در خیابان باشد اما انجام دهندگان آن می‌توانند به دلیل نمایندگی از سوی یک سازمان تروریستی مورد اعمال قوانین ضد تروریسم قرار گیرند (لفری و فری لیچ،۱۳۹۹:۲۰۲).

برخی دیگر از تعاریف تروریسم نیز مبتنی بر برخی ویژگی‌ها به تعریف تررویسم پرداخته‌اند. داشتن انگیزه سیاسی یکی از مهمترین ویژگی‌هایی است که در بسیاری از تعاریف دیده می‌شود. در این تعاریف شرط اینکه اعمال خشونت‌آمیز، تروریستی قلمداد شوند به انگیزه سیاسی نهفته در آن‌ها بستگی دارد(بل،۲۰۲۱:۲۱) (پورپورا،۲۰۰۶:۱۷).

در برخی از تعاریف نیز علاوه بر انگیزه سیاسی به ویژگی‌های دیگری نیز توجه شده است که به

برخی از این تعاریف نیز اشاره می‌شود. به عنوان مثال از منظر الکس اشمیت، تروریسم «از یکسو دکترین تأثیرگذاری نوع خاص یا تاکتیک ویژه‌ای از ایجاد وحشت، خشونت‌آمیز سیاسی و در سوی دیگر اعمال حساب‌شده، خشونت نابودگر و مستقیم بدون محدودیت حقوقی و اخلاقی که هدف اصلی آن غیرنظامیان هستند و برای دستیابی به تأثیرگذاری روانی و تبلیغاتی بر روی شنوندگان مختلف طرف‌های مخاصمه انجام می‌گیرد»(اشمیت،۸۶:۲۰۱۱) در یک تعریف دیگر تروریسم روش جنگ است که در آن قربانیان تصادفی یا نمادین، هدف خشونت قرار می‌گیرند. این قربانیان ابزاری، دارای خصوصیات گروهی یا طبقه اجتماعی مشخصی هستند که مبنای انتخاب آن‌ها را به‌عنوان قربانی شکل می‌دهد(اشمیت‌و جانگمن،۶:۲۰۰۵).

لذا در این مقاله با بررسی تعاریف مطرح شده می‌توان بیان کرد که هر نوع اقدام نابودگر و مستقیمی که بدون محدودیت حقوقی، اخلاقی و مبتنی بر اهداف سیاسی علیه دارایی‌های انسانی جمهوری اسلامی ایران صورت گیرد در چارچوب اقدامات تروریستی قلمداد می‌شود.

هشداردهی اطلاعاتی

در مورد هشداردهی اطلاعاتی نیز تعاریف مختلفی ارائه شده است که در زیر به بخشی از این تعاریف پرداخته می‌شود.

هشداردهی در حوزه اطلاعاتی و امنیتی به «مجموعه اقدامات یک سرویس اطلاعاتی که منجر به آگاهی یافتن از تهدیدها و جلوگیری از غافلگیری و شکست اطلاعاتی شود را گویند»(صالحی و مهدوی،۴۶:۱۳۹۷). هشدار اطلاعاتی در واقع مکانیسم احساس خطر و انجام اقداماتی برای رهایی از تبعات آن است.

هشداردهی اطلاعاتی بیان و انتقال سریع هرگونه نشانه‌ای از تغییرهای محتمل در سیاست‌ها، نیت‌ها، اهداف، اغراض، توانمندی‌ها، تدارکات و اقدامات خصمانه حریف است. اقدامات حریف می‌تواند مثبت، منفی و مشروط به منافع ملی خودارزیابی شود (مزینانی و ایمانی پور،۱۵۶:۱۳۹۷).

در دانشنامه موساد هشدار اطلاعاتی به «ارائه اطلاع از خطر، تهدید یا حوادث مترقبه به‌منظور پیشگیری از غافلگیری تصمیم‌سازان و عمل‌کنندگان گفته می‌شود»(وبسایت موساد[1] ، بی تا).

هشداردهی اعلام و ابراز نشانه‌های بروز یک واقعه از سوی دستگاه‌های اطلاعاتی به مراجع ذی‌ربط است (صالحی و مدبری،۹:۱۳۹۷)

در هشدار اطلاعاتی «تحلیلگران اطلاعات پس از دریافت داده‌های جمع‌آوری‌شده از طرف تیم‌های

1. The Mossad Website

جمع آوری صحنه، ضمن بررسی شواهد و تأیید اصالت داده‌ها، اقدام به تحلیل و رمزگشایی از اطلاعات می‌کنند تا بتوانند از ترکیب آن‌ها، اطلاعات جدیدی را به دست آورند. درصورتی‌که تحلیلگران به‌خوبی از عهده تحلیل شرایط و پدیده‌ها برآیند و بتوانند قبل از شکل‌گیری، به‌روز شدن، توسعه، تغییر شکل، جهت و شدت بحران را پیش‌بینی نمایند، نیاز به برداشتن گامی دیگر برای جلوگیری از وقوع غافلگیری و درنتیجه شکست اطلاعاتی دارند و آن اطلاع‌رسانی به مدیران و متصدیان امر (تصمیم‌گیران) برای اخذ بهترین و مناسب‌ترین تصمیم جهت مدیریت بحران است که به‌اصطلاح هشداردهی نامیده می‌شود»(صالحی و کوشا،۱۳۹۸:۵).

بررسی تعاریف ارائه‌شده نشان می‌دهد هشداردهی از منظر ایجابی می‌تواند واجد ویژگی‌های ذیل باشد.

هشدار مبتنی بر احتمالات است: بررسی‌ها نشان می‌دهد که مشهود بودن اقدامات خصمانه قریب‌الوقوع یا مقاصد معین مهاجم امری بسیار نادر است(علیخانی،۱۳۹۳:۳۶) بنابراین نباید انتظار قطعیت در هشدار را داشت.

هشدار مبتنی بر پیش‌آگاهی است. همان‌گونه که عنوان شد درست است که هشدار اطلاعاتی از قطعیت برخوردار نبوده و مبتنی بر احتمالات صورت می‌گیرد اما مبتنی بر یک آگاهی و شناختی صورت می‌گیرد. این نوع آگاهی به دلیل اتکا بر تحلیل نشانه‌ها و علائم ضعیف پیش‌آگاهی نامیده می‌شود. این گزاره می‌تواند با گذر زمان تقویت یا تضعیف شود اما رد یا تایید آن می‌تواند گزاره یا فرضیه ایجادشده را از دایره هشدار خارج نماید. اهمیت این پیش‌آگاهی به حدی است که ریچارد هلمز، رئیس اسبق سازمان اطلاعات مرکزی امریکا، وظیفه تحلیلگران اطلاعاتی را فراهم آوردن پیش‌آگاهی از امور دانسته است (هالت،۱۹۹۵:۸۰).

هشدار مبتنی بر خطر است. در نبود خطر هشدار هیچ معنایی نخواهد داشت. هشدار باید به‌طور مشخص احتمال بروز خطر[1] ، مخاطره[2] ، تهدید و درنهایت هر آنچه عنوان بحران بر آن گذاشته می‌شود را روشن سازد (حاجیانی، ۱۳۹۰:۱۳۷).

هشدار اعلام به هنگام و به‌موقع است. اعلام به هنگام و به‌موقع از ویژگی‌های خاص هشدار دهی است. از این‌رو هشدارها به‌شدت وابسته به زمان هستند به‌گونه‌ای که «اگر نظام هشداردهی نتواند هشداری را حتی چند دقیقه قبل از حمله اعلام کند، هر ویژگی دیگری که داشته باشد در انجام‌وظیفه خود شکست‌خورده است»(علیخانی،۱۳۹۳:۴۵).

هشدار مبتنی بر مشتری است. هشدار بسته به مخاطب مفهوم پیدا می‌کند. یعنی به‌خودی‌خود یک

1 Denger.
2 risk.

خبر نمی‌تواند هشدار باشد.

هشدار مبتنی بر قراین و شواهد است. پایه و اساس هشدار جست‌وجوی نشانه‌ها است(گرابو،۱۳۹۸:۲۴). هشدار دهی نسبت به یک موضوع تنها با نمایش و بروز یک هشدار صورت نمی گیرد بلکه مجموعه‌ای از شاخص‌ها و نشانه‌ها کنار هم قرار می‌گیرند تا تولید هشدار نمایند. «برای مثال عملی شدن یک اقدام تروریستی منوط به تحقق ده‌ها شرایط یا همان نشانه‌های است که در نهایت می‌توان به هشدار منجر شود (حاجیانی، ۱۳۹۰:۱۳۶).

هشدار مبتنی بر فرایند است. «هشدار دهی محصول نهایی فعالیت‌های مبتنی بر طراحی، سازمان‌دهی و اجرای جستجو اخبار در شبکه جمع‌آوری، پیرایش، پردازش و پیدایش اخبار و اطلاعات با بار امنیتی است»(مزینانی،۱۳۹۷:۸۳).

در مقابل رویکرد ایجابی به هشداردهی، رویکرد سلبی نیز می‌تواند در تمایزگذاری با سایر مفاهیم مشابه نیز کمک کننده باشد از این رو در تعاریف سلبی از هشداردهی موارد ذیل را می‌توان مطرح کرد.

هشدار، آگاه‌سازی امنیتی نیست. منظور از آگاه‌سازی، آگاهی بخشی عمومی نسبت به چالش‌های امنیتی پیش روی عمومی سرمایه انسانی است.

هشدار اطلاع‌رسانی امنیتی نیست. منظور از اطلاع‌رسانی، خبررسانی رسمی از موضوعات، مسائل و تلاش‌های صورت گرفته است.

هشدار ارشاد امنیتی نیست. منظور از ارشاد، تذکر پیشگیرانه به افراد در معرض خطا یا گرفتار آسیب امنیتی یا شبه امنیتی است.

هشدار توجیه و آموزش امنیتی نیست. منظور از آن، تلاش برای توانمندسازی کارکنان و مدیران امنیتی است (مزینانی و ایمانی پور،۱۳۹۷:۱۵۴).

هشدار تحلیل امنیتی نیست. تحلیل و به طرق اولی تر تحلیلگر برحسب داده‌هایی که به او رسیده است شروع به تحلیل می‌کند. این کار تحلیلگر که بر اساس دریافت یک سری از داده‌ها صورت می‌گیرد باعث می‌شود تحلیلگر در جریان داده‌های جدید کمتر قرار گیرد. به عبارتی بین دریافت داده‌ها و خروجی کار تحلیلگر یک فاصله زمانی وجود دارد. این فاصله زمانی در هشداردهی که ممکن است فاصله بین بروز یک نشانه تا رسیدن به بروز تهدید بسیار کوتاه باشد بسیار مهم است. همین نکته می‌تواند تفاوت بین تحلیل و هشداردهی را نشان دهد(معاونت پژوهش و تولید علم،۱۳۹۴:۲۴).

بنابراین با توجه به مباحث مطرح شده، هشداردهی اقدامات تروریستی را می‌توان چنین تعریف کرد:

فرایند شناخت هوشمندانه نشانه‌های ظهور احتمالی خطر اقدامات تروریستی و اعلام به هنگام آن به مشتری که باهدف اجتناب از غافلگیری صورت می گیرد.

پایش

جستجوی جهت دار یا اصطلاحاً پایش[1]، جستجوی حوزه‌های خاص که مورد نیاز صریح سازمان و جز نیازهای کلیدی و گلوگاهی است تعریف می‌شود(میرشاه ولایتی و نظری زاده،۷۳:۱۳۹۶). معمولاً در ادبیات نظامی از آن به مانیتورینگ یاد می‌شود. در یک تعریف از مانیتورینگ آمده است: مشاهده و سنجش مطابق با اسلوبی مشخص و استاندارد شده که به طور مستمر یا متناوب از محیط صورت می گیرد که معمولاً برای اهداف کنترلی و هشداردهی استفاده می شود. در پایش، بر اساس نیازمندی سازمان و حساسیت‌های مدنظر روی برخی موارد تمرکز ویژه شده و به طور خاص موضوع منتخب مورد رصد و مراقبت قرار می گیرد. پایش معمولاً در محیط نزدیک صورت می گیرد و موضوع یا موضوعات تحت پایش تا حدودی روشن و مبرهن است (صحرایی و همکاران،۱۱۷:۱۳۹۸).

پویش

جستجوی بدون جهت گیری خاص یا اصطلاحاً پویش[2]، جستجوی فرصت‌های موضوعی در فضاهای سفید که هنوز در سازمان مورد استفاده مشخص ندارد و با حوزه ماموریتی و موضوع سازمان پوشش داده نشده است تعریف می‌شود(میرشاه ولایتی و نظری زاده،۷۳:۱۳۹۶). پویش محیطی به عنوان نوعی مراقبت محیط به صورت نظام‌مند برای دریافت علایم کوچک و بزرگ، جدید و غیر منتظره است(صحرایی و همکاران،۱۱۶:۱۳۹۸). درواقع پویش محیطی را روشی برای مقابله با آن دسته از علائمی تعریف می کنند که به سختی قابل مشاهده و شناسایی هستند اما در عین حال نمی‌توان آن‌ها را نادیده گرفت و به خودی خود نیز دفع نمی‌شوند(آدما و روئل،۲۰۲:۲۰۱۰).

ب)روش شناسی

سنتز پژوهی حاصل دانش تلفیقی است. دانشی که دانسته‌های مطالعات گوناگون و شاید پراکنده را که می‌توانند با نیاز های خاص میدان عمل مرتبط باشد، گردهم آورد(شورت،۱۳۹۶). ارزش این نوع پژوهش در ایجاد همخوانی بین دانش و نیاز و نیز مهارت‌هایی است که به وسیله آنها فرایندهای ترکیب و تلفیق دانش انجام می‌پذیرد، چرا که دانش موجود در مطالعات و پژوهش‌های منفرد معمولاً

1Monitoring
2 Scanning

برای استفاده در تصمیم‌گیری مناسب نیست. در نظر گرفتن پژوهش‌ها به صورت منفرد، نه تنها گاهی اوقات تکلیف کنشگر را در قبال سؤال تعیین نمی‌کند بلکه یافته‌های ضد ونقیض، سبب گمراهی نیز می‌گردد. سنتز پژوهی یکی از راه‌های نزدیک شدن است به آنچه متولیان از هشداردهی اقدامات تروریستی انتظار دارند، زیرا در پی تلفیق یافته‌های پژوهش‌هایی است که به دنبال پاسخ دادن به سوالات پرسشی مشترک‌اند.

در پژوهش حاضر آنچه مدنظر است، راهبرد سنتز پژوهی حول هشدار اقدامات تروریستی از زمان مطرح شدن این مفهوم در ادبیات علمی عمومی از سال ۱۳۹۱ تا ۱۴۰۰ است. سنتز پژوهی دارای چهار مرحله است که این مراحل برای پژوهش حاضر در جدول زیر ارائه شده است.

جدول(۱): مراحل سنتز پژوهی

مرحله	زیر مرحله	توضیحات در مورد پژوهش حاضر
مرحله نخست:تعیین سوالات و اهداف پژوهش	اولین گام در سنتز پژوهی مشخص کردن سوالات و اهداف پژوهش است.یک سوال خوب به عنوان راهنما عمل کرده و ساختار تمرکز بر سنتز را مشخص می سازد(ساینی و شلون اسکای،۲۰۱۲).	بررسی های اولیه حاکی از آن بود که هشداردهی از برخی جنبه ها مورد بررسی قرار گرفته، اما با توجه به فقدان نگاه جامع به الگوی تولید هشدار در حوزه اقدامات تروریستی، این موضوع به عنوان سوال اصلی پژوهش مطرح گردید.
مرحله دوم:تعیین جغرافیای پژوهش، تعیین پژوهش هایی که مقرر است از یافته های آنها استفاده گردد.	الف. تعیین پارامتر های جستجو، همانند تاریخ انتشار و نوع پژوهش: این مرحله در واقع تعیین گستره پژوهش هایی است که مقرر است از یافته های آنان استفاده گردد. معیار و محدودیت هایی که در این مرحله در نظر گرفته می شود، می تواند مرز های زمانی ،جغرافیایی، شیوه های پژوهش و انتشار یافته ها باشد.	بازده زمانی مطالعات منتخب از سال ۱۳۹۱ تا سال ۱۴۰۰ انتخاب شده است. گستره جغرافیایی مطالعات انجام شده حول هشدار دهی اطلاعاتی در سراسر دنیا است. نوع پژوهش نیز مطالعات نظریه پردازی، مروری، تجربی و ارزیابانه است. و در نهایت نوع اسناد، مقالات داوری و منتشر شده، کتاب های چاپ شده و نیز پایان نامه های ارشد و دکتری در این زمینه است.
	ب. تعیین معیار های انتخاب اسناد گرد آوری شده از مرحله قبل	معیار های مورد نظر جهت انتخاب اسناد مرتبط بودن با سوال اصلی پژوهش، کیفیت پژوهش و نیز اعتبار روش های تحلیل مورد استفاده است.
از جستجوی اولیه ۶۳ مقاله و سند در حوزه هشداردهی به دست آمد		

مرحله	زیر مرحله	توضیحات در مورد پژوهش حاضر
مرحله سوم؛ نقد نظام مند اسناد منتخب	الف- غربالگری درشت	از نظر سایینی و شلون اسکای(۲۰۱۲) استاندارد های دقیقی برای راهنمایی در مورد این مرحله وجود ندارد. دو معیار «کیفیت» و«مرتبط بودن» در این مرحله لحاظ شده است. پس از مطالعه چکیده اسناد با توجه به دو معیار ذکر شده ۶۳ سند انتخاب شد.
	ب- عنوان غربالگری	کل متن مورد مداقه قرار گرفت. در این مرحله تعداد۳۳ سند از مجموع اسنادمورد بررسی کنار گذاشته شده و در نهایت ۳۰ سند جهت تحلیل و بررسی بیشتر در فهرست اسناد باقی ماند.
	ج- واکاوی عمیق	طبقه بندی، تحلیل و بررسی، ترجمه یافته ها و توضیحات رقیب از جمله فعالیت های این مرحله است. از آنجایی که پژوهشگر به دنبال سنتز یکپارچه از یافته های پژوهش است. در این پژوهش از راهبرد تحلیل کیفی برای پاسخگویی به سوال و طراحی الگو بهره گرفته شد.
مرحله چهارم؛ سنتز؛ خلق چیزی جدید از عناصر جدا از هم	سایینی و شلون اسکای(۲۰۱۲)، سه نوع سنتز را معرفی می کنند. تجسمی، یکپارچه سازی و تفسیری. سنتز یکپارچه یافته های دیگران و خود مبدل به داده هایی می شود که با داده های دیگر ترکیب و سپس با هویت جدید بازآفرینی می شوند.	با توجه به سوالات این پژوهش، پژوهشگر از روش سنتز تفسیری بهره گرفته شده است.

برای نیل به الگوی هشداردهی اقدامات تروریستی چهار گام اصلی تشریح شده است.

گام نخست، نشانه شناسی است. گام نشانه شناسی خود مشتمل بر سه زیر مرحله است که عبارتنداز: بررسی منابع شناسایی نشانه‌های ظهور اقدامات تروریستی، پردازش و طبقه‌بندی نشانه‌ها و سوم ایجاد پایگاه اطلاعات پایه‌ای.

گام دوم، رصد نشانه‌ها است. رصد نشانه‌ها نیز خود مشتمل بر دو زیر مرحله است که عبارتند از: آماده‌سازی مقدمات رصد نشانه‌ها با عنوان پیش رصد نشانه ها و دوم رصد محیطی.

گام سوم، پردازش داده‌ها است. در این گام داده‌های جمع‌آوری شده در گام قبلی مورد ارزیابی قرار گرفته و بعد از ارزیابی مورد پالایش و طبقه بندی قرار می‌گیرند و در نهایت داده‌ها با توجه به

ارزیابی‌ها و طبقه‌بندی‌های صورت گرفته در پایگاه اطلاعات جاری ثبت می گردند.

گام چهارم، تحلیل نشانه‌ها جهت خلق معنا است. این گام که آخرین گام در فرایند تولید هشدار محسوب می‌شود خود مشتمل بر سه زیر مرحله است که عبارتنداز؛کشف فرضیه، ارزیابی فرضیه و آزمون فرضیه.

در ادامه به تمامی این مراحل که تشکیل دهنده الگوی تولید هشدار اقدامات تروریستی است پرداخته می‌شود.

نشانه‌شناسی ظهور اقدامات تروریستی

نشانه‌ها می‌توانند هر چیز را شامل شوند به شرطی که معنایی به آن چیزها منصوب کنیم. به قول پیرس «هیچ چیز نشانه نیست مگر اینکه به عنوان نشانه تفسیرش کنیم» (چندلر،۴۵:۱۳۸۷). در واقع نشانه‌ها ذاتاً معنادار نیستند. پس لازم است برای تبدیل شدن به نشانه، معنایی به آنها منصوب کرده و بین نام[1] و مصداق[2] رابطه برقرار گردد.(چندلر،۲۱:۱۳۸۷). به عبارتی هر داده‌ای با داشتن هرگونه تمایل جهت بیشتر یا کمتر محتمل ساختن یک اتفاق است که می‌خواهیم رخداد آن را بررسی کنیم معنا می‌یابد. به هر میزان که ارتباط معنایی نام و مصداق قوی‌تر باشد به همان نسبت نیز رابطه معنایی محکمی بین آنها برقرار است. با توجه به این موضوع می‌توان نشانه‌ها را بر اساس قدرت رابطه معنایی که بین نام و مصداق بر قرار می‌شود به سه دسته تقسیم کرد که عبارتند از : شاخص، قرائن و شواهد، علایم ضعیف.

در شاخص‌ها، روابط معنایی ایجاد شده با تغییر افراد تغییر نمی‌کند و سلایق در ایجاد ارتباط در آن نقش کمتری دارند. در سطح پایین‌تر که قرائن و شواهد است. روابط با تغییر افراد و تخصص آنها ممکن است تفاوت‌هایی در برداشت معانی ایجاد شوند. در این سطح ایجاد ارتباط معنایی دشوارتر می‌شود. اما در سطوح پایین‌تر یعنی در حوزه علائم ضعیف، ارتباط‌های معنایی به حدی مشکل می‌شوند که به راحتی نمی‌توان ارتباط معنایی یکسانی را بین نام و مصداق ایجاد کرد و به عبارتی نوع ارتباط سیالیت بالایی دارد. از این رو مشخص کردن ارتباط پیچیده‌تر می گردد.

هر چه از نشانه‌های آشکارتر(شاخص‌ها) به لایه‌های زیرین نشانه‌ها(علایم ضعیف) نزدیک‌تر می‌شویم تلاش ارتباطی مضاعف‌تری برای برقراری رابطه معنایی بین دلالت کننده و دلالت‌گر ایجاد می‌شود. به گونه‌ای که قرائن و شواهد در لایه پایین‌تری از ایجاد معنا به نسبت شاخص‌ها قرار داد. هر چه از قدرت

1 name.
2 referent.

راهنمایی نشانه‌ها در رسیدن به کشف حقیقت کاسته می‌شود از لایه‌های معنایی قرائن و شواهد به سمت لایه‌های زیرینی همچون علائم ضعیف نزدیک‌تر می‌شویم. به گونه‌ای که در حوزه علائم ضعیف دیگر به درستی مشخص نیست دقیقاً دنبال چه می گردیم. لذا شاخص‌ها را نشانه اقدامات یا اقدامات احتمالی، قرائن و شواهد را نشانه‌هایی ظهور و بروز اقدامات احتمالی و علائم ضعیف را می‌توان بسترهای برای رسیدن به نشانه‌های ظهور و بروز اقدامات احتمالی دانست.

منابع شناسایی نشانه‌های اقدامات تروریستی

سوال این است که نشانه‌های ظهور و بروز اقدامات تروریستی که مبنای هشداردهی در اقدامات تروریستی بوده را از چه مجاری می‌توان شناسایی و تهیه کرد؟ از چهار منبع مهم برای شناسایی نشانه‌ها می‌توان استفاده می کرد که عبارتنداز:

الف) سابقه تاریخی بلند مدت بازیگران تروریستی

ب)دانش نظری و دکترین‌های مطرح در مورد بازیگران تروریستی

ج) رفتار و اقدامات فعلی بازیگران تروریستی

د) آینده‌پژوهی عملیاتی اقدامات تروریستی

پردازش و طبقه‌بندی نشانه‌ها

داده‌های بدست آمده از چهار منابع ذکر شده لازم است در گام بعدی پردازش شده و طبقه‌بندی شوند. طبقه‌بندی نشانه‌ها با مؤلفه‌های مختلف در واقع دقت در نوع ارتباطاتی است که نشانه‌ها ممکن است با همدیگر برقرار نمایند که این مؤلفه‌ها عبارتنداز:

الف) ترتیب اقدام: نشانه‌ها به لحاظ تقدم و تأخری که در اقدامات تروریستی ممکن است رخ دهند مرتب شده و نشانه‌های قبل و بعد از هر نشانه مشخص می گردد.

ب) میزان اشتراک نشانه در سایر اقدامات تروریستی.

ج) زمان رخداد نشانه تا اقدام: فاصله زمانی رخدادن نشانه تا بروز حادثه را نشان می‌دهد.

د) قابلیت دسترسی به نشانه: میزان توانایی سرویس‌های اطلاعاتی وامنیتی در دسترسی به نشانه‌ها.

ه) سرعت دسترسی به نشانه.

و) میزان اثرپذیری و اثرگذاری از سایر نشانه‌ها: تکنیک تحلیل ماتریس اثرات متقابل می‌تواند اثرات متقابل نشانه‌ها را بر هم بررسی کند.

ز) بسامد تکرار نشانه در هر اقدام: برخی از نشانه‌ها در طول یک اقدام تروریستی ممکن است تنها

یکبار رخ دهند اما برخی دیگر ممکن است به دفعات در یک اقدام تروریستی تکرار شوند.

ح) دامنه تغییرات نشانه: مشاهده تغییرات نشانه‌ها به لحاظ مقایری کمی و کیفی که به خود اختصاص می دهند.

ط) زمان رخداد نشانه.

ی) مکان رخداد نشانه.

ک) فاصله نشانه‌ها تا اهداف بالفعل.

ل) عامل بروز نشانه: نشانه‌ها در خلأ شکل نمی‌گیرند بلکه توسط افراد یا عواملی ایجاد می‌شوند.

م) طبقه‌بندی نشانه‌ها بر اساس نوع اقدام تروریستی: هر اقدام تروریستی ممکن است نشانه‌های متفاوتی از سایر اقدامات تروریستی داشته باشد.

س) طبقه‌بندی نشانه‌ها بر اساس بازیگران تروریستی.

ع) طبقه‌بندی نشانه‌ها بر اساس فعالیت‌های هم پوشان(تمایز سیگنال از نویز): میزان همپوشانی نشانه‌ها با سایر فعالیت‌های امنیتی و حتی غیر امنیتی را در بر می‌گیرد.

ف) طبقه‌بندی نشانه‌ها براساس ماهیت: نشانه‌ها ممکن است کمی یا کیفی، صوتی یا تصویری، عینی یا ذهنی و غیره باشند.

س) طبقه‌بندی نشانه‌ها بر اساس سطوح فعالیت: در این نوع تقسیم‌بندی نشانه‌ها بر اساس سطح راهبردی(سیاست‌گذاری)، عملیاتی(پشتیبانی) و تاکتیکی(اجرای عملیات) تقسیم‌بندی می‌شوند.

ایجاد پایگاه اطلاعات پایه‌ای

تمامی فرایندی که در این بخش انجام گرفت از جمله شناخت مفهومی نشانه‌ها، تعیین منابع برای شناسایی نشانه‌ها، شناسایی و کشف نشانه‌ها و تقسیم‌بندی آنها در سه سطح راهبردی، عملیاتی و تاکتیکی و در نهایت پالایش نشانه‌ها ، بستری را فراهم می‌سازد که گام نخست در فرایند هشداردهی تکمیل شده و به اتمام برسد. البته این اتمام و تکمیل شدن به فرایند تولید هشدار بر می‌گردد و به معنای بسته بودن فرایند شناسایی نشانه‌ها نیست، چرا که با توجه به منابع به روز شناسایی نشانه‌ها، این فرایند به سیستمی پویا مبدل می‌شود که همواره در جریان بود و دارای ورودی و خروجی‌های مداومی است. تجمیع نشانه‌های ارزشمندی که از منابع مختلف احصاء شده و مورد پالایش قرار گرفته می‌تواند به پایگاه داده‌ای ارزشمندی مبدل شود که دو گام مهم رصد و تحلیل نشانه‌ها بر روی آن سوار می شوند.

رصد نشانه‌ها

پیش رصد نشانه‌ها

در این مرحله لازم است قبل از رصد نشانه‌ها، مقدمات و زمینه‌های رصد فراهم شود. این مقدمات را می‌توان در گام بندی‌های زیر مورد توجه قرار داد. گام بندی‌های لازم قبل از ورود به رصد نشانه‌ها عبارتنداز:

الف) شناسایی منابع دریافت نشانه‌ها (سنجش وضعیت مطلوب): در نظر گرفتن منابع دریافت نشانه‌ها بدون توجه به محدودیت‌های موجود در هر محیط.

ب) تطبیق منابع دریافت نشانه‌ها با توان محیطی(سنجش وضعیت موجود): توجه به محدودیت‌های موجود در جمع‌آوری از جمله: محدودیت در تجهیزات جمع‌آروی در دسترس، محدودیت در بودجه، زمان و افراد ماهر، محدودیت‌های قانونی و غیره.

ج) ترمیم شکاف در مسیر منابع جمع‌آوری: تلاش در مسیر کاهش فاصله بین وضعیت مطلوب و موجود، از جمله این موارد شامل: تلاش در جهت تجمیع توانایی‌های منابع جمع‌آوری، ایجاد بسترهای مناسب (ایجاد پیوست‌های اطلاعاتی و امنیتی درخدمات ارائه شده) جمع‌آوری، تعریف قالب‌های قابل استفاده (فرمت‌های مناسب ذخیره اطلاعات)برای داده‌های جمع‌آوری، خلاقیت جهت کشف مسیرهای جایگزین و غیره.

رصد محیطی

با فعالیت‌های صورت گرفته بستر جمع‌آوری نشانه‌ها مهیا خواهد شد. حال زمان رصد محیطی است. برخی سیستم‌های رصد محیطی مثل رادارها مشخصاً برای رویت برخی موارد خاص تعبیه می‌شوند از این‌رو متناسب با مشخصاتی که به رادار داده شده به مشاهده محیط می‌پردازند در چنین سیستم‌هایی، از قبل کاملاً مشخص است که رادار باید به دنبال چه چیزهایی بگردد. این سیستم همان پایش محیطی است.

در مقابل، سیستمی مثل نور چراغ ماشین که برای مشاهده محیطی در شرایط تاریکی شب استفاده می‌شود هیچ مشخصه‌ای از قبل به مشاهده‌گر که در اینجا ممکن است راننده باشد داده نشده است. از این رو راننده با مشاهده هر مانعی پیش روی خود بلافاصله باید دست به کار شود. این سیستم همانند پویش محیطی است. از این رو در پویش محیطی نظام رصد به دنبال تغییرات جدید، غیر منتظره

و خاص می‌گردد که قبلاً در فرایند نشانه‌شناسی برای آن خصوصیاتی مشخص عنوان نشده است. منطق کشف در پویش محیطی مبتنی بر کشف علائم ضعیف عمل می‌کند. منطق کشف علائم ضعیف نیز مبتنی بر ناهنجاری‌ها است. لازمه شناخت ناهنجاری(امر غیرعادی) این است که بدانیم چه زمانی مسائل هنجاری(امر عادی) است (مک کیو،۳۲۰:۱۳۹۶). لذا فقط وقتی رفتار به صورت کلی و در زمینه رفتار معمولی در نظر گرفته می‌شود می‌توان به الگوی ناهنجاری پی برد(مک کیو،۴۲۸:۱۳۹۶). بنابراین ناهنجاری را می‌توان در سه قسم تقسیم بندی نمود.

الف) افزایش و کاهش نسبت به روند قبلی

ب) بود و نبود مبتنی بر روند قبلی

ج) نادر بودن علائم

پردازش داده‌ها

پردازش داده‌ها در دو زیر مرحله صورت می‌گیرد. در مرحله اول داده‌های جمع‌آوری شده از گام قبلی مورد ارزیابی قرار می‌گیرند و بعد از ارزیابی بر اساس مؤلفه‌های مختلف پالایش و طبقه‌بندی می‌شوند.

ارزیابی داده‌ها

ارزیابی داده‌ها در واقع تفکیک داده‌ها بر اساس باورپذیری است. در بررسی باورپذیری داده‌ها لازم است دو موضوع را مورد توجه قرار داد. یکی باورپذیری منابع است و دیگری باورپذیری داده‌ها. از این رو برای رسیدن به هشدار لازم است بعد از جمع‌آوری داده‌های حاصل از مراحل پایش و پویش به باورپذیری این دو بخش توجه شود.

الف)باورپذیری منابع

هر داده‌ای که جمع‌آوری می‌شود دارای منابعی است. این منابع می‌توانند تمامی اینت‌ها [1] را در بر گیرند. داده‌های بدست آمده از منابع یاد شده می‌توانند شواهدی ملموس و یا غیر ملموس باشند.

ب)باورپذیری داده‌ها

علاوه بر باورپذیری منابع لازم است نسبت به باورپذیری و اعتبارسنجی خود داده‌ها نیز بررسی اولیه‌ای صورت گیرد. در مورد باورپذیری محتوای داده‌ها می‌توان شش حالت را مشخص کرد که عبارتنداز: تایید شده، امکان صحت، احتمال صحت، شک بر درستی آن، نامحتمل و غیر قابل قضاوت. (ستاد فرماندهی نیروی زمینی ایالات متحده،۵۰۸:۱۳۹۵).

1. INT's

پالایش و طبقه‌بندی داده‌ها

لازم است بعد از ارزیابی، داده‌های بدست آمده مورد پالایش قرار گیرند. پالایش داده‌ها می‌تواند بر اساس مؤلفه‌های پالایش در گام اول صورت گیرد.

ثبت اطلاعات در پایگاه اطلاعات جاری

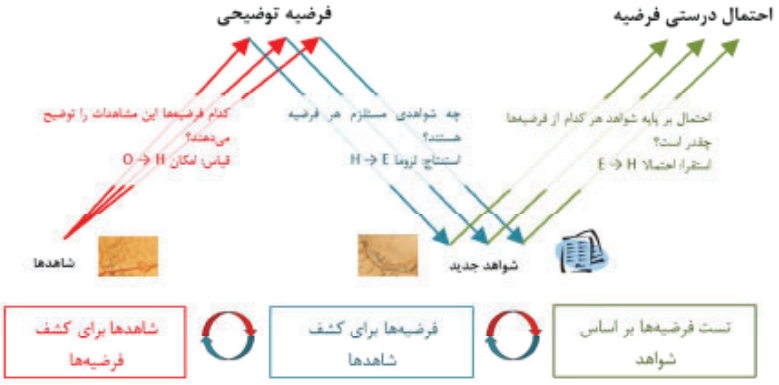
با پالایش صورت گرفته حال لازم است تمامی داده‌ها که اکنون می‌توان آنها را اطلاعات نامید در پایگاه اطلاعات ذخیره شوند. این پایگاه اطلاعاتی به دلیل ذخیره اطلاعات محیطی که هر لحظه بر اساس پایش و پویش محیطی جمع‌آوری می‌شود به عنوان پایگاه اطلاعات جاری شناخته می‌شود. اطلاعات در اینجا بر اساس تمامی خصوصیاتی که در مرحله پالایش برای داده‌ها مشخص شد تفکیک و در نهایت ذخیره می‌گردند. این گام زمینه را برای تحلیل اطلاعات فراهم می‌سازد. از این رو در گام بعدی فاز تحلیل اطلاعات مورد بررسی قرار می‌گیرد.

تحلیل نشانه‌ها

هر نشانه‌ای که نظام رصد در پی آن است تا آن را وارد گام تحلیل اطلاعات نماید لازم است درست همان نشانه‌ای باشد که نظام رصد مدنظر دارد. به عبارت دیگر لازم است نظام رصد همان چیزی را که به دنبالش می‌گردد پیدا کند نه چیز دیگری را. به اصطلاح باید دال روی مدلول بنشیند. اما این اتفاق هیچ‌گاه عیناً رخ نمی‌دهد و همین امر باعث پیچیدگی نظام رصد و تحلیل نشانه‌ها می‌گردد. در نتیجه هر تطبیقی بین دال و مدلول با میزانی از عدم قطعیت همراه است.

نشانه‌شناسان این موضوع را اینگونه بیان می‌کنند که هیچ نشانه‌ای را نمی‌توان یافت مگر اینکه بتوان به آن معنایی را اطلاق کرد. این اطلاق با ماهیت خود همواره یک فاصله‌ای را ایجاد می‌کند و به بیان لاکان «اگر دال را بر روی خط نمایشی با حرف S بزرگ و مدلول را پایین خط به وسیله s کوچک نمایش دهیم. آنگاه مدلول به طرز اجتناب‌ناپذیری در زیر دال قرار دارد و از قلمرو تعریف شده مشخص سر باز می‌زند.» بارداک، ۲۰۱۵). این اتفاق باعث می‌گردد، نظام رصد سایر نشانه‌های نزدیک به نشانه‌های اقدامات تروریستی را نیز مهم دانسته و آنها را وارد پایگاه اطلاعات ذخیره‌ای نماید. حال چالشی که پیش روی تحلیلگر قرار دارد این است که با وجود غربالگری اما همچنان عمده شواهد اطلاعاتی ناتمام، معمولا غیرقطعی، مبهم، ناموزون و دارای درجات مختلفی از باورپذیری هستند. از این رو اطلاعاتی که جمع‌آوری شده‌اند در ذات خود احتمالاتی بوده و درنتیجه سبب افزایش عدم قطعیت می‌شوند.

با در نظرگرفتن عوامل مذکور می‌توان به این نتیجه رسید که به راحتی نمی‌توان از اطلاعات بدست آمده و ذخیره شده در پایگاه اطلاعاتی به هشدار دست یافت. فرایند تبدیل اطلاعات جمع‌آوری شده به هشدار بسیار پیچیده بوده و لازم است فرایند ترکیب اطلاعات را در مسیری هدایت و مدیریت کرد که بتوان تدریجاً به سطوح احتمالاتی بالاتری برای ارائه هشدار قدم برداشت. بر این اساس پرسش اساسی در بخش تحلیل اطلاعات این خواهد بود که چگونه می‌توان این اطلاعات جمع‌آوری شده را تحلیل کرده و از آن به هشدار دست یافت؟ در این مرحله باید بتوان تکه‌های پراکنده و مشابهی از پازلی هزار قطعه‌ای که نیمی از آنها هم آسیب دیده و مفقود شده هستند را به نوعی با هم ترکیب کرد که به هشدار رسید. رسیدن به هشدار در فاز تحلیل اطلاعات مسیری است بی‌وقفه و مداوم که در آن سه گام به صورت متناوب تکرار می شود. این سه گام در واقع چارچوب اصلی تحلیل را شکل می دهد. این سه گام عبارتند از ترکیب اطلاعات برای یافتن فرضیه‌ها، فرضیه‌ها برای یافتن شواهد و آزمایشِ فرضیه‌ها بر پایه شواهد. این سه گام در شکل زیر نمایش داده شده است.



چارچوب محاسباتی تحلیل نشانه ها

با در نظر گرفتن این چارچوب لازم است گام نخست به این سوال پاسخ داد که فرضیه‌ها چگونه ایجاد می‌شوند.

کشف فرضیه‌ها

احتمالاً فرقی نمی‌کند که ما چگونه لباس‌های درون کمد، مواد غذایی داخل آشپرخانه، یا کتاب‌های

درون قفسه را مرتب کنیم. اما در تحلیل اطلاعات و سایر امور استنباطی بسیار مهم است که چگونه افکار و شواهد خود را مرتب نماییم. در واقع در علم نشانه‌شناسی نوع ارتباط است که معنا را تولید می‌کند.

از نظر سوسور، مفاهیم فی‌نفسه هیچ معنایی ندارند و معنای خود را تنها بر اساس ارتباط با سایر مفاهیم، تفاوت و تمایز به دست می‌آورند. مفاهیم در عین ارتباط، مبتنی بر تفاوت نیز هستند و بر اساس ویژگی‌های مثبتشان تعریف نمی‌شوند بلکه به شکل منفی و بر مبنای روابطشان با سایر اصطلاحات در درون نظام تعریف می‌گردند. (عباس پور، ۱۳۹۰:۱۲۰).

با توجه به این موضوع، هر چیزی که مورد مشاهده قرار می‌گیرد زمانی دارای معنا خواهد شد که بتوان آن را وارد زنجیره ارتباط و تفاوت کرد. در واقع در اینجا فرضیه‌ها که همان نشانه‌های احتمالی هستند با توجه به ارتباط و تفاوت‌ها معنا پیدا می‌کنند. به عبارتی این ارتباط و تفاوت است که می‌تواند به تولید فرضیه منجر شود. لذا به هر میزان نشانه‌شناسی مبتنی بر ارتباط و تفاوت با دقت و ظرافت بیشتری صورت گیرد به همان میزان قادر است فاصله بین دال و مدلول را کاهش داده و در رسیدن به فرضیه مورد بررسی راهگشا باشد.

در واقع فرضیه‌سازی به عنوان گام اول در تحلیل داده‌ها بر این اساس استوار است که به دلیل وجود عدم قطعیت حاکم بین دال و مدلول، لازم است دو اصل ایجاد ارتباط و داشتن تفاوت همزمان مورد توجه قرار گیرد.

الف) ایجاد ارتباط

ایجاد ارتباط بیان می‌کند که وقتی شواهدی به طور مستقل یا جداگانه در نظر گرفته شوند مشکل است که بتوانند مورد ارزشمندی را حکایت کنند اما وقتی این شواهد با هم ترکیب شوند نتایج جدید و متفاوتی را نشان می‌دهند. به عبارتی در هم‌افزایی شواهد[1]، دو یا چند مورد از شواهد در کنار هم، معنای کاملاً متفاوتی دارند، نسبت به زمانی که جداگانه یا به طور مستقل بررسی شده‌اند. آن‌چه در انتخاب ترکیبات نقاط برای بررسی کاملاً حیاتی است، تجربه و توانایی استدلال ابتکاری تحلیلگر است. چیزی که باید وجود داشته باشد،« یک "ارتباط دهنده[2]" مفهومی است که لازم است آن را به میان نقاطِ بر پایه شواهد هدایت کرد تا ترکیبات جالب و مهم از نقاط را با هم ارتباط دهد»(جورج و همکاران،۲۰۱۶:۷). وظیفه ارتباط دهنده ها "اتصال نقاط" است که به مرتب کردن افکار[3] و شواهد[4] در ایجاد و کشف فرضیه‌ها [5] و شواهد جدید اشاره دارند(جورج و همکاران،۲۰۱۶:۱).

1. evidential synergism
2. magnet
3. thoughts
4. evidences
5. hypotheses

برای رسیدن به فرضیه‌ها ارتباط دهنده‌های متعددی نقش دارند. این ارتباط دهنده‌ها، نقاط بر پایه شواهد را بر اساس نوع مفهوم ارتباطی کنار هم قرار داده و می‌توانند معناهای جدیدی برای تولید و کشف فرضیه خلق نمایند. به عنوان مثال: ارتباط دهنده زمان- بازیگر، بین زمان رخداد نشانه‌ها با بازیگران آن ارتباط برقرار می‌سازد. سایر ارتباط دهنده‌ها را می‌توان با مراجعه به مؤلفه‌های طبقه‌بندی نشانه‌ها و تقاطع‌گیری از متغیرهای موجود بدست آورد.

ب) تمایزگذاری (تفکیک علائم فریب از علائم نشانه)

مبحث ارتباطات مفهومی و ایجاد ارتباط اگرچه بسیار مهم است اما به دلیل اطلاعات همپوشان احتمال خطا و اشتباه در تحلیل اطلاعات بالا است، چرا که نسبت سیگنال به نویز بالا می‌رود. سیگنال در اینجا به معنای سرنخ یا نشانه یا تکه‌ای مدرک است که درباره خطر خاص یا حرکت یا نیت خاص دشمن سخن می‌گویند. سر و صدا نیز به معنای زمینه سیگنال‌های نامربوط یا ناهماهنگ است که به جهت‌های اشتباه اشاره دارد و همواره تمایل به تیره و تار کردن نشانه‌هایی دارد که به راه درست اشاره می کند»(موشراش،۱۳۹۷:۱۶).

روبرتا ولستیتر در کتاب خود درباره پرل هاربر استدلال می‌کند که هشداردهی‌های متعددی مبنی بر خطر از سوی ژاپن وجود داشت اما بالا بودن نسبت پارازیت‌های نامربوط به سیگنال‌های معنادار تحلیل داده‌ها را مشکل کرده بود،(ولستیتر،۱۹۶۲:۳۸۷). پس از یازده سپتامبر نیز بسیاری از پژوهشگران چنین مشکلی را بیان کرده‌اند(بایمن،۲۰۰۴:۱۴۵). امروزه به جای نسبت سیگنال‌ها در برابر پارازیت‌ها مناسب‌ترین و مختصرترین توضیح برای شکست اطلاعاتی آن است که جامعه اطلاعاتی قادر به اتصال نقاط نبوده است(جی وریتز،۱۳۹۹:۴۵). به عبارت دیگر بهتر است اینگونه بیان شود که به دلیل وجود حجم بالایی از نشانه‌های نشانه‌نما اتصال داده عملاً نمی‌توانست پاسخ تحلیلگران را بدهد از این رو اتصال داده‌ها با مشکل مواجه می‌شود. در واقع اتصال نقاط تا سطح ارتباط دهندگان پیش رفته است در حالی که روی دیگر سکه گمشده اتصال نقاط تمایزگذاری‌ها بودند که کمتر بدان توجه شده است. هر اندازه که به مبحث ارتباطات در اتصال نقاط توجه می‌شود، لازم است به تمایزگذاری نیز به مراتب توجه بیشتری شود، چون این تمایزگذاری است که باعث می‌گردد گام به گام نویزها و پارازیت‌ها از نشانه‌های اصلی جدا شده و فرضیه‌های با احتمالا بالاتری شکل گیرد. از این رو آنچه که می‌تواند از حجم این نویزها کاسته و تاثیر آنها را کمرنگ کند توجه به تمایزها است. تمایزگذاری

به این معنی است که اگر نشانه‌ای همچون نشانه مشاهده نحوه تهیه بمب از یک سروری دریافت شد، این نشانه درست است که همانند نشانه‌ای است که قبلاً در نشانه‌شناسی اقدامات تروریستی کشف شده و حتی امتیاز بسیار بالایی نیز کسب کرده است اما وقتی مکان رصد چنین نشانه‌ای به یک دانشگاه نظامی بر می‌گردد که تحقیقاتی را در این حوزه انجام می‌دهند آنگاه تمایزگذاری این نشانه را اگر چه با نشانه اقدامات تروریستی ارتباط داشته اما با تمایز ایجاد شده، آن را از لیست نشانه‌های دریافتی جدا می‌کند. اینگونه باعث می‌گردد حجم بالایی از نشانه‌های مشابه با نشانه‌های اقدامات تروریستی از پایگاه اطلاعات کنار گذاشته شده و اثرات مخرب آنها در ارتباطات ایجاد شده کمتر شود. این یک مثال بسیار ساده از تمایزگذاری بود؛ لذا هر چه سامانه‌های تمایزگذاری قوی‌تری وجود داشته باشد به طبع می‌توانند نشانه‌های پیچیده‌تری را نیز از فهرست پایگاه اطلاعاتی حذف یا کمرنگ نمایند.

ارزیابی فرضیه‌ها(یافتن شواهد برای فرضیه‌ها)

در این گام با توجه به فرضیه‌های تولید شده، طرح پیشرفته جمع‌آوری داده‌ها به گام رصد ارجاع داده می‌شود. در رسیدن به طرح پیشرفته جمع‌آوری از رویکردهای مختلفی می‌توان بهره گرفت. در زیر به برخی از این رویکردها پرداخته می‌شود.

الف)ارائه فرضیه به پایگاه اطلاعات

در این نوع ارتباط، داده‌های موجود را با پایگاه اطلاعات حاصل از پایش نشانه‌های اقدامات تروریستی که در مرحله نشانه‌شناسی بدست آمده‌اند تطبیق می‌دهند. این کار باعث می‌گردد ارتباطات احتمالی که از دید تحلیلگران دور مانده مورد توجه قرار گیرد. ارتباط مبتنی بر تطبیق اطلاعات پایه با اطلاعات جاری می‌تواند به عنوان راهنمای مؤثری در یافتن شواهد برای فرضیه‌ها نقش مهمی ایفا نماید(معاونت پژوهش و تولید علم،۲۶:۱۳۹۴). این اقدام در کشف فریب‌های احتمالی و جداسازی سیگنال‌ها از نویزها نیز بسیار کمک کننده خواهد بود.

ب)ارائه فرضیه به خبرگان

فرضیات مطرح شده به خبرگان ارائه می‌شود تا خبرگان با توجه به تجربیات و توان استدلالی و میزان اشراف به موضوع مورد بررسی، پیشنهادهای خود را برای جمع‌آوری پیشرفته داده‌ها به نظام رصد ارائه نمایند.

ج)ارائه فرضیه به آسیب پذیری دارایی‌ها

یکی از حوزه‌هایی که می‌تواند در ارائه طرح جمع‌آوری جدید داده‌ها برای تقویت یا تضعیف فرضیه‌ها کمک کند تکیه بر آسیب‌پذیری دارایی‌ها است. طبیعتاً هر تهدیدی اگر قرار باشد عملیاتی شود لازم است بر نقاط آسیب‌پذیری دارایی‌ها تمرکز نموده و آنها را شناسایی کند. این مجاری در واقع به شناسایی تهدید از منظر دارایی و نه عامل تهدید توجه دارد. به عبارت دیگر در این بخش تمرکز جمع‌آوری بر روی محیط زیست دارایی است، تا نشانه‌های احتمالی تقویت یا تضعیف فرضیه‌ها را بر اساس دارایی‌ها بدست آورد.

د)ارائه فرضیه به هزینه فایده حریف

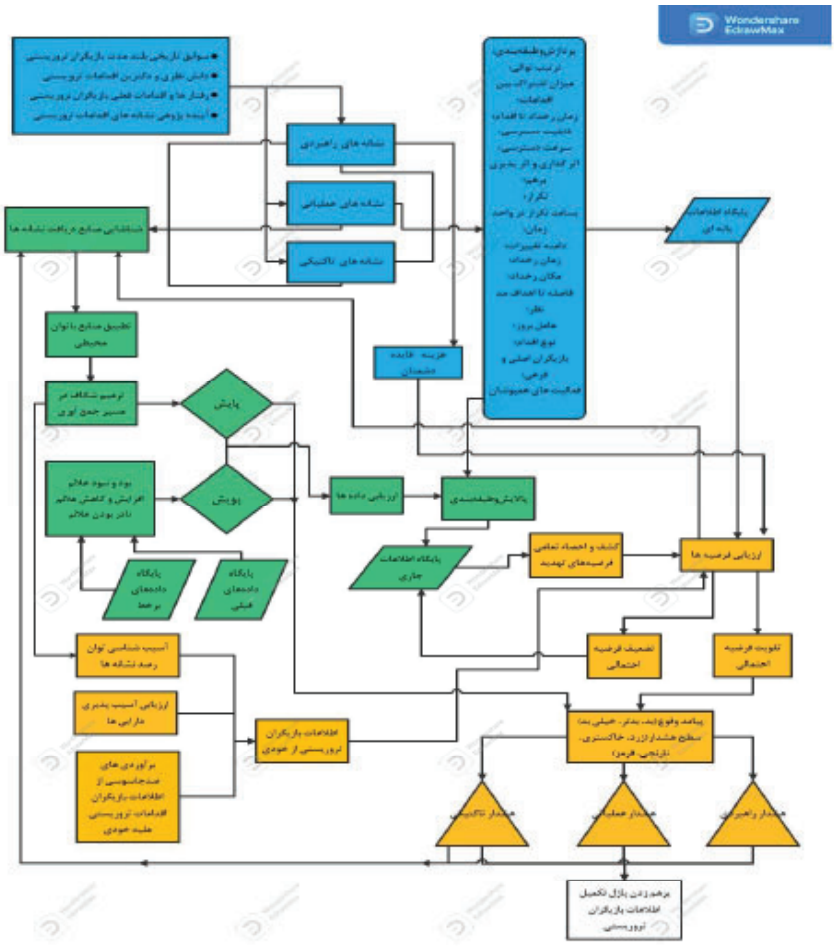
در هر اقدام تروریستی عامل تهدیدکننده در عین توجه به آسیب‌پذیری‌های اهداف انتخابی مدنظر خود و با وجود آمادگی و توانایی در انجام عملیات به هزینه فایده اقدام تروریستی در تمامی مراحل توجه ویژه‌ای دارد. اینکه چگونه می‌شود با کمترین هزینه بیشترین فایده را از اقدام تروریستی دریافت کرد نکته‌ای است که ازنظر تروریست‌ها هیچ‌گاه مغفول نمی‌ماند.

آزمون فرضیه‌ها(تقویت یا تضعیف فرضیه‌ها)

در این گام مهمترین سوالی که مطرح می‌شود این است که به چه میزان اگر فرضیه‌ای تضعیف یا تقویت شود می‌تواند آن را به سطح اعلام یا عدم اعلام هشدار برساند؟ پاسخ به این سوال در دو بخش داده می شود: بخش نخست به خود هشدار بر می‌گردد و آن اینکه هشداری که تولید می‌شود در یک سیستم صفر و یکی پدید نمی‌آید بلکه هشدار تولید شده حاصل یک سیستم فازی است که هشدار را به بود و نبود خلاصه نمی‌کند بلکه برای هشدار سطوحی قائل است که می‌تواند بسته به دقت صورت گرفته، درجات و سطوح مختلفی را شامل شود. هر سطح هشداری اقدامات خاصی را برای دریافت کننده هشدار تداعی می‌کند. از این رو لازم است متناسب با هر سطحی پاسخ مقتضی داده شود. بخش دوم پاسخ به سوال را می‌توان در اجماع نخبگان بر روی شاخص‌های سطح حساسیت بیان کرد. به این صورت که لازم است برای تمامی داده‌ها و شواهد به دست آمده نسبت به تعیین توان یا وزن شواهد اقدام نمود. در واقع در این گام بر حسب ارزش عددی که تک تک داده‌ها و ماتریس متقابل آنها پیدا می‌کنند داده‌ها ارزش‌گذاری شده و در نهایت با رسیدن ارزش جمعی داده‌ها به یک وضعیت از قبل مشخص شده هشدار لازم داده می‌شود.

الگوی تولید هشدار در اقدامات تروریستی

بعد از اتمام طراحی الگو لازم است نسبت به اعتبار سنجی آن از سوی خبرگان اقدام گردد. در این گام الگوی طراحی شده به شش نفر ازخبرگان ارائه گردید و نظرات آنها با توجه به دغدغه های بیان شده در الگوی اولیه اعمال گردید. در ادامه الگوی نهایی با در نظرگرفتن نظرات خبرگان ارائه شده است.



نتیجه‌گیری

همان‌گونه که مشاهده می‌گردد، الگوی تولید هشدار بدست آمده، یک الگوی فرایندی است که گام‌ها در امتداد هم در جریان هستند. این الگوی فرایندی در عین حال ایستا نبوده و با ورودی‌هایی که دارد یک فرایند پویایی را به نمایش می‌گذارد که دائماً در حال به روز شدن است. مفاهیم مورد بحث در این الگو کیفی بوده و می‌تواند با بسترسازی الگوی مفهومی زمینه ورود از الگوی مفهومی

به الگوی ریاضی را فراهم می‌آورد. از طرف دیگر این الگو با درک سه وجهی از تهدید که شامل شناخت دشمن(نشانه شناسی)، شناخت خود و شناخت دشمن از خود(اطلاعات بازیگران تروریستی از خودی)است، عملاً از حالت انفعالی خارج شده و رویکردی تهاجمی به مقوله ضدتروریسم داشته و در چارچوب ضداطلاعات تهاجمی ایفای نقش می‌کند. فرایند تولید هشدار در این الگو گام‌های: شناسایی نشانه‌های ظهور اقدامات تروریستی، رصد نشانه‌ها، پردازش داده‌ها و تحلیل نشانه‌ها در رسیدن به خلق معنا را شامل می‌شود.

گام نخست ابتدا به شناسایی منابع نشانه‌ها اختصاص داده شد. در این موضوع چهار منبع برای شناسایی نشانه‌ها مشخص گردید. این چهار منبع عبارتنداز: سوابق تاریخی بلندمدت بازیگران تروریستی، دانش نظری و دکترین اقدامات تروریستی، رفتارها و اقدامات فعلی بازیگران تروریستی و آینده‌پژوهی نشانه‌های اقدامات تروریستی. با بررسی این منابع، نشانه‌ها به‌مرور شناسایی‌شده و در ادامه نشانه‌ها بر اساس سطح اثرگذاری در فرایند یک اقدام تروریستی به سه سطح نشانه‌های راهبردی، نشانه‌های عملیاتی و نشانه‌های تاکتیکی تقسیم می‌شود. نشانه‌ها در ادامه در فرایند پردازش و طبقه‌بندی قرار می‌گیرند. در این بخش نشانه‌ها بر اساس ترتیب توالی، میزان اشتراک بین اقدامات تروریستی، زمان رخداد تا اقدام، قابلیت دسترسی، سرعت دسترسی، اثرگذاری و اثرپذیری نشانه‌ها بر روی یکدیگر، تکرار نشانه‌ها، بسامد تکرار در واحد زمان، دامنه تغییرات، زمان رخداد، مکان رخداد، فاصله تا اهداف مدنظر، عامل بروز، نوع اقدام، بازیگران اصلی و فرعی و فعالیت‌های همپوشان پردازش و طبقه‌بندی می‌شوند. با انجام این فرایند هستان‌شناسی اولیه‌ای از روابط بین نشانه‌ها شکل گرفته و در انتها در پایگاه داده‌ها با عنوان پایگاه اطلاعات پایه‌ای ذخیره می‌شود. در شکل زیر این فرایند ترسیم‌شده است.

در گام دوم برای تک‌تک نشانه‌هایی که در گام اول شناسایی‌شده‌اند منابع و ابزارهای رصد نشانه‌ها مورد شناسایی قرار می‌گیرد. در ابتدا شناسایی منابع بدون توجه به توانایی‌های محیطی و تکنولوژیکی صورت می‌گیرد تا وضعیت مطلوب منابع رصد مشخص گردد. در گام بعدی منابع مشخص‌شده با توان محیطی و تکنولوژیکی سرویس اطلاعاتی و امنیتی مقایسه می‌شود. با مقایسه وضعیت مطلوب و موجود در منابع و ابزارهای رصد، ترمیم شکاف مسیر جمع‌آوری صورت می‌گیرد. درنهایت با توجه به نشانه‌های مشخص‌شده و منابع دریافتی پایش محیطی صورت می‌گیرد. در پایش محیطی، هم نشانه مشخص است و هم منبع دریافت نشانه. در مقابل در پویش محیطی نشانه با توجه به ماهیت ناهنجار خود مشخص می‌گردد. ازاین‌رو نظام رصد ناهنجاری‌ها بر اساس پویش محیطی مبتنی بر تطبیق داده‌های گذشته با داده‌های بر خط صورت می‌گیرد.

در گام سوم به پالایش و طبقه‌بندی داده‌ها پرداخته می‌شود. اطلاعات به‌دست‌آمده درگام قبلی مورد ارزیابی و طبقه بندی قرار گرفته و در نهایت در پایگاه اطلاعات جاری ذخیره می گردد.

در گام چهارم، احصاء و کشف تمامی فرضیه‌ها، ارزیابی فرضیه ها و آزمون فرضیه ها صورت می گیرد. برای احصاء و کشف تمامی فرضیه‌ها از ارتباط دهی و تمایز گذاری بهره گرفته می‌شود. برای ارزیابی فرضیه ها همزمان از داده های پایگاه اطلاعات پایه ای، داده های هزینه فایده دشمن برای اقدام تروریستی، برآوردهای حاصل ازآسیب پذیری دارایی ها و نظرات خبرگان بهره گرفته می شود. در زیر مرحله آزمون فرضیه نیز به تقویت و تضعیف فرضیه ها پرداخته می شود. در این زیرمرحله به دلیل اهمیت جلوگیری از سوگیری‌های احتمالی به همان میزان که در تقویت فرضیه احتمالی تلاش می‌شود لازم است در تضعیف فرضیه احتمالی نیز تلاش صورت گیرد. در نهایت با تقویت فرضیه احتمالی، پیامد تهدید وقوع آن سنجیده شده و سطح هشدار متناسب با آن تهدید مشخص شده و درعین‌حال بر اساس نوع نشانه تهدید که راهبردی، عملیاتی یا تاکتیکی است هشدار متناسب با تهدید صادر می‌شود. با توجه به نوع هشدار صادر شده طرح جمع‌آوری جدیدی بر پایه تقویت و تضعیف فرضیه مطرح‌شده نیز به‌نظام جمع‌آوری داده می‌شود تا بر مبنای فرضیه مطرح‌شده به جمع‌آوری داده‌ها بپردازد.

منابع

۱. پور سعید، فرزاد. ۱۳۹۷. مجموعه مقالات دومین کنفرانس امنیتی، تهران: پژوهشکده مطالعات راهبردی.

۲. جی وریتز، جیمز. ۱۳۹۹. شناخت شکست اطلاعاتی، ترجمه: سید سعادت حسینی، تهران:مرکز مطالعات و پژوهش های امنیتی ساحفاسا،موسسه چاپ و انتشارات.

۳. چندلر، دانیل. ۱۳۸۷. مبانی نشانه شناسی، ترجمه: مهدی پارسا، چ۳، تهران:سوره مهر.

حاجیانی، ابراهیم. ۱۳۹۰. «هشداردهی: کارکرد تحلیل اطلاعاتی در پیش گیری از غافلگیری.» فصلنامه مطالعات راهبردی،سال چهارم، شماره سوم، ۱۲۷-۱۵۲.

۴. ستاد فرماندهی نیروی زمینی ایالات متحده. ۱۳۹۵. دستور العمل جمع آوری اطلاعات انسانی، مترجم: معاونت پژوهش و تولید علم، تهران: دانشگاه اطلاعات و امنیت ملی.

۵. شورت، ادموند سی. ۱۳۹۶. روش شناسی مطالعات برنامه درسی، ترجمه: محمود مهر محمدی. تهران:سمت

۶. صالحی، محمود، ومحمد مدبری. ۱۳۹۷. «چرخه بهینه هشدار در سازمانهای اطلاعاتی- امنیتی (مؤلفه‌ها و شاخص‌ها).» فصلنامه پژوهش‌های حفاظتی- امنیتی دانشگاه جامع امام حسین (علیه السلام)، سال هفتم، شماره ۲۶، ۱-۲۶.

۷. صالحی، محمود، و مهدی یعقوبی. ۱۳۹۷. «هشدار دهی در بحران های امنیتی.» کتاب مجموعه مقالات هشدار دهی اطلاعاتی امنیتی، جایگاه و فرایند هشداردهی. تهران: مرکز مطالعات و پژوهش‌های امنیتی.

۸. صالحی، محمود، و محمود کوشا. ۱۳۹۸. جایگاه شاخص ها در هشداردهی بحران های امنیتی، مجموعه مقالات جایگاه و فرایندهای هشداردهی همایش هشداردهی اطلاعاتی- امنیتی، تهران: مرکز مطالعات و پژوهش های امنیتی.۱-۴۲

۹. صحرایی، مهدی، عبدالرضا ترقی، علی نیک نفس، حامد دهقانی، علی دلگیر، و حمیدرضا حسنی اصل. ۱۳۹۸. نظام رصد، پایش و هشداردهی سایبری با رویکرد امنیت ملی،تهران: مطالعات گروهی دانشگاه عالی دفاع ملی.

۱۰. عباس پور، ابراهیم. ۱۳۹۰. در آمدی بر نشانه شناسی، دو فصلنامه علمی تخصصی، اسلام و علوم اجتماعی، س۳، ش۵، پاییز و زمستان ۱۳۹۰. ص ۱۰۹ تا ۱۳۷

۱۱. علیخانی، علی. ۱۳۹۳. هشدارشناسی، تهران: دانشکده اطلاعات.

۱۲. گرابو، سینتیا ام.۱۳۹۸. پیش بینی غافلگیری:تحلیلی برای هشدار راهبردی، ترجمه:محمد یوسفی خرایم و احمد رضا میرزایی، تهران: انتشارات دانشگاه عالی دفاع ملی.

۱۳. لفری، گری، و جاشوا فری لیچ.۱۳۹۹. راهنمای جرم شناسی تروریسم، جلد اول: نظریه‌ها. ترجمه معاونت پژوهش و تولید علم. تهران: دانشگاه اطلاعات و امنیت ملی،موسسه چاپ و انتشارات.

۱۴. مزینانی، احمد. ۱۳۹۷. «معماری سازمانی و هشداردهی» کتاب مجموعه مقالات معماری و الزامات هشداردهی، تهران:مرکز مطالعات و پژوهش های امنیتی، موسسه چاپ و انتشارات.۷۹-۱۱۱

۱۵. مزینانی، احمد، و احمد ایمانی پور.۱۳۹۷. «فرایند هشداردهی اطلاعاتی-امنیتی.» کتاب مجموعه مقالات هشدار دهی اطلاعاتی امنیتی، جایگاه و فرایند هشداردهی. تهران: مرکز مطالعات و پژوهش‌های امنیتی.

۱۶. معاونت پژوهش و تولید علم. ۱۳۹۴. تحلیل هشدار، ترجمه: معاونت پژوهش و تولید علم، تهران: دانشکده

۱۷. مک کیو، کولین. ۱۳۹۶. پیش بینی در تحلیل اطلاعات جرم، ترجمه: معاونت پژوهش و تولید علم، تهران: دانشگاه اطلاعات و امنیت ملی.

۱۸. موشراش، برایون دی. ۲۰۱۷. «ارتقای هشدار اطلاعاتی در عصر پیچیدگی» ترجمه نصر اله رضایی. ۱۳۹۷. کتاب مجموعه مقالات هشدار دهی اطلاعاتی-امنیتی، تهران:مرکز مطالعات و پژوهش های امنیتی، موسسه چاپ و انتشارات.۱-۸۰

۱۹. میرشاه ولایتی، فرزانه، و فرهاد نظری زاده. ۱۳۹۶. مفاهیم و روش های دیده بانی فناوری، تهران: موسسه آموزش و تحقیقاتی صنایع دفاع.

20. Adema. Katiel and wesleys. Roehl. 2010. Enviromental Scanning the Future of event design, International Journal of Hospitality Management, Vol. 29,pp199-207

Bell, Laura N.(2021). Targets of Terror: Contemporary Assassination, Rowman & Littlefield Publisher.

21. Burdek, Burdek.2015. Design: The History, Theory and Practice of Product Design. Birkhäuser; 2nd ed. edition (August 28, 2015).

22. Byman, Daniel.2004. Strategic Surprise and the September 11 Attacks,

Annual Review of Political Science 8(1):145-170

23. Holt, Pat M. (1995), Secret Intelligence and Public Policy:A Dilemma of Democracy, Washington: CQ Press.

24. Gheorghe Tecucl, David A. Schum, Dorin Marcu and Mihai Bolcu. 2016. Intelligence analysis as discovery of evidence, hypotheses and arguments: Connecting the dots. NewYork NY. Cambridge university press.

25. Purpura, Philip.2006. Terrorism and Homeland Security:An Introduction with Applications, ISBN: 9780080475417.

26. Saini, M., & Shlonsky, A. (2012). Systematic synthesis of qualitative research. Oxford University Press

27. chmid, A.(2011). The Routlege Handbook of Terrorism Research, londan:Routledge.

Schmid, A .& Tongman, A .(2005). Political terrorism: A new guide to actors, authors, concepts, data bases, theories &literature. New Brunswick: Transaction Publishers.

The Mossad Website: www.mossad.gov.il/about/dictionary.aspx.

28.Wohlstetter, Roberta. 1962. Pearl Harbor: Warning and Decision, Stanford University Press; 1st edition (June 1, 1962)