تاریخ دریافت: ۱۴۰۳/۰۷/۱۲ تاریخ پذیرش: ۱۴۰۳/۱۲/۱۰ صفحه ۳۲ تا ۵۷

نقش سازمان حفاظت‌کننده در نظام هشداردهی اقدامات تروریستی

حسین حسینی جیردهی[۱]، ابراهیم حاجیانی[۲]، محمد جعفر جوادی[۳]، غلامعلی زوارزاده[۴]، حسین عربیان[۵]

چکیده

هشداردهی در حوزه اقدامات تروریستی از پیچیده‌ترین موضوعاتی است که همواره مورد چالش سازمان‌های اطلاعاتی، امنیتی و حفاظتی بوده است. یکی از چالش‌های اساسی تقسیم وظایفی است که هر یک از سازمان‌ها در نظام هشداردهی ممکن است برعهده داشته باشند. این پژوهش در نظر دارد به این سوال پاسخ دهد که سازمان حفاظت کننده از دارایی‌ها در نظام هشدار چه نقشی دارد؟ این پژوهش بر اساس هدف، پژوهشی کاربردی است. راهبرد انتخاب شده برای این پژوهش، راهبرد مطالعات زمینه‌ای(داده بنیاد) است که داده‌های بدست آمده از طریق مصاحبه با۱۷ نفراز خبرگان با روش تحلیل مضمون با استفاده از نرم افزار اطلس تی آی ۹ مورد تجزیه و تحلیل قرار گرفته است. یافته‌ها و نتایج پژوهش نشان می‌دهد که مسیر هشدار مسیر یکطرفه از سازمان اطلاعاتی به سازمان حفاظت کننده نبوده و مدام در حال رفت و برگشت در چرخه نظام هشداردهی است و از سوی دیگر در هر یک از مراحل نظام هشدار، وظایفی در عرض هر مرحله ایجاد می‌شود که می‌بایست سازمان‌ها برای تقویت و اثرگذاری آن مرحله با هم و در عرض فرایند طولی هشدار انجام دهند تا هشدار بتواند کارکرد خود را به درستی ایفا نماید.

واژگان کلیدی: هشدار، سازمان حفاظت کننده، نظام هشداردهی، اقدامات تروریستی

۱. دانشیار گروه دانشکده مطالعات فرهنگی اجتماعی دانشگاه جامع امام حسین (علیه السلام) (نویسنده مسئول)
hosein.hoseini@gmail.com

۲. دانشیار و مدیر گروه پژوهش‌های فرهنگی اجتماعی، دانشگاه باقرالعلوم (ع)

۳. استادیار دانشکده امنیت ملی دانشگاه عالی دفاع ملی

۴. استادیار دانشکده حفاظت و حراست دانشگاه جامع امام حسین (علیه السلام)

۵. دکتری مطالعات منطقه‌ای – پژوهشگر دانشگاه جامع امام حسین (علیه السلام)

The Role of Protecting Organization in the Warning System of Terrorist Acts

Husein Huseini Jirdehi[1], Ebrahim Hajiani[2], Mohammad Jafar Javadi[3], Gholam Ali Zavar Zadeh[4], Husein Arabian[5]

Abstract

Warning in the field of terrorist acts is one of the most complex issues that has been always a chalenge for intelligence and security agencies. One of the essential challenges is dividing duties of each of the agencies in the warning system that may be responsible for. This research intends to answer the question of what role the protecting agency plays in protecting the assets in the warning system? This research is of applied type in terms of objectives. The selected strategy for this research is the field studies (data-based) in which the acquired data were analyzed through interviewing seventeen experts using content analysis method and ulilyzing TI 9 Almanac.

Findings and results of this research show that the warning route is not a one-way route from the intelligence agency to the protecting agency and is continuously moving back and forth in the warning system cycle and on the other hand, in each of the steps of the warning system, certain duties are established which the agencies should do in order to improve and affect that step together and across the longitudinal process of warning so that warning can implement its function correctly.

Key Words: warning, protecting agency, warning system, terrorist acts

---

1. Associate Professor, the Faculty of Social-Cultural Studies Department, Imam Husein University. @ gmail .com hosein.hoseini

2. Associate Professor and Director, Department of Social-Cultural Studies, Bagher Al Olum University

3. Assistant Professor, Faculty of National Security, National Defense University

4. Assistant Professor, Faculty of Protection, Imam Husein University

5. Ph.D in Regional Studies, Researcher, Imam Husein University

مقدمه

هشـــدار به‌عنوان اصلی‌ترین فراورده اطلاعاتی در سازمان‌های اطلاعاتی در نظر گرفته می‌شود. اگر سازمان‌های اطلاعاتی نتوانند در تولید بهنگام و کارآمد هشدارها به‌درستی عمل نمایند مجبور خواهند بود به بحران‌ها به‌صورت واکنشـــی پاسخ دهند. پاسخ واکنشی نتیجه‌ای جز غافلگیری در برابر تهدیدها و شکست جامعه اطلاعاتی و امنیتی از مأموریت‌های محوله نخواهد داشت.

یکی از حوزه‌هایی که هشدار می‌تواند نقش مهمی ایفا نماید حوزه مقابله با اقدامات تروریستی است. این حوزه از موضوعات پیچیده و حساسی است که از یک‌سو اقتدار یک کشور را نشان می‌دهد و از ســـوی دیگـــر می‌تواند در صورت قصور و ناتوانـــی در آن، ضربه جبران‌ناپذیری بر پیکره امنیت یک حکومت وارد نماید. بر همین اســـاس هشـــداردهی نقش بی‌بدیلی در جلوگیری از غافلگیری و شکست اطلاعاتی و حفاظتی در مقابله با اقدامات تروریستی ایفا می‌نماید.

این نقش بی‌بدیلی که هشدار بر عهده دارد در رسیدن به هدف اصلی خود که عبارتند از «پیش‌آگاهی متقاعدکننده برای واکنش پیشگیرانه تصمیم گران و جلوگیری از غافلگیری منجر به شکست اطلاعاتی - امنیتی» (مزینانی،۱۳۹۷:۸۸). با چالش‌های متعددی روبرو اســـت. برخی از مهم‌ترین چالش‌های هشـــدار در مقابله با اقدامات تروریســـتی عبارتند از: «تعدد و تکثر هشدارهای ارائه‌شده»(ارتباطات شـــخصی، کد ۱۳: تیرماه ۱۴۰۰). و «نبود تاریخ انقضایی برای هشـــدارها» (ارتباطات شخصی، کد ۱۴: تیرماه ۱۴۰۰). «کمبود نیروی انسانی در حوزه عملیات حفاظتی»(ارتباطات شخصی، کد ۱۵: تیرماه ۱۴۰۰) «کاهش باور فرماندهان به هشدارهای اقدامات تروریستی و بی‌اعتبار شدن هشدارهای صادر از ســـوی سازمان‌های اطلاعاتی» « مشـــخص نبودن احتمال نزدیکی یا دوری و سطح تهدید تروریســـتی» (ارتباطات شخصی، کد ۱۴: تیرماه ۱۴۰۰). «مجاری متعدد اعلام هشدار» (ارتباطات شـــخصی، کد ۱۵: تیرماه ۱۴۰۰).«کلی‌گویی و گرد گویی در هشدارهای اعلام شده» وغیره. چنین چالش‌هایی ســـبب شده عملاً هشـــدارهای داده‌شده کارآمدی کمتری برای سازمان‌های حفاظتی- امنیتی داشته باشد (ارتباطات شخصی، کد ۱۶: مهرماه ۱۴۰۱). چنین وضعیتی نظام هشداردهی را درگیر چرخه‌ای معیوب می‌کند. نتیجه چنین چرخه‌ای تحمیل هزینه‌های سنگین به سازمان‌های اطلاعاتی و امنیتی-حفاظتی و درنهایت اقتدار و امنیت ملی کشور خواهد بود.

تداوم چنین چرخه معیوبی با چالش‌هایی که پیش روی آن قرار گرفته سبب شده معمولاً بعد از هر حادثه تروریســـتی، سازمان‌های حفاظتی(ســـازمان‌هایی که متولی حفاظت از امکان حیاتی و حســـاس، شخصیت‌ها و نخبگان کشور هســـتند) بخش مهمی از شکست را متوجه سازمان‌های

اطلاعاتی دانسته و بر این باور باشند که قبل از شکست حفاظتی، شکست اطلاعاتی رخداده است و این شکست اطلاعاتی است که زمینه‌ساز شکست حفاظتی را ایجاد کرده است(ارتباطات شخصی، کد ۱۰: تیرماه ۱۴۰۱). در مقابل سازمان‌های اطلاعاتی معمولاً قائل به شکست اطلاعاتی نبوده وبر این باورند که هشدارهای دقیقی از حملات تروریستی به سازمان‌های حفاظتی ارائه شده است(ارتباطات شخصی، کد ۱۴: تیرماه ۱۴۰۰).

پژوهش حاضر با درک پیچیدگی‌های حاکم بر نظام هشدار در مقابله با اقدامات تروریستی و نقشی که سازمان‌های درگیر در نظام هشداردهی ایفا می‌نمایند در صدد است با توجه به چالش‌های احصا شده به این سوال پاسخ دهد که سازمان‌های حفاظتی و سازمان‌های اطلاعاتی چه نقشی در نظام هشداردهی می‌توانند ایفا نمایند که زمینه ارتقای سیستم هشداردهی را فراهم آورد؟

فرضیه نگارندگان بر این مفروض مبتنی است که سازمان‌های حفاظت کننده و سازمان‌های اطلاعاتی در عمل تعریف مضیقی از هشدار ارائه می‌دهند که در آن سازمان‌های اطلاعاتی تنها وظیفه تولید هشدار و انتقال آن و سازمان‌های حفاظتی تنها به مصرف‌کنندگان هشدار مبدل شده‌اند. این درحالی است که نقش سازمان‌های حفاظتی و اطلاعاتی را می‌بایست غیر خطی و در چرخه مداوم رفت و برگشتی در نظام هشدار و زیر گام‌های آن معنا کرد.

روش پژوهش

این پژوهش بر اساس هدف، پژوهشی کاربردی است. راهبرد انتخاب شده برای این پژوهش، راهبرد مطالعات زمینه ای(داده بنیاد) است که داده‌های بدست آمده از طریق مصاحبه با خبرگان با روش تحلیل مضمون با استفاده از نرم افزار اطلس تی آی ۹ مورد تجزیه و تحلیل قرار گرفت. در این پژوهش از ۱۷ نفر از خبرگان اطلاعاتی، امنیتی –حفاظتی در دو مرحله مصاحبه انجام گرفت. مصاحبه‌های مرحله اول از نوع مصاحبه باز و در گام دوم مصاحبه نیمه ساختمند انجام شد. افراد مصاحبه شونده بر اساس روش گلوله برفی انتخاب شدند. خروجی‌های پژوهش در نشست تخصصی مورد بررسی قرار گفته و خروجی‌های پژوهش به تایید نظر خبرگان دانشی و روشی رسید.

مبانی نظری و پیشینه‌شناسی تحقیق

تعریف هشدار

قبل از پرداختن به چالش‌های سازمانی در نظام هشداردهی لازم است تعریف جامعی از هشدار

ارائه گردد تا با اتکا به این تعریف و نظام بر آمده از آن بتوان به بررسی چالش‌های پیش روی فرایند هشدار پاسخ مناسب ارائه داد. بررسی ادبیات اطلاعاتی و امنیتی نشان میدهد که تعاریف مختلفی از هشدار وجود دارد که بخش مهمی از این تعاریف پرداخته شده است.

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،۱۳۹۷:۴۶). هشدار اطلاعاتی درواقع مکانیسم احساس خطر و انجام اقداماتی برای رهایی از تبعات آن است.

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

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

هشـــدار اطلاعاتی محصول تلاش عمده تحقیقاتی و فرایند گسترده جمع‌آوری اطلاعات، نوعی برآورد احتمالی، قضاوت و داوری برای تصمیم‌گیرندگان و سیاست‌گذاران و کمک به آمادگی‌های مسئولیت اجرایی است. هشدار باید در خدمت نظام تصمیم‌گیری و با توجه به مجموع سلیقه‌ها و امکانات آن‌ها ارائه شود (حاجیانی،۱۳۹۰:۱۳۶).

هشـــداردهی اعلام و ابراز نشـــانه‌های بروز یک واقعه از سوی دســـتگاه‌های اطلاعاتی به مراجع ذی‌ربط است (صالحی و مدبری،۱۳۹۷:۹)

در تعریفی جامع‌تر «هشـــداردهی را فرایند شـــناخت هوشـــمندانه و اعلام بـــه هنگام علائم و نشـــانه‌های ضعیف ناشـــی از احتمال ظهور تدریجی پدیده مخاطره‌آمیز یا قریب‌الوقوع بودن رخ دادهای پرخطر برای مراجع ذی‌نفع (منافع نظام سیاسی یا سرمایه‌های نهادی و انسانی) است که باهدف پیش‌آگاهی متقاعدکننده برای واکنش پیشـــگیرانه تصمیم‌گیران و جلوگیری از غافلگیری منجر به شکست اطلاعاتی- امنیتی صورت می‌گیرد»(مزینانی،۱۳۹۷:۸۸).

بررســـی اولیه از تعاریف هشـــدار نشان می‌دهد که مفهوم هشدار وســـیع‌تر از اعلام‌خطر حمله تروریستی از سوی سازمان‌های اطلاعاتی و دریافت آن از سوی سازمان‌های حفاظتی است. هشدار دارای ماهیت پیچیده‌ای است که نه‌تنها خود سازمان‌های اطلاعاتی بلکه سایر سازمان‌های امنیتی،

1. The Mossad Website

حفاظتـــی و انتظامی را نیز درگیر مأموریت می‌کند. ازاین‌رو هشـــدار با توجه به کارکردی که قرار است ایفا نماید از یک مفهوم فراتر رفته و در چارچوب نظام تعریف می‌شود.

همان‌گونه که در بررسی تعاریف هشدار نشان داده شد، هشدار در یک فرایند پیچیده ایفای نقش می‌کند که یک‌سوی آن تولید هشدار است و سوی دیگر آن اقدام. به‌عبارت‌دیگر هشدار وقتی معنا می‌یابد که در زنجیره تولید هشدار، انتقال هشدار، به باور رساندن هشدار، سیاست‌گذاری پیش از وقوع و درنهایت گام اقدام بتوان آن را تعریف کرد(حاجیانی،۱۴۰۱).

تجزیه و تحلیل داده‌ها

تجزیه و تحلیل دا ده‌ها در پنج گام و یک مولفه مرکزی نظام هشـــدار مورد بحث و بررســـی قرار گرفته است که شامل ۱- تولید هشدار ۲- انتقال هشدار ۳- به باور رساندن هشدار ۴- سیاستگذاری ۵- آمادگی و اقدام ۶- بازخوردگیری و تجربه نگاری و مدیریت دانش اســـت که در ادامه به آنها پرداخته شده است. تمام مباحثی که در ادامه می‌آید از دل مصاحبه‌ها به دست آمده و نگارندگان صرفا تحلیل دادها را با رویکردی تشریحی بر عهده داشته‌اند.

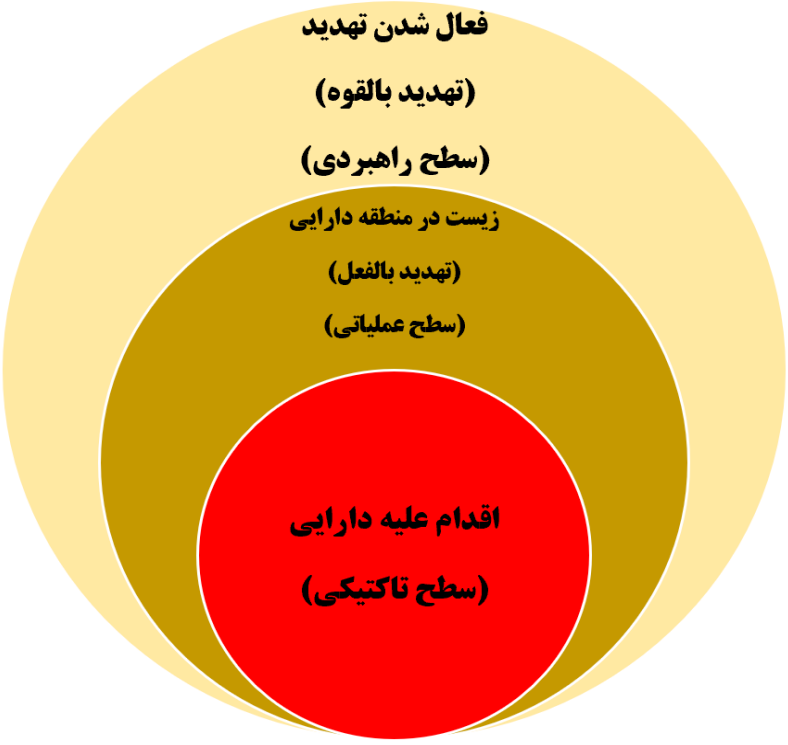
۱-تولید هشدار

تولید هشـــدار مهم‌ترین واصلی‌ترین گام در نظام هشـــداردهی اقدامات تروریستی است. تولید هشدار، ارتباط مستقیمی با فهم تهدید دارد به گونه‌ای که آگاهی از تهدید و فرایند رسیدن به این آگاهی منجر به تولید هشـــدار خواهد شـــد. بنابراین توجه به تولیدهشدار یعنی توجه به تهدید چو اینکه تولید هشدارها وابسته به تهدیدات بوده و متناسب با آن عمل می‌کنند.

در مواجه با تهدید ابتدا لازم اســـت احتمال وجود تهدید علیه دارایی[۱]، ســـپس نســـبت آن را با منطقه جغرافیایی دارایی و در نهایت نسبت آن را با نوع اقدام عملیاتی علیه دارایی سنجید. ازاین‌رو فرایند آگاهی از تهدید که درنهایت قرار اســـت به تولید هشـــدار ختم شود در نسبت سنجی مداوم بین عامل یا عوامل تهدیدکننده در تمامی سطوح با عامل یا عوامل تهدیدشونده در تمامی سطوح معنا می‌یابد. در شـــکل زیر این نســـبت نشان داده شـــده است که در ادامه نیز به تشریح هر یک از سطوح پرداخته می‌شود.

---

۱. دارایی می‌توان شخصیت‌ها، اماکن حساتی و حساس، اماکن پرجمعیت شهری، مقرهای نظامی، پاسگاه‌های مرزی، کلانتری‌ها و هر چیزی که ارزش مادی یا معنوی برای نظام جمهوری اسلامی داشته باشد را شامل شود.



منبع: مصاحبه با خبرگان. طراحی از نگارنده‌گان

۱-۱-فعال شدن تهدید

این سطح اولین سطح مواجهه با تهدید است که سطحی راهبردی است به این معنا که با قصد و نیت عامل تهدیدکننده ارتباط بر قرار می‌کند و نه سطوح برنامه ریزی و بسترسازی‌های عملیاتی آن. تهدید در این سطح تهدیدی بالقوه است و هنوز از دایره نیت فراتر نرفته است که تبدیل به برنامه عملیاتی برای اقدام علیه امنیت ملی کشور گردد. هر تهدیدی در صورت فعال شدن دارای سه بعد مهم است که توسط این سه بعد معنا می‌یابد. ۱- درک عامل یا عوامل تهدیدکننده ۲- درک عامل یا عوامل تهدید شونده(دارایی) ۳- درک حوزه تهدید.

الف) درک عامل یا عوامل تهدیدکننده: عامل یا عوامل تهدیدکننده می‌توانند هر کشور، سازمان و فردی باشند که نیت و بعضاً توان تهدیدکنندگی علیه دارایی را داشته باشند. هر عامل تهدیدکننده‌ای که درصد تهدید دارایی موردحفاظت است را می‌توان به‌عنوان تهدید بالقوه در نظر گرفت.

عوامل تهدیدکننده ممکن است از قبل وجود داشته و شناخت مناسبی از آن‌ها و اهداف انتخابی صورت گرفته باشـــد و یا اینکه گروه‌ها و عوامل جدیدی ایجاد شـــوند که در اهداف تروریستی خود دارایی‌های حفاظتی را مدنظر قرارداد باشـــند. بنابراین در این بخش از تعریف تهدید، شـــناخت عامل تروریســـتی و تغییر و تحول آن و یا ایجاد هر عامل تروریســـتی جدید بسیار مهم بوده و لازم اســـت اشراف مناســـبی از نیت و اهداف آن‌ها صورت گیرد. بر این اساس هر تهدیدکننده بالقوه‌ای که درنیات و اهداف خود اقدام علیه دارایی‌های موردحفاظت را برگزیده، لازم است به‌عنوان عامل فعال شدهِ تهدیدکننده مورد شناسایی قرار گرفته و به آن پرداخته شود.

ســـازمان‌های اطلاعاتی با توجه به میزهای تخصصی که برای هر یک از عوامل تهدیدکننده در نظر گرفته و یا رصد تحولات برای شناسایی عوامل تهدید جدید و نوپدید، نقش اصلی را در این گام ایفا می‌کند. با این حال سازمان حفاظتی نیز می‌تواند در این گام نقش ایفا نماید. نقشی که سازمان حفاظتـــی می‌تواند ایفا نماید تمرکز بر دایره و محدوده حفاظتی خود اســـت که ظهور تهدیدهای جدید در محدوده همســـایگان و افراد متردد به محدوده‌های حفاظتی و حتی نارضایتی کارکنان و .. را درک کـــرده و مـــورد رصـــد خود قرار دهد. از این رو در درک عامـــل یا عوامل تهدیدکننده، سازمان‌های اطلاعاتی عمدتا بر تهدیدکنندگان و شکل گیری و ایجاد آنها در سطح ملی، منطقه‌ای و بین‌المللی تمرکز دارند اما ســـازمان حفاظتی اختصاصا بر تهدیدکنندگان و شکل گیری و ایجاد آن‌ها در سطح سازمانی و محدوده‌های حفاظتی.

ب) درک عامل تهدید شونده:

عامل تهدیدشـــونده حیاتی و حســـاس درواقع همان دارایی است که طی ابلاغیه و دستور العمل از ســـوی نهادها و سازمان‌های حاکمیتی، ماموریت حفاظت از آن به سازمان‌های حفاظتی واگذار می‌گردد. این عامل تهدیدشـــونده در سطح حیاتی و حســـاس می‌تواند شخصیت‌های ارزنده یک کشـــور یا اماکن حیاتی و حســـاس و سایر موارد باشند که ارزش حفاظت در سطح بالایی را به خود اختصاص داده‌اند و تهدیدکنندگان به‌عنوان آماج حمله آن‌ها را انتخاب کرده‌اند.

در درک عامل تهدید شونده سازمان‌های حفاظتی نقش چندانی نداشته و سازمان‌های اطلاعاتی بیشترین نقش را در درک عامل یا عوامل تهدید شونده و شناسایی آنها برای قرار گرفتن در دایره حفاظت بر عهده دارند.

پ)درک حوزه‌های تهدید: درک حوزه تهدید به این معنی است اگر قرار باشد تهدیدی از سوی

عاملی علیه دارایی صورت گیرد به چه اشـــکالی احتمال دارد این تهدید اعمال شـــود. درک حوزه تهدید را می‌توان به شناخت اشکال(ابزارها و شیوه‌ها) اعمال تهدید خلاصه کرد. شناخت شیوه‌ها و ابزارهای اعمال تهدید علیه دارایی‌ها بخش مهمی از شناخت تهدید است. در شناخت حوزه تهدید می‌توان هر نوع تهدیدی که علیه دارایی‌های حفاظتی قادر است به کار گرفته شود، فارغ از عامل تهدیدکننده موردبحث و بررسی قرارداد. با این وجود شناخت ابزارها و شیوه‌های تهدید مرتبط با عوامل تهدیدکننده از اولویت بالایی برخوردار است. چراکه هر گروه تروریستی برحسب توان نیروی انسانی، تکنولوژیکی و اطلاعاتی خود شیوه‌های متناسب با آن را برای اعمال تهدید به کار می‌گیرد.

در درک حوزه‌های تهدید، شـــرایط عکس شـــناخت عامل تهدید شونده صورت می‌گیرد. در این حوزه بیشترین نقش را سازمان‌های حفاظتی بر عهده دارند. سازمان‌های حفاظتی لازم است رصد دقیقی از شـــیوه‌ها و ابزارهای حوزه تهدید داشـــته و نســـبت به تحولات صورت گرفته در مرزهای دانشی این حوزه آگاهی کاملی کسب نمایند. سازمان‌های اطلاعاتی نیز با دسترسی به شبکه‌های تروریســـتی و عوامل آن می‌توانند نقش مکملی را در ارائه دانش موجود در این حوزه ایفا نمایند. یکی از تعاملات ضروری بین ســـازمان‌های حفاظتی و اطلاعاتی در این حوزه بررســـی‌های دقیق اقدامات تروریستی رخ داده و کسب تجارب حاصل از آن است.

آنچه در گام فعال شـــدن تهدید و درک مکانیســـم آن بسیارمهم است نقش‌آفرینی موثر هر دو سازمان اطلاعاتی و حفاظتی است. سازمان‌های اطلاعاتی در شناخت دارایی‌ها و عوامل تهدیدکننده و نیات و مقاصد آن‌ها نقش پررنگی دارند که عمدتا لایه‌های پنهانی تر تهدید را شـــامل می‌شـــوند و در مقابل ســـازمان‌های حفاظت کننده در شـــناخت شیوه‌های و ابزارهای اعمال تهدید که عمدتا لایه‌های آشـــکار را مد نظر داشـــته اگر چه از ابزارهای جمع آوری پنهان، فنی نیز در کنار ابزارهای آشـــکار بهره می‌گیرد. لذا از ابتدای شـــروع فرایند تولید هشدار می‌طلبد هر دو سازمان اطلاعاتی و حفاظتی هم‌افزایی‌هایی موثری باهم داشته باشند.

۱-۲ زیست در منطقه دارایی

در این گام لازم اســـت نســـبت تهدید با منطقه جغرافیایی ســـنجیده می‌شود. در این مرحله به نسبت سنجی نیات و توانایی‌های عملیاتی حریف در منطقه جغرافیایی که دارایی در آن قرارگرفته توجه می‌شود.

ســـؤالی که در اینجا مطرح می‌شـــود این است که آیا عوامل تهدیدکننده بدون امکان زیست در

محیط دارایی امکان عملیاتی کردن نیت خود را خواهند داشـــت یا خیر؟ اگر عوامل تهدیدکننده بخواهند نیت خود را علیه دارای موردحفاظت عملیاتی کنند لازم اســـت بسترهای این عملیات را فراهم آورند. زمینه‌ســـازی برای انجام هر نوع عملیاتی نیازمند زیســـت در محیط هدف است. این زیســـت ممکن اســـت فیزیکی و در برخی مواقع مجازی و فنی باشـــد. اما آنچه مهم است این است که بتوانند اطلاعاتی را در مورد هدف به دســـت آورده و عوامل و ابزارهای خود را برای انجام اقدام تروریستی هم‌مکان باهدف قرار دهند.

در این گام در کنار نقش ســـازمان‌های اطلاعاتی، ســـازمان‌های حفاظتی نیز نقش پررنگی ایفا کرده و در همبستگی کامل باهم قرار دارند. به‌گونه‌ای که با حذف هر یک از این دو آسیب جدی بر فرایند تولید هشدار ایجاد خواهد شد. در گام‌های قبلی برآورد تهدید با تمرکز بر عوامل تهدیدکننده صورت می‌گرفت. با شـــناخت و اشرافی که به عوامل تهدیدکننده ایجاد می‌شد درنهایت شناختی نســـبت به نیات و اهداف عوامل تهدیدکننده صورت می‌گرفت؛ این مسیر نگاهی بالا به پایین دارد که ابتدا تهدید شناسایی‌شده و آنگاه نسبت آن با دارایی سنجیده می‌شود. اما در وجه دیگر که در محیط دارایی و با تمرکز بر آن انجام می‌پذیرد، برآورد تهدید از پایین به بالا انجام می‌شود. در این مسیر برآورد تهدید به‌جای تمرکز بر عامل یا عوامل تهدیدکننده، بر دارایی یا به‌عبارت‌دیگر به عامل تهدیدشـــونده متمرکز اســـت و هر داده‌ای که می‌تواند نشانه‌ای از ظهور و بروز تهدید علیه دارایی باشد مدنظر قرار می‌گیرد. در این مسیر بیشتر به محیط‌زیست دارایی تمرکز می‌شود و داده‌ها در بستر سازمان حفاظت کننده و حفاظت شونده تولید و معنا دهی می‌شوند.

درواقع در مســـیر برآوردی از بالا به پایین از داده‌ها برای یافتن هدف بهره گرفته می‌شـــود اما در مسیر برآوری از پایین به بالا از هدف برای یافتن داده‌ها بهره گرفته می‌شود. این دو مسیر مکمل یکدیگر هســـتند و می‌توانند در معنا دهی به تهدید و درنتیجه تولیدهشـــدار کارآمد، بســـیار مؤثر باشند.

متناســـب با این دو مســـیر سؤالاتی که برای ســـازمان‌های اطلاعاتی و حفاظتی ایجاد می‌شود نیز دوســـویه خواهد بود. ســـازمان‌های حفاظتی می‌بایست به این سؤال پاسخ دهند که اگر عوامل تهدیدکننده فعال‌شده در گام قبلی بخواهد علیه دارایی موردحفاظت اقدامی انجام دهد قبل ازآن چه زمینه‌سازی‌هایی لازم است در محیط دارایی انجام دهد؟ در مقابل سازمان‌های اطلاعاتی باید به دنبال پاسخ به این سؤال باشند که اگر قرار باشد عامل یا عوامل تهدیدکننده فعال‌شده در گام قبلی بخواهند اقدامی انجام دهند چه بسترســـازی‌های در حال شـــکل‌گیری است؟حال اگر جواب‌های

این دو سؤال هم‌زمان موردبررسی قرار گیرند می‌توانند اطلاعات ارزشمندی در مورد فعالیت‌های عوامل تهدیدگر به دست آورند که نقش مهمی در تولید هشدار در سطح عملیاتی ایفا می‌کند.

۱-۳ اقدام علیه دارایی

در این مرحله نسبت تهدید با مرجع حفاظتی مدنظر موردبررسی قرار می‌گیرد. در این سطح لازم است به دنبال پاسخ به این سؤال بود که اگر عامل تهدیدکننده بخواهد اقدامی علیه دارایی مدنظر انجام دهد این اقدام را کی، کجا، توسط کی، و چگونه انجام خواهد داد. سطح پاسخ به این سؤال کاملاً راهکنشی است و نیازمند داشتن اطلاعات دقیقی است تا بتوان به این سؤالات پاسخ داد. این سطح معمولاً حساست بالایی داشته و به دلیل ماهیت پنهانی و تعداد عاملین محدود در اقدامات تروریستی، رسیدن به پاسخ از سطح پیچیدگی‌های بالایی برخوردار بوده و اشراف اطلاعاتی بالایی را می‌طلبد.

سؤالی که برای سازمان‌های اطلاعاتی در سطح راهکنشی مطرح می‌شود این است که اگر عوامل تهدیدکننده دارایی با توجه به دو گام قبلی بخواهند اقدام خود را عملیاتی کند این قدام را توسط کی، چه زمانی، کجا و چگونه قرار است انجام دهند؟ پاسخ به این سؤال نیازمند نفوذ به لایه‌های تصمیم‌گیری و هدایت عملیاتی در گروه‌های تروریستی است و ازاین‌رو فعالیتی کاملاً اطلاعاتی است. در برخی از موارد ممکن است داده‌هایی از برخی سؤالات چهارگانه بالا توسط عوامل انسانی به سازمان‌های اطلاعاتی رسیده باشد اما در چنین شرایطی بازهم سؤالات بی‌پاسخ بسیاری ممکن است وجود داشته باشد که بدون پاسخ بماند. ازاین‌رو سازمان‌های اطلاعاتی لازم است تقاطع‌گیری‌های مکرری در طول فرایند تولید هشدار انجام دهند تا بتوانند برخی از پازل‌های اقدام تروریستی را تا حدودی آشکار سازند.

سؤالی که سازمان حفاظت شوند در کمک به این سطح می‌تواند از خود بپرسد این است که اگر عوامل تهدیدکننده مراجع حفاظتی با توجه به دو گام قبلی بخواهند اقدام خود را عملیاتی کند چه نشانه‌هایی دال بر اقدام از سوی عاملین می‌توان در محیط مشاهده کرد؟ در اینجا ممکن است حتی تولید هشدار مستقیماً توسط سازمان حفاظتی تولید شود.

سه گام طی شده نشان می‌دهد که تولید هشدار نیازمند هماهنگی و هم‌افزایی برون‌سازمانی به‌ویژه بین سازمان‌های حفاظتی و اطلاعاتی است تا از این طریق بتوان به تولد هشدار کارآمد دست‌یافت.

۲- انتقال هشدار

انتقال هشدار بسته به اینکه قبل از شروع اقدامات تروریستی است یا حین شروع حمله تروریستی و همچنین بسته به اینکه هشدار درون‌سازمانی یا برون‌سازمانی است، نقش‌ها و وظایف مختلفی را بین سازمان‌های اطلاعاتی و حفاظتی در انتقال هشدار نشان می‌دهد. هشدارهای قبل از شروع یک اقدام تروریستی با هشدارهای حین اقدام تروریستی نیازمند سرعت و مسیر انتقال متفاوتی است لذا نقش‌ها و وظایف متفاوتی را برای سازمان‌ها ایجاد می‌کند که در زیر به آن پرداخته می‌شود.

۲-۱هشدار قبل از وقوع اقدامات تروریستی

هشدار قبل از وقوع اقدام تروریستی مبتنی بر عدم قطعیت است. اگر این عدم قطعیت به‌تنهایی مدنظر قرارگرفته و به سایر مؤلفه‌های هشدار در گام تولید هشدار توجهی صورت نگیرد، هشداردهی از کارکرد خود خارج‌شـــده، آنگاه توانایی ایجاد آگاهی و جلوگیری از غافلگیری را از دســـت خواهد داد. دلیل اصلی این موضوع به هزینه‌هایی برمی‌گردد که با هر بار هشدار وقوع اقدامات تروریستی بر سازمان‌های حفاظتی و امنیتی بار می‌شود.

هشـــدار برای ســـازمان‌های حفاظت کننده نیازمند نیروی انسانی بیشتری است. در شرایطی که سازمان‌ها در اجرای مأموریت روزانه خود با کمبود نیرو مواجه باشند آنگاه نیاز بالای نیروی انسانی در شرایط اعلام هشدار باعث افزایش فاصله کمبود نیروی انسانی می‌گردد. افزایش کمبود نیرو باعث می‌گردد به نیروها فشـــار مضاعفی آورده شـــده، فرسودگی و عدم کارایی نیروها را تشدید کرده و در مواردی نیز زندگی خانوادگی آن‌ها را تحت‌الشعاع مأموریت قرارداده و چالش آفرین باشد. همچنین هشـــدار برای سازمان حفاظت کننده نیازمند وجود هزینه‌های اضافی برای خرید برخی تجهیزات، اقامت نیروها و هزینه‌های جانبی ازجمله تهیه غذا تا سوخت خودروها و... را در برمی‌گیرد.

حال اگر در تولید هشـــدار دقت کافی صورت نگیرد و با چالش‌های مطرح‌شـــده عجین شده و در ادامه به‌دفعات متعدد تکرار گردد آنگاه حساســـت‌های اعلام و عدم اعلام هشـــدار را بالا خواهد برد. ازاین‌رو در این بخش که به انتقال هشدار اقدام تروریستی قبل از وقوع آن پرداخته می‌شود با فرض اینکه گام اول (تولید هشـــدار) به‌درســـتی طی شده بیان می‌گردد. چو اینکه اگر گام اول به‌درستی طی نشود هر اهتمامی در گام دوم و گام‌های بعدازآن به شکست منتهی خواهد شد.

در ادامه گام انتقال هشدار با توجه به دو بعد درون‌سازمانی و برون‌سازمانی موردبررسی قرارگرفته و نقش سازمان‌های اطلاعاتی و حفاظتی نیز در هر یک از ابعاد تشریح می‌گردد.

۲-۱-۱ انتقال فرا سازمانی هشدار قبل از وقوع

اگرچه وظیفه اصلی تولید هشدار بر عهده سازمان‌های اطلاعاتی است اما همان‌گونه که در گام اول تشـــریح شد سازمان‌های حفاظتی نیز در تولید هشـــدار نقش ارزنده‌ای ایفا می‌کنند. گذشته از موضوع هماهنگی و هم‌افزایی فرا ســـازمانی در تولید هشـــدار، فرایند طی شده برای رسیدن به هشـــدار نیز طولانی و بســـیار پیچیده بوده و نیازمند دقت نظر ویژه‌ای است. از این مقدمه کوتاه و بررسی‌های صورت گرفته در حوادث تروریستی می‌توان نتیجه گرفت که عمده چالش‌های موجود در گام انتقال هشدار به سبب ضعف در گام تولید هشدار رخ‌داده است و نقش انتقال هشدار در این میان کمرنگ بوده است درنتیجه به نظر می‌رسد تقلیل علل شکست‌های رخ‌داده در برابر حملات تروریستی به اعلام یا عدم اعلام هشدار بیش از اینکه موضوعی علمی باشد جنبه ظاهری دارد.

بااین‌وجود برای نیل به انتقال هشـــدار مطلوب لازم اســـت برخی موارد موردتوجه قرار گیرد که در ادامه به برخی از این موارد که دارای تکرارپذیری بالاتری بوده‌اند موردبررسی قرار می‌گیرند.

یکی از موارد مهم این است که مبدأ انتقال‌دهنده هشدار و مقصد دریافت‌کننده هشدار مشخص باشد. اینکه مجاری مختلفی و بعضاً توسط افراد مختلفی هشدار اطلاعاتی صادر می‌شود سازمان‌های حفاظت کننده را با سردرگمی مواجه ساخته و مانع از تصمیم‌گیری و برنامه‌ریزی مناسب می‌گردد. ســـازمان‌های اطلاعاتی و امنیتی اگر بخواهند جدا از هم و به‌صورت جزیره‌ای و در مواردی بدون تقاطع گیری‌ها هشدار اطلاعاتی صادر نمایند قطعاً نمی‌توان توقع عملکرد و پاسخ مناسبی از سوی سازمان حفاظت کننده به این مسیرهای متعدد داده شود. از سوی دیگر دریافت‌کننده هشدار نیز در برخی مواقع به‌درستی مشخص نیست و در عرصه عمل مشاهده می‌گردد هشدارهای تولیدشده به بخش‌های مختلف و بعضاً افراد مختلفی در ســـازمان حفاظت کننده منتقل‌شـــده است. لذا لازم اســـت در انتقال هشدار هم انتقال‌دهنده هشـــدار مرجع واحدی باشد و هم دریافت‌کننده هشدار بخش واحدی در ســـازمان‌های حفاظتی باشد. این کار باعث می‌گردد وظایف هر بخش به‌درستی تفکیک‌شـــده و متولیان امر نتوانند به‌راحتی بابیان الفاظـــی مانند «ما گفته بودیم»، «ما نامه زده بودیم» از زیر بار مســـئولیت‌های محوله شـــانه خالی کرده و سلب مســـئولیت نمایند. عدم وجود مراجع صدور و دریافت هشـــدار در برخی مواقع باعث می‌گردد هشـــدار در گام تولید باقی‌مانده و در مسیر انتقال قرار نگیرد. تولید هشدار با هر ظرافت و ارزشی که باشد در صورت عدم انتقال آن هیچ کارکردی نخواهد داشت.

مؤلفه دیگر تعدد بالای هشـــدارهای صادرشـــده اســـت. همان‌گونه که بیان شـــد هر نوع اعلام

هشـــداری نیازمند پاســـخ است و اگر تعدد اعلام هشدارها بالا برود آنگاه سازمان حفاظت کننده را به ســـمت روزمرگی و نیروها را به‌سوی بی‌توجهی به هشـــدارها سوق می‌دهند. این موارد معمولاً درزمانی رخ می‌دهند که تولید هشدار به‌درستی در مسیر خود پیش نرفته باشد.

نکته دیگر هدفمند بودن انتقال هشدار است. هشدار آگاه‌سازی امنیتی نیست که هر نوع هشداری برای هر رده‌ای را به‌عنوان هشـــداری به ســـایر رده‌های غیر مرتبط هم انتقال داد. هشداردهی در برخی مواقع مربوط به رده خاص می‌گردد درحالی‌که آن هشـــدار به‌تمامی رده‌ها ارســـال می‌شود و ازآن‌رو فاقد دریافت‌کننده مناســـبی اســـت. لذا لازم است تناســـبی بین ماهیت دارایی و هشدار انتقال‌یافته وجود داشته باشد.

همچنین هشدار، اطلاع‌رسانی امنیتی هم نیست، در برخی مواقع اطلاعات بسیار دقیق و کاملی از نفرات و تجهیزات همراه عاملین تهدیدکننده بیان می‌شـــود که این نوع اطلاعات در وهله اول این مطلب را در ذهن گیرنده هشـــدار ایجاد می‌کند که با این اطلاعات دقیق چرا تا به آلان اقدام به دستگیری و انهدام این تیم نشده است. یا اینکه ممکن است اقدام شده و این هشدار صرفاً وجه اطلاع‌رســـانی به خود گرفته اســـت. این موارد نیز عمدتاً به دلیل ضعف در مسیر تولید هشدار رخ می‌دهند که عمدتاً نتایج آن در گام انتقال هشدار خود را نشان می‌دهد.

۲-۱-۲ انتقال درون‌سازمانی هشدار قبل از وقوع

هر هشداری که به سازمان‌های حفاظتی می‌رسد انتهای فرایند هشدار نیست بلکه در دل سازمان حفاظت کننده شـــروع فرایندی‌های جدیدی را می‌طلبد که لازم اســـت متناسب با سطح هشدار پاســـخ متناســـبی هم در نظر گرفته شود. ازاین‌رو لازم است در انتقال درون‌سازمانی هشدار قبل از وقوع نیز برخی نکات موردتوجه قرار گیرد. مســـیر انتقال هشـــدار در درون سازمان، نحوه انتقال، توان بازخورد گیری، سرعت انتقال و اطمینان از دریافت هشدار نمونه‌هایی از مواردی است که در ادامه به آن‌ها پرداخته می‌شود.

مســـیر انتقال هشـــدار: مســـیر انتقال هشـــدار در درون ســـازمان، زنجیـــره‌ای از گیرنده‌ها و دریافت‌کننده‌های هشـــدار را شـــامل شود که هر یک بر اساس وظیفه مأموریتی خود لازم است به فرایند انتقال هشـــدار ادامه داده و هم‌زمان اقدامات متناســـب با سطح هشدار را نیز در دستور کار خود قرار دهند.

تعدد مراجع انتقال دهنده هشـــدار در درون ســـازمان‌های حفاظتی و حراســـتی نیز می‌تواند

مسیرهای موازی و نامشخصی از انتقال هشدار را ایجاد نماید. ازاین‌رو نیاز است در خود سازمان‌های حفاظتی نیز واحد مرجعی به‌عنوان مرجع اصلی انتقال هشدار مشخص گردد.

اینکه در هر انتقال و دریافتی چه الزاماتی برحسب نوع هشدار باید صورت گیرد نیازمند طرح مباحث دیگری است که برحسب کفایت جزئی در گام اجرا به آن پرداخته می‌شود. در اینجا بیشتر تمرکز بر سلسله‌مراتب انتقال هشدار است. البته باید دقت داشت همان‌گونه که بیان شد سلسله‌مراتب انتقال هشدار در برخی هشدارها نیازمند فراتر رفتن از مسیر سلسله مراتبی است که به‌سرعت به اطلاع نیروهای رده‌های حفاظتی برسد.

موضوع دیگر در انتقال هشدار به نحوه انتقال هشدار برمی‌گردد. اگر قرار است هشدار در نظام جامعی تعریف شود که گام‌های تعریف‌شده در آن به‌هم‌پیوسته بوده و بر هم اثرگذار باشند آنگاه نحوه انتقال هشدار نیز اهمیت ویژه‌ای پیدا می‌کند. به‌عنوان‌مثال اگر نحوه انتقال هشدار در اغلب موارد توسط تابلو اعلانات به نیروها اطلاع‌رسانی شود طبیعی است که این هشدار در مسیر انتقال از فرایند نظام هشدار خارج‌شده و جنبه خبررسانی صرف به خود می‌گیرد؛ چراکه مقصد مشخصی برای رسیدن هشدار در نظر گفته نشده است. در این شرایط هشدارها مانند اخباری برای اطلاع کلیه نیروها همانند سایر خبرها قلمداد می‌شود که جایی جز نصب در تابلو اعلانات نداشته است. هشداری که منتهی به نصب در تابلو اعلانات شود یعنی انسداد مسیر هشداردهی که در آن، گام‌های بعدی نظام هشدار جایگاهی ندارد. این نحوه از انتقال و موارد مشابهی چون نامه‌نگاری‌ها و جلساتی که الزامی برای افراد در مسیر پاسخ‌گویی به هشدار ایجاد نکند نمی‌تواند نحوه انتقال مناسبی برای هشدار باشد.

سرعت انتقال نیز از مواردی است که باید در انتقال هشدار مدنظر قرار گیرد. برخی هشدارها راهکنشی بوده ازاین‌رو لازم است سرعت انتقال بالاتری داشته و تصمیم‌گیری برای آن با سرعت بیشتری صورت گیرد. در مقابل برخی دیگر از هشدارها از جمله هشدارهای راهبردی الزامی به‌سرعت انتقال بالایی ندارد زیرا بسترسازی‌های لازم برای پاسخ‌گویی به آن زمان‌بر بوده و نیازمند طی کردن فرایندهای مختلف است. ازاین‌رو لازم است برحسب نوع هشدار سرعت انتقال مناسب با آن نیز در نظر گرفته شود.

اطمینان از دریافت هشدار: با رعایت تمامی موارد در انتقال هشدار لازم است درنهایت از دریافت هشدار توسط رده‌های عملیاتی اطمینان حاصل آید. هر نوع اشکالی در مسیر هشداردهی درنهایت منجر به بازماندن نیروها از دریافت هشدار می‌شود. عدم دریافت هشدار و یا عدم اطمینان از دریافت هشدار به‌منزله قطع ارتباط هشدار در بدنه سازمان است.

این بخش از نظام هشـــداردهی دهی صرفاً در سازمان حفاظت کننده مطرح می‌شود و درنتیجه تمامی وظایف محوله در این بخش به سازمان حفاظت کننده برمی‌گردد و سازمان‌های اطلاعاتی نقشی در انتقال درون‌سازمانی هشدار قبل از وقوع ایفا نمی‌کنند.

۲-۲ انتقال درون سازمانی هشدار در زمان حمله

در زمان شـــروع حمله تروریســـتی لازم است سامانه‌های اعلام هشـــدار سریع در کل مجموعه حفاظتی وجود داشـــته باشـــد تا در ثانیه‌های اول تمامی نیروهـــای حفاظتی از وضعیت به وجود آمده اطلاع یافته و به‌ســـرعت وارد مرحله مقابله‌ای شـــوند. در این وضعیت ایجاد هر نوع مســـیر سلسله مراتبی به‌شدت به فرایند انتقال هشدار آسیب جدی وارد کرده و فرایند مقابله را با چالشی اساســـی روبرو می‌کند. ازاین‌رو انتخاب ابزار اطلاع‌رســـانی بســـیار مهم است. تعبیه زنگ خطر در چنین مجموعه‌هایی ضرورتی انکارناپذیر اســـت. عدم وجود چنین سامانه‌هایی باعث افزایش زمان اطلاع‌رسانی و درنتیجه افزایش شدت غافل‌گیری و زمان‌بر شدن سد رخنه و نفوذ را در پی دارد که هر یک می‌توانند هزینه‌های مقابله با حمله تروریستی را به‌شدت تغییر دهند.

به دلیل اینکه زنگ خطر درصدد اطلاع همگانی از حادثه رخ‌داده اســـت و از طرفی اطلاع کامل از نوع حادثه و جنبه‌های دیگر تهدید در ثانیه‌های ابتدایی مشـــخص نیســـت. لذا اگر در طراحی سیســـتم‌های زنگ خطر بتوان شـــرایطی را ایجاد نمود که برحســـب میزان افزایش اشراف به نوع حادثه، با تغییر در نوع زنگ‌ها و هشـــدارها اطلاعات بیشـــتری از نوع حادثه به همه نیروها رســـاند حائز اهمیت بالایی اســـت. افزایش داده‌ها و تغییر در میزان اطلاعات نیروهای امنیتی و حفاظتی نقش مهمی در نوع آرایش نیروها و بهره‌گیری از تجهیزات حفاظتی و سرعت مقابله خواهد داشت.

در طراحی زنگ‌های خطر لازم است علاوه بر اطلاع‌رسانی به کارکنان، برخی از اقدامات حفاظتی با شـــروع زنگ خطر به‌صورت سیستمی و هوشـــمند اجرا شوند مانند بسته شدن برخی درب‌ها و ... در اینجا اقدامات حفاظتی که ممکن اســـت توســـط ســـامانه زنگ خطر صورت گیرد لازم است در تعاملی تنگاتنگ با هشـــدارهای راهبردی، عملیاتی و راهکنشـــی صورت گرفته و متناسب با آن به‌روزرســـانی شوند. چراکه اگر کارکرد سیستم‌های زنگ خطر با تهدیدات روز تغییر نیابند چه‌بسا خود این موارد به ایجاد آسیب‌پذیری بیشتر منجر شوند.

این نوع هشـــدار زمانی تولید می‌شـــود که حمله شروع‌شده و تمامی فعالیت‌ها در حوزه سازمان حفاظت کننده در حال انجام بوده ازاین‌رو نقش ســـازمان اطلاعاتی در آن کمرنگ اســـت. آنچه در

اینجا مطرح است افزایش سرعت‌بالای انتقال هشدار و آگاهی نسبت به حادثه رخداده برای انجام واکنش‌های به‌موقع و مقابله‌ای است.

۲-۳ انتقال فرا سازمانی هشدار در زمان حمله

درزمانی که حمله تروریستی رخداده است لازم است به‌سرعت هشدار حمله تروریستی به سایر یگان‌های عملیاتی و پشتیبانی، یگان‌های معین و سازمان‌های خدماتی، درمانی، آتش نشانی و ... انتقال یابد. این امر علاوه بر افزایش سرعت مقابله باعث می‌گردد در مواردی که معمولاً اقدامات تروریستی هم‌زمان علیه دارایی‌های مختلفی انجام می‌گیرد اطلاع به سایر یگان‌های حفاظتی نیز صورت گیرد. آنچه در اینجا مدنظر است خارج شدن از مدار سلسله مراتبی و اعلام هوشمند و آنی آن به سایر یگان‌های حفاظتی توسط سامانه‌های هشدار منطقه‌ای و ملی است. هر نوع سلسله مراتبی در مسیر انتقال هشدار حمله تروریستی به‌مثابه از دست دادن زمان طلایی آگاهی از حمله تروریستی است. بنابراین سرعت انتقال به‌شدت مهم است و این سرعت انتقال، زمانی می‌تواند به‌درستی کارایی خود را داشته باشد که از مسیر اعلام سلسله مراتبی خارج‌شده و وارد مدار هوشمند اطلاع‌رسانی شود.

در این نوع هشدار نیز اگرچه موضوع هشدار فرا سازمانی مطرح است اما نقش پررنگ را سازمان‌های حفاظتی دارند چراکه با وقوع حمله تروریستی، از سوی سازمان‌های حفاظتی به سایر سازمان‌ها اطلاع‌رسانی صورت می‌گیرد. در این بخش سازمان‌های اطلاعاتی می‌توانند با اولین اطلاعی که از حمله تروریستی صورت گرفته به دنبال عقبه پشتیبانی و برنامه‌ریزی کننده حمله باشند تا بتوانند عوامل را شناسایی کنند. بااین‌وجود سرنخ یابی بعد از عملیات و حتی شروع عملیاتی مسیر متفاوتی از تولید هشدار را در پی دارد که ممکن است درنهایت برای سایر حملات برنامه‌ریزی‌شده سرنخ‌های مهمی باشد اما برای حادثه رخداده هشدار کارآمدی در پی نخواهد داشت.

۳- به باور رساندن هشدار

به باور رساندن هشدار نزد رده‌های عملیاتی نقطه ثقلی است که می‌تواند بنای هشدار را با این فرض که هشدار در مسیر درستی تولیدشده باشد تا مسیر رسیدن به مقصد پیش ببرد. ازاین‌رو

پذیریش و باور به وجود تهدید با صرف اعلام آن بسیار متفاوت است. اعلام هشدار اگر نتواند به باور فرمانده و نیروها برسد، وارد عرصه سیاست‌گذاری و اقدام نیز نخواهد شد و تنها ممکن است در سطح برگزاری جلسات باقی‌مانده و مسیر نظام هشداردهی را منحرف سازد. به عبارت دیگر باور به وجود تهدید وقتی قابل‌قبول است که بتوان نشانه‌های سیاست‌گذاری و اقدامات پیشگیری از آن نیز در تاروپود مأموریت مشاهده گردد.

با توجه به اهمیت بسیار بالایی که موضوع ایجاد باور به هشدار در نظام هشداردهی دارد بااین‌وجود شکل‌گیری این باور با مشکلات متعددی روبه‌رو است که به برخی از این موارد در جهت رفع موانع نظام هشداردهی پرداخته می‌شد. در ادامه به برخی از مهم‌ترین این عوامل پرداخته می‌شود.

۳-۱ افزایش فاصله زمانی بین سطوح هشدار (راهبردی، عملیاتی و راهکنشی)

یکی از دلایلی که باعث عدم ایجاد باور به وقوع اقدام تروریستی می‌گردد ایجاد فاصله طولانی بین هشدار راهبردی تا وقوع اقدام تروریستی است. معمولاً هشدارهای راهبردی اعتبار زمانی بسیار بلندی دارند. این هشدارها ممکن است سال‌ها پابرجا بوده و تاریخ انقضایی را نتوان برای آن‌ها مشخص کرد. اگر اعلام‌کنندگان هشدار تنها به هشدار راهبردی اکتفا کنند این هشدارها به دلیل پایداری زمانی بالا معمولاً موردتوجه جدی نیروهای حفاظتی قرار نگرفته و باور لازم برای مقابله و.. را فراهم نمی‌آورد. لذا لازم است برای ایجاد باور به هشدار، بین سطوح هشدار (راهبردی و عملیاتی و راهکنشی) ارتباط معناداری هم به لحاظ محتوایی و هم به لحاظ زمانی ایجاد کرد. در چنین شرایطی تولیدکننده هشدار برحسب تغییر سطوح هشدار، باور به وقوع آن را در ذهن مخاطب تغییر داده و ذهن دریافت‌کننده را متناسب با سطح هشدار تنظیم می‌نماید. درست مانند سخنران ماهری که با تغییر تن صدا و لحن بیان و محتوای سخن مانع از خواب‌آلودگی مخاطب می‌شود.

ایجاد فاصله زمانی عمدتاً به دلیل هوشمندی بازیگران تروریستی رخ می‌دهد چراکه اصولاً تروریست‌ها بافهم آمادگی حریف، اقدامات خود را به حدی به تأخیر می‌اندازند که باور به اقدام به‌مرور به عدم باور تغییر کرده و سطح اقدامات حفاظتی نیز متناسب با عدم باور ایجادشده دچار تغییر عملی و مشهود گردد. این رفتارهای هوشمندانه را می‌توان در بسیاری از اقدامات تروریستی مشاهده کرد.

۳-۲ گذشته‌نگری

گذشـــته‌نگری نســـبت به تهدیدات و شباهت یابی ذهنی حوادث آینده به گذشته یکی از عوامل مهم در ایجاد عدم باور به وقوع اقدامات تروریســـتی اســـت. به هر میزان که نوع رخدادهای جدید با گذشـــته تفاوت بیشـــتری داشته باشد به همان میزان نیز باور به رخداد جدید می‌تواند با چالش بیشتری مواجه شود.

ســـازمان حفاظت کننده‌ای که ســـال‌ها جنس تجربیات تهدیدش عموماً انتظامی بوده؛ مانند: اعتـــراض، نارضایتی، درگیری‌های جزئی و تجمعات اعتراضی و کمتر با تهدیدهای امنیتی مواجه شـــده و اگر هم تهدید امنیتی در ذهن دارد بیشـــتر به گشـــته‌های دور برمیگردد؛ نمی‌توان انتظار مناسبی از باور به هشدار را در آن‌ها مشاهده کرد. عمده نیروها و فرماندهانی که سال‌ها ذهن خود را درگیر تهدید انتظامی کرده نه‌تنها در باور به تهدید قبل از بروز حمله تروریســـتی دچار ضعف هســـتند بلکه در صورت حمله تروریســـتی نیز از سرعت عمل کافی برخوردار نخواهند بود چراکه در وهله نخست هر اعلام‌خطری را ممکن است با تهدیدهای گذشته همسان‌سازی کرده و باور به حمله تروریستی را به اذهان خود متبادر نسازند.

۳-۳ احساس امنیت بیش‌ازحد

نبود تهدیدهای تروریستی در طولانی‌مدت علیه دارایی‌های موردحفاظت؛ اعتماد به سازمان‌های اطلاعاتی در خنثی‌ســـازی تهدیدات تروریســـتی و همچنین در برخی مواقع ارزیابی غیرواقعی از تـــوان بازدارندگی ســـازمان حفاظت کننـــده و درنهایت غلبه روزمرگی بر مأموریت ســـبب ایجاد احساس امنیتی در اذهان نیروهای حفاظتی می‌شودکه این حس امنیت زمینه باور به وقوع تهدید تروریســـتی را کاهش می‌دهد.اگر تا به امروز هیچ حادثه تروریســـتی در منطقه زیست دارایی رخ نداده؛ اگر نیروی حفاظتی تا به امروز با هیچ حادثه تروریستی مواجه نبوده و بعضاً روال مشخصی را به‌صورت متناوب تکرار نموده است؛ به معنای این نیست که در آینده چنین حوادثی پیش نیاید.

۳-۴ ضعف دانشی در مورد گروه‌های تروریستی و اقدامات آن‌ها

یکی از عوامل مهم در ایجاد ضعف دانشـــی را می‌توان در شـــکل‌گیری دو رویکرد مجزا در دو سازمان متفاوت برای مقابله با اقدامات تروریستی دانست. این تفکیک و تفاوت را می‌توان در غلبه رویکرد تدافعی در سازمان‌های حفاظتی و غلبه رویکرد تهاجمی در سازمان‌های اطلاعاتی مشاهده

کرد که باعث می‌گردد هر یک به بخشی از دانش شناخت داشته و در بخش دیگر با ضعف دانشی مواجهه شوند.

در رویکرد تدافعی اهداف احتمالی حمله تروریستی از قبل مشخص‌شده و برای حفاظت از آن‌ها، سازمان‌های حفاظتی را موظف به انجام پیشگیری‌های لازم ازجمله طرح ریزی‌های حفاظتی، اختصاص تجهیزات حفاظتی و غیره می‌کنند. این رویکرد کاملاً پدافندی است. به‌عبارت‌دیگر جانمایی نیروی حفاظتی-امنیتی در کالبد یک تروریست (تروریست چگونه می‌اندیشد) در بهترین حالت جای خود را به نیروی حفاظتی-امنیتی در کالبد یک مدافع (محافظ چگونه می‌اندیشد) می‌دهد که توجه بیشتر آن بر کاهش آسیب پذیری است.

در رویکرد دوم که رویکرد آفندی است به‌جای انتظار بروز تهدید برای مقابله با آن (اگر تهدیدی بروز کرد چه باید کرد) به جلوگیری از بروز تهدید توجه می‌شود. وظیفه اصلی در این رویکرد بر عهده سازمان‌های اطلاعاتی است. فعالیت‌های عمده در این رویکرد متمرکز بر شناسایی تهدید بوده و کمتر به آسیب‌پذیری دارایی‌ها توجه می‌شد.

ضعف عمده این نگرش که سازمان‌های اطلاعاتی بر تهدید تمرکز کرده و سازمان‌های حفاظتی بر آسیب‌پذیری، در این است که در آن فهم معادله وقوع یک اقدام تروریستی با چالش مواجه می‌شود. در احتمال وقوع یک اقدام تروریستی سه متغیر مهم نقش دارند که عبارتنداز: فهم تهدید، فهم آسیب‌پذیری و فهم هزینه فایده دشمن در اعمال تهدید. توجه به هر یک از این متغیرها و نادیده انگاشتن متغیر دیگر سبب درک ناقصی از فهم معادله وقوع اقدام تروریستی و در نتیجه زمینه ایجاد عدم باور به وقوع اقدام تروریستی را در پی خواهد داشت.

بنابراین باور به هشدار تولیدشده زمانی می‌تواند ایجاد شود که سازمان‌های حفاظتی یا مصرف‌کننده هشدار هم پای تولیدکننده هشدار حرکت کرده و در ذهنیت ایجادشده شریک باشد. این هم‌افزایی ذهنی و عملی نه‌تنها باور به تهدید قبل از وقوع اقدام تروریستی را در مسیر مناسب جهت سیاست‌گذاری سوق می‌دهد بلکه در ایجاد و عمق‌بخشی باور به حمله در زمان وقوع اقدام تروریستی را نیز نقش ارزنده‌ای دارد.

۴-سیاست‌گذاری پیش از آمادگی

سازمان‌های حفاظت کننده لازم است متناسب با هشدار دریافت شده سیاست‌گذاری مناسبی برای پیشگیری و مقابله با اقدامات تروریستی داشته باشند. برای رسیدن به این مهم لازم است

هشـــدار دریافت شـــده در قالب سناریو تهدید طراحی شود، متناســـب با سناریوهای طراحی‌شده نیازمندی‌هـــای پیشـــگیری و مقابلـــه در نظر گرفته و درنهایت با در نظـــر گرفته این دو مقدمه به سیاست‌گذاری پرداخته شود.

برای انجام هر یک از این مراحل لازم اســـت در عین توجه به هشـــدار دریافت شده، هم‌زمان به دو مؤلفه دیگر هم توجه شود. این دو مؤلفه عبارتنداز: برآورد آسیب‌پذیری از دارایی و طبقه‌بندی حفاظتی برای دارایی.

الف-برآورد آسیب‌پذیری

برآورد آســـیب‌پذیری علاوه بر این گام در گام نخســـت نیز انجام می‌گیرد؛ اما این دو برآورد تا حدودی باهم متفاوت هســـتند. آنچه باعث ایجاد تفاوت می‌شود بیشتر به نوع خروجی تولیدشده برمی‌گردد.

در گام نخســـت برآورد آســـیب‌پذیری به‌منظور تولید هشدار مورداستفاده قرار می‌گیرد. در گام نخست آسیب‌پذیری مفهومی مستقل است و الزاماً با تهدید معنا نمی‌یابد و الزامات سطح حفاظتی در آن کمتر موردتوجه قرار گیرد.

در مقابل در این گام برآورد آســـیب‌پذیری کاملاً مبتنی بر تهدید و درواقع هشـــدار دریافت شده انجام می‌گیرد. در اینجا برآورد آسیب‌پذیری یک‌سویه (بالا به پایین) بوده و به‌منظور ایجاد سناریو، احصا نیازمندی‌ها و سیاست‌گذاری انجام می‌پذیرد. از سوی دیگر لازم است طبقه‌بندی حفاظتی در این برآورد موردتوجه جدی قرار گیرد.در برآورد آســـیب‌پذیری بالا به پایین، مبنای شـــناخت آســـیب‌پذیری مبتنی بر برآورد تهدیدی است که از سوی سازمان‌های اطلاعاتی دریافت می‌شود. در مقابل در رویکرد پایین به بالا اصولاً تمرکز شناســـایی آســـیب‌پذیری نه بر اساس تهدید بلکه بر اساس دارایی صورت می‌گیرد که در اینجا برآوردهای صورت گرفته عمدتاً گذشته‌نگر بوده و مبتنی بر تجارب کسب‌شده در محیط انجام می‌شود.

ب- طبقه‌بندی حفاظتی

هر دارایی دارای سطح مشخصی ازلحاظ طبقه‌بندی حفاظتی است. هر چه دارایی دارای ارزش بالاتری باشد از سطح حفاظتی بالاتری نیز برخوردار است؛ لذا مؤلفه‌های اثرگذار و اثرپذیر با دقت بالاتری موردبررسی قرار می‌گیرند به‌عنوان‌مثال هر چه سطح طبقه‌بندی حفاظتی برای یک دارایی

بالا برود طبیعتاً توجه به سطوح آسیب‌پذیری نیز بیشتر می‌گردد. دارایی با سطح طبقه‌بندی حفاظتی حیاتی و حساس متفاوت از دارایی با سطح طبقه‌بندی حفاظتی مهم خواهد بود.

۴-۱ سناریونویسی بر مبنای هشدار جدید: بسیاری از هشدار به‌تنهایی نمی‌توانند مورد بهره‌برداری سازمان‌های حفاظتی قرار گیرند ازاین‌رو لازم است اقداماتی روی هشدارهای دریافت شده ایجاد گردد تا بتواند برای سازمان حفاظت کننده قابل بهره‌برداری باشد. یکی از گام‌های مهم در این مسیر ایجاد سناریو تهدید مبتنی بر هشدارهای دریافت شده است. در اینجا لازم است دوباره این نکته یادآوری شود که زمانی می‌توان برای هشدار تولیدشده سناریو نوشت که در قالب موارد مطرح‌شده در گام تولید هشدار باشد نه اینکه هر خبر و اطلاع را بدون تبدیل‌شده به هشدار و تعیین سطح آن (راهبردی، عملیاتی، راهکنشی) به‌عنوان هشدار قلمداد کرده و توقع سناریوسازی از آن را داشته باشیم.

ایجاد سناریو تهدید می‌بایست متناسب با ویژگی‌های محیطی یا به‌عبارت‌دیگر متناسب با محیط‌زیست دارایی انجم پذیرد. اشراف سازمان‌های حفاظت کننده به محیط خود باعث می‌گردد نوشتن سناریو تهدید به سازمان‌های حفاظت کننده محول شود. ازاین‌رو سازمان‌های اطلاعاتی نقش چندانی در این مرحله نخواهند داشت.

۴-۲ احصا نیازمندی‌های جدید مبتنی بر سناریو

سناریوهای تهدید جدید نیازمندی‌های جدیدی را می‌طلبد و این روند منجر به تغییر سیاست‌گذاری‌های پیشین و ورود به سیاست‌های جدیدی مقابله‌ای می‌گردد. در این گام متناسب با باوری که به سناریوهای احتمالی تهدید علیه دارایی‌ها ایجادشده است فرایند احصاء نیازمندی‌ها برای پیشگیری و مقابله با تهدیدهای احتمالی آغاز می‌شود. در این مرحله سؤالی که باید به آن پاسخ داد این است که اگر سازمان حفاظت کننده بخواهد به سناریو تهدید علیه دارایی پاسخ مناسب داده و از بروز تهدید جلوگیری نماید نیازمند چه چیزهایی است؟

در پاسخ به این سؤال، نیازمندی‌های مختلفی وجود دارد که به برخی از مهم‌ترین آن‌ها در ادامه پرداخته می‌شود

۱- طرح‌ریزی حفاظتی به‌روز: اگر قرار باشد سناریو تهدیدی علیه دارایی موردحفاظت اجرا شود لازم است در اولین گام طرح‌ریزی حفاظتی متناسب با نوع تهدید به‌روزرسانی شود.

۲-شناسایی امکانات و تجهیزات متناسب با تهدید: لازم است متناسب با سناریوهای احتمالی تهدید امکانات و تجهیزات متناسب با آن نیز وجود داشته باشد.

۳-شناسایی آموزش متناسب با تهدید: نیروهای حفاظت لازم است آموزش‌های متناسب با تهدید را طی کرده و نسبت به نوع تهدید و مقابله با آن شناخت کافی داشته باشند و غیره

۵-آمادگی و اقدام

گام آمادگی گامی است که نیازمند پذیرش باور به هشدار، همدلی، خلاقیت و انعطاف بالایی است. چراکه از یک‌سو تغییر در هر عرصه‌ای معمولاً با مقاومت همراه است. تغییر سبب خروج انسان‌ها از ناحیه راحتی می‌شود که به آن عادت کرده‌اند. ازاین‌رو برای بسیاری سخت است که تن به تغییر داده و رویه‌های گذشته خود را تغییر دهند. این درحالی‌که است که در کار حفاظت تغییر امری ضروری و اجتناب‌ناپذیر است و اگر به سمت سکون و مقاومت در برابر تغییر پیش رود به‌سرعت زمینه شکست در برابر تهدیدات را به دنبال خواهد داشت. لذا باور به تهدید یعنی همراهی و استقبال از تغییر برای آمادگی و مقابله با تهدید. مرحله باور مرحله‌ای است که به‌تمامی مراحل و ازجمله گام اقدام مستقیماً اثرگذار است. تا زمانی که فرایند هشداردهی به اقدام منجر نگردد هر فعالیتی بی‌نتیجه مانده و درنهایت نتیجه‌ای جز شکست در پی نخواهد داشت. گام اقدام به دلیل محدودیت منابع ازجمله هزینه‌های مالی و نیرو انسانی، به‌شدت تحت تأثیر نظرات فرماندهان سازمان‌های حفاظت کننده و مسئولین سازمان‌های حفاظت شونده دچار تغییر و تحول می‌گردد. اگر باور به تهدید به‌درستی در اذهان فرماندهان و مسئولین شکل نگرفته باشد به‌شدت گام اجرا را با چالشی اساسی روبرو خواهد کرد.

در گام آمادگی تمامی پیوست‌های تهیه‌شده برای رده‌های مختلف لازم است به اجرا درآمده و مبتنی بر زمان‌بندی مشخص پیش رود. اگر پیوستی برای تهیه امکانات و تجهیزات تهیه‌شده است لازم است در این گام بر اساس اولویت بندی، زمان‌بندی و هزینه‌های اختصاص‌یافته مشخص به اجرا درآید. اگر پیوستی برای آموزش نیروها تهیه‌شده است لازم است در این گام رده‌های آموزش نسبت به اجرای آموزش‌های مقرر اقدام نمایند و همین‌طور برای سایر پیوست‌هایی که تهیه‌شده است. یکی از موارد مهم در گام اقدام، آمادگی برای دریافت هشدارهای راهکنشی و عملیاتی است که این امر نیازمند اجرای زرم‌های یگانی متعددی است تا نوع واکنش‌ها و سرعت عمل در آن‌ها از زمینه خودآگاه خارج‌شده و درزمینه ناخودآگاه کارکنان سازمان حفاظت کننده قرار گیرد.

۶- بازخورد گیری، تجربه نگاری و مدیریت دانش

این گام خود مشـــتمل بر دو اقدام مهم اســـت ۱- بازخورد گیری و ۲- تجربه نگاری و مدیریت دانش. این دو اقدام در طول سایر گام‌ها نبوده و بیشتر در عرض گام‌های قبلی در جریان هستند.

۶-۱ بازخورد گیری

الزام وجود این مرحله به این دلیل است که لازم است در تمامی گام‌ها بازخورد گیری هم‌زمان صورت گرفته و اگر نیازمند اصلاح و تغییراتی درروند نظام هشداردهی است اصلاح گردد. در این گام به صورت مستمر به تقویت یا تضعیف تهدیدی که عامل ایجاد هشدار بوده توجه شده و متناسب با آن نظارت فعالی برای تمامی مجموعه‌ها صورت می‌گیرد. ســـوالی که در این بخش می‌بایســـت به آن پاســـخ داد این اســـت که متناسب با سطح هشدار اعلام شده، چه کسانی چه‌کارهایی در چه زمان‌هایی لازم بود انجام دهند و آیا انجام داده‌اند یا خیر؟

۶-۲ تجربه نگاری و مدیریت دانش

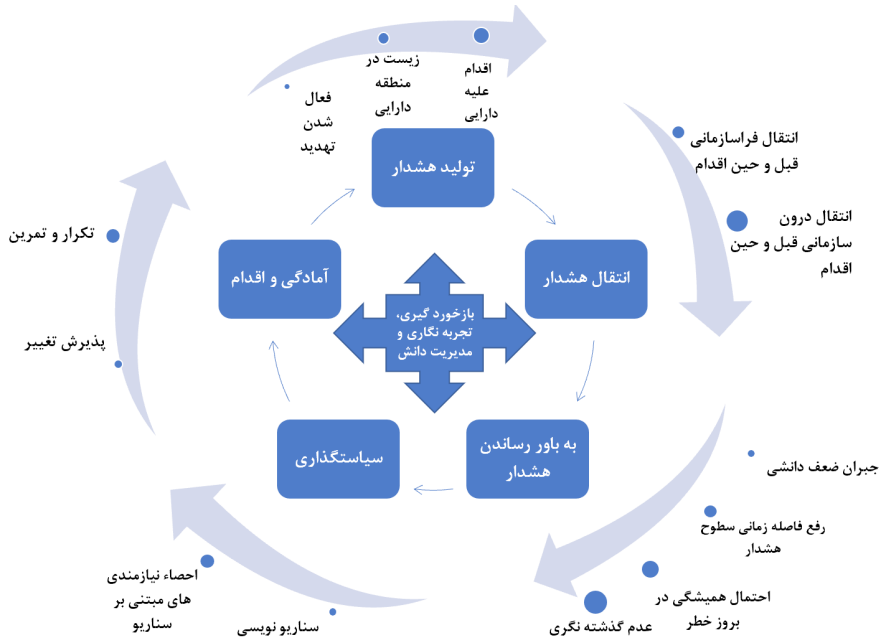
هر تجربه‌ای چه تجربه شکســـت و چه تجربه پیروزی و موفقیت در نظام هشـــداردهی می‌تواند تغییرات مهمی در فرایند و اجزای نظام هشداردهی ایجاد نماید. ازاین‌رو لازم است تمامی تجربیات مورد تجربه نگاری قرارگرفته و در نظام هشداردهی به کار گرفته شوند.

نتیجه‌گیری

اگر قرار باشد هشدار بتواند به جلوگیری از غافلگیری از حادثه تروریستی منتهی شود و کارنامه درخشانی را از خود بر جای گذارد لازم است فرایندهای درهم‌تنیده دررسیدن به هشدار هماهنگ و باهم به وظایف خود عمل کنند. ازاین‌رو اگر در هر یک از مراحل کوتاهی صورت گیرد این امر بر کل فرایند اثرگذار خواهد بود. لذا تمامی افراد و ســـازمان‌های تأثیرگذار بر نظام هشدار می‌بایست به این امر واقف باشـــند که هر نوع اعمال نظری خارج از فرایند خود و اعمال ســـلیقه‌های شخصی می‌تواند در صورت بروز هر حادثه تروریســـتی احتمالی اثرات جبران‌ناپذیری بر امنیت ملی کشور داشته باشد.

این پژوهش نشان می‌دهد که برخلاف تقسیم بندی هشدار به تولید کننده یا ارائه دهنده هشدار و مصرف کننده یا مشـــتری هشـــدار؛ اما واقعیت در حوزه هشداردهی اقدامات تروریستی پیچیده

تر از یک تقســـیم وظیفه دو گانه بوده اســـت. در تمامی گام‌های نظام هشـــداردهی هر دو سازمان حفاظتـــی و اطلاعاتـــی نقش‌های مهم و موثری بر عهده دارند که این وظایف عمدتا تکمیل کننده هم در مســـیر جلوگیری از غافلگیری اســـت. نتایج پژوهش نشان می‌دهد مسیر هشدار یک مسیر یکطرفه نیســـت و مدام در حال رفت و برگشـــت در چرخه نظام هشدار است و از سوی دیگر در هر یک از مراحل نظام هشـــدار، وظایفی در عرض هر مرحله ایجاد می‌شـــود که می‌بایست سازمان‌ها برای تقویت و اثر گذاری آن مرحله با هم و در عرض فرایندی طولی هشدار انجام دهند چیزی که در شکل زیر ترسیم شده است.



فهرست منابع

۱. حاجیانی، ابراهیم(۱۴۰۱). درس هشداردهی،دانشگاه جامع امام حسین(ع).

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

۳. صالحی، محمود، و محمد مدبری(۱۳۹۷). «چرخه بهینه هشـــدار در ســـازمان‌های اطلاعاتی-امنیتی (مؤلفه‌ها و شـــاخص‌ها).» فصلنامه پژوهش‌های حفاظتی_امنیتی دانشـــگاه جامع امام حسین (علیه‌السلام)، سال هفتم، شماره ۲۶، ۱-۲۶.

۴. صالحی، محمود، و ناصر مهدوی(۱۳۹۷). مجموعه مقالات مبانی نظری همایش هشـــداردهی اطلاعاتی- امنیتی، ۱۳۹۷، تهران: مرکز مطالعات و پژوهش‌های امنیتی.

۵. مزینانی، احمد(۱۳۹۷). «معماری ســـازمانی و هشـــداردهی» کتاب مجموعه مقالات معماری و الزامـــات هشـــداردهی، تهـــران: مرکـــز مطالعـــات و پژوهش‌های امنیتی، موسســـه چاپ و انتشارات.۷۹-۱۱۱

۶. مزینانـــی، احمد، و احمد ایمانی پور(۱۳۹۷). «فرایند هشـــداردهی اطلاعاتی-امنیتی.» کتاب مجموعـــه مقالات هشـــداردهی اطلاعاتی امنیتی، جایگاه و فرایند هشـــداردهی. تهران: مرکز مطالعات و پژوهش‌های امنیتی.

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