فصلنامه پژوهش‌های حفاظتی ـ امنیتی
دانشگاه جامع امام حسین(علیه‌السلام)
سال سیزدهم، شمارهٔ ۱ (بهار ۱۴۰۳) صص۱۶۲—۱۹۵

ارائه الگوی مناسب هشداردهی اطلاعاتی بحران‌های امنیتی

● مجید شامانی[1] ●
دکتری امنیت ملی، گرایش تهدیدات، دا شگاه عالی دفاع ملی، تهران ایران (نویسنده مسئول)
● بهرام بیات ●
استاد گروه امنیت ملی، دا شگاه عالی دفاع ملی، تهران، ایران
●هادی جمشیدیان ●
استادیار گروه امنیت ملی، دا شگاه عالی دفاع ملی، تهران، ایران
● هادی تاجیک●
دانشیار دا شگاه جامع امام حسین علیه‌السلام، تهران ایران

تاریخ دریافت: ۱۴۰۳/۰۱/۱۸ تاریخ پذیرش: ۱۴۰۳/۰۳/۱۵

چکیده

سرعت تحولات، روندها و رویدادهای نوظهور امروزی پرشتاب، غافلگیری و شکست‌های اطلاعاتی زیادی را در جوامع مختلف به‌همراه داشته است. این مسئله لزوم توجه به سامانه‌های هشدار و الگوهای مناسب هشداردهی را دوچندان می‌نماید؛ بنابراین در پژوهش حاضر الگوهای مختلف هشداردهی بررسی و با مطالعه اسنادی در این حوزه تلاش می‌گردد ضمن شناسایی ابعاد، مؤلفه‌ها و شاخص‌های هشداردهی اطلاعاتی در بحران‌های امنیتی، الگو مطلوب هشداردهی اطلاعاتی حاصل گردد. این پژوهش ازنظر هدف، کاربردی و با رویکرد کیفی و بر مبنای روش تحلیل محتوا از نوع اکتشافی است که با مشارکت ۱۲ نفر از خبرگان، صاحب‌نظران، مدیران حوزه اطلاعاتی، امنیتی، سایبری، بحران و جنگال که دارای سوابق علمی مدیریتی و اجرایی بوده‌اند و با روش نمونه‌گیری هدفمند در جامعه آماری هدف و با ابزار مصاحبه، جمع‌آوری، پیاده‌سازی و تجزیه و تحلیل داده‌ها انجام شده است که پس از کدگذاری و تطبیق، انطباق و انسجام‌بخشی، نتایج زیر به‌دست آمده است: ۶۸ شاخص، ۱۳ مؤلفه و ۴ بُعد. مؤلفه‌های حاصل، عبارت است از: علائم (ادراک)، آگاهی (جمع‌آوری)، پردازش، تجزیه‌وتحلیل (بررسی)، پایگاه دانش، سطوح، ابزار، عناصر و عوامل مؤثر هشدار، موضوع، بازیگران، شبکه هوشمند، مراحل و زمان هشدار؛ که در ۴ بُعد مشاهده، تشخیص و جهت‌دهی، تصمیم‌سازی و اقدام به‌دست آمده است. درنهایت، الگوی هشداردهی اطلاعاتی بحران‌های امنیتی، طراحی و موضوع ارزیابی، بازخورد و یادگیری در هر مرحله به مرحله قبل نیز موردتوجه و تأکید قرار گرفته است.

کلید واژگان: بحران؛ بحران‌های امنیتی؛ هشداردهی؛ هشداردهی اطلاعاتی.

1.m.shamani99@sndu.ac.ir

مقدمه

بحران به اشکال مختلفی می‌تواند در یک جامعه بروز کند، این بحران‌ها می‌تواند ناشی از یک حمله ناگهانی، جنگ، کودتا، سقوط یک دولت، احتمال بروز روزافزون ناآرامی و شورش، تظاهرات خشونت‌آمیز خیابانی، خیزش‌های اجتماعی، ترور چهره‌های سرشناس سیاسی یا از بین رفتن آنها، شیوع یک بیماری همه‌گیر دریک زمان کوتاه برای طولانی مدت، مثل کرونا و بسیاری از اشکال و انواع گوناگون دیگر باشد.

در هر جامعه‌ای وجود تشکیلات اطلاعاتی به عنوان یک ضرورت برای رسیدن به امنیت و آرامش قابل درک و فهم است و هرگاه که آن جامعه دچار آشوب و ناآرامی گردد، ضرورت چنین مجموعه‌ای به مراتب بیش از گذشته احساس خواهد گردید. به همین جهت مدیران بحران و تصمیم گیرندگان، بدون دارا بودن یک تشکیلات اطلاعاتی قوی و کارآمد قادر به مدیریت بحران نخواهند بود. مهم‌ترین کارکرد این سازمان‌ها هشداردهی است؛ در واقع می‌توان این‌گونه تعبیر نمود که محصول نهایی کار اطلاعاتی، هشداردهی است که برای پیش‌گیری از وقوع حوادث امنیتی انجام می‌شود و در مقابل مفهوم غافل گیری قرار دارد و منظور از آن، طراحی الگویی منسجم از علائم وقوع شرایط جدید درآینده و ثبت منظم شواهد است، به‌گونه‌ای که سازمان‌های مسئول همواره قبل از وقوع بحران امنیتی از آن آگاه باشند و تدابیر لازم را اتخاذ نمایند. هشداردهی و آینده‌شناسی وقایع قبل از بروز و ظهور آن، مأموریت ذاتی و کارویژه اصلی دستگاه‌های اطلاعاتی و امنیتی است

هر پدیده اجتماعی برای هستی‌یافتن، محتاج یک سری پیش‌نیازها و علل است که بدون آن امکان شکل‌گیری و وقوع نخواهد داشت. ناآرامی‌های اجتماعی و بحران‌های امنیتی ناگهان ایجاد نمی‌شوند، بلکه این حوادث به‌تدریج در بستر و زمینه‌های دور و نزدیک شکل‌گرفته، در موقعیت مناسبی سربرآورده و ظاهر می‌شوند. هیچ حرکت اجتماعی و سیاسی و ناآرامی‌های اجتماعی بدون نشانه و به‌تعبیر آینده‌پژوهان، بدون علائم قوی و ضعیف اتفاق نمی‌افتد. زمینه‌ها و بسترهای شکل‌گیری بحران‌های امنیتی می‌تواند در قالب تحولات بلندمدت بین‌المللی، منطقه‌ای و داخلی ایجاد گردد. توجه به این نشانه‌های دور و نزدیک برای هشداردهی و مهار بحران بسیار حیاتی است

بنابراین مسایل امنیتی حادثه نیستند که به‌یک‌باره و بدون علائم و نشانه رخ دهند، بلکه عموماً دریک روند و فرایند رخ می‌نمایند. الگوی هشداردهی می‌تواند از بروز غافل‌گیری و خطرات جدی

و بحران‌ها کاسته یا از آن ممانعت به‌عمل آورد. تصمیم‌گیران و سیاست‌گذاران یا به عبارت دیگر، نظام تصمیم‌گیری به هشداردهی از طریق برآوردها نیاز دارد. ویژگی اصلی هشدار آن است که به‌طور مشخص، احتمال بروز تهدید، خطر و درنهایت بحران را روشن سازد با این امید که موجب تولید و تشدید حساسیت‌ها نزد تصمیم‌گیرندگان گردد تا از غافلگیری جلوگیری یا شدت آن را کاهش دهد.

ازجمله مسایل و مشکلات پیش روی نظام در مدیریت بحران‌ها، بروز مسئله غافلگیری و شکست اطلاعاتی در ناآرامی‌های اجتماعی است. یکی از دلایل اساسی و ساختاری آن، نبود یا ضعف الگوی هشداردهی و پیش‌بینی در این حوزه ا ت که نظام، فرصت مناسب برای پیشگیری از بروز یا تشدید و گسترش بحران را ازدست‌داده، با موضوع امنیتی روبرو می‌گردد.

این مسئله می‌تواند با بهره‌گیری از یک الگوی پایش و هشداردهی به‌موقع و سریع، مدیران، تصمیم‌سازان و تصمیم‌گیرندگان مدیریت بحران را یاری رسانده، در کاهش هزینه‌های مقابله با آن و نیز در حفظ و تقویت امنیت ملی کشور نقش اساسی ایفا نماید؛ بنابراین سؤال این است که الگوی هشداردهی اطلاعاتی بحران‌های امنیتی چگونه است؟ و از چه ابعاد، مؤلفه‌ها و شاخص‌هایی برخوردار می‌باشد؟

مبانی نظری و پیشینه پژوهش

در راستای پیشینه این پژوهش به لحاظ موضوعی، می‌توان به مقاله پژوهشی «سارا لوهمن» و «تیم تپل» به زبان لاتین (۲۰۱۴) اشاره داشت که الگوهای هشدار مبتنی بر شاخص و پیش‌بینی دقیق تهدیدات امنیتی به همراه ترکیب قضاوت انسانی را بهترین روش آینده‌شناسی مطرح نموده است. پژوهش لاتین «ابراهیم ال لوهیدان» و «الرازانی» (۲۰۱۸) نقش شاخص‌های کلیدی هشدار زودهنگام را در کمک به تصمیم‌گیری رهبران با انتخاب تیم برنامه‌ریزی شایسته، مؤثر ارزیابی می‌کند. مطلب «نقش اطلاعات در بحران سال ۷۸» با نگاهی گذشته‌نگر به این بحران پرداخته، عبداله‌زاده(۱۳۸۶) به عملکرد ناموفق و غافلگیری کامل سازمان‌های اطلاعاتی در مرحله قبل و حین بحران می‌پردازد که ضرورت نظام هشداردهی با نگاهی آینده‌پژوهانه به بحران‌های امنیتی را نشان می‌دهد. مقاله «ولوی، صحرایی» (۱۳۹۵)، الگوی رصد، پایش هشداردهی سایبری براساس چرخه اوودا را در بُعد امنیت سایبری دنبال نموده‌اند که می‌تواند راهنمایی برای این پژوهش باشد. «فخری» (۱۳۹۶) که در رساله خود الگوی راهبردی دیدبانی نیروهای مسلح را طراحی نموده، به‌درستی دیدبانی را

مقدم و پیش‌نیاز هشداردهی توصیف نموده است و از این نگاه با موضوع این پژوهش هم‌راستاست. «فیلیپ دیویس» و «دیل ربا کریم» (۲۰۲۱) در مقاله لاتین دیگری به موضوع پیش‌بینی و به‌کارگیری ابزارهای احتیاط در مورد بحران‌های بانکی با استفاده از سامانه‌های هشدار اولیه و افزایش رشد پژوهش‌های دانشگاهی در این حوزه تأکید نموده‌اند. همه پژوهشات فوق و نتایج حاصل از آنها به‌ضرورت موضوع آینده‌پژوهی و پیش‌بینی و هشداردهی به‌نوعی اتفاق‌نظر داشته، تأکید می‌نمایند که وجه اشتراک آنها با این پژوهش به لحاظ موضوع هشدار است؛ لیکن این پژوهش به دنبال الگوی هشدار اطلاعاتی بحران‌های امنیتی از جنس ناآرامی‌های اجتماعی است که ابعاد و مؤلفه‌ها و شاخص‌های آن با سایر تهدیدات متفاوت بوده و می‌تواند وجه افتراق آن با پژوهش‌های فوق را نشان دهد. یکی از پژوهشات فوق که با نگاه گذشته‌نگر به بحران پرداخته و پژوهش دیگری که با نگاه اقتصادی در حوزه بانک‌داری به هشدار توجه نموده است، نیز با این مقاله متفاوت می‌باشد.

مأموریت ذاتی دستگاه‌های امنیتی – اطلاعاتی، هشداردهی آینده‌نگرانه بحران‌ها قبل از ظهور است؛ چراکه درغیر این‌صورت، این دستگاه‌ها صرفاً در حد وقایع‌نگاری، متوقف و نسبت به بحران‌ها، فرصت‌ها و تهدیدها ناآگاه می‌شوند. بنابراین اگر رویکرد آینده‌پژوهانه بر این دستگاه‌ها حاکم نباشد، تشکیلات اطلاعاتی و به تبع آن، نظام سیاسی حاکم، مرتباً با ناآرامی‌های اجتماعی و حوادث پیش‌بینی‌نشده‌ای روبرو می‌شود و در بهترین شرایط، صرفاً به ارائه گزارش‌های پرحاشیه وقایع پیشین می‌پردازد. این درحالی است که مأموریت ذاتی اطلاعات، پیش‌بینی قبل از وقوع رخدادهاست؛ چرا که پدیده‌های ضدامنیتی درصورت بروز، معضلات جدی را برای کشور، جامعه و نظام حاکم به‌وجود می‌آورد. درواقع، اهمیت و ضرورت آینده‌نگری در همه حوزه‌ها و موضوعات در شرایط کنونی اثبات شده است؛ اما در حوزه مطالعات و بررسی‌های امنیتی، این امر به دلیل پیامدهای ناگوار و حیاتی مسایل و بحران‌های ضدامنیتی، ضرورت دوچندان پیدا کرده است و امروزه کارآمدی و کفایت نظام اطلاعاتی امنیتی به توانایی آن در پیش‌بینی درست و به‌موقع این پدیده‌ها بستگی دارد و این امر در تحلیل‌ها و گزارش‌های آن نظام، منعکس و قابل ردیابی و ارزیابی است.

سخن حق آن است که غافلگیری و آینده‌نگری، دو روی یک سکه است؛ به این معنی که با دقت در آینده‌شناسی پدیده‌ها و روندهای مورد مطالعه، از حجم غافلگیری و شکست‌های اطلاعاتی نیز کاسته می‌شود. نظام هشداردهی، سازمان‌ها و دستگاه‌های مرتبط با مسایل امنیتی را درمقابل چالش‌ها و خطرات محتمل آگاه نموده، تا با آمادگی بیشتر از حجم غافلگیری و درنهایت شکست اطلاعاتی

جلوگیری نماید و این مهم در گرو وجود سامانه هشداردهی آینده‌نگرانه است.

بهترین زمان مدیریت بحران‌های امنیتی که هزینه‌های کمتری را در اداره و فروکش کردن بحران دربردارد مرحله قبل از آن می‌باشد که با هشدار به‌موقع و دقیق می‌توان ازفرصت‌ها استفاده کرد و نقاط آسیب‌پذیر را کاهش داد و نقش موثری در پیش‌بینی و به تبع آن پیشگیری از غافلگیری عوامل مدیریت بحران‌های امنیتی ایفا نمود.

بنابراین طراحی الگوی هشداردهی می‌تواند به متولیان امنیت ملی و خط‌مشی‌گذاران و تصمیم‌گیران حکمرانی کشور کمک نماید و نمونه‌ای برای سایر دستگاه‌ها و نهادهای مسئول در کشور با سطوح متفاوت و شاخص‌های مربوط به آن نهاد و سازمان محسوب شده، طراحی، پیاده سازی، اجرا و مورد بهره‌برداری قرار گیرد. در این الگو برای جمع‌آوری داده‌ها سعی شده از تمامی منابع جمع‌آوری بهره‌برداری شود. الگوی هشدار بحران‌ها از جنس ناآرامی‌های اجتماعی که شاخص‌های هشداری آن با سایر الگوهای هشدار متفاوت است. در این پژوهش ابعاد و مؤلفه‌های این نوع الگو معرفی و بیان شده که تاکنون کمتر بدین‌صورت به موضوع توجه و تأکید شده است.

تعریف هشداردهی

هر موجود زنده‌ای دارای تنظیمات و ابزارهای تشخیص وقوع خطر و انجام عکس‌العمل مناسب در مقابل آن است. این واقعیت، حتی در موجودات میکروسکپی هم قابل‌مشاهده است. در دستگاه‌های غیرطبیعی و انسان‌ساخت[1] نیز ابزارهایی برای حفاظت تعبیه شده تا در صورت تغییر ناگهانی شرایط، مثل دما یا فشار، سامانه حفاظتی واکنش مناسب را نشان دهد.

سازمان‌های اطلاعاتی، یکی از مصادیق این ابزارهای هشداردهنده به شمار می‌آیند. در هشدارهای اطلاعاتی[2] با علائم و نشانه‌هایی روبرو هستیم که نشان‌دهنده به خطر افتادن منافع ملی و ارزش‌های اساسی است. درعین‌حال، هشدارها بایستی نشان‌دهنده تحقق این شرایط باشد نه شاخص‌های تهدید به عبارت دیگر، بین شاخص‌های تهدید (که ممکن است محقق شود یا محقق شده باشد) و هشدار، تفاوت وجود دارد. هشدار صرفاً نشانه و علامت است نه خود تهدید. درواقع، هر نظامی از هشدارها باید گویای شکل‌گیری تهدید خاص باشد نه اینکه هر هشدار، استعداد نمایش تهدیدات و

1. Man-made
2. Intelligence Warning

بحران‌های متفاوت را داشته باشد. البته، منظور مجموعه هشدارهای مربوط به یک تهدید است و نه صرف یک هشدار، چراکه در طراحی نظام هشداردهی در برابر بروز یک تهدید، بایستی مجموعه‌ای از شاخص‌ها و نشانه‌ها را به‌عنوان هشدارهای هر رخداد یا واقعه تهدیدآمیز در نظر گرفت.(سیسک[1]، ۱۲:۲۰۰۷)

ازاین‌رو، هرچند یک علامت می‌تواند در تشخیص چند هشدار به کار رود، اما مجموعِ علائم و نشانه‌های هر تهدید، به‌عنوان بسته منسجم[2]، باید متفاوت از مجموع علائم و نشانه‌های دیگر تهدیدات باشد. هشدار، محصول تلاش عمده پژوهشاتی و فرایند گسترده جمع‌آوری اطلاعات، نوعی برآورد احتمالی[3]، قضاوت و داوری برای تصمیم‌گیرندگان و سیاست‌گذاران[4] و کمک به آمادگی‌های مسئولین اجرائی است. به‌عبارت‌دیگر، هشدار باید در خدمت نظام تصمیم‌گیری و با توجه به مجموع سلایق و امکانات ارائه شود.(گرابو[5]، ۳۰:۲۰۱۰-۲۳)

در تعریف هشداردهی آمده است:«آگاه‌سازی نسبت به رخدادهایی که منافع فرد، سازمان یا نظام ملی و بین‌المللی را در سطوح مختلف به مخاطره اندازد.» (هشداردهی والاترین مأموریت اطلاعات،۱۳۹۳، ۱۵۹ -۱۵۷).

درمجموع، می‌توان گفت هشدار سه بُعد دارد و هر اشاره‌ای به خطرات و تهدیدات، متضمن تأکید بر این ابعاد است:

احتمالات

هشدارها بیان و تصریح احتمالی حادثه نامطلوب خاص در یک دوره زمانی معین است.

تأثیرات

بیان اینکه هرکدام از حالات (اتفاقات محتمل)، چه پیامدهایی به‌جا خواهد گذاشت و تأثیرات آن کدام است، این بُعد اهمیت فراوانی در هشداردهی دارد. درواقع آنچه هشدار را معنی می‌کند و تصورات تصمیم‌گیرندگان و دریافت‌کنندگان محصولات هشداردهی را تحریک می‌کند، درجه

1. cisc
2. Package
3. Assessment of Probabilities
4. Policy Makers
5. Graboo

بزرگی پیامدهای خاص اتفاق یا روند(اتفاق‌های) پیش روست. بیان دامنه تأثیر هشدارهاست که تصورات در مورد مخاطره را ایجاد می‌کند، در غیر این صورت هشداردهی بی‌تأثیر خواهد بود.

اولویت‌دهی

در نظام هشداردهی، بایستی اتفاق یا خطرات به‌طور منطقی رتبه‌بندی شود، یعنی مشخص شود احتمال وقوع کدام اتفاق یا حالت از هشدار بیشتر است. این امر از آن‌رو اهمیت دارد که هشدارهای مربوط به هر موضوع امنیت ملی (برای مثال، تدابیر عملیاتی گروه تروریستی در شرق کشور) تک‌حالتی نبوده، آن گروه، احتمالاً چند راهکار پیش روی خود دارد؛ آنچه در این میان مهم است و به‌طور ویژه برای مدیران تصمیم‌ساز کاربرد فراوان دارد، اولویت احتمالات است و این‌که احتمال وقوع کدام حالت بیشتر است و به چه میزان؟ تعیین این اولویت، موجب می‌شود تصورات مدیران در مورد مخاطره احتمالی دقیق‌تر و حرفه‌ای‌تر شکل گیرد، ضمن آن‌که پیش‌آگاهی نسبی آنها نسبت به سایر احتمالات نیز به وجود آمده است.

این پیش‌آگاهی نسبی - نسبت به سایر احتمالات و هشدار- موجب می‌شود درصورتی که اگر سایر حالت‌های کم‌اهمیت‌تر محقق شود، مدیریت اجرایی، کمتر دچار شرایط غافل‌گیری ذهنی شود و درعین‌حال، پیش‌بینی‌ها و تدابیر عملیاتی لازم را برای حالات کم‌اهمیت‌تر درنظر بگیرد؛ بنابراین، منظور از الویت‌بندی آن است که هشدارهای ارائه‌شده درباره هر خطر امنیتی مشخص، ازنظر احتمال وقوع و نیز دامنه تأثیرات، رتبه‌بندی شود. (حاجیانی،۱۳۹۰: ۱۳۹- ۱۳۵)

هشدارها شاخص‌هایی[1] است که از بروز بحران (و به‌طور مشخص‌تر، از شکل‌گیری غافل‌گیری) خبر می‌دهد. شاخص‌های اطلاعاتی، آن دسته از علائم[2] و نشانه‌هایی است که در صورت رصد و پایش مستمر آنها می‌توان از آینده حوادث و کم و کیف وقوع آنها مطلع شد.(گرابو،۲۰۱۰: ۱۲) کارکرد و وظیفه تحلیل اطلاعاتی و تحلیل‌گران آن است که با طراحی نظامی منسجم از شاخص‌ها که هر مجموعه‌ای از آنها حاکی از بروز یک پدیده بحرانی است، از شکل‌گیری غافل‌گیری‌ها ممانعت نمایند. بر این مبنا، می‌توان گفت هشداردهی فرایندی مهم پس از آینده‌نگری است و آینده‌نگری، فی‌نفسه ارزش و اعتبار ندارد، جز اینکه شرایط پیش‌رو را به تصویر می‌کشد، اما هشداردهی نحوه شکل‌گیری

1. Signals
2. Monitoring

و تکوین[1] شرایط را مشخص می‌سازد. هشداردهی ابزار و فن مهم برای پیش‌گیری است؛ ضمن آن‌که هشداردهی به‌واسطه رصد و پایش مستمر محیط یا موضوع، تحولات و تغییرات احتمالی پدیده تحت مطالعه را که قبلاً پیش‌بینی نشده بود نیز نشان می‌دهد. این جنبه از کار هشداردهی، ازآن‌رو اهمیت دارد که پدیده‌ها و روندهای امنیتی - بنا به ماهیت سیاسی، اجتماعی و فرهنگی آنها - از فرایند خطی پیروی نمی‌کنند و همواره احتمال و امکان تغییر در آنها وجود دارد. (حاجیانی،۱۳۹۰: ۱۴۲-۱۴۱)

هشداردهی اطلاعاتی

هشدارهای اطلاعاتی اصلی‌ترین فرآورده دستگاه‌های اطلاعاتی محسوب می‌شود.(علیخانی،۱۳۹۳، ۵) به‌عبارت‌دیگر، محصول نهایی در تجزیه و تحلیل اطلاعاتی، ارائه هشدار است. هشدارها آن دسته از علائم و نشانه‌ها هستند که بیانگر بروز رویداد یا پدیده ضدامنیتی یا حتی فرصت می‌باشد. در حقیقت اِعلام و ابراز نشانه‌های بروز یک واقعه از سوی دستگاه اطلاعاتی به مراجع ذی‌ربط را هشداردهی می‌گویند و این اطلاعات را اطلاعات هشدار نامند. به سخن دیگر، هشدارها مجموعه سازوکارهای انتقال علائم بُروز یک پدیده است که موجب شکل‌گیری یک نظام هشداردهی می‌شود.(زندی،۱۳۸۷، ۲۳)، (فکوری،۱۳۹۲، ۳۳۳)

بحران امنیتی

بحران امنیتی بحرانی است که روند کارکردی و جاری دستگاه‌ها و سازمان‌های مسئول امنیت کشور را مختل می‌کند. (مهری،۱۳۹۸:۲۳) به‌عبارت‌دیگر، بحران امنیتی مرحله‌ای از حاد شدن اوضاع را نشان می‌دهد که در آن، مداخله نهادها و سازمان‌های امنیتی به امری پذیرفته‌شده تبدیل می‌گردد. در این شرایط، بحران فرصت یافته است که سازوکارهای کنترل‌کننده اداری و سیاسی را کنار بزند و به‌صورت پدیده‌ای آشکار و در سطح نمایان گردد. برای ورود به چنین اوضاع و احوالی فعال شدن یک سری متغیرهای تأثیرگذار ضروری است. (امیری،۱۳۹۱: ۲۲۳)

1. Generation

الگوهای هشداردهی

الف- تشریح حلقه OODA

شکل زیر بیانگر حلقه بسته تصمیم‌گیری است که مجموعه فعالیت‌ها به نحوی به‌سمت یک حلقه بسته هدایت شده، همه به یک نقطه بازمی‌گردد و آن نقطه مرکز تصمیم‌گیرنده یا فرماندهی است. در حال حاضر حلقه OODA فراتر از یک حلقه موردتوجه فرماندهان قرارگرفته، مفهوم وسیع‌تری یافته است و به‌عنوان دایره تولید توان رزم از آن نام برده می‌شود. هر مرحله‌ای از حلقه، خود یک فرایندی است که به شرح فرایندهای زیر ساخته می‌شود:

شکل ۱: حلقه اوودا (مشاهده، تشخیص، تصمیم، اقدام)

فرایند مشاهده

فرایند مشاهده هم شامل تصمیم بر مشاهده فعالیت‌های خاص و اقدامات فیزیکی موردنیاز برای دریافت داده مربوط به اطلاعات مراقبت و هدف‌گیری بوده، هم شامل تصمیم برای ارسال آن به افراد موردنظر است. در فرایند مشاهده به‌منظور بهینه نمودن تأثیر دقت، به چیزی بیشتر از آگاهی مبتنی بر حسگر نیازمندیم و باید آسیب‌پذیری‌های خاص راشناسایی کنیم؛ بنابراین به شناخت بیشتر از دشمن نیاز خواهیم داشت. هرچند این شناخت نیازمند اطلاعات کامل و جامعی از سوی حسگر بوده، درنتیجه در معرض محدودیت زمانی است. دانش برتر از صحنه نیز به نظرات کارشناسی در

رابطه با منطقه موردنظر و به پایگاه‌های اطلاعاتی متکی است که بسیار قبل‌تر از آغاز توسعه‌یافته است؛ بنابراین، حسگرها و فناوری اطلاعاتی جدید تنها تا حدی می‌تواند دایره را کوتاه کند که اقدامات فیزیکی موردنیاز برای جمع‌آوری و تحلیل طولانی‌مدت، از قبل کامل شده، دانش لازم از پیش در شبکه موجود باشد.

فرایند تشخیص

شامل داده‌کاوی جهت کشف یا یادگیری مشخصات ناشناخته قبلی در داده است که می‌توان از آن به‌عنوان قالب‌هایی جهت آشکارسازی و پیش‌گویی بعدی در فرایندهای تجمیع داده‌ها استفاده کرد. فناوری اطلاعات جدید، زیرساخت‌های شبکه‌ای را ایجاد می‌کند، به انقلاب حسگرها اهمیت جدیدی می‌بخشد و دلیل این مطلب نیز به دو بخش کلیدی وابسته است: اول، آن‌که شبکه‌ای کردن، ما را توانمند می‌سازد که با یک‌پارچه‌سازی بهتر داده جمع‌آوری‌شده و نیز با توانمند ساختن حسگرها به این‌که از خروجی‌های یکدیگر استفاده کنند، ظرفیت آنها را افزایش دهیم. درنتیجه این شبکه‌سازی می‌تواند ساده‌سازی حسگرها را نتیجه دهد؛ به‌طوری‌که آنها را همچنان ارزان‌تر و متعددتر سازد. دوم، گستره و مقیاس داده تولیدشده توسط حسگر، به‌طورقطع باید از چنان کمیتی برخوردار باشد که فقط یک برداشت اطلاعاتی از آن برآید، برداشتی که درمجموع با اطلاعات دیگر حسگرها افزایش تصاعدی و هم‌افزایی داشته، برای پردازش، مرتب کردن و تحلیل کمیت حاصل از داده حسگر، موجب آگاهی و دانش بیشتر گردد.

فرایند تصمیم‌گیری

فرایند تصمیم‌گیری شامل فرایندهای خودکار و دستی(توسط انسان) است. پاسخ‌های ساده و سریع را می‌توان برمبنای آشکارسازی شرایط ازپیش‌تعیین‌شده به‌صورت خودکار تنظیم نمود؛ درصورتی‌که قضاوت فرماندهان برای تصمیم‌گیری‌های پیچیده‌تر و حیاتی نیاز بود، شرایط را جهت دخالت به وجود می‌آورد. با توجه به حجم بالای اطلاعات و پیش‌گیری از سردرگمی فرماندهان در تصمیم‌گیری لازم است تا سرعت پردازش اطلاعات در داده‌کاوی و تجمیع و تلفیق آن افزایش یابد. دیتا فیوژن یا تلفیق اطلاعات یک فرایند تطبیقی تولید دانش است که در آن عناصر گوناگون مشاهدات مشابه و غیرمشابه، داده‌ها را مرتب، هم‌بسته و ترکیب کرده، به‌صورت مجموعه سازمان‌یافته و دارای فهرست تبدیل می‌کند. با رشد سریع حساسه‌ها و پایگاه‌های داده برای پشتیبانی فرماندهان

در به‌کارگیری حجم رو به افزایش داده به‌منظور تصمیم‌گیری، فنآوری‌های خودکار ادغام اطلاعات اهمیت خاصی پیداکرده است.

فرآیند اقدام

به مجموعه مراحل طی شده از زمان ابلاغ تا اجرای آن، فرایند اقدام گویند.

به‌طورکلی مرکز رصد از چهار گام پیروی می‌کند

۱- مشاهده Observation

۲- تشخیص Orientation

۳- تصمیم‌گیری Desiion

۴- اقدام Action

در واحد مشاهده به‌صورت باز و بدون سوگیری بر اساس دریافت از عامل‌های موجود، به جمع‌آوری اطلاعات پرداخته می‌شود. طبیعتاً برای این کار باید از مولدهای رویداد بهره گرفت. این مولدها یا از پیش در مراکز گلوگاهی نصب و اقدام به تولید اطلاعات برای مرکز می‌نماید و درمواردی نیز بسته به اهمیت زمانی، مکانی، جغرافیایی، حدوثی اقدام به نصب پایش‌گرهای خاص خواهد شد که اطلاعات دقیق‌تر و کامل‌تری تولید و عرضه گردد.

در واحد تشخیص، جمع‌آوری رویدادهای تولیدی از پایش‌گرها و پویش‌گرها به روش ایمن و مطمئن صورت پذیرفته، پس از پالایش اولیه برای نگهداری در انباره رویدادها آماده‌سازی می‌شود دسته‌بندی، همبسته‌سازی رویدادها و طبیعتاً حذف برخی از آن، از اقدامات این مرحله خواهد بود.

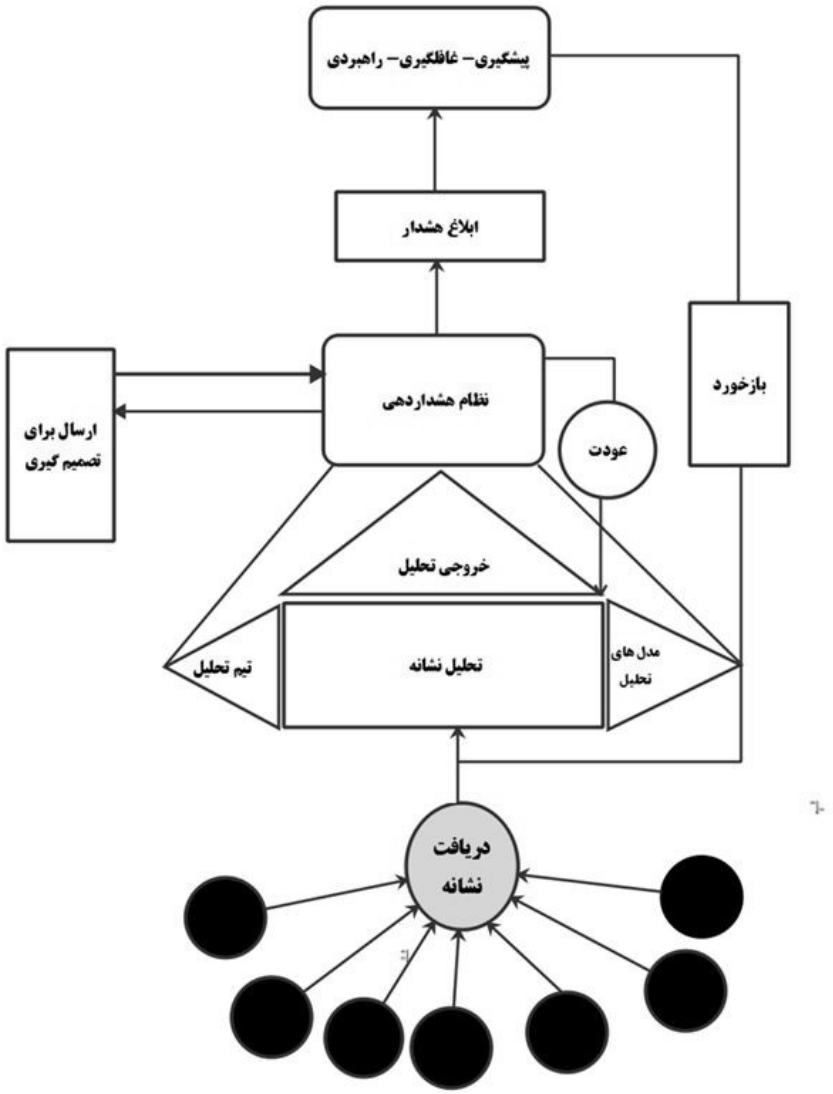
در واحد تصمیم‌گیری، رویدادها مورد پردازش موتور تحلیل قرار می‌گیرد. این موتور نابهنجاری‌ها را تشخیص می‌دهد و طبیعتاً باید توانایی تشخیص موارد مجاز از غیر مجاز را داشته باشد. این موتور با استفاده از داده‌های گذشته و با نگاه به الگوهای آینده‌نگر اقدام می‌کند و بیعتاً باید قلمرومحور و جامع‌نگر عمل کند و حداکثر اقدامات لازم را برای تصمیم سازی در لایه‌های مختلف تاکتیکی، عملیاتی و راهبردی انجام دهد. (صحرایی همکاران،۱۳۹۸: ۱۸۹-۱۸۱)

در واحد اقدام با توجه به قلمرو معرفی‌شده برای این مقاله، تنها هشداردهی مدنظر است.

ب- هشداردهی بر اساس نشانه‌شناسی

این شیوه هشداردهی نسبت به وضعیتی که در آینده رخ خواهد داد هشدار می‌دهد، اما زمان و مکان آن مشخص نیست. تشکیلات هشداردهی با توجه به تجربه (دانش سازمانی)، علم (روش‌های تحلیل)، محیط و فرهنگ، به‌صورت موضوع محور و محیط محور فعالیت می‌کند. در اعلام‌خطر برخلاف هشداردهی، زمان و مکان و بازیگران را مشخص می‌شوند. (صالحی،۱۳۹۵)

فرایند هشداردهی باید آن‌قدر سریع باشدکه بتواند تغییر یا تغییراتی را در طیف وسیعی از مؤلفه‌ها کشف و شناسایی نماید. «احمدی» فرایند هشداردهی مؤثر را مشتمل بر وجود نشانه، دریافت نشانه (صوتی، گفتاری، تصویری، نوشتاری)، تحلیل نشانه (توسط متخصصین حوزه‌های مختلف براساس الگوهای تحلیل و استخراج تحلیل)، نظام و نحوه هشداردهی (صوتی، گفتاری، تصویری، نوشتاری)، ارسال به فرماندهی (مدیریت) برای تصمیم‌گیری (تائید ارسال، اصلاح و ارسال، منع ارسال)، دریافت بازخورد (مثبت، منفی) و تحلیل مجدد و مستندسازی هشدار، به‌صورت نمودار ۱ طراحی نموده است:



نمودار ۱: هشداردهی بر اساس نشانه‌شناسی

محقق معتقد است در هریک از فرایندهای شناخت، دریافت، تحلیل نشانه، مرحله تصمیم‌گیری و نحوه هشداردهی ممکن است غافلگیری شکل بگیرد.

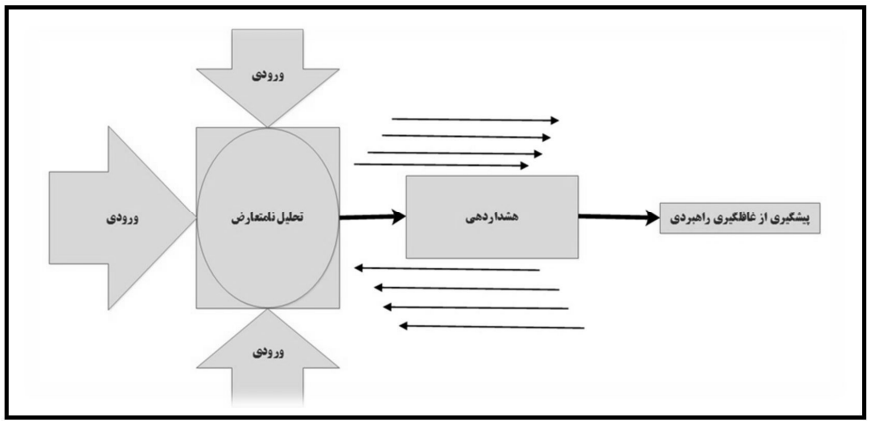
برای پیشگیری از غافلگیری در شناخت نشانه، سازمان اطلاعاتی یا ضداطلاعاتی باید بتواند خوب پیش‌بینی کند. در مرحله دریافت نشانه، بخش تجهیزات و قدرت تشخیص کاربرد اساسی دارد؛ نباید این بخش دچار عقب‌ماندگی ذهنی و فناوری باشد. زمان، یکی از مصادیق تأخیر هشداردهی به علت فقدان دریافت و تشخیص به‌موقع و صحیح است. در مرحله تحلیل که به‌وا طه بُروز ذهنیت‌های متفاوت تحلیل‌گران و

تعارض در برداشت‌های مختلف از نشانه‌های دریافتی یا کوچک شمردن و بی‌توجهی سیاست‌گذاران به خطرهای احتمالی اعلام‌شده از سوی تحلیل‌گران اطلاعاتی، سبب انحراف در اعلام هشدار و غافلگیری می‌شود، تسلط به راهنمای جمع‌آوری اطلاعات، تخصص چند رشته‌ای، کسب اطلاعات از همه منابع، فن‌ها و فرایندهای مناسب برای مواجهه با عدم قطعیت، به تقویت هشدارها کمک می‌کند.

ضعف توانایی ادراکی، شکاف تحلیل بین نظامیان و سیاسیون و تحلیل‌گران و تأخیر در تصمیم‌گیری قبل از وقوع در مرحله تصمیم‌گیری و عدم اثربخشی لازم و تأثیرگذاری عمیق، محملی برای شکل‌گیری شکاف و رخ‌نمایی غافل‌گیری در نحوه هشداردهی می‌گردد. مستندسازی، دستاوردهای قابل‌توجهی در رفع ایرادات و شناخت زوایای فرایند هشداردهی و نقاط ضعف و قوت دارد. درصورتی‌که غافل‌گیری متأثر از شکاف‌های سایر مراحل و فرایند هشداردهی شکل گرفته باشد، مستندسازی می‌تواند به‌عنوان یکی از فرصت‌های حیاتی، اثربخشی و کارآیی هشداردهی را در آینده ارتقا داده، از غافلگیری مجدد پیشگیری کند. (احمدی، ۱۳۹۸)

پ- چارچوب تعاملاتی هشداردهی با تحلیل نامتعارض

نقش تحلیل نامتعارض در هشداردهیِ صحیح و به‌موقع بی‌بدیل است. بین نظام هشداردهی (در نحوه اقدام، پذیرش نتیجه تحلیل، انعکاس به‌موقع و...) از یک‌طرف و مؤلفه‌هایی همچون گروه تحلیل‌گر، محتوای تحلیل و خروجی تحلیل از سوی دیگر تعامل وجود دارد. ازاین‌رو دائماً بین این عناصر ارتباط برقرار است.



در هشداردهی با تحلیل نامتعارض سه وضعیت طبق شکل ۲ متصور و حادث می‌گردد.

وضعیت اول: بین هشداردهی و تحلیل نامتعارض، هم‌راستایی، انطباق و پویایی وجود دارد. این تعامل دوطرفه و بهترین وضعیت است.

وضعیت دوم: یکی از طرف‌های مؤثر در برخورد با هر موضوع یا پدیده امنیتی با طرف دیگر میل به تعامل و انطباق سازی دارد. طرف دیگر سکون اختیار نمی‌کند اما تعامل پویا مشاهده نمی‌شود و این مهم ممکن است از سوی تحلیل‌گر با تحلیل نامتعارض یا نظام هشداردهی باشد. در این صورت وضعیت پویا، یک‌طرفه و البته بینابینی است.

وضعیت سوم: تعامل و ارتباط بین هیچ‌کدام از طرفین مشاهده نمی‌شود و این بدترین وضعیت است که در این صورت هیچ‌گاه هشداردهی موفق در راستای پیشگیری از غافل‌گیری محقق نخواهد شد.

ت- الگو هشداردهی در فرآیند بررسی اطلاعات (بر اساس نظریه سیستمی):

حیدری‌بنی (۱۳۹۸) در مقاله خود مدار اطلاعاتی را در قالب نظریه سیستمی بیان و تشریح نموده است

گام اول: ورودی سیستم که شامل طرح‌ریزی (تتبع) و گردآوری (تألیف) است.

گام دوم: پردازش (تجزیه، تنقید، تعلیل، تحلیل، تخمین).

گام سوم: خروجی (تمتع عملی و تمتع نظری همانند هشداردهی).

گام چهارم: بازخورد.

گام پنجم: تعامل با محیط.

در ورودی نظام هشداردهی، نخست، نیازمندی‌ها و شکاف‌های اطلاعاتی امنیتی، مشخص، طرح‌ریزی و در ادامه جمع‌آوری می‌گردد. در مرحله پردازش، ابتدا اطلاعات تجزیه‌شده تا اولویت و حق تقدم رسیدگی، مشخص شود؛ همچنین با تفکیک اطلاعات، شرایط برای ارزیابی صحیح، استفاده مطلوب و بایگانی مناسب، فراهم می‌شود. قطعه‌های مرتبط در کنار یکدیگر دسته‌بندی می‌شود و میزان تأیید، تکمیل یا تناقض این قطعه‌ها در قبال یکدیگر مشخص می‌گردد. در ارزیابی داده‌های جمع‌آوری‌شده، اقداماتی چون تعیین قابلیت اطمینان و اعتبار داده‌ها، انجام می‌شود.

در مراحل بعدی بررسی نیز فرایند تحلیل و تخمین انجام می‌شود. تحلیل و پیش‌بینی از اهمیت ویژه‌ای برخوردار است؛ چراکه بدون تحلیل، پیوند میان داده‌های جمع‌آوری‌شده به‌عنوان یک کلّ درک نخواهد شد، اطلاعات جمع‌آوری‌شده هرقدر هم مناسب و دقیق باشد هرگز به‌خودی‌خود گویا نخواهند بود. مشکل‌تر از مرحله تجزیه‌وتحلیل، فرایند پیش‌بینی و تهیه تصویر جدید است، به

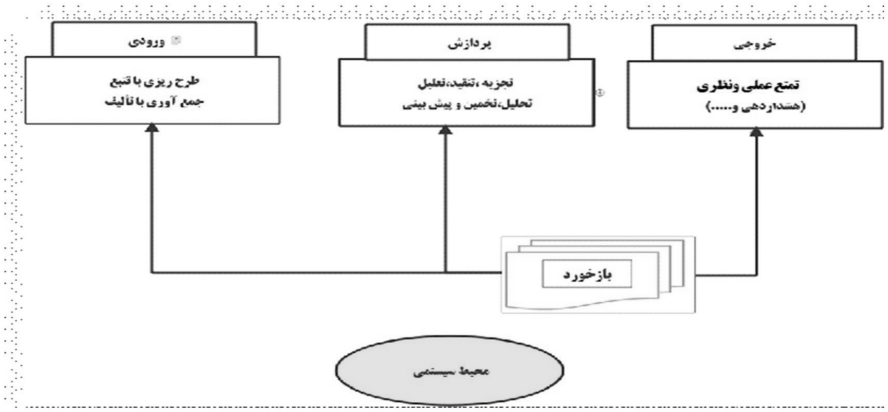
تعبیر بهتر، «هنر دستگاه اطلاعاتی درنتیجه گیری کافی، از مفروضات ناکافی است».

۱ – خروجی چرخه، به توزیع و بهره‌دهی و تمتع عملی و نظری (هشداردهی یا اقدام عملیاتی و...) می‌انجامد. بدون انتشار اطلاعات، هیچ بهره‌ای از فعالیت‌های چندگانه پیشین نخواهیم برد.

۲ – تعامل با محیط

۳ – بازخورد نظام هشداردهی نیز از اهمیت خاصی برخوردار بوده، نشان از میزان سلامت، کارایی و اثربخشی عملکرد دارد.

الگو هشداردهی با توضیحات فوق در شکل ۳ نمایش داده‌شده است.



شکل ۳: الگو هشداردهی در فرا د بررسی اطلاعات

پس از انجام تحلیل و پیش‌بینی و ارائه تصویری جدید از آینده، مرحله توزیع و سرویس‌دهی فرامی‌رسد که بهره حاصله، خصوصاً کار ویژه تحلیل، یعنی هشداردهی باید به طراحان خط‌مشی، ذهن‌های سیاست‌گذار و تصمیم‌گیرنده جهت بهره‌برداری و اقدام ارسال شود. بهره‌برداری قابل‌استفاده در دو حوزه قابل انجام است.

الف– بهره‌برداری نظری (هشداردهی و ...)

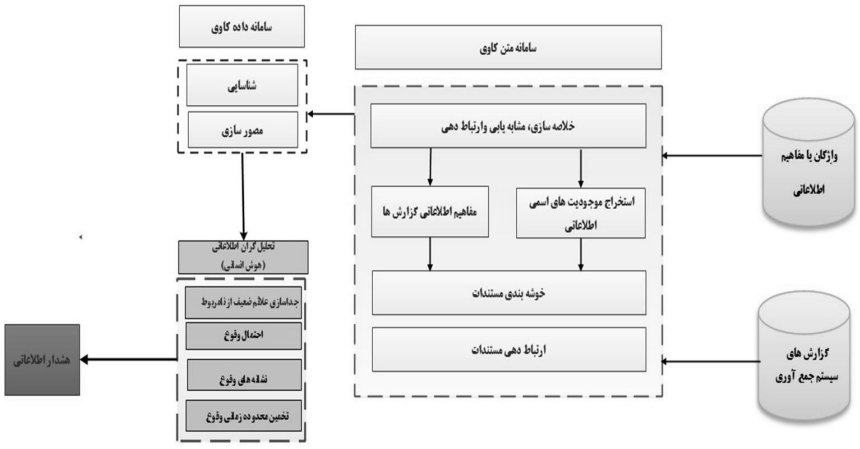
ب– بهره‌برداری عملی (شامل اقدامات عملیاتی ت.م، دستگیری، شنود، ورود پنهان و...)

ث- الگو سامانه هشداردهی اطلاعاتی امنیتی مبتنی بر داده‌کاوی

هشداردهی برای تصمیم‌گیران در حوزه امنیت ملی از بایدهای سازمان‌های اطلاعاتی – امنیتی است. درنتیجه ابتدا باید محیط را برای تحلیل‌گران جهت هشداردهی مؤثر و پیش‌دستانه آماده

کنیم. سامانه‌های جمع‌آوری داده‌های موردنیاز را از طرق مختلف جمع‌آوری و گزارش‌های خبری را به تحلیل‌گران ارجاع می‌دهد و ازآنجایی‌که این داده‌ها دارای حجم انبوه با نرخ تغییرات بالا می‌باشد و زمان برای تحلیل این گزارش‌ها محدود است و از طرفی تعداد تحلیل‌گران خُبره کم است، می‌توان با گرفتن مصاحبه از خبرگان، تحلیل اطلاعاتی مفاهیم و نشانه هر تغییر را که می‌تواند اثرات جبران‌ناپذیری برای امنیت ملی داشته باشد احصاء و با استفاده از سامانه متن‌کاوی به تحلیل آن پرداخت.

با ساختارمندشدن داده‌ها، فن تشخیص علائم ضعیف و مصورسازی در داده‌کاوی، می‌توان داده‌های دورافتاده را شناسایی و آنها را برای تحلیل به خبرگان تحلیل سپرد. این امر مستلزم ساخت و تولید سامانه‌ای است. «امامی» (۱۳۹۸) برای این منظور الگوی پیشنهادی طبق شکل ۴ را ارائه نموده تا با استفاده از مفاهیم و واژگان اطلاعاتی، موجودیت‌های اسمی را استخراج و با انجام عملیات داده‌کاوی و شناسایی علائم ضعیف، تحلیل‌گران، هشداردهی لازم را به تصمیم‌سازان و تصمیم‌گیران منتقل نمایند. نکته موردتوجه این است که نقش هوش انسانی در این فرایند هشداردهی را نمی‌توان نادیده گرفت و می‌بایست در هر مرحله تحلیلگر حضور داشته باشد.



شکل ۴: الگو سامانه هشداردهی اطلاعاتی امنی ی مبتنی بر داده‌کاوی

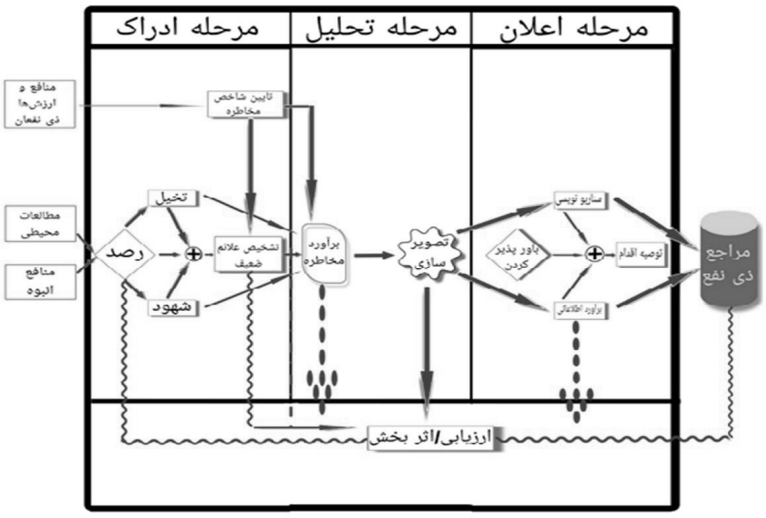
ج- الگوی فرایندی هشداردهی اطلاعاتی - امنیتی

مقاله حاضر ضمن بررسی مطالعات و مستندهای قبلی و ارائه تعریف عملیاتی از هشدار و هشداردهی و کارکردهای آن، با یاری یک کارگروه متمرکز هشت نفره اندیشه‌ورز متشکل از خبرگان موضوعی و مدیریتی، تلاش نموده الگوی جامع‌تری ارائه نماید. الگوی ارائه‌شده یک الگوی مدیریت فرایندی شامل سه مرحله و یازده گام مدیریتی برای هر مرحله به شرح زیر است:

۱- مرحله ادراک هشدار در هشداردهی که شامل چهار گام تشخیص علائم، تمییز علائم، انطباق علائم و ارتباط علائم است. ادراک هشدار در هشداردهی همچنین محصول دو اقدام مدیریتی رصد و تشخیص علائم ضعیف است.

۲- مرحله تحلیل هشدار در هشداردهی که شامل چهار گام تجزیه، ترکیب، تعلیل عناصر مسئله امنیتی و استنتاج پدیده مخاطره‌آمیز است. تحلیل هشدار در هشداردهی همچنین محصول دو اقدام مدیریتی برآورد مخاطره و تصویرسازی است.

۳- مرحله اعلان هشدار در هشداردهی شامل سه‌گام: آگاهی بخشی، برانگیختگی در ذی‌نفعان و واکنش طلبی از ذی‌نفعان است. مرحله اعلان هشدار در هشداردهی همچنین محصول دو اقدام مدیریتی باورپذیرکردن و توصیه برای اقدام است که برآیند نهایی آن برای مشارکت‌جویی ذی‌نفعان ارائه می‌شود. به‌منظور تضمین اثربخشی هشداردهی، ارزیابی فرایند در کلیه مراحل اقدام از الزامات هشداردهی اطلاعاتی امنیتی است. درمجموع فرایند هشداردهی و مراحل و اجزای آن، در الگوی فرایندی و طرح‌واره به شکل زیرترسیم شده است. (مزینانی، ایمانی پور وهمکاران، ۱۳۹۸)



شکل ۶: الگوی فرا ندی هشداردهی اطلاعاتی امنیتی

روش‌شناسی پژوهش

پژوهش حاضر به دنبال الگوی مناسب هشداردهی اطلاعاتی بحران‌های امنیتی است. روش پژوهش، کیفی برمبنای تحلیل محتوا و به لحاظ هدف و برحسب دستاورد از نوع پژوهشات کاربردی – توسعه‌ای و اکتشافی محسوب می‌شود. روش پژوهش در دو مرحله انجام‌شده است: در مرحله اول با مرور سامانمند به‌دلیل غنای نسبی ادبیات در حوزه موضوع و روش اسنادی (کتابخانه‌ای و فیش‌های تحقیقاتی) و بررسی پژوهشات پیشین در مورد الگوی هشداردهی اطلاعاتی اقدام شد. در این مرحله الگوی اولیه هشدار و رصد احصاء گردید. در مرحله دوم برای اتقان و تعمیق الگو اولیه و یافته‌های مرحله اول، به مصاحبه با نخبگان و خبرگان موضوع به‌عنوان جامعه آماری پرداخته شد. نمونه آماری با استفاده از روش نمونه‌گیری هدفمند، ۱۲ نفر با قاعده اشباع نظری مورد مصاحبه قرار گرفتند. در این پژوهش از روش کیفی در قالب گام‌های روش پژوهش برای شناسایی ابعاد، مؤلفه‌ها و شاخص‌ها استفاده شد که شرح آن درشکل ۶ آورده شده است.

شکل ۶: روش تحقیق

تجزیه و تحلیل یافته‌ها

یافته‌های گام اول (احصای الگو اولیه)

در گام اول این پژوهش مطالعه اسنادی با هدف استخراج شاخص‌ها انجام شد.

جدول ۱: استخراج شاخص

ردیف	شاخص‌ها
۱	شیوه گزارش دهی، پیامک، کتبی
۲	شیوه‌ها و روش‌های اطلاع‌رسانی و هشدار مثل جلسه و توجیه افراد
۳	بازخورد
۴	بازخورد و اصلاح

۵	بازخورد برای پیشگیری از اقدام غلط
۶	بازسازی و ترمیم
۷	تعامل دوسویه بین سه بخش جمع‌آوری‌کننده، تحلیل‌گر و تصمیم‌گیر بایستی وجود داشته باشد.
۸	بازخورد و اصلاح
۹	ارزیابی در کلیه مراحل و اقدامات هشداردهی
۱۰	اعلان هشدار به‌مثابه اقدام
۱۱	(هشداردهی) که درواقع تصمیم‌سازی است.
۱۲	نظام اقدام، درواقع اقدام برای هشدار، یعنی آگاه‌سازی لایه مدیران و تصمیم‌گیران
۱۳	اقدام به‌مثابه هشدار
۱۴	اوسینت، گاورنمنت اینتلیجنس، ایمینت، هیومینت، مشاهده، جمع‌آوری داده
۱۵	مشاهده قرائن و شواهد
۱۶	گزارش‌های نوبه‌ای، مثل گزارش‌های روزانه، هفتگی، سالانه، گزارش‌های ویژه
۱۷	نشانه و نشانه‌شناسی خطوط رسانه‌ای
۱۸	جمع‌آوری یا collection
۱۹	نشانه‌شناسی، شامل جمع‌آوری علائم آشکار، پنهان، سایبری، اوسینت(جمع‌آوری در منابع آشکار)
۲۰	بولتن یا گزارش اطلاعاتی
۲۱	رسانه‌هاوشبکه‌های بیگانه و فضای مجازی
۲۲	تقویم امنیتی (۷ آبان،۱۸ تیر،۹ دی و...)
۲۳	پایگاه داده و مدیریت دانش، تشخیص و تحلیل
۲۴	پایگاه دانش در ارتباط با تحلیل
۲۵	رویکرد مبتنی برداده‌کاوی
۲۶	دیتا ماینینگ یا داده‌کاوی، پایگاه دانش
۲۷	روندها و رویدادها
۲۸	بیگ دیتاهای کشور
۲۹	دسته‌بندی، سازمان‌دهی، تشخیص موجودیت‌های مشابه (انطباق)
۳۰	ادغام اطلاعات
۳۱	پردازش
۳۲	تولید اطلاعات (شهود)
۳۳	ارائه وضعیت موجود، وضع محتمل، وضعیت مطلوب (راهکار)
۳۴	پردازش

۳۵	کشف و شهود
۳۶	پردازش، مهم‌ترین شیوه‌های پردازش مکس کیودا، اس‌پی‌اس‌اس و سامانه‌های تحلیل، تحلیل انسانی و قدرت تحلیل
۳۷	رصد و تشخیص، تمیز، انطباق علائم، تخیل و شهود درمرحله ادراک قرار دارد.
۳۸	مرحله پردازش در داخل مشاهده قرار می گیرد؛ ابتدا مرحله جمع‌آوری، بعد تجزیه و تحلیل، سپس گزارش‌دهی است.
۳۹	سازمان‌دهی، دسته‌بندی، تقاطع گیری
۴۰	تصمیم‌گیری شامل دو بخش تجزیه و تحلیل و پایگاه دانش
۴۱	تصمیم سازی
۴۲	پیش‌بینی
۴۳	تلفیق چرخه اوودا و چرخه بحران و اقدامات آن جهت پیش‌بینی، کنترل و محدودسازی دامنه و کاهش تبعات بحران
۴۴	آینده‌نگری
۴۵	پیش‌بینی
۴۶	مدیریت بحران چرخه است، بررسی ریشه‌ها و مطالبات
۴۷	ترکیب، تجمیع، تقاطع، اشراف اطلاعاتی
۴۸	هشداردهی ناظر بر پیش‌بینی
۴۹	تحلیل اطلاعاتی اشراف می‌دهد و اشراف پیش‌بینی و تصمیم‌سازی
۵۰	چرایی‌ها و چگونگی‌های ایجاد بحران با مهندسی معکوس
۵۱	تجزیه و تحلیل
۵۲	تجزیه، ترکیب، تعلیل عناصر امنیتی در مرحله تحلیل قرار دارد.
۵۳	بررسی شامل تجزیه و تحلیل و تطبیق است.
۵۴	جهت‌دهی
۵۵	تشخیص و جهت‌دهی
۵۶	اطلاعات یعنی تصمیم‌سازی
۵۷	خطا درتخمین زمان اقدام
۵۸	سطوح هشدار
۵۹	سطح هشدار تاکتیکی، راهبردی
۶۰	سطوح هشدار متفاوت محلی، منطقه‌ای، ملی، فراملی، گاهی موضوعی
۶۱	سطوح هشدار، شامل محلی، منطقه‌ای و ملی است.
۶۲	علائم ضعیف، علائم قوی

۶۳	علائم و سیگنال‌ها
۶۴	لایه‌لایه نمودن داد ه‌ها به‌صورت جایستگی در سامانه جی‌آی‌اس
۶۵	دیده‌بانی
۶۶	موضوع طرح‌ریزی قبل از مرحله مشاهده، پیش‌آگاهی یا ادراک است.
۶۷	علائم ضعیف
۶۸	علائم قوی
۶۹	هشداردهی درست، تصمیم‌گیری غلط، بحران‌آفرین است.
۷۰	هشداردهی ناقص منجر به بحران می‌شود.
۷۱	هشداردهی، تصمیم‌سازی درست، تصمیم‌گیری و اقدام دارای اشکال، منتج به بحران می‌شود
۷۲	هشدار صحت‌سنجی‌شده (راستی آزمایی شده)، هشدار پیشگیرانه، هشدار به هنگام و به‌موقع
۷۳	رویکرد پیشگیرانه
۷۴	آگاهی، برانگیختگی و واکنش‌طلبی از ذی‌نفعان درمرحله اعلان هشدار است.
۷۵	طرح‌ریزی عملیات
۷۶	حوزه اجتماعی، حوزه سایبر
۷۷	آسیب‌پذیری‌های اجتماعی، آسیب‌پذیری‌های پنهانی
۷۸	حوزه‌های اقتصادی، حوزه‌های فناورانه
۷۹	نشانه‌های سیاسی
۸۰	حوزه اقتصاد
۸۱	حوزه فرهنگی، بازیگران هشدار
۸۲	رصد همه مؤلفه‌ها و حوزه‌ها از بالا
۸۳	هشدار در حوزه اقتصاد و اجتماعی
۸۴	هشدار حوزه اجتماعی، فرهنگی
۸۵	حوزه‌های اجتماعی سیاسی، اقتصادی، امنیتی، زیست‌محیطی می‌تواند تولید بحران امنیتی نماید.
۸۶	حوزه اجتماعی
۸۷	حوزه سیاسی
۸۸	داده، اطلاعات، دانش
۸۹	بیگ‌دیتا، اطلاعات، دانش

یافته‌های گام دوم (اتقان الگو)

در گام دوم به وسیله ابزار مصاحبه با ۱۲ نفر از خبرگان اطلاعاتی، امنیتی، سایبری، بحران و پیاده‌سازی متن مصاحبه‌های انجام شده و تحلیل آن، مؤلفه‌ها و ابعاد الگو نمایان و الگو نهایی براساس نتایج حاصل طبق جدول ۲ ترسیم گردید.

جدول ۲: استخراج مؤلفه‌ها و ابعاد

ردیف	مولفه‌ها	ابعاد
۱	آگاهی (جمع‌آوری)	مشاهده (جمع‌آوری)
	علائم (ادراک)	
۲	پردازش	تشخیص و جهت دهی
۳	تجزیه و تحلیل (بررسی)	تصمیم سازی
	پایگاه دانش	
۴	سطوح هشداردهی ابزار هشدار عناصر مؤثر در هشدار موضوع هشدار بازیگران هشدار شبکه هوشمند مراحل هشدار زمان هشدار	اعلان و اقدام (هشدار)

در گام اول ابتدا ضمن مرور نظام‌مند در مبانی نظری و مطالعه منسجم و پیوسته و تحلیل حجم گسترده‌ای از مقالات، رساله‌ها و کتب مرتبط که در متن اشاره و لیست کامل آنها در بخش منابع قید شده است، ابعاد الگو احصاء و ایده‌های اولیه درخصوص الگوی هشداردهی اطلاعاتی بحران‌های امنیتی در قالب الگوی مفهومی اولیه تدوین شد؛ که ابعاد چهارگانه الگوی ما به‌لحاظ کاربردی و محتوایی با چرخه اوودا[1] در فرماندهی و کنترل شباهت داشت.

در گام دوم به‌منظور تأیید یا ردّ چارچوب مفهومی و ابعاد مستخرج از مبانی نظری و به‌منظور بررسی روایی، نظر استادان راهنما و مشاور و افراد صاحب‌نظر اخذ گردید؛ که پس از مراجعه به خبرگان و انجام اصلاحات لازم، مورد تأیید آنان نیز قرار گرفت. سپس با استفاده از روش نمونه‌گیری هدفمند به

1 OODA.

شیوه گلوله برفی، به‌صورت میدانی و مصاحبه با خبرگان، صاحب‌نظران، کارشناسان دارای تحصیلات عالی، جایگاه مدیریتی و سابقه خدمت در مشاغل اطلاعات، امنیت، سایبری، فنی و مدیریت بحران، اقدام به شناسایی و تحکیم شاخص‌ها، مؤلفه‌ها و ابعاد شد که پس از مصاحبه با ۱۲ نفر از این متخصصان که به صورت هدفمند انتخاب شده بودند، یافته‌های حاصل به اشباع نظری رسید.

در ادامه، متن مصاحبه‌ها پیاده‌سازی و نظرات مشترک یا نزدیک به هم استخراج و ادغام شد، سپس ابعاد، مؤلفه‌ها و شاخص‌ها در قالب گزاره‌های معنایی و به‌صورت کدگذاری آورده شد؛ که در انتها ضمن تعیین ابعاد، مؤلفه‌ها و شاخص‌ها، الگوی نهایی هشداردهی اطلاعاتی بحران‌های امنیتی به دست آمد. نتایج نهایی حاصل از این تحلیل در جدول ۳ گردآوری‌شده است.

جدول ۳: شاخص‌ها،مؤلفه‌ها و ابعاد

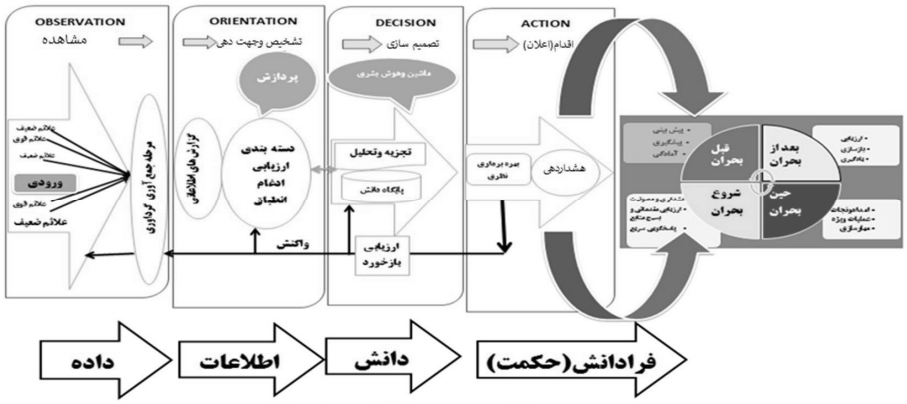
ردیف	(شاخص‌ها)	(مولفه‌ها)	ابعاد
۱	علائم ضعیف: (Weak signal)	**علائم(ادراک)**	**مشاهده (ادراک، جمع‌آوری)**
۲	علائم قوی: (Power signal)		
۳	آگاهی از منابع انسانی (HUMINT)	**آگاهی (جمع‌آوری)**	
۴	آگاهی از منابع آشکار (OSINT)		
۵	آگاهی از طریق علائم (SIGINT)		
۶	شنود مخابراتی (کامینت) (COMINT)		
۷	شنود الکترونیکی (الینت)(ELINT)		
۸	آگاهی از طریق تصویربرداری و عکس‌برداری (IMINT)		
۹	آگاهی از طریق سنجش و اثر (MASINT)		
۱۰	شناسایی سیگنال‌های تجهیزات بیگانگان (SIGNAL)		
۱۱	اطلاعات دولتی (GOVERNMENT INTELLIGENCE)		
۱۲	اطلاعات تصویری (IMAGE INT)		
۱۳	انواع سنتی جمع‌آوری اطلاعاتcollection types Traditional intelligence		

۱۴	ارزیابی داده‌های گردآوری‌شده (اعتبار سنجی)		**پردازش**	**تشخیص و جهت‌دهی**
۱۵	ادغام و انسجام‌بخشی داده‌ها			
۱۶	تشخیص موجودیت‌های مشابه (انطباق)			
۱۷	برآورد وبیان وضع موجود (توصیف جامع)			
۱۸	کشف و شهود			
۱۹	تجزیه (تفکیک و جداسازی عناصر اصلی شکل‌دهنده)		**تجزیه و تحلیل (بررسی)**	**تصمیم سازی**
۲۰	اتقان			
۲۱	تقاطع			
۲۲	ترکیب عناصر امنیتی			
۲۳	تعلیل (علت‌یابی)، تبیین			
۲۴	(تحلیل) استنتاج پدیده مخاطره‌آمیز و دستیابی به شناختی نو از پدیده‌ها			
۲۵	تخمین و پیش‌بینی و آینده‌نگری روند آتی			
۲۶	تقویم امنیتی (۷آبان، ۱۸ تیر، روز دانشجو...)		**پایگاه دانش**	
۲۷	سالگرد مراسمات و برگزاری آن، چهلم، ایام انتخابات، (رویدادهای ملی)			
۲۸	رویدادهای نوظهور (شگفتی‌ساز)			
۲۹	کاربردی (تاکتیکی)	محلی (سطح ۱)	**سطوح (مکانی)**	**اقدام (اعلام هشدار)**
۳۰	کاربردی (تاکتیکی)	استانی (سطح ۲)		
۳۱	راهبردی	ملی (سطح ۳)		
۳۲	راهبردی	فراملی (سطح ۴)		
۳۳	گزارش‌های ویژه		**ابزار**	
۳۴	نوشتاری (گزارش‌های نوبه‌ای روزانه)			
۳۵	نوشتاری (گزارش‌های نوبه‌ای هفته‌ای)			
۳۶	نوشتاری (گزارش‌های نوبه‌ای ماهانه)			
۳۷	هشدار گفتاری			
۳۸	هشدار صوتی			
۳۹	هشدار تصویری			
۴۰	احتمالات (بیان و تصریح احتمالی دریک دوره)		**عوامل موثر در هشدار**	
۴۱	تأثیرات (پیامدها و تأثیرات هریک از حالات محتمل)			
۴۲	اولویت‌دهی (رتبه‌بندی منطقی هریک از احتمالات و حالات هشدار)			

۴۳	سیاسی	موضوع	اقدام (اعلام هشدار)
۴۴	اجتماعی		
۴۵	اقتصادی		
۴۶	فرهنگی		
۴۷	زیست‌محیطی		
۴۸	علم و فناوری		
۴۹	ترکیبی		
۵۰	نخبگان	بازیگران	
۵۱	کارگران		
۵۲	دانش آموزان		
۵۳	دانشجویان		
۵۴	زنان		
۵۵	اصناف		
۵۶	بازنشستگان		
۵۷	فرهنگیان		
۵۸	رسانه‌ها فضای مجازی		
۵۹	هشداردهی مبتنی بر فناوری‌های نوین، مانند هوش مصنوعی	شبکه هوشمند	
۶۰	تدوین و تولید هشدار	مراحل هشدار	
۶۱	انتقال و دریافت هشدار		
۶۲	باور تصمیم‌گیران به هشدار		
۶۳	اقدام عملی تصمیم‌گیران و فرماندهان		
۶۴	قریب‌الوقوع	زمان	
۶۵	آینده بسیار نزدیک		
۶۶	آینده نزدیک (کوتاه‌مدت)		
۶۷	به‌زودی (میان‌مدت)		
۶۸	آینده قابل پیش‌بینی (بلندمدت)		

الگو نهایی پژوهش

محقق با بررسی انواع الگوهای هشداردهی و مطالعات صورت‌گرفته و مصاحبه با خبرگان و صاحب‌نظران اطلاعاتی امنیتی و سایبری، درنهایت به الگو هشداردهی اطلاعاتی بحران‌های امنیتی طبق شکل ۷ رسیده است.



شکل ۷: نظام هشداردهی اطلاعاتی بحران‌های امنیتی

نتیجه‌گیری

به‌منظور ارائه الگوی مناسب هشداردهی اطلاعاتی بحران‌های امنیتی با مرور مبانی نظری و ادبیات این حوزه و بررسی انواع نظام‌ها و الگوهای هشدار در مطالعات اسنادی و کتابخانه‌ای و نیز مطالعات میدانی با ابزار مصاحبه و اخذ نظرات و دیدگاه‌های مدیران و خبرگان اطلاعاتی، امنیتی، بحران، سایبری و فنی، پس از تعدیل و اصلاح نتایج حاصل از این فرایند، شاخص‌ها، مؤلفه‌ها و ابعاد در جدول بالا احصاء و سپس الگوی مناسب با توجه به نتایج فوق تکوین و ترسیم شد. نتایج حاصل از مبانی نظری، مصاحبه و کدگذاری، به ۶۸ شاخص، ۱۳ مؤلفه و ۴ بُعد منجر گردید. مؤلفه‌های حاصل عبارت است از: علائم (ادراک)، آگاهی (جمع‌آوری)، پردازش، تجزیه و تحلیل (بررسی)، پایگاه دانش، سطوح، ابزار، عناصر و عوامل مؤثر هشدار، موضوع، بازیگران، شبکه هوشمند، مراحل و زمان هشدار در قالب ۴ بُعد: مشاهده، تشخیص و جهت‌دهی، تصمیم‌سازی و اقدام طبقه‌بندی شد که با توجه به آن، الگوی هشداردهی اطلاعاتی طراحی و در هریک از گام‌ها، موضوع ارزیابی،

بازخورد و یادگیری در هر مرحله به مرحله قبل نیز مورد توجه و تأکید قرار گرفت. در تطبیق نتایج حاصل از این پژوهش با سایر پژوهش‌های انجام‌شده باید اشاره نمود به مقاله «احمدی» (۱۳۹۸) که در آن فرایند هشداردهی مؤثر را، وجود، دریافت، تحلیل نشانه، نظام و نحوه هشداردهی، ارسال به فرماندهی برای تصمیم‌گیری، دریافت بازخورد و تحلیل مجدد و مستندسازی به‌عنوان مراحل هشدار دانسته که با یافته‌های این پژوهش، در بعد اعلان و اقدام و همچنین موضوع هشدار، سطوح هشدار، ابزار و زمان هشداردهی به‌عنوان مؤلفه‌های هشدار و دیگر ابعاد، دارای انطباق می‌باشد. «احمدی»، هشداردهی صحیح و به‌موقع را نتیجه تحلیل دقیق و تعامل نزدیک بین هشداردهی و تحلیل می‌داند. همچنین انتقال هشدار به سیاست‌گذار و ارائه انواع پیش‌بینی‌های محتمل و در نظر گرفتن انواع حالت‌ها یا وضعیت‌های ممکن و توجه به علائم ضعیف را جزو عوامل مؤثر در پیشگیری از هشدار غلط دانسته است. در این مقاله نیز تحت عنوان شاخص تحلیل و نیز مؤلفه مراحل هشدار که شامل تدوین، انتقال ، باور و اقدام عملی تصمیم‌گیران و همچنین در مؤلفه عناصر و عوامل مؤثر در هشدار به سه شاخص مهم، یعنی احتمالات، تأثیرات و اولویت‌دهی و نیز علائم ضعیف، به‌عنوان یک شاخص پرداخته شده که با مقاله مذکور در این شاخص‌ها و مؤلفه‌ها هم‌راستاست.

«شمشیری» و «دانش تبار» (۱۳۹۸) در مقاله خود بیشتر پیرامون فریب بحث نموده که انطباق کمی با الگوی هشداردهی دارد و تنها در بخش ارزیابی باهم مشترک می‌باشد.

«حیدری بنی» (۱۳۹۸) الگو هشداردهی را در فرایند بررسی اطلاعات ترسیم نموده است که در آن گام‌های طرح‌ریزی و گردآوری، پردازش، خروجی و بازخورد با مؤلفه‌های پژوهش ما، یعنی ادراک و جمع‌آوری، پردازش، تجزیه و تحلیل، اعلان و اقدام، همچنین ارزیابی هم‌راستا است.

«امامی» (۱۳۹۸) در الگو سامانه هشداردهی اطلاعاتی امنیتی مبتنی بر داده‌کاوی به‌منظور غلبه بر محدودیت زمان تحلیل و تشخیص علائم ضعیف از داده‌های نامربوط، ساخت و تولید سامانه داده‌کاوی تحت نظارت هوش انسانی را پیشنهاد نموده که با مؤلفه‌های تجزیه و تحلیل و پایگاه دانش در بعد تصمیم‌سازی این پژوهش منطبق است.

«مزینانی»، «ایمانی‌پور» و همکاران (۱۳۹۸) یک الگوی فرایندی هشداردهی که مشتمل بر سه مرحله و یازده گام مدیریتی است را ارائه نموده‌اند که تقریباً بخش زیادی از این فرایند با الگوی هشداردهی این پژوهش هم‌راستا و دارای انطباق است.

پیشنهاد

به‌منظور پیش‌بینی و پیشگیری از بحران‌های امنیتی پیش‌رو با نگاهی به علم و دانش آینده‌پژوهی نسبت به طراحی، تقویت و پیاده‌سازی الگوها و نظام‌های هشدار اطلاعاتی در ابعاد مختلف امنیت ملی و اجرای آن، بایستی دستگاه‌ها و سازمان‌های مسئول اقدام نمایند

همچنین با توجه به‌احتمال خطا در تصمیم‌گیری‌های انسانی به‌ویژه مدیریت بحران‌های امنیتی و هشدارهای اطلاعاتی، تدوین، استانداردسازی و طراحی شاخص‌های بحران و شاخص‌سازی در حوزه‌های مختلف مرتبط با امنیت ملی واجب و ضرورتی اجتناب‌ناپذیر است؛ بنابراین انجام مطالعات علمی در قالب پروژه‌های پژوهشاتی برای تدوین این شاخص‌ها می‌تواند در سامانه‌های هشدار به تحلیل‌گران، مجموعه‌های اطلاعاتی و تصمیم‌سازان و متولیان سامانه‌های رصد و پایش و هشدار و درنهایت تصمیم‌گیری مدیران بحران، سیاست‌مداران و مسئولان حکمرانی نظام یاری رسانده، با رویکردی دستگاهی در کنترل انسان به اتخاذ بهترین تدابیر و اقدامات نائل آمد و شکست‌های اطلاعاتی و غافلگیری‌ها را کاهش داد.

منابع

الف) منابع فارسی

۱. احمدی، صادق، (۱۳۹۸)، «**نقش تحلیل نامتعارض درهشداردهی با رویکرد پیشگیری از غافلگیری راهبردی**» مجموعه مقالات چالش‌های هشداردهی، همایش هشداردهی اطلاعاتی امنیتی. تهران: مرکز مطالعات و پژوهش‌های امنیتی ساحفاسا

۲. امامی، محمدرضا،(۱۳۹۸). **کاربرد داده‌کاوی درهشداردهی اطلاعاتی- امنیتی**. مجموعه مقالات چالش‌های هشداردهی ، همایش هشداردهی اطلاعاتی امنیتی. تهران: مرکز مطالعات و پژوهش‌های امنیتی ساحفاسا.۱۹۶-۱۹۵

۳. امیری، عبدالرضا، (۱۳۹۱). **مطالعه فرا ند متغیرهای مؤثر برامنیتی شدن بحران‌های اجتماعی در ایران**. نشریه پژوهش‌های مدیریت انتظامی، شماره ۲، تهران، سال هفتم (۲۳۷-۲۱۹).

۴.حاجیانی، ابراهیم، (۱۳۹۰). **هشداردهی: کارکرد تحلیل اطلاعاتی در پیشگیری از غافلگیری**. فصلنامه پژوهشی مطالعات راهبردی، (۴)۳، مسلسل ۵۳،۱۲۷-۱۵۷.

۵. حیدری بنی، مسلم، (۱۳۹۸). **هشداردهی کارکردی برای پ ش‌بینی از غافلگیری**. مجموعه مقالات چالش‌های هشداردهی ، همایش هشداردهی اطلاعاتی امنیتی. تهران: مرکز مطالعات و پژوهش‌های امنیتی ساحفاسا.۱۲۱-۱۱۹

۶. دیویس، جک، (۱۳۸۶). **هشدار استراتژیک: اگر شگفتی غیرقابل‌اجتناب است، تحلیل چه نقشی را ایفا می‌کند؟** فصلنامه دانش اطلاعاتی، شماره ۴، دانشکده امام باقر (ع)،۸۳-۶۱

۷. زندی، ابراهیم، (۱۳۸۷). **مفهوم بررسی اطلاعاتی**. تهران: دفتر پژوهش‌های اطلاعاتی - گروه علمی پژوهش‌های تدوین تجارب.

۸. شمشیری، مهدی، دانش تبار، بهمن، (۱۳۹۸). **نقش فریب در هشداردهی اقدام اطلاعاتی امنیتی**، مجموعه مقالات چالش‌های هشداردهی، همایش هشداردهی اطلاعاتی امنیتی. تهران: مرکز مطالعات و پژوهش‌های امنیتی ساحفاسا.۸۴-۷۷

۹. صالحی، محمود، (۱۳۹۵). **ماهیت و مفهوم هشداردهی، مباحث درسی دوره دکتری مدیریت اطلاعات**، تهران: دانشکده اطلاعات.

۱۰. صحرایی، مهدی، ترقّی، عبدالرضا، نیک‌نفس، علی، دهقانی، حامد، دلگیر، علی و دیگران،

(۱۳۹۸). **طراحی نظام رصد، پایش و هشداردهی سایبری با رویکرد امنیت ملی**. (رساله دکتری منتشرنشده)، دانشگاه و پژوهشگاه عالی دفاع ملی و پژوهشات راهبردی، تهران، ایران

۱۱. عبدالله زاده، احمد، (۸۶-۸۵). **نقش اطلاعات در بحران ۱۸ تیر سال ۷۸**

۱۲. علیخانی، عبدا...،(۱۳۹۳). **هشدارشناسی**. تهران: دانشکده اطلاعات

۱۳. علیخانی، علی، هدایتی، علی‌رضا، (۱۳۹۵) **روش پژوهش کاربردی در اطلاعات و امنیت ملی، معاونت پژوهش و تولید علم دانشگاه اطلاعات و امنیت ملی**

۱۴. فخری، مجید، (۱۳۹۶). **طراحی الگوی راهبردی دیدبانی برای نیروهای مسلح جمهوری اسلامی ایران**. (رساله دکتری منتشرنشده)، دانشگاه عالی دفاع ملی، تهران، ایران.

۱۵. فکوری، محمدعلی،(۱۳۹۲). **فرهنگ واژگان اطلاعاتی**. چاپ اول، تهران: دانشکده اطلاعات

۱۶. گرابو، سینتیاام، (۱۳۹۸). **پیش‌بینی غافلگیری تحلیل برای هشدار راهبردی** (محمد یوسفی خرابم، احمدرضا میرزایی، مترجمان). تهران: انتشارات دانشگاه و پژوهشگاه عالی دفاع ملی و پژوهشات راهبردی

۱۷. گرابو، سینتیاام، (۱۳۹۸). **دستنامه هوشمندی هشداردهنده (سجادمحسنی، محمد صالحی علی‌آباد علیا، مترجمان)**. تهران: انتشارات دانشگاه و پژوهشگاه عالی دفاع ملی و پژوهشات راهبردی

۱۸.مزینانی، احمد، ایمانی‌پور، احمد همکاران، (۱۳۹۸). **فرایند هشداردهی اطلاعاتی _ امنیتی**. مجموعه مقالات جایگاه فرایند هشداردهی در اقدامات اطلاعاتی- امنیتی، همایش هشداردهی اطلاعاتی - امنیتی، مرکز مطالعات و پژوهش‌های امنیتی ساحفاسا.

۱۹. معین، محمد، (۱۳۶۴). **فرهنگ فارسی متوسط**. مؤسسه انتشارات امیرکبیر، چاپ هفتم، جلد چهارم، تهران.

۲۰. مهری، علی، (۱۳۹۸). **ارائه الگوی راهبردی در اداره امور بحران‌های امنیتی بر اساس گفتمان امام و رهبری، قانون اساسی، تجارب ج.ا.ا و بهره‌گیری از تجارب موفق بشری**. (رساله دکتری منتشرنشده)، دانشگاه عالی دفاع ملی، تهران، ایران.

۲۱. ولوی، محمدرضا، صحرایی، مهدی، (۱۳۹۵). **ارائه الگو رصد، پایش و هشداردهی سایبری براساس چرخه فرماندهی وکنترل OODA مبتنی بر مطالعه تطبیقی کشورهای هدف**

۲۲. **هشداردهی، وا رین مأموریت اطلاعات**، (۱۳۹۳).وزارت اطلاعات، ویژه‌نامه ۳۰ سال

مجاهدت‌های خاموش، دانشکده اطلاعات،(۱۵۹-۱۵۷).

۲۳.یوسفی رامندی، رسول، محمدی، مجید، (۱۴۰۱). «**تبیین عوامل مؤثر در بروز بحران‌های اجتماعی - امنیتی مورد مطالعاتی ناآرامی آبان ۱۳۹۸**». پژوهش‌های سیاست اسلامی- شماره ۲۲ (۳۶۴ - ۳۳۶).

ب) منابع لاتین

24. CISC:Criminal Intelligence Service Canada(2007);**Strategic Early Warning for Criminal Intelligence.**

25. E. Philip Davis and Dilruba Karim "**Looking ahead: early warning systems**" https://www.elgaronline.com/view/edcoll/9781789904512/9781789904512.00026.xml.

26. Graboo,Cynthiy؛ (2010) **Handbook Of Warning Intelligence (Assesment The ThrathTo National Security),Forward By Jon Goldman**.

27. Ibrahim Al Luhaidan, Daifallah M. Alrazeeni(2018)" **The Role of Key Early Warning Indicators in Crisis Management: Analytical Review**"; Ministry of Interior Saudi Arabia, King Saud University: Analytical Review.

28. SARAH LOHMANN.TIMTEPEL" (2014) **Will the real security foresight expert please stand up?**".