تدوین و ارائه‌ی الگوی ارزیابی تهدیدات، آسیب‌پذیری و تحلیل خطرپذیری زیرساخت‌های حیاتی با تأکید بر پدافند غیرعامل

حسن مشهدی* - کارشناسی ارشد مهندسی پدافند غیرعامل، دانشگاه صنعتی مالک اشتر؛ Paydar1357@gmail.com
سعید امینی ورکی - کارشناسی ارشد مهندسی پدافند غیرعامل، موسسه مهندسین مشاور طاها، قرارگاه سازندگی خاتم الانبیاء(ص).

تاریخ دریافت: ۹۴/۲/۱۵
تاریخ پذیرش: ۹۴/۷/۱۵

چکیده

ارزیابی تهدیدات و آسیب‌پذیری زیرساخت‌ها یکی از دغدغه‌های اصلی و همیشگی مسئولان حوزه امنیت در یک کشور است. این موضوع چنان مهم است که در بسیاری از موارد می‌تواند باعث کاهش چشمگیر آسیب‌پذیری‌ها شود یا پیامدهای یک تهدید را به حداقل ممکن کاهش دهد. در واقع ،توصیف و ارزیابی تهدید و خطرپذیری در زیرساخت‌های ملی، چارچوبی برای تحلیل و مدیریت خطرات مرتبط با حملات احتمالی علیه زیرساخت‌های حیاتی است. آنچه در این مقاله به دنبال آن هستیم، عبارت است از دستیابی به یک الگوی مناسب ارزیابی تهدیدات، آسیب‌پذیری و تحلیل خطرپذیری مطابق با شرایط و وضعیت تهدید در کشور.

در واقع، این مقاله به دنبال ارائه‌ی چارچوبی برای ارزیابی صحیح و دقیق تهدیدات، آسیب‌پذیری و خطرپذیری زیرساخت‌های حیاتی کشور با ملاحظات پدافند غیرعامل است، چرا که بر اساس راهبردهای دشمنان خارجی به ویژه آمریکا زیرساخت‌های اساسی یک کشور به عنوان اولین اهداف در تهاجم محسوب می‌شوند. آنچه در این مجال به آن پرداخته می‌شود، رویکردی جستجوگرانه به منظور تدقیق معیارهای دفاع غیرعامل و تلاشی برای یافتن ابزار و امکاناتی برای تبدیل مفاهیم و توصیه‌های کیفی به ضابطه‌های کمّی و قانونمند است. اگر دفاع غیرعامل به‌کارگیری اقدامات، تدابیر و تمهیداتی غیرمسلحانه به‌منظور مقابله با تهدیدات دشمن قلمداد شود، دو وجه این معادله، تهدید و تمهید در مرحله اول و چگونگی مقابله در مرحله بعدی باید مورد تحلیل و ارزیابی قرار گیرد.

واژگان کلیدی: *زیرساخت‌های حیاتی، آسیب‌پذیری، دارایی، پدافند غیرعامل، خطرپذیری.*

Develop and present a model for threat assessments, vulnerability and risk analysis of critical infrastructure with a focus on passive defense

Hasan Mashhadi*[1] Saeed Amini Varaki[2]

Abstract

Threat assessment and vulnerability of infrastructure have always been the main concerns of those responsible for security in a country. This issue is so important that in many cases can lead to a significant reduction of vulnerabilities or to minimize the consequences of a threat. In fact, describe and assess threats and risks in the national infrastructure, is a framework for analyzing and managing the risks associated with the possible attacks against critical infrastructure. Thus, this study seeks an appropriate model for the assessment of threat, vulnerability and risk analysis in accordance with the threatening situation in the country. The aim of this paper is to provide a framework for the precise assessment of threat, vulnerability and risk of critical infrastructures of the country with passive defense considerations in accordance with the strategies of the foreign enemies. In this perception, the critical national infrastructures are considered as the first targets of possible attacks. The approach of this paper is an investigative approach to achieve the passive defense criteria and trying to find tools and resources to transform concepts and recommendations qualitative and quantitative criteria. If the passive defense is defined as unarmed actions, contrivance and prepararion against of the external threats should be analyzed and evaluated.

Keywords: Critical infrastructures, vulnerability, property, passive defense, risk assessment.

1 M.Sc Passive defence Eng., Malek ashtar University of Technology, Tehran, Iran; Paydar1357@gmail.com
2 M.Sc Passive defence Eng., Taha Institute of Consultant Engineers, Khatam Al-Anbiya Construction Headquarters, Tehran, Iran.

ارزیابی تهدیدات و آسیب‌پذیری‌ها، یکی از دغدغه‌های اصلی و همیشگی مسئولان حوزه امنیت در یک کشور است. این موضوع چنان مهم است که در بسیاری از موارد می‌تواند باعث کاهش چشمگیر آسیب‌پذیری‌ها شود یا پیامدهای یک تهدید را به حداقل ممکن کاهش دهد. بر این اساس، هدف اصلی این مقاله پاسخ دادن به نیاز فعلی بسیاری از مدیران دستگاه‌های اجرایی کشور است که به دنبال پیاده کردن اصول و ملاحظات پدافند غیرعامل در مجموعه خود هستند. رسیدن به این مهم، نیازمند به‌کارگیری روش‌هایی است که بتواند ارزیابی و براورد صحیحی از وضعیت تهدیدات و آسیب‌ها در یک مجموعه ارائه دهد. در این زمینه اقداماتی صورت پذیرفته است، اما آنچه در بررسی‌های اولیه مشخص شد، حکایت از آن دارد که یک الگو یا چارچوب مدون و بومی شده‌ای که بتواند فهرستی از تهدیدات دشمن را پوشش دهد، وجود ندارد و آنچه اکنون ملاحظه می‌شود، غالباً ترجمه روش‌ها یا الگوهایی است که در خارج از کشور تدوین شده‌اند. از این منظر ، مقاله حاضر به دنبال ارائه‌ی روشی برآمد که در تمایز با الگوهای دیگر، محور را بر بومی شدن آن استوار گرداند. در واقع، نوآوری صورت گرفته در این تحقیق حول دو محور اصلی است که نخست تطبیق آن با شرایط و وضعیت تهدیدات در کشور ایران و دیگری کاربردی کردن آن به صورتی است که با استفاده از مباحث کیفی و توصیفی به دنبال کمّی کردن آن برای پیاده‌سازی در قالب‌های مهندسی و ریاضی است. اینکه اقدامات مؤثر علمی در همه‌ی زمینه‌ها به شاخص‌ها، معیارها و زمینه‌های مناسب و متناسب نیاز دارد، شرایط و بستری را برای مشخص و معلوم کردن حوزه‌های مؤثر فراهم می‌آورد. تعیین تهدیدات، مبنایی برای به‌کارگیری تمهیدات و تدابیری است که بعضاً بر حوزه‌های اقتصادی، اجتماعی، عملیاتی مجموعه‌های مختلف تأثیراتی متفاوت اعمال می‌کند. بنابراین، ضروری است که کلیه‌ی تهدیدات در مرحله‌ی نخست و سپس تهدیدات پایه با روش‌ها و شاخص‌های علمی شناسایی، تعریف، براورد، تجزیه و تحلیل، غربالگری و نهایتاً فهرست شود و به عنوان سند مبنای راهبردهای دفاع غیرعامل قرار گیرد.

بیان مسئله

توصیف و ارزیابی تهدید و ریسك در زیرساخت‌های ملی، چارچوبی برای تحلیل و مدیریت خطرات مرتبط با حملات احتمالی علیه زیرساخت‌های حیاتی است. ارزیابی تهدید و ریسك در زیرساخت‌های ملی شامل روش‌های تعیین، تحلیل، کمّی‌سازی و کشف ارتباطات میان ویژگی‌های است که مهاجم را به سمت هدف خاصی سوق می‌دهد و باعث تشخیص نقاط آسیب‌پذیر برای ارائه‌ی راهکارهای پدافندی خواهد بود (۱).

با توجه به اهداف حوزه پدافند غیرعامل و تجارب حاصل از پروژه‌ها و طرح‌های اجرا شده و در حال اجرا توسط مشاوران و محققان مرتبط، این موضوع کاملاً روشن می‌شود که ارزیابی تهدید و خطرپذیری در فرایند انجام مطالعات پدافند غیرعامل نقش بسزا و تعیین‌کننده‌ای را در هدایت طرح به سمت اهداف از پیش مشخص شده در راستای کاهش آسیب‌پذیری زیرساخت‌های ملی در کشور دارد. بنابراین، مسئله‌ی اساسی ما تطابق نداشتن جامع روش‌های علمی موجود با شرایط و طیف گسترده تهدیدات علیه ماست.

اهمیت و ضرورت تحقیق

ضرورت انجام این تحقیق ناشی از این واقعیت است که بررسی‌های انجام شده حاکی از نبود یک روش نظام‌مند مهندسی است که بتواند به‌طور کامل و جامع پوشش‌دهنده‌ی طیف وسیعی از تهدیدات متنوع باشد. با عنایت به اینکه ارزیابی‌ها باید به‌گونه‌ای باشد که فارغ از قضاوت‌های فردی و بر مبنای یک واقعیت استوار شود، اهمیت یک کار علمی بیش از پیش مشخص می‌شود. مسلماً هدف از شناسایی پیامدهای ناشی از تهدیدها، پایش و مقابله با آن است. در این خصوص هنگامی‌که صحبت از محدودیت‌های منابع پیش می‌آید تصمیم‌گیری در مورد اینکه کدام تهدید، اهمیت بیشتر و اولویت بالاتری دارد مشکل‌تر می‌شود.

روش تحقیق

برای رسیدن به اهداف مورد نظر هر تحقیق و پژوهش، استفاده از یك روش تحقیق علمی و نظام‌مند ضروری است. روش تحقیق مورد استفاده در این پژوهش «توصیفی- تحلیلی» است. بدین منظور، سعی می‌شود از روش‌های کمّی و کیفی به صورت توأمان استفاده شود و علاوه بر این، در گردآوری اطلاعات از روش‌های متداول مانند بررسی کتابخانه‌ای و اسنادی، جستجوی اینترنتی و روش پرسشنامه‌ای استفاده شده است.

روش گردآوری اطلاعات

برای گردآوری اطلاعات از روش‌های متداول مانند بررسی کتابخانه‌ای و اسنادی، جستجوی اینترنتی و روش پرسش‌نامه‌ای استفاده خواهد شد، اما به دلیل ماهیت موضوع، مبنا روش پرسش‌نامه‌ای قرار داده شده است و در کنار آن از دیگر روش‌ها برای تکمیل مطالب استفاده می‌شود. شایان ذکر است که در این تحقیق از طریق گزینش روش‌های مورد قبول و کاربردی، به بومی‌سازی و نهایتاً ارائه الگوی کاربردی ارزیابی در پدافند غیرعامل پرداخته خواهد شد.

جامعه آماری

از آنجا که گرایش به علم پدافند غیرعامل در سال‌های اخیر ایجاد شده است، تعداد متخصصان و صاحب‌نظران این رشته کم‌شمارند. از این رو، تعداد افرادی که در این رشته تخصص دارند یا صاحب‌نظرند از سایر رشته‌های علمی کمترند. در تحقیقی که صورت پذیرفت، ۳۱ نفر شناسایی شدند که این تعداد به عنوان جامعه آماری محسوب می‌شوند.

مشارکت‌کننده		جمع کل
کارشناسی ارشد	۲۱	۳۱
(Phd) دکتری	۱۰	

جدول۱:مشخصات مشارکت‌کنندگان پژوهش

ویژگی‌های جامعه آماری تعیین شده

در انتخاب جامعه آماری با توجه به موضوع تحقیق، به افرادی رجوع شد که ویژگی‌هایی نظیر: آشنایی با پدافند غیرعامل، آشنایی با مفاهیم تهدید، آشنایی با خطرپذیری و همچنین آشنایی با علوم دفاعی و امنیتی را داشتند.

تجزیه و تحلیل داده‌ها

با توجه به روش پرسش‌نامه‌ای که روش اصلی در گردآوری اطلاعات این تحقیق است، خروجی داده‌های پرسش‌نامه توسط نرم‌افزار SPSS تحلیل شده است. آلفای کرونباخ به دست آمده به کمک نرم‌افزار ۰/۸۳۴ است. از آنجا که عدد به دست آمده بزرگ‌تر از ۰/۷ است، اعتبار یا پایایی پرسشنامه مورد تایید است.

همچنین در ۳ جلسه تحت عنوان بازمهندسی در پدافند غیرعامل در سازمان پدافند غیرعامل کشور، الگو ارائه و در ساختار سمینار و فرایند «آزمون باز آزمون» بخش‌های مختلف الگو از لحاظ اعتباری سنجیده و از نظر خبرگان و متخصصان معتبر شناخته شد.

چارچوب نظری الگو

با توجه به تحقیقات صورت گرفته و گستره‌ی شمول الگوهای ارزیابی که در قسمت بعد مورد اشاره قرار خواهد گرفت، مشخص شد که اکثر الگوهای موجود بر اساس چارچوب ارزیابی خطرپذیری عمل می‌کنند (این الگو نیز بر این مبنا عمل می‌کند). با وجود این، آنچه کمبود آن احساس می‌شود نبود الگویی بومی در زمینه ارزیابی زیرساخت‌ها با تأکید بر ملاحظات پدافند غیرعامل است. پس، در این مقاله سعی می‌شود با توجه به راهبردهای مختلف تهاجمی دشمن از جمله استراتژی واردن، الگویی پدافندی طراحی و ارائه شود که بتواند دارایی‌ها، تهدیدات و آسیب‌پذیری‌های یك زیرساخت را به خوبی شناسایی و با توجه به رویکردهای پدافند غیرعامل، راهبردی ارائه دهد که بتواند در مواقع بحران، تداوم فعالیت‌های زیرساخت را در برابر تهدیدات تا اندازه مطلوبی تضمین کند.

تجزیه و تحلیل الگوها و روش‌های موجود

تعداد بسیار زیادی از روش‌های موجود از جمله آنهایی که توسط شرکت‌های مهندسی و طراحی اصلاح شده‌اند، راهنمایی‌های کافی را در خصوص چگونگی اعمال یك رهیافت نظام‌مند برای حل مسائل را ندارند و استانداردها و معیارهای قطعی برای سنجش عملکرد، که طی فرایند تصمیم‌سازی نیاز

تخصص مشارکت کنندگان				جمع کل
پدافند غیرعامل	۱۷	لشگری	۲۰	۳۱
مدیریت دفاعی	۱۱	کشوری	۱۱	
تخصص های مختلف	۳			

جدول۲ :ویژگی‌های جامعه آماری

هست، ندارند. مدل‌هایی که مبهم و غیردقیق هستند بیشتر به هم ریخته‌اند و در بعضی اوقات پیاده‌سازی آنها آزاردهنده و سخت خواهد بود. علاوه بر این ،بسیاری از مدل‌ها برنامه و خط‌مشی یکسانی ندارند و برای یك استفاده خاص طراحی می‌شوند و این اغلب خطر بازنگری عمده را به همراه دارد.

تمامی این مدل‌ها بیشتر بر راهکارهای امنیت فیزیکی تأکید دارند. این مدل‌ها به عنوان نمونه، به منظور بررسی حصارهای امنیتی، دروازه‌ها و درها، نصب سیستم‌های امنیتی و گسترش سیستم امنیتی در راستای پوشش نیازهای امنیتی در حال ظهور ارائه شده‌اند. آنها به جنبه‌های دیگر یک برنامه جامع نمی‌پردازند. علاوه بر این، توجه کم یا ناچیزی به کارکردها، فرایندها و وابستگی‌های داخلی و خارجی زیرساخت در این روش‌ها می‌شود.

از آنجا که ارزیابی خطرپذیری از یك بخش زیرساختی به بخش دیگر و از زمانی به زمان دیگر متفاوت است، یك چارچوب واحد برای ارزیابی، صحیح نبوده و غیرعملیاتی خواهد بود. برای بسیاری از بخش‌های زیرساختی، برخی تهدیدات پدیده‌ای نسبتاً نوظهور هستند. در نتیجه، تعیین تدابیر پدافندی موفق برای این بخش‌ها بسیار دشوار است، چرا که بسیاری از آنها برای اولین بار به اجرا درآمده‌اند و کارایی آنها هنوز ارزیابی نشده است. علاوه بر این، فعالیت‌ها و دارایی‌های برخی زیرساخت‌ها طوری پراکنده‌اند که پیاده‌سازی راهکارهای استاندارد و تدوین شده برای دارایی‌های متمرکز، دشوار است.

حال با توجه به آنچه گفته شد چند روش مطرح را مورد تجزیه و تحلیل قرار خواهیم داد:

۱. دستورالعمل‌های معیارهای طراحی ضد تروریسم فما[1]،
۲. ضوابط طراحی یکپارچه وزارت دفاع ایالات متحده امریکا،
۳. راهبردهای مبانی امنیت ساختمان،
۴. روش مدیریت خطرپذیری رمکپ[2].

فما یك رشته دستورالعمل‌های اطلاعاتی را به منظور کمك به صاحبان سرمایه در مناطق محلی و ایالتی آمریکا برای دستیابی به آمادگی در مواجهه با تهدید ارائه می‌کند. این دستورالعمل‌ها، بر مبنای لزوم ارزیابی تهدیدات تروریستی با توجه به خطرات مختلف آن ارائه می‌شوند که در اینجا به چند مورد از آنها خواهیم پرداخت :

1 .Fema (Federal Emergency Management Agency)
2 . ramcap

۱. فمای ۴۲۶: «دستورالعمل مرجع کاهش حملات تروریستی بالقوه در مقابل ساختمان‌ها» اطلاعاتی را برای طراحان و مهندسان در باره‌ی نحوه‌ی کاهش صدمات فیزیکی به ساختمان‌ها، زیرساخت‌های مربوط و افرادی که در معرض حمله تروریستی قرار دارند، ارائه می‌کند. این دستورالعمل رهیافت‌های متعددی را که می‌تواند به مرور زمان اجرا شود در راستای کاهش آسیب‌پذیری ساختمان‌ها در برابر تهدیدات تروریستی ارائه می‌دهد (۲).

۲. فمای ۴۲۷: «مبانی طراحی ساختمان‌های تجاری در راستای کاهش حملات تروریستی» یك رشته مفاهیمی را معرفی می‌کند که می‌تواند به مالکان و طراحان ساختمان‌ها و مقامات ایالتی و دولتی کمك کند تا تهدید را کاهش دهند. این دستورالعمل اطلاعات جامعی برای طراحی کیفی به منظور کاهش تأثیرات حملات تروریستی ارائه می‌کند. تمرکز آن در مرحله اول بر انفجارها و در مرحله دوم بر حملات شیمیایی، بیولوژیکی و رادیولوژیکی است (۳).

۳. فمای ۴۲۸: «مبانی پروژه‌های طراحی مدارس ایمن در برابر حملات تروریستی» اصول پایه و فن‌هایی به منظور طراحی یا مدل‌سازی مجدد مدارس ایمن در برابر حمله تروریستی برای طراحان و مسئولان مدارس فراهم می‌سازد (۴).

۴. فمای ۴۲۹: «جوامع نظارتی، مالی و بیمه ساختمان» مسائل مربوط به مدیریت خطرات تروریستی در ساختمان‌ها و ابزارهای موجود برای مواجهه با آنها را معرفی می‌کند (۵).

۵. ضوابط طراحی یکپارچه وزارت دفاع ایالات متحده امریکا: در جولای سال ۲۰۰۲ با توزیع نامحدود، برای استانداردهای طراحی سایت، طراحی سازه، طراحی معماری و طراحی مکانیکی و الکترونیکی برای محافظت ساختمان‌ها در برابر تهدیدات انفجاری، منتشر شده است.

۶. راهبردهای مبانی امنیت ساختمان: این راهبردها در سال ۲۰۰۳ در راستای کمك به مالکان و مدیران تأسیسات در ارزیابی خطر و آسیب‌پذیری ساختمان‌ها، ایجاد برنامه‌های واکنش سریع و تصمیم‌گیری در باره‌ی تدابیر و طرح‌های حفاظتی منتشر شد. مبانی امنیت ساختمان، براورد هزینه مرتبط با اجزای متعدد یک طرح امنیتی، نظیر: سیستم‌ها، تجهیزات و نیز نیروی کار لازم برای عملیات نصب را شامل می‌شود.

۷. روش رمکپ[1] که شامل ارزیابی تهدید و خطر در زیرساخت‌ها بوده و با هدف تأمین موارد زیر اقدام می‌کند (۶):

۸. استراتژی‌ها و خط مشی‌هایی برای توجه به ویژگی‌های خاص فعالیت‌های تروریستی،

۹. راهنمایی برای اقدامات متقابل علیه دشمن تروریست و استراتژی کاهش آسیب‌ها،

۱۰. روش‌هایی برای تخمین خطرات توسط معیارهایی که در تمام بخش‌ها کاربرد دارد،

۱۱. شناسایی و بررسی سرمایه‌های ملی در نقاط بحرانی و حیاتی .

همان‌طور که ملاحظه شد، اغلب این روش‌ها بر مبنای تهدیدات امنیتی استوار شده‌اند و بیشتر به دنبال ارائه‌ی راهکارهایی برای افزایش حفاظت فیزیکی تأسیسات و ابنیه در برابر موج انفجار هستند. از سویی دیگر ،نتایج این روش‌ها محدود به یک بخش خاص است و به‌گونه‌ای تدوین می‌شوند که غالباً جوابگوی تهدیدات نوظهور نبوده و فقط برای برخی از زیرساخت‌ها قابل استفاده‌اند.

در جدول۳ مقایسه‌ای از ویژگی‌های الگوی ارائه شده توسط نگارندگان با برخی از روش‌های موجود بیان شده است (تطبیق روش‌های موجود با ویژگی‌های بیان شده با علامت (√) نشان داده شده است).

تعریف الگو

الگویی که بدان پرداخته خواهد شد از پنج مرحله کلی تشکیل یافته است و هر مرحله نیز دارای چارچوبی برای استخراج عدد مؤلفه‌های خطرپذیری (دارایی، تهدید، آسیب‌پذیری) خواهد بود. در واقع، چارچوب ارائه شده در نهایت فهرستی از مؤلفه‌هایی را که در ارزیابی خطرپذیری یک زیرساخت اهمیت دارند، استخراج می‌کند تا سهولت در امر اندازه‌گیری تحقق یابد.

مشخصات الگو

۱. شناخت کامل از وضعیت زیرساخت،
۲. شناسایی ارزش دارایی‌ها ،
۳. شناسایی پشتیبانی‌کننده‌های حیاتی،
۴. آشکارسازی ارتباطات نهفته میان‌بخشی،
۵. شناسایی زمینه‌های آسیب‌پذیری،
۶. جذابیت هدف-دافعه هدف،
۷. مبنا قرار دادن کاربرد داده‌ها و اطلاعات قابل اطمینان،
۸. قابلیت فراهم کردن ابزارهای مناسب برای بازخورد،
۹. امکان به‌روز رسانی داده‌های ارزیابی شده،
۱۰. توجه به فیزیک ، هویت و سمت‌وسوی تهدید،
۱۱. ایجاد نوعی اتحاد بین ملاحظات جزئی و مؤلفه‌های کلان تهدید،
۱۲. شناسایی ارتباط بین پدیده‌های متفاوت با توجه به تنوع تهدید و لحاظ آن در تحلیل،
۱۳. قابلیت شناخت ابعاد تهدید،
۱۴. پیامدسنجی حوادث.

1 .ramcap

ویژگی‌های الگو ارائه شده / روش های موجود	FEMA	S۳E	RamCap	TRAM	RVA	Mays
شناسایی ارزش دارایی	√	√	-	-	-	-
استفاده از سناریو نویسی	√	-	-	√	-	-
شناسایی پشتیبانی کننده دارایی‌ها	-	-	√	-	-	-
آشکارسازی ارتباطات نهفته میان‌بخشی در زیرساخت‌ها	-	-	√	-	-	-
اصل غربالگری چند مرحله‌ای	-	-	√	-	-	-
پیامدشناسی	-	-	√	√	√	√
اولویت بندی حوزه‌ها	-	-	-	-	-	-
پرداختن به تهدیدات به صورت طیفی	-	-	-	-	√	-
کمّی‌سازی	√	-	√	-	-	-

جدول۳ :مقایسه ویژگی‌های الگوی ارائه شده با برخی از روش های موجود

تفاوت الگو با دیگر روش‌های ارزیابی

در این روش اساس کار بر پایه شناخت صحیح زیرساخت و استخراج دارایی‌های حیاتی آن بر مبنای اصل غربالگری است و همین مبنا باعث شده تا این روش در بهینه کردن خروجی‌ها به موفقیت چشمگیری نائل شود. الگوی پیشنهادی بر خلاف دیگر روش‌ها سعی دارد که با معرفی زیرساخت و اجزای آن، نقش و جایگاه هر یك را در فرایند مربوط بیان کند. همچنین با این نگرش به موضوع بپردازد که دشمن در انتخاب اهداف خود هوشمندانه عمل کرده و برای پیاده‌سازی تهدید به دنبال کسب بیش‌ترین موفقیت برای رسیدن به بالاترین نتیجه دلخواه است. از دیگر وجوه تمایز الگوی پیشنهادی با دیگر روش‌ها تأکید بر کمّی کردن مباحث توصیفی است به این معنا که با وزن‌دهی به شاخص‌های علمی در صدد به دست آوردن نتایجی مهندسی و کاربردی خواهد بود.

نوآوری‌های این الگو

روش‌های دیگری که در این زمینه مطرح شده‌اند غالباً بدون توجه به تحلیل جامع از دارایی‌ها و تنها با تأکید بر تهدیدات محتمل به بررسی زیرساخت مربوط می‌پردازند و حال آنکه الگوی پیشنهادی مبتنی بر درک درست محیط زیرساخت، رویکرد دشمن، تهدیدات، پیامدها و آسیب‌پذیری‌ها، آن هم با یک چارچوب کاملاً ریاضی گونه و کاربردی است که در نهایت پیش‌بینی رفتار دشمن و فهم وضعیت بحرانی ناشی از وقوع تهدید را برای ما آسان می‌کند. بر این اساس و به‌طور نمونه، نوآوری‌های این الگو در زیر ارائه می‌شود:

۱. استفاده از اصل غربالگری چند مرحله‌ای در بخش‌های مختلف به صورت کمّی و کیفی ؛
۲. پرداختن به بحث پیامدها به صورت ویژه در فرمول؛
۳. تعریف شاخص‌های منطبق با وضعیت کشور؛
۴. پرداختن به سناریوهای مختلف دشمن ؛
۵. پرداختن به فضاهای عملکردی با تعریفی جدید؛
۶. اولویت‌بندی حوزه‌ها و زیرساخت‌ها؛
۷. تعیین ضرایب ارزشی برای هر شاخص،
۸. ارائه چارچوب جدید برای تدوین سناریوی معیار؛
۹. تعیین سطوح امنیتی مبتنی بر درجه خطرپذیری؛
۱۰. جداول سطح‌بندی و شاخص‌های بومی شده با طیف تعاریف متفاوت؛
۱۱. ارائه طرح‌واره ساختار یك زیرساخت برای درك درست فضاهای عملکردی.

محورهای الگوی پیشنهادی

محورهای انجام ارزیابی خطرپذیری زیرساخت‌ها در این الگو شامل موارد زیر است:

الف) ارزیابی دارایی‌های حیاتی و دسته‌بندی آن؛
ب) ارزیابی تهدیدات و پیامد سنجی؛
ج) تحلیل آسیب‌پذیری؛
د) بررسی خطر.

دارایی‌ها و دسته‌بندی آن

در تعریف دارایی آمده: هر آنچه برای زیرساخت دارای ارزش باشد دارایی تلقی می‌شود که شامل دارایی‌های فیزیکی، سایبری، منابع انسانی و معنوی است. در هر زیرساخت مجموعه‌ای از دارایی‌ها وجود دارد. این دارایی‌ها اموال منقول و غیرمنقولی هستند که زیرساخت‌ها را تشکیل می‌دهند. در این بخش به مفهوم دارایی حیاتی در گام نخست و سپس در بخش مربوط به

یافته‌های تحقیق به معرفی یک نوع از دسته‌بندی دارایی‌های حیاتی خواهیم پرداخت که در آن سعی شده با توجه به ماهیت دارایی‌ها و فضاهای عملکردی آنها تعریف روشنی از ارتباط بین دارایی و زیرساخت ارائه کند.

دارایی‌ها همانند زیرساخت‌ها به دو دسته غیرحیاتی و حیاتی تقسیم می‌شوند. دارایی‌های غیرحیاتی دسته‌ای هستند که خسارت، آسیب و نابودی آنها تأثیر مهمی برای زیرساخت ندارد و حفاظت از آنها تنها نیازمند اقدامات حفاظتی جزئی است. در مقابل، دارایی‌های حیاتی در صورت صدمه دیدن و نابودی تأثیر بسیار مهمی بر زیرساخت می‌گذارند. دارایی‌هایی که به این دسته متعلقند مستقیماً در تداوم تولید محصولات و ارائه‌ی خدمات نقش دارند. این دارایی‌ها شامل مواد خام، تجهیزات تولید، قطعات یدکی و سیستم‌های انرژی می‌شوند. بنابراین، حیاتی بودن یک دارایی به میزان اهمیت آن در انجام مأموریت زیرساخت بستگی دارد.اگر دارایی الف ارزش بالاتری نسبت به دارایی ب داشته باشد اقدامات حفاظتی مرتبط با آن نیز بیشتر خواهد بود. میزان حیاتی بودن یا حساسیت، عاملی در تعیین میزان حفاظتی است که دارایی برای پشتیبانی از فعالیت‌های جاری به آن نیازمند است. شناسایی دارایی‌های حیاتی برای حفاظت مهم است، اما به همان اندازه نادیده گرفتن دارایی غیرحیاتی نیز اهمیت دارد.ایجاد اقدامات حفاظتی ویژه برای دارایی‌های غیرحیاتی باعث به هدر رفتن سرمایه می‌شود.

ارزیابی تهدیدات

به نظر می‌رسد که بررسی و شناخت تهدیدات و توانمندی‌های تسلیحاتی و فناورانه دشمن شرط اول و الزامی برای پی بردن به توانایی‌ها و اهداف دشمن است و بی توجهی در این خصوص آسیب‌ها و ضررهای جبران‌ناپذیری را در پی خواهد داشت؛ زیرا پس از آشکار شدن جنبه‌های مختلف تهدید است که شرایط و امکانات لازم برای بررسی و محاسبه توان و مقدورات دفاعی و کاهش آسیب‌پذیری‌ها فرا می‌رسد. کشف به‌موقع تهدید و چگونگی آن و تمرکز به‌موقع امکانات برای اتخاذ تدابیر هوشمندانه مقابله‌ای، موجب رفع نقاط ضعف و کاهش آسیب‌پذیری می‌شود. در باور کارشناسان امور دفاعی، اهتمام به تهدیدات می‌تواند آن را به فرصتی برای کسب توان دفاعی و خنثی‌سازی نقشه‌های تهاجمی دشمن و حتی بازدارندگی تبدیل کند.

نکته کلیدی این است که هر چه دشمن نیرومندتر و دارای شرایط بهتری باشد، برای طرف مقابل، زمان، امکانات و فرصت‌ها کم و نیاز به بهره‌گیری از تمامی امکانات و مقدورات ممکن، اجتناب‌ناپذیر می‌شود. در حقیقت، فرصت‌های دو حریف با هم برابری ندارد و به عوامل زیادی وابسته است که بیش از همه به تولید توان و آمادگی هر یک مرتبط است (۱).

تجزیه و تحلیل آسیب‌پذیری

برای تأمین مناسب و مطلوب نیازهای پدافندی برای برقراری امنیت در زیرساخت مورد نظر متناسب با سطوح دسترسی، پیش از هر چیز باید تجزیه و تحلیل دقیقی برای مشخص کردن میزان آسیب‌پذیری صورت گیرد.

بدیهی است که صفر شدن آسیب‌پذیری، وضعیتی است که صرفاً از لحاظ نظری امکان‌پذیر است. در دنیای واقعی، وضعیتی که در آن پایداری مطلق برقرار باشد، وجود خارجی ندارد و به همین علت باید در منتهای دقت ممکن میزان خطر موجود در منطقه و مکانی که قرار است امنیت آن تأمین شود، مورد تجزیه و تحلیل قرار گیرد. بر این اساس، آسیب‌پذیری باید به عنوان ضعف‌های زیرساخت در برابر تهدیدات احتمالی دشمن قلمداد شود (۷).

این نکته را می‌دانیم که آسیب نتیجه وضعیتی مخاطره‌آمیز است که وقوع تهدید به وجود می‌آورد. هر چه احتمال وقوع تهدید زیادتر باشد، در نتیجه ،میزان آسیب نیز افزایش خواهد یافت. با توجه به آنچه گفته شد، میزان آسیب مستقیماً به مقدار شدت تهدید بستگی دارد (۷).

میزان آسیب‌پذیری، روشی برای ارزیابی و اندازه‌گیری وضعیت‌هایی که می‌توان آنها را ردیابی کرد، به‌دست می‌دهد. ارزیابی صحیح و دقیق میزان آسیب‌پذیری، داده‌های مهم را برای مطالعه و برطرف کردن خلأهای حفاظتی و پدافندی فراهم می‌آورد (۸).

بررسی خطر

تعریف خطر

برای خطر تعاریف مختلفی ارائه شده است؛از جمله: « در معرض نابودی احتمالی بودن»، «تهدید با احتمال بسیار بالای تحقق یافتن »، «وجود شرایط مستعد برای صدمه دیدن» و « اقدامی مشخص که به آسیب و صدمات جدی بینجامد» (۱).

با توجه به این تعاریف، مفهوم خطر در چارچوب واژگان تهدید را می‌توان بر اساس معیارهای زیر معنا کرد:

-تهدید با احتمال بسیار بالای تحقق یافتن؛

-کافی نبودن قابلیت‌ها و توانمندی‌ها برای ایجاد موازنه با تهدید؛

علاوه بر معیارهای فوق از معیارهای زیر نیز می‌توان برای تشخیص دقیق‌تر خطر استفاده کرد:

۱. قطعی بودن تهدید اجتناب‌ناپذیر: یعنی مدیریت تهدید مستلزم قرار دادن آن در شرایط خاص شده است به‌گونه‌ای که با رویه‌های عادی تهدید دیگر قابل مدیریت کردن نباشد.
۲. مقابله کردن: یعنی حذف، نابودی، خنثی، مهار یا دفع کردن تهدید، عاجل‌ترین و ضروری‌ترین اقدام در برابر تهدید است.

مرحله‌بندی خطر

خطر را می‌توان در سه درجه یا وضعیت «هشدار»، «مخاطره» و «بحران» مرحله‌بندی کرد که این موضوع شامل «وضعیت هشدار»، «وضعیت مخاطره‌آمیز» و «وضعیت بحرانی» می‌شود. هر سه وضعیت، شدت و گستره تهدید علیه زیرساخت را نشان می‌دهد، اما به نظر نمی‌رسد که هر نوع تهدیدی با هر نوع ظرفیت

و قابلیتی بتواند تا مرحله بحران‌زایی پیش برود؛ زیرا همه‌ی تهدیدات از قابلیت نفوذ در تمام زیرساخت برخوردار نیستند (۱).

معیارهای تشخیص خطر

معیارهای تشخیص وضعیت زیرساخت نسبت به تهدیداتی که تبدیل به خطر شده‌اند، شامل معیارهای عمومی و معیارهای اختصاصی می‌شود. معیارهای عمومی همان معیارهای مربوط به مفهوم خطر هستند. بنابراین، به‌طور خلاصه معیارهای عمومی برای قرار گرفتن یک تهدید در زمره خطر به شرح زیر است:

۱. تهدید، زیرساخت‌ها را نشانه رفته است؛
۲. تهدید تحقق‌یافته یا با احتمال بسیار بالای تحقق‌پذیری؛
۳. کافی نبودن قابلیت‌ها و توانمندی‌ها در زیرساخت برای ایجاد موازنه با تهدید؛
۴. حمایت طیف وسیعی از تصمیم گیران در زمینه قطعی دانستن تهدید؛
۵. تبدیل شدن مقابله با تهدید به عنوان عاجل‌ترین و فوری‌ترین اقدام.

معیارهای اختصاصی در تعیین تهدیداتی را که تبدیل به خطر شده‌اند، با «پیامدهای تهدید» می‌توان تقسیم‌بندی کرد که با سه شاخصه‌ی شدت تهدید، گستره‌ی تهدید و عمق تهدید اندازه‌گیری انجام می‌شود.

شدت تهدید به حجم تجهیزات و ادوات نظامی تهدیدگر و آثار تخریبی آن بر زیرساخت‌ها بستگی دارد در حالی که گستره‌ی تهدید پوشش محیطی تهدید را مد نظر قرار می‌دهد. هر قدر محیط اعمال تهدید وسیع‌تر باشد، تهدید از گستردگی بیشتر برخوردار است. در نهایت ،عمق تهدید به میزان نفوذ آن در لایه‌های درونی زیرساخت بستگی دارد (۹).

با توجه به شاخصه‌ها، سه درجه‌ی پیامد برای سه درجه‌ی وضعیت تهدیداتی که تبدیل به خطر شده‌اند به شرح زیر می‌توان تعیین کرد:

۱. پیامدهای ویرانگر- وضعیت بحرانی: آن دسته از تهدیداتی که به صورت سخت‌افزاری یا نرم‌افزاری موجودیت نظام سیاسی، تمامیت ارضی و بقای جمعیت یک کشور را مورد هدف قرار داده باشد و تهدیدگر از قابلیت‌ها و ظرفیت‌های متناسب با چنین هدفی نیز برخوردار باشد.
۲. پیامدهای شدید- وضعیت مخاطره آمیز: آن دسته از تهدیداتی که به صورت سخت‌افزاری یا نرم‌افزاری در سطوح عملیاتی و تاکتیکی، هسته مرکزی زیرساخت‌ها را هدف قرار داده باشد.
۳. پیامدهای قابل توجه- وضعیت هشدار: آن دسته از تهدیدات سخت‌افزاری یا نرم‌افزاری که قابلیت ایجاد اختلال در تعدادی از زیرساخت‌ها در گستره‌ی محدودی از محیط را داراست؛ ضمن آنکه تهدید، هسته مرکزی زیرساخت‌ها را هنوز نشانه نرفته است (۱).

ارائه‌ی الگو

الگویی که در این بخش بدان پرداخته خواهد شد از پنج مرحله کلی تشکیل یافته است و هر مرحله نیز دارای چارچوبی برای استخراج عدد مؤلفه‌های خطرپذیری (دارایی، تهدید، آسیب‌پذیری) خواهد بود. در واقع، چارچوب ارائه شده در نهایت فهرستی از مؤلفه‌هایی را که در ارزیابی خطرپذیری یک زیرساخت اهمیت دارند، استخراج می‌کند تا سهولت در امر اندازه‌گیری تحقق یابد. بر این اساس، چهار مرحله کلی در زیر و سپس چارچوب‌های آن به تفصیل ارائه خواهد شد (۱۰):

الف) زیرساخت و دارایی‌ها
۱. تعاریف و کلیات
۲. بررسی و ارزیابی
۳. براورد و کمّی‌سازی
۴. فهرست کردن

ب) تهدیدات و پیامدها
۱. تعاریف و کلیات
۲. بررسی و ارزیابی
۳. فهرست کردن

براورد و کمّی‌سازی

ج) آسیب‌پذیری
۱. تعاریف و کلیات
۲. بررسی و ارزیابی
۳. براورد و کمّی‌سازی
۴. فهرست کردن

د) خطرپذیری
۱. ارزیابی و براورد خطرپذیری
۲. تعیین تهدید پایه

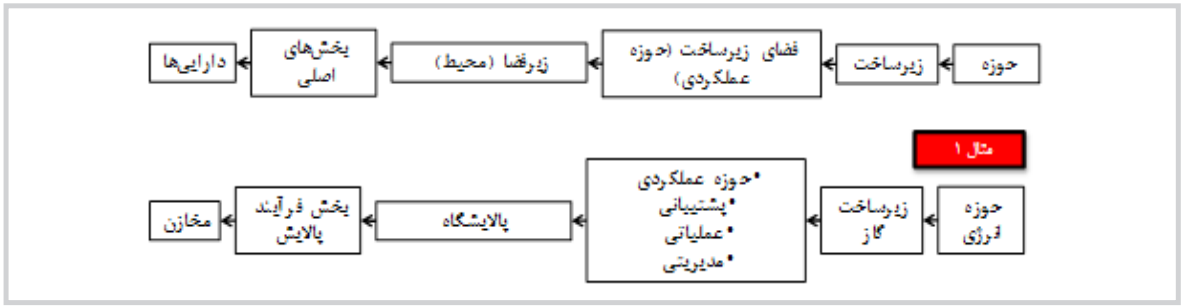
ه) سناریوی معیار
۱. تبیین سناریوهای متفاوت
۲. بررسی خطرپذیری هر سناریو

منطق فازی

تاریخچه

نظریه مجموعه‌های فازی و منطق فازی را اولین بار پرفسور لطفی‌زاده در رساله‌ای به نام»مجموعه‌های فازی اطلاعات و کنترل»در سال (۱۹۶۵-۱۳۴۴) معرفی کرد. هدف اولیه‌ی او در آن زمان، توسعه‌ی الگویی کارامدتر برای توصیف فرایند پردازش زبان‌های طبیعی بود. او مفاهیم و اصلاحاتی چون مجموعه‌های فازی، رویدادهای فازی، اعداد فازی و فازی‌سازی را وارد علوم ریاضیات و مهندسی کرد. از آن زمان تاکنون، پرفسور لطفی زاده به دلیل معرفی نظریه بدیع و سودمند منطق فازی و تلاش‌هایش در این زمینه، موفق به کسب جوایز بین‌المللی متعددی شده است.

پس از معرفی منطق فازی به دنیای علم، در ابتدا مقاومت‌های بسیاری در برابر پذیرش این نظریه صورت گرفت. بخشی از این مقاومت‌ها، چنان‌که ذکر شد، ناشی از برداشت‌های نادرست از منطق فازی و کارایی آن بود. جالب اینکه، منطق فازی



شکل ۱: طرح‌واره ساختار یك زیرساخت (نگارندگان)

در سال‌های نخست تولدش بیشتر در دنیای مشرق زمین، به ویژه کشور ژاپن با استقبال روبه‌رو شد، اما استیلای اندیشه کلاسیك صفر و یك در کشورهای مغرب زمین، اجازه رشد اندکی به این نظریه داد. با این حال به تدریج که این علم کاربردهایی پیدا کرد و وسایل الکترونیکی و دیجیتالی جدیدی وارد بازار شدند که بر اساس منطق فازی کار می‌کردند، مخالفت‌ها نیز اندك اندك کاهش یافتند.

کاربردهای منطق فازی

بهترین روش کمّی کردن اطلاعات کیفی بر اساس منطق فازی بنا شده و در تحلیل خطرپذیری و تعیین خسارت این روش کاملاً جاافتاده است و به عنوان مثال، دستورالعمل‌های فما نیز از آن بهره می‌برد. تحلیل و ارزیابی خطرپذیری یک محل در برابر تهدیدات از دیدگاه منطق فازی از مواردی است که جای بررسی زیادی دارد و می‌تواند در آینده مورد توجّه قرار بگیرد.

منطق وزن دهی به مؤلفه‌ها در این الگو

در این الگو از منطق فازی برای وزن‌دهی به مؤلفه‌ها استفاده شده است. این منطق سعی می‌کند که مفاهیم کیفی و توصیفی طی عملیاتی، کمّی شود. بر این اساس، نخست شاخص‌هایی برای سه مؤلفه کلیدی در فرمول خطرپذیری (یعنی دارایی، تهدید و آسیب‌پذیری) منطبق با فضای تهدید در کشور تهیه شد. بعد از آن، هر یک از شاخص‌ها در یک مقیاس پنج‌درجه‌ای که هر درجه با وزن عددی که از بازه یك تا ده تقسیم شده وزن مخصوص به خود را پیدا می‌کنند و کمّی می‌شوند. لازم به ذکر است که این مقیاس و بازه‌ی عددی اختیاری بوده و هرچه این بازه بیشتر باشد خروجی ارزیابی دقیق‌تر خواهد بود. برای نمره‌دهی باید در نظر داشت که معیارهای هر شاخص مطابق با وزن عددی درست توصیف شود. در این الگو ابتدا پس از مطالعه و بررسی مستندات گوناگون شاخص‌هایی که مبنای علمی داشته استخراج می‌کنیم و پس از تطبیق آن با شرایط کشور با ابزار پرسش‌نامه، آن را در معرض نظر خبرگان حوزه پدافند غیرعامل و امنیت قرار می‌دهیم.

فرمول ارزیابی ریسك

در این الگوی پیشنهادی، ارزیابی خطرپذیری زیرساخت بر اساس شاخص‌هایی انجام می‌پذیرد که در جداول سطح‌بندی، میزان کمّیت آن لحاظ شده است. در این الگو ضمن تحلیل دارایی‌های حیاتی، تهدیدات احتمالی و آسیب‌پذیری‌ها در ماتریس‌های جداگانه، به ارزیابی خطرپذیری مجموعه خواهیم پرداخت.

البته درجه اهمیت و آسیب‌پذیری نقاط و دارایی‌ها مختلف زیرساخت، شاخص مهمی است و نقاطی را که عدد شاخص آنها از عدد معینی بالاتر باشد، در فهرست بخش‌های قابل محافظت ویژه قرار می‌دهند. در این مرحله نیز سطح دوم پالایش بخش‌های مختلف صورت می‌پذیرد و برای نقاط و دارایی‌هایی که دارای خطرپذیری بالا باشند، تمهیدات دفاع غیرعامل پیشنهاد می‌شود.

خطرپذیری، از حاصل‌ضرب ارزش دارایی در تهدید در آسیب‌پذیری به دست می‌آید. فرمول ذکر شده مقتبس از روش فما است و در آن، عدد خروجی هرچه بالاتر باشد نشان‌دهنده‌ی خطرپذیری بالا برای آن دارایی خواهد بود که قطعاً باید برای آن راهکارهای خاصی را اندیشید (۱۱):

تهدید (ضریب پیامد) × آسیب‌پذیری × ارزش دارایی= ریسك

اینجا لازم است این نکته یادآوری شود که اگر چه فرمول فوق از روش فما اخذ شده، اما این الگو در نحوه ارزیابی و استخراج اعداد به یک نوآوری بر اساس مقتضیات خاص کشور دست یافته و در این مورد به‌گونه‌ای عمل کرده است که بتواند سطح وسیعی از تهدیدات را پوشش دهد.

حال در این قسمت چارچوب ۴ مرحله کلی را که در ابتدای این فصل بدان اشاره شد به صورت تفصیلی شرح خواهیم داد:

زیرساخت و دارایی‌ها

در این گام ابتدا لازم است تا ساختار کلی یک حوزه زیرساختی را تشریح کنیم، به همین منظور و برای سهولت در بررسی یک زیرساخت، ساختار پیشنهادی زیر که به‌صورت طرح‌واره ارائه شده، گویای نوع رویکرد این الگو به مقوله زیرساخت است:

همان‌طور که در شکل می‌بینید، این ساختار کمک شایانی به درک صحیح درباره فضای زیرساخت خواهد داشت؛ چرا که در نهایت در ارتباط با سناریوهای راهبردی دشمن می‌تواند دورنمایی از نوع رویکرد دشمن به آن زیرساخت را نشان دهد.در این راستا طبقه‌بندی زیرساخت‌های یک کشور بسیار مهم ارزیابی می‌شود زیرا با تعیین اولویت‌بندی زیرساخت‌ها از حیث اهمیت، حساسیت

	ارزش راهبردی				ارزش اقتصادی					ارزش سیاسی			ارزش اجتماعی				ارزش دفاعی			
اهداف مرجع	منحصر به فرد بودن	اداره مردم	قوام کشور	بقای حاکمیت	تمرکز سرمایه‌های حیاتی	رشد توسعه و بهروری	افزایش تولید ناخلص ملی	وابستگی اقتصاد کشور به آن	تأمین نیازهای مردم	تحمیل خواسته‌های به دیگران	افزایش قدرت چانه‌زنی	ارتقای نقش بین‌المللی	کاهش بحران و نامنجاری‌های اجتماعی	ارتقای سطح رفاه مردم	هویت ملی و فرهنگی	اثرگذاری بر بافت جمعیتی	افزایش آستانه مقاومت ملی	پشتیبانی از نیروهای مسلح	تولید بازدارندگی	امکان دفاع همه‌جانبه	پایداری در برابر تهدیدات
A																					
B																					
C																					
D																					
E																					

جدول۴ :ارزش هدف

و نقشی که در اداره جامعه خواهند داشت، امکان تخصیص صحیح منابع با هدف کاهش آسیب‌پذیری و تداوم فعالیت‌های آن را فراهم می‌آورد. برای این منظور، شناخت صحیح کارکردهای هر زیرساخت، دسته‌بندی آنها و شناسایی دقیق فضاهای هریک بسیار ضروری است. تعیین ارزش هدف در این راستا کمک شایانی به طبقه‌بندی زیرساخت‌ها و اولویت‌بندی آن می‌کند که بی‌شک تعریف شاخص‌هایی استاندارد برای این مهم، از ضروری‌ترین اقدامات لازم است. شاخص‌هایی نظیر ارزش راهبردی، ارزش اقتصادی، سیاسی، دفاعی و... شاخص‌های مناسبی برای کشف میزان اهمیت هر زیرساخت خواهند بود. در جدول۱ ارزش اهداف را که به منظور طبقه‌بندی زیرساخت‌ها تهیه شده است، می‌بینید.

بررسی و ارزیابی

در این گام پس از اولویت‌بندی زیرساخت‌ها به بررسی فضاهای عملکردی و دارایی‌های هرزیرساخت اقدام می‌شود. در واقع، در این گام اساسی‌ترین کار محیط‌شناسی فضاهای عملکردی یک زیرساخت است. به همین منظور، ابتدا محیط زیرساخت از حیث ماهیت، جنس، تنوع، پیوستگی و... ارزیابی می‌شوند سپس کنش این محیط با محیط‌های پیرامون خود، ارزیابی محیط پیرامونی، وضعیت جانمایی عناصر و.... مورد تحلیل قرار می‌گیرند. بعد از آن، میزان دارایی‌های زیرساخت مربوط، فعالیت‌هایی که در محیط در حال انجام است و نیروی انسانی موجود را بررسی خواهیم کرد.

براورد و کمّی‌سازی

در این گام ابتدا به منظور براورد اولیه وضعیت دارایی‌های یک زیرساخت، ضمن تعریف شاخص‌هایی و با استفاده از اصل غربالگری هم فضاهای عملکردی (کاربردی) و هم دارایی‌ها، اعم از تجهیزات و سیستم‌ها را بررسی و با تحلیل فرایند سیستمی ضمن معرفی گلوگاه‌های زیرساخت به تعیین دارایی‌های حیاتی از غیرحیاتی اقدام می‌کنیم. قدر مسلم تنوع دارایی‌ها با توجه به نرم‌افزاری یا سخت‌افزاری بودن محیط مورد مطالعه متفاوت خواهد بود؛پس، هنگام غربال کردن دارایی‌ها توجه به مستقل بودن یا به‌هم پیوسته بودن دارایی‌ها بسیار مهم است. از دیگر موارد حائز بررسی و براورد، پشتیبانی‌کننده‌ها هستند که نقش ویژه‌ای در تقویت و ادامه فعالیت‌های دارایی‌ها به عهده دارند. برای کمّی‌سازی، منطق به‌کار گرفته شده در این الگو منطق فازی است. در این منطق ابتدا شاخص‌های ارزشیابی دارایی‌ها پس از دریافت تأییدیه توسط خبرگان به معیارهای کوچک‌تری تعریف می‌شود که هر معیار با دو مؤلفه‌ی ارزش کیفی و ارزش کمّی وزن مخصوص به خود را پیدا خواهد کرد و نهایتاً در جدول ارزشیابی، کلیه‌ی دارایی‌ها را مورد سنجش قرار می‌دهیم. نکته بسیار مهم، این است که هر چه بازه‌ی ارزش کمّی در جداول بیشتر باشد یا هر چه شاخص‌های تعریف شده صحیح باشد به همان نسبت خروجی اعداد با واقعیت‌ها منطبق‌تر خواهد بود. بر این اساس، تعریف شاخص‌های صحیح برای کشف دارایی‌های حیاتی، نیازمند یک کارشناسی دقیق خواهد بود که در این خصوص جدول۲ پیشنهاد می‌شود.

دارایی‌ها	ارزش اقتصادی	ارزش عملکردی	حیطه اثر	سطح بهره‌مندی	حساسیت	جمع
دارایی الف	۵	۸	۵	۴	۷	۲۹
دارایی ب	۳	۵	۴	۶	۱	۱۹
دارایی ج	۳	۲	۸	۹	۴	۲۶
دارایی د	۳	۶	۸	۷	۴	۲۸
دارایی ه	۳	۲	۴	۵	۴	۱۸
دارایی و	۳	۸	۸	۷	۹	۳۵

جدول ۵ :ارزشیابی دارایی

ردیف	معیارها	حداکثرامتیاز
۱	حیاتی بودن هدف	۱۰
۲	(قابلیت دسترسی) سهولت هدف‌گیری	۱۰
۳	قابلیت مرمت و بازسازی	۱۰
۴	آسیب‌پذیری	۱۰
۵	میزان تأثیر	۱۰
۶	قابلیت کشف و شناسایی هدف	۱۰
	جمع کل	**۶۰**

جدول ۶:معیارهای اولویت‌بندی کارور

فهرست کردن

پس از کمّی کردن ارزش دارایی‌ها با عنایت به خروجی اعداد در ستون جمع کل، فهرستی از دارایی‌های حیاتی استخراج خواهد شد که در ادامه ارزیابی‌های این الگو به عنوان مبنای فعالیت‌های بعدی قرار خواهد گرفت.ناگفته پیداست که این فهرست همان اهداف جذاب دشمنان است که درصدد آسیب زدن به آن خواهند بود. در این زمینه جدول۳ کارور[1] برای تعیین اولویت جذابیت اهداف استفاده می‌شود (۱۲).

تهدیدات

در این گام ابتدا بررسی را در دو بخش عمومی و تخصصی پی خواهیم گرفت. در این قسمت نخست بخش عمومی را که شامل وضعیت تهدیدگر (دشمن) و چشم‌اندازی از وضعیت تهدید است، بررسی خواهیم کرد سپس در بخش تخصصی تهدیدات احتمالی را در زیرساخت مورد مطالعه مورد کنکاش قرار خواهیم داد.

بخش عمومی:

در بخش عمومی ابتدا ضمن معرفی و شناسایی دقیق دشمنان اعم از خارجی و داخلی به بررسی انگیزه‌ها و اهداف احتمالی آنان می‌پردازیم و در ادامه، ضمن شرح توانمندی‌ها و نظام هدف‌گیری آنان،نیم‌نگاهی به قوت‌ها، ضعف‌ها و رویکردهایشان خواهیم کرد (۱۳).

بخش تخصصی:

در این بخش، هدف، پرداختن به تهدید به‌طور تخصصی در زیرساخت مورد مطالعه است که باید در آن، ضمن معرفی اندیشه و نگاه دشمن برای پیش‌بینی رفتار او در اجرای تهدید، راهبردهای احتمالی، محدودیت‌ها، فرصت‌ها، ابزارها، روش‌ها و تاکتیک‌ها و همچنین به بررسی سطوح تهدید و نحوه تحقق آن در سه سطح راهبردی، عملیاتی و تاکتیکی و همین طور به ویژگی‌های خاص هر تهدید نظیر ابعاد، پیامدها، فوریت‌ها، هم‌افزایی‌ها و... توجه جدی کرد. بررسی سوابق دشمن در جنگ‌های گذشته و چگونگی اتصال فضای راهبردی به فضای تاکتیکی توسط دشمن از جمله مواردی است که در این بخش بدان پرداخته می‌شود (تعیین این محورها زیر سناریوهای راهبردی دشمن قابل حصول و پیگیری است)(۱۳).

1 .CARVER

حوزه تهدید		سناریوی تهدید احتمالی	شاخص ها						جمع نمرات	درصد
			وجود زمینه	امکان پذیری	سابقه	جذابیت	هدف گیری	الرگذاری		
نرم	غیر انتحاری	F	۵	۸	۴	۷	۵	۶	۳۵	۵۸
		P	۵	۵	۸	۳	۱	۵	۲۷	۴۵
		N	۸	۵	۷	۶	۱	۵	۳۲	۵۳
	انتحاری	M	۸	۶	۷	۷	۴	۳	۳۵	۵۸
		G	۸	۷	۷	۶	۵	۵	۳۸	۶۳
		Q	۶	۵	۳	۶	۱	۵	۲۶	۴۰
نیمه سخت		D	۸	۸	۲	۶	۸	۴	۳۶	۶۰
		E	۳	۶	۱	۳	۶	۵	۲۴	۴۰
سخت	انتحاری	K	۶	۵	۸	۶	۴	۳	۳۰	۵۰
		H	۸	۶	۷	۶	۴	۵	۳۴	۵۷
		S	۵	۵	۵	۲	۴	۲	۲۳	۳۸
	نظامی	A	۶	۸	۶	۶	۹	۵	۳۶	۶۰
		I	۶	۷	۶	۳	۸	۵	۳۳	۵۵
		C	۸	۵	۵	۵	۲	۴	۲۹	۴۸
		B	۵	۵	۳	۵	۶	۷	۳۱	۵۲
ویژه										

جدول۷ :امکان‌پذیری تهدیدات

تهدید / دارایی	حمله سایبری	خرابکاری(فنی)	حمله تروریستی	حمله موشکی
اسکله	۱	۵	۷	۵
کانال ورودی	۱	۳	۶	۵
تجهیزات پهلوگیری	۱	۵	۵	۵
تجهیزات تخلیه و بارگیری	۱	۵	۵	۵
تجهیزات سوخت‌گیری شناورها	۱	۷	۷	۵
سیستم برق‌رسانی	۹	۹	۷	۵
موج‌شکن	۱	۱	۸	۵
مجموعه اداری و مدیریتی	۹	۶	۷	۵
مجموعه رادیویی و مخابراتی	۹	۹	۷	۵
انبارها	۱	۲	۵	۵
لنگرگاه	۱	۶	۵	۵
حراست	۱	۵	۷	۵

جدول ۸ :ارزیابی تهدید

بررسی و ارزیابی

در این گام نخست فهرستی از تهدیدات متصور علیه زیرساخت استخراج می‌شود سپس برای آنکه میزان امکان وقوع هر تهدید بررسی شود با استفاده از جدول۴ و با تعریف شاخص‌هایی، امکان‌پذیری هر تهدید مورد بررسی قرار خواهد گرفت. بی‌شک دسته‌بندی تهدیدات قبل از تشکیل جدول امکان‌پذیری کمک شایانی به درک درست از روش و ابزارهای احتمالی و قابل به‌کارگیری توسط دشمن خواهد داشت و ما را به نتایج مطلوب خواهد رساند (جدول ۷ به عنوان نمونه تکمیل شده است).

براورد و کمّی‌سازی

در این گام پس از غربال تهدیدات متصور در جدول امکان‌پذیری و استخراج تهدیداتی که به لحاظ وزنی، عدد بیشتری را به خود اختصاص داده‌اند، هریک از تهدیدات استخراج

ارزش دارایی	سطح آسیب						
	خیلی زیاد	زیاد	متوسط زیاد	متوسط	متوسط کم	کم	خیلی کم
خیلی زیاد	شدت پیامد خیلی‌بالا	شدت پیامد بالا	شدت پیامد بالا	شدت پیامد متوسط بالا	شدت پیامد متوسط بالا	شدت پیامد متوسط	شدت پیامد متوسط
زیاد	شدت پیامد بالا	شدت پیامد بالا	شدت پیامد متوسط بالا	شدت پیامد متوسط بالا	شدت پیامد متوسط	شدت پیامد متوسط	شدت پیامد متوسط کم
متوسط زیاد	شدت پیامد بالا	شدت پیامد متوسط بالا	شدت پیامد متوسط بالا	شدت پیامد متوسط	شدت پیامد متوسط	شدت پیامد متوسط کم	شدت پیامد متوسط کم
متوسط	شدت پیامد متوسط بالا	شدت پیامد متوسط بالا	شدت پیامد متوسط	شدت پیامد متوسط	شدت پیامد متوسط کم	شدت پیامد متوسط کم	شدت پیامد کم
متوسط کم	شدت پیامد متوسط بالا	شدت پیامد متوسط	شدت پیامد متوسط	شدت پیامد متوسط کم	شدت پیامد متوسط کم	شدت پیامد کم	شدت پیامد کم
کم	شدت پیامد متوسط	شدت پیامد متوسط	شدت پیامد متوسط کم	شدت پیامد متوسط کم	شدت پیامد کم	شدت پیامد کم	شدت پیامد خیلی کم
خیلی کم	شدت پیامد متوسط	شدت پیامد متوسط کم	شدت پیامد متوسط کم	شدت پیامد کم	شدت پیامد کم	شدت پیامد خیلی کم	شدت پیامد خیلی کم

جدول ۹: شدت پیامد

شده را در جدول ۵ ارزیابی تهدید و با شاخص‌هایی که برای کشف احتمال وقوع تهدید مورد نظر به‌کار گرفته شده‌اند، کمّی می‌کنیم و براوردی از احتمال وقوع هر تهدید انجام می‌دهیم (جدول ۸ به عنوان نمونه برای یک بندر فرضی تکمّیل شده است).

پیامدها

پیامدها معیار مهمی در تعیین تهدیدات خطرناک هستند و در واقع به نتایج آسیب‌هایی گفته می‌شوند که از ناحیه تهدید به مجموعه اهداف وارد می‌شود. در تعیین درجه‌ی پیامدهای تهدید می‌توان از سه شاخصه‌ی شدت تهدید، گستره‌ی تهدید و عمق تهدید استفاده کرد (۱۴).

برای براورد درست پیامدهای هر تهدید و میزان بحران‌زایی هر کدام، جدول ۹ را به عنوان مبنای عمل پیشنهاد می‌کنیم که در آن، وزن کیفی هر تهدید از حیث شدت پیامد قابل دستیابی خواهد بود (۱۲).

فهرست کردن

در این گام پس از کمّی کردن و غربالگری تهدیدات احتمالی،فهرستی از تهدیداتی را که احتمال وقوع و اثرگذاری بالایی دارند برای استفاده در مرحله بعدی که بحث ارزیابی آسیب‌پذیری زیرساخت مورد مطالعه باشد استخراج می‌کنیم.

آسیب‌پذیری

در این بخش نخست آسیب‌های قبلی زیرساخت که در اثر اجرای تهدیدات گذشته ایجاد شده مورد بررسی قرار می‌گیرد سپس با توجه به دارایی‌هایی که به عنوان اهداف جذاب مورد توجه دشمن هستند، به‌صورت توصیفی نقاط ضعف عمده و آسیب‌پذیر زیرساخت را استخراج می‌کنیم.در این قسمت توجه به چیدمان دارایی‌ها،به‌هم پیوستگی آنها و تراکمشان در یک منطقه بسیار حائز اهمیت است. همچنین کشف ماهیت نقاط آسیب‌پذیر از حیث جنس، پیچیدگی و فیزیک می‌تواند سهولت در امر شناسایی آسیب‌پذیری‌ها را موجب شود (۱۵).

بررسی و ارزیابی

در این گام ابتدا بر اساس روش‌های احصای آسیب‌پذیری نظیر بازدید میدانی و پر کردن چک‌لیست، مصاحبه و دریافت نظر خبرگی و همچنین بررسی نقاط ضعف به تهدید با این شیوه که فهرست تهدیدات احتمالی استخراج شده در مرحله قبلی را در برابر فهرست دارایی‌های حیاتی زیرساخت قرار داده سپس ضمن بررسی دقیق مجموعه عواملی که می‌تواند باعث ایجاد و یا افزایش آسیب‌پذیری در آن مجموعه شود، به بررسی وضعیت جانمایی و پراکندگی دارایی‌ها همچنین سطوح حمایتی بیرون از سیستم پرداخته و بعد از آن با تشریح تدابیر حفاظتی و پدافندی موجود در مجموعه از حیث حفاظت فیزیکی، سایبری، انسانی، تجهیزاتی و ... ضریب کارایی این تدابیر را در برابر تهدیدات احتمالی تحلیل

دارایی / تهدید	حمله سایبری	خرابکاری(فنی)	حمله تروریستی	حمله موشکی
اسکله	۱	۷	۷	۶
کانال ورودی	۱	۱	۱	۶
تجهیزات پهلوگیری	۴	۵	۸	۶
تجهیزات تخلیه و بارگیری	۲	۶	۶	۶
تجهیزات سوخت‌گیری شناورها	۲	۶	۶	۶
سیستم برق‌رسانی	۸	۸	۸	۶
موج‌شکن	۱	۱	۱	۶
مجموعه اداری و مدیریتی	۸	۶	۶	۶
مجموعه رادیویی و مخابراتی	۸	۹	۹	۶

جدول ۱۰: ارزیابی آسیب‌پذیری

کرده و پس از آن به بررسی اثرات متقابل نقاط آسیب‌پذیر بر یکدیگر، خواهیم پرداخت.

براورد و کمّی‌سازی

در این گام شاخص‌هایی را که به عنوان عوامل اثرگذار در آسیب‌پذیری تعریف شده است، بر اساس منطق فازی در جدول ارزیابی (۹) قرار می‌دهیم، کلیه‌ی دارایی‌های زیرساخت را در نسبت با تهدیدات متصور بررسی و میزان آسیب‌پذیری هر کدام را با عنایت به آن شاخص‌ها کمّی می‌کنیم. همچنین در براورد آسیب‌پذیری زیرساخت که بیانگر شدت آسیب‌پذیری است، دو مؤلفه عمق و دامنه‌ی آسیب‌پذیری را مورد کنکاش قرار می‌دهیم و احتمال تسری آسیب‌پذیری هر بخش بر بخش‌های دیگر را تشریح می‌کنیم (جدول زیر به عنوان نمونه برای یک بندر فرضی تکمیل شده است).

فهرست کردن

در این گام پس از غربالگری، فهرستی از دارایی‌های آسیب‌پذیر مجموعه که به لحاظ کمّی وزن بیشتری را به خود اختصاص داده است، استخراج و در نهایت با کمک نقشه‌ای مجموعه را از حیث آسیب‌پذیری پهنه بندی و با علائمی نظیر رنگ، درجه‌بندی آن را معلوم می‌کنیم (۱۶).

خطرپذیری

ارزیابی و براورد خطرپذیری

در این قسمت ابتدا بر اساس فرمول ارزیابی خطرپذیری که در ضرب سه مؤلفه ارزش دارایی، تهدید و آسیب‌پذیری صورت می‌پذیرد، اعداد به‌دست آمده در سه جدول قبلی را در هم ضرب می‌کنیم تا عدد خطرپذیری هر تهدید به دست آید. سپس برای براورد خطرپذیری به دست آمده ضمن تهیه یک جدول سطح‌بندی مطابق شکل ۱۱-۱۲ که در بازه‌ای از اعداد متفاوت مشخص شده- و با استفاده از رنگ تفکیک شده‌اند، میزان درجه‌ی خطرپذیری هر تهدید را در جدول دیگری استخراج می‌کنیم. این کار برای سهولت در تشخیص میزان خطرپذیری هر تهدید است (۱۶).

تعیین تهدید پایه

یکی از خروجی‌های جدول درجه خطرپذیری، مشخص شدن تهدید پایه است. در واقع، تهدید پایه به تهدیدی اطلاق می‌شود که در نسبت با بقیه تهدیدات متصور از درجه خطرپذیری بالاتری برخوردار است. این کار به منظور مبنا قرار دادن یک تهدید در یک مجموعه برای بررسی‌های بعدی و ارائه‌ی راهکارهای منطبق با بدترین وضعیت احتمالی صورت می‌پذیرد (۱۶).

تدوین سناریوی معیار

در این گام بر اساس تهدید پایه استخراج شده باید برای وضعیت احتمالی که فرض آن پیاده شدن این تهدید است، یک شبیه‌سازی صورت پذیرد تا درک بهتری نسبت به زمان بحران و پیامدهای آن و همچنین کشف ضعف‌های مجموعه در برابر این تهدید به دست آید. برای این منظور تدوین یک سناریو پیشنهاد می‌شود. در واقع، سناریو یکی از ابزارهایی است که به ما کمک می‌کند تا با یاری شاخص‌های راهنما، عدم قطعیت‌های احتمالی را مدیریت و حجم کل حادثه را تجسم کنیم. در این راستا چارچوب کلی فرایند تدوین سناریوی معیار را مشاهده می‌کنید.

چارچوب کلی فرایند تدوین سناریوی معیار

در این بخش تلاش شده که این چارچوب کلی برای نوشتن سناریو در حوزه دفاعی و در برابر تهدیدات دشمن تبیین شود. گام‌های اصلی این فرایند عبارتند از:

گام اول: تبیین موضوع
گام دوم: دشمن شناسی
گام سوم: شناخت زیرساخت
گام چهارم: انتخاب تهدیدات
گام پنجم: ارزیابی تهدید و تعیین سناریوهای پایه

	ریسک پایین	ریسک متوسط	ریسک بالا
میزان ریسک	۱-۱۰۰	۷۵-۲۲۵	بیش از ۲۲۵

جدول ۱۱: درجه‌بندی ریسک

دارایی / تهدید	حمله سایبری	خرابکاری (فنی)	حمله تروریستی	حمله موشکی
اسکله	۸،۲	۲۸۷	۴۰۱،۸	۲۴۶
ارزش دارایی	۸،۲	۸،۲	۸،۲	۸،۲
شدت تهدید	۱	۵	۷	۵
شدت آسیب‌پذیری	۱	۷	۷	۶
کانال ورودی	۴	۱۲	۹۶	۱۰۰
ارزش دارایی	۴	۴	۴	۴
شدت تهدید	۱	۳	۶	۵
شدت آسیب‌پذیری	۱	۱	۴	۵
تجهیزات پهلوگیری	۲۴	۱۵۰	۲۴۰	۱۸۰
ارزش دارایی	۶	۶	۶	۶
شدت تهدید	۱	۵	۵	۵
شدت آسیب‌پذیری	۴	۵	۸	۶
تجهیزات تخلیه و بارگیری	۱۴،۲	۲۱۳	۲۱۳	۲۱۳
ارزش دارایی	۷،۱	۷،۱	۷،۱	۷،۱
شدت تهدید	۱	۵	۵	۵
شدت آسیب‌پذیری	۲	۶	۶	۶
تجهیزات سوخت‌گیری شناورها	۱۰،۴	۲۱۸،۴	۲۱۸،۴	۲۱۸،۴
ارزش دارایی	۵،۲	۵،۲	۵،۲	۵،۲
شدت تهدید	۱	۷	۷	۵
شدت آسیب‌پذیری	۲	۶	۶	۶

جدول ۱۱: درجه‌بندی ریسک

گام ششم: احصای آسیب‌پذیری زیرساخت

گام هفتم: ترسیم وضعیت (پیامد شناسی شرایط ناشی از تهدید و توسعه سناریوها)

گام هشتم: تدوین سناریو

گام نهم: شاخص‌های راهنما

ویژگی‌های سناریوی معیار

سناریوهای معیار باید دارای ویژگی‌های زیر باشند تا بتوانند ما را به نتایج مطلوب برسانند (۱۷):

۱. با شناخت کامل از محیط زیرساخت تهیه شود.

۲. جامع باشد.

۳. اثرات و عملکرد ناشی از وقوع تهدید در آن احصا شود.

۴. واقعی و منطبق با شرایط و امکانات باشد.

۵. مطابق با اهداف، رفتار و توانایی دشمن تدوین شود.

۶. پاسخگوی مقابله با تهدیدات باشد.

۷. فرایند اجرای مراحل سناریو، هماهنگ باشد.

۸. در آن به جزئیات پرداخته و همزمان به کلیات کار توجه شود.

۹. یکنواخت نباشد و از منحنی شروع، اوج و پایان تبعیت کند.

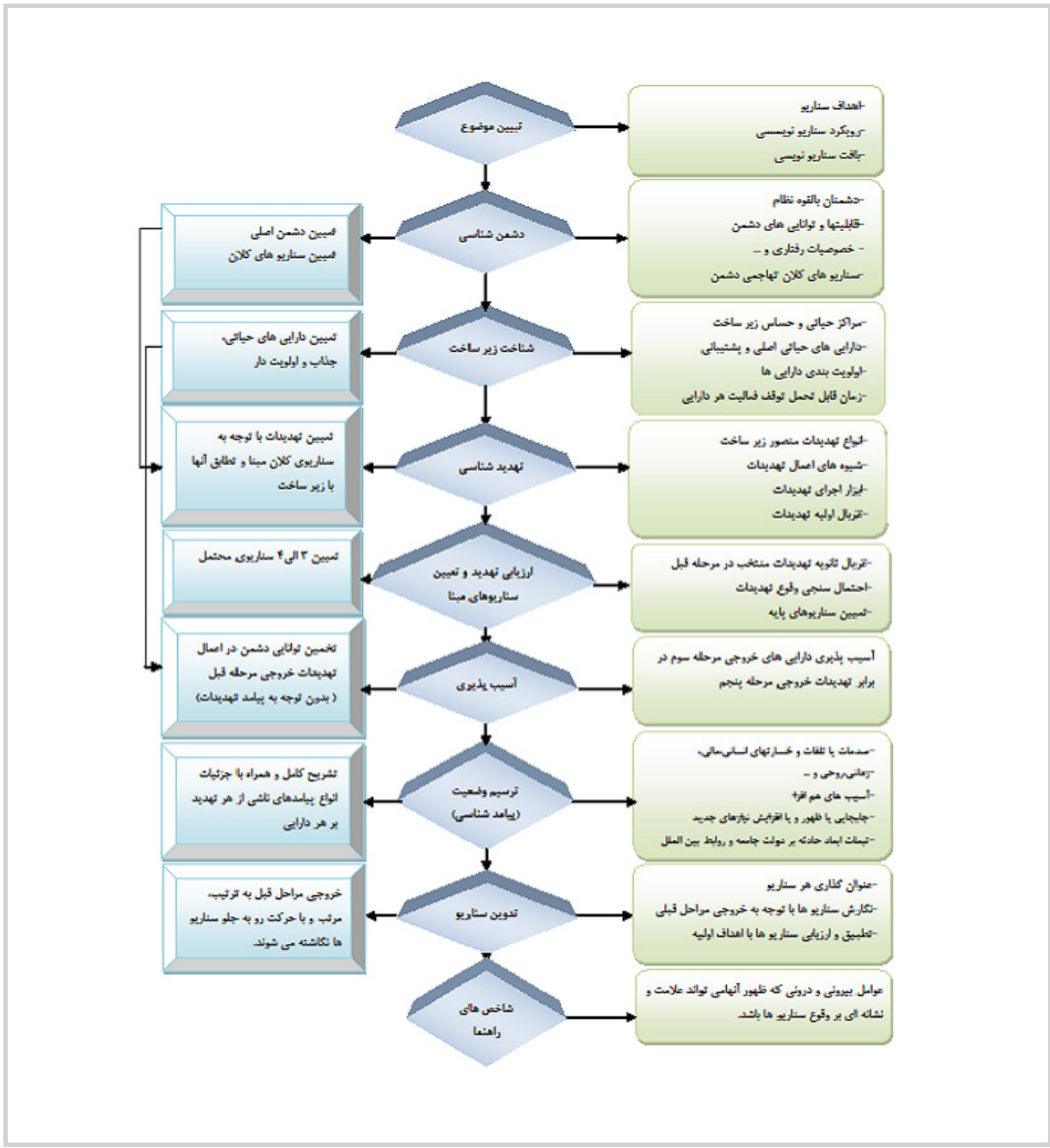
۱۰. قابل اجرا باشد.

۱۱. منعطف باشد و با افزایش یا کاهش دامنه‌ی تهدید به راحتی تغییر کند.

انتظارت پیش رو از یك سناریوی معیار

یك سناریو زمانی به معنای واقعی کلمه اثربخش است که بتواند:

۱. میزان شناخت ما را نسبت به دشمن و قابلیت‌هایش ارتقا دهد.



شکل ۲: چارچوب کلی فرایند تدوین سناریوی معیار (نگارندگان)

۲. از بین کلیه تهدیدات احتمالی ما را به تهدید مبنا نزدیک‌تر کند.

۳. سلسله علت‌ها و معلول‌ها را پس از کشف، تبیین کند.

۴. ارتباط بین بخشی و تعامل با مجموعه‌های درگیر در سناریو را مشخص کند.

۵. تصویری هرچند کلی از حادثه و پیامدهای آن و هم‌افزایی تهدیدات ارائه کند.

۶. ما را به راهکارهای برون‌رفت از بحران احتمالی راهنمایی کند.

تجزیه و تحلیل و نتیجه‌گیری

همان‌گونه که اشاره شد، الگوی ارائه شده با عنایت به فضای تهدید و شرایط خاص کشورمان به‌گونه‌ای تعریف شده است که بتواند دربرگیرنده بسته‌ای از تهدیدات برای یك زیرساخت باشد. نظر به اهمیت این موضوع و از آنجا که سناریوهای دشمن در طول زمان دچار تغییر می‌شود، باید در ارائه‌ی الگو، تمامی احتمالات متصور را مد نظر قرار داد که بر این اساس، جداول و خروجی‌های هر یك از آنها در این بخش مورد تجزیه و تحلیل قرار خواهد گرفت. همان‌طور که قبلاً عنوان شد، در این الگو نخست باید فضای مورد ارزیابی به دقت بررسی شود و اهمیت آن برای کشور لحاظ شود. همچنین میزان اثرگذاری یك زیرساخت در مدیریت و اداره‌ی

جامعه، فضای تحت پوشش و وابستگی دیگر زیرساخت‌ها به آن و ... از جمله مواردی است که باید در ارزیابی ماهیتی یك زیرساخت بدان توجه کرد. بر این اساس، جدول ارزش هدف ارائه شد. در این جدول ارزش‌های گوناگونی نظیر اقتصادی، سیاسی، اجتماعی، دفاعی و ... برای تعیین اولویت زیرساخت‌ها و مشخص شدن سطوح حیاتی، حساس و مهم آن پیشنهاد شد که کمك شایانی به گروه ارزیاب می‌کند و در واقع، اولویت نیازها را که با توجه به محدودیت زمان و منابع همراه است، پیش چشم مدیران قرار می‌دهد. پس از تعیین اولویت‌ها و مشخص شدن زیرساخت مورد ارزیابی، لازم است که فضاهای عملکردی زیرساخت و دارایی‌های آن مورد تحلیل قرار گیرد. بر این اساس، ابتدا با تعریف یك جدول سطح‌بندی که در آن ۵ شاخصه برای ارزشیابی دارایی مطرح شده بود، ارائه و سپس ضمن تعریف طیفی هر شاخص و دادن یك ضریب عددی وضعیت هر دارایی در نسبت با این شاخص‌ها سنجیده و عدد مورد نظر استخراج می‌شود. در نهایت نیز اعداد استخراجی در یك جدول بالادستی دیگر قرار می‌گیرند و با هم جمع می‌شوند که در نهایت، وزن کمّی هر دارایی مشخص می‌شود. در این حالت چنانچه وزن هر دارایی از یك بازه عددی بیشتر باشد می‌توان آن را به عنوان اهداف جذاب دشمن لحاظ کرد که در این خصوص نیز جدول کارور با توجه به کاربرد آن معرفی شد.

جدول کارور در واقع کمك شایانی به اولویت‌بندی دارایی‌های حیاتی در یك زیرساخت می‌کند و به نوعی به ارائه‌ی فهرستی از اهداف جذاب می‌پردازد. در گام بعدی برای بررسی و شناسایی تهدیدات، ابتدا فهرستی از سناریوهای احتمالی دشمن تهیه و با استفاده از جدول امکان‌پذیری، ابعاد هر کدام تعریف می‌شود. سپس برای فهم درست از وضعیت سناریوها در نسبت با زیرساخت، یك جدول سطح‌بندی ۵ شاخصه ارائه می‌شود که در آن، هر شاخص به صورت طیفی تعریف و وزن کمّی مشخصی را به خود اختصاص می‌دهد سپس اعداد خروجی حاصل از آن را در جدول امکان‌پذیری تهدیدات قرار می‌دهیم و برای هر سناریو یك وزن کمّی محاسبه می‌کنیم. ضرورت این کار از آنجا ناشی می‌شود که می‌خواهیم فضای بروز تهدیدات را از حیث امنیتی بودن یا نظامی بودن تعریف و حجم واقعی هر تهدید در فضاهای مختلف را بررسی کنیم. در ادامه، مجدداً ضمن ارائه‌ی یك جدول سطح‌بندی که در آن شاخص‌هایی برای کمّی کردن تهدیدات ارائه و به تهدیدات احتمالی که از جدول قبلی استخراج شده است، وزن لازم اختصاص می‌یابد که در نهایت با جمع اعداد داده شده، تهدیدات که وزن بیشتری را به خود اختصاص داده‌اند به عنوان مبنای عمل در جداول بعدی مورد استفاده قرار می‌گیرند. از آنجا که هر تهدید می‌تواند پیامد خاصی داشته باشد که از حیث دامنه و اثر متفاوت از یکدیگرند، بر آن شدیم که با بهره‌گیری از ماتریس شدت پیامد، پیامدهای احتمالی هر تهدید را ارزیابی کنیم که در این خصوص جدول شدت پیامد معرفی شد.

در بخش آسیب‌پذیری نیز همانند بخش‌های قبلی ابتدا جدول سطح‌بندی پنج شاخصه‌ای با تعریف طیفی هر شاخص برای کمّی کردن وضعیت آسیب‌پذیری در هر زیرساخت تهیه و سپس با در نظر گرفتن وضعیت هر دارایی در نسبت با تهدیدات تعیین شده میزان آسیب‌پذیری هر دارایی در جدولی دیگر کمّی می‌شود. خروجی جدول مذکور بیانگر ضریب ضعف‌های موجود در یك زیرساخت است که این ضعف‌ها در برابر تهدیدات مختلف، آسیب‌پذیری زیرساخت را شامل می‌شوند. در واقع، پس از جمع اعداد جدول، آسیب‌پذیری هر دارایی مشخص می‌شود که می‌توان برای راحتی فهم این جدول از یك طیف رنگی که با یك بازه عددی مشخص شده است، استفاده کرد. مثلاً چنانچه هر چه این طیف رنگی به رنگ سرخ تمایل داشته باشد، نشان‌دهنده‌ی آسیب‌پذیری بالای دارایی و چنانچه این تمایل به سمت رنگ سبز باشد نشان‌دهنده‌ی آسیب‌پذیری کم دارایی خواهد بود.

در بخش آخر که در واقع مهم‌ترین بخش در این الگو است، باید ریسك زیرساخت استخراج شود. به این منظور ابتدا با تهیه جدول ریسك و به‌کارگیری فرمول ارزش دارایی × تهدید × آسیب‌پذیری، عددهای لازم در این فرمول را از جداول ارزش دارایی، ارزیابی تهدید و ارزیابی آسیب‌پذیری استخراج و پس از ضرب هر یك، حاصل آن را در جدول پیش‌بینی شده قرار می‌دهیم. آنگاه با تعریف یك بازه‌ی عددی که از یك طیف رنگی برای بیان آن استفاده شده است، ریسك‌های حاصله را دسته‌بندی می‌کنیم. چنانچه فی‌المثل ریسك به دست آمده در بالاترین دسته‌بندی قرار داشت، در جدول، رنگ مخصوص به خود را دریافت خواهد کرد و در نهایت به‌راحتی بالاترین ریسکی که هر یك از تهدیدات می‌توانند برای مجموعه به وجود آورند، مشخص خواهد شد. همچنین آن تهدیدی که بیش‌ترین ریسك را می‌تواند برای مجموعه‌ای از دارایی‌ها به وجود آورد، به عنوان تهدید پایه تعیین می‌شود و باید در ادامه‌ی کار بر اساس آن سناریوی معیار را تعریف کرد.

همان‌طور که اشاره شد، بر اساس آنچه در جدول پیش‌بینی شده در این الگو به دست می‌آید یك فرایند علمی برای شناخت ما از زیرساخت و دارایی‌های آن، وضعیت اهداف جذاب برای دشمن، وضعیت سناریوهای احتمالی تهدید و تهدیدات ممکن، وضعیت آسیب‌پذیری مجموعه در برابر طیفی از تهدیدات، وضعیت پیامدهای تهدید در صورت وقوع و در نهایت، وضعیت ریسك زیرساخت در برابر طیفی از تهدیدات است. در این الگو سعی شده است که مطابق با شرایط و فضای متنوع تهدیدات، ضمن برشماری شاخص‌های صحیح و تبیین درست آن، براورد کمّی دقیق از مؤلفه‌های ریسك حاصل شود و این مهم نیز با به‌کارگیری منطق فازی و بر اساس اصل تبدیل مباحث توصیفی- کیفی به اعداد کمّی به دست خواهد آمد.

پیشنهادهای مبتنی بر الگو

نظر به کاربرد این الگو در مطالعات پدافندی به‌ویژه در حوزه امنیت زیرساخت‌ها که بخش مهم آن برای رسیدن به راهکارهای افزایش امنیت زیرساخت‌ها و کاهش آسیب‌پذیری آنها صرف می‌شود، به‌کارگیری الگوی پیشنهادی امری ضروری و اجتناب‌ناپذیر خواهد بود .

بر این اساس و با توجه به مطالعات ارزیابی خطرپذیری در زیرساخت‌ها که هدف آن ایجاد سپر پدافند غیرعامل در یک کشور است، پیشنهادهای زیر که می‌تواند از الگوی ارزیابی به صورت عمومی منتج شود، ارائه می‌شود:

۱. پیشنهاد می‌شود که هنگام بررسی دارایی‌ها بر اساس این الگو سازه‌ها، فضاها و تجهیزات موجود در آن به‌صورت جداگانه مورد بررسی قرار گیرد.

۲. پیشنهاد می‌شود که هنگام ارزیابی پیامدها بر اساس این الگو، به‌گونه‌ای ویژه به ارتباطات بین بخشی عناصر زیرساخت توجه شود.

۳. پیشنهاد می‌شود که هنگام ارزیابی جذابیت هدف بر اساس این الگو، سناریوهای احتمالی تهدید مد نظر قرار گیرد.

۴. پیشنهاد می‌شود که مدیران دستگاه‌ها برای ارزیابی زیرساخت‌ها بر اساس این الگو، از مشاوران پدافندی و گروه کارآمد استفاده کنند.

۵. پیشنهاد می‌شود که در ارزیابی زیرساخت‌ها بر اساس این الگو، سطوح حمایتی زیرساخت مورد تحلیل قرار گیرد.

پیشنهاد می‌شود که در سه مرحله مطالعه، طراحی و ساخت سازه‌ها، اثربخشی راهکارهای ارائه شده در امنیت آن سازه‌هایی که مبتنی بر خروجی این الگو است، مورد توجه قرار گیرد.

منابع

۱. عبداله خانی، علی (۱۳۸۵)، بررسی و نقد نظریه امنیتی ساختن، فصلنامه مطالعات راهبردی، شماره ۳۳، تهران

2. FEMA (2003), Risk Management Series ,Risk Assessment FEMA 426, www.fema.gov.

3. FEMA (2003), Risk Management Series ,Risk Assessment FEMA 427, www.fema.gov.

4. FEMA (2003), Risk Management Series ,Risk Assessment FEMA 428, www.fema.gov.

5. FEMA (2003), Risk Management Series ,Risk Assessment FEMA 429, www.fema.gov.

6. Ramcap.the faramework.asme innovative technologies institute (2006), llc.ve2. www.asme-iti.org

۷. علمداری، شهرام (۱۳۸۷)، دستورالعمل براورد تهدید و تدوین سناریو در دستگاه‌های کشور و استانی، سازمان پدافند غیرعامل، تهران

۸. عبداله خانی، علی (۱۳۸۶)، تهدیدات امنیت ملی، انتشارات موسسه ابرار معاصر تهران، تهران

۹. ستاره، علی اکبر (۱۳۹۰)، مدیریت خطرپذیری در پدافند غیرعامل، انتشارات دانشگاه صنعتی مالک اشتر، تهران

۱۰. جلالی، غلامرضا (۱۳۸۹)، روش و الگو براورد تهدیدات در پدافند غیرعامل، انتشارات دانشگاه امام حسین (ع)، تهران

۱۱. ستاره، علی اکبر (۱۳۸۸)، الگوسازی مدیریت خطرپذیری برای تداوم حیات و فعالیت‌های سازمان در برابر تهدیدات، پایان‌نامه کارشناسی ارشد، رشته مهندسی پدافند غیرعامل، دانشکده آمایش و پدافند غیرعامل، دانشگاه صنعتی مالک اشتر

۱۲. علوی‌فر، سید ناصر (۱۳۸۹)، جزوه آموزشی سناریوی تهدید طراحی برای زیرساخت‌های حیاتی، تهران

۱۳. مرادیان، محسن (۱۳۸۵)، درآمدی بر ابعاد و مظاهر تهدیدات، انتشارات مرکز آموزشی و پژوهشی شهید سپهبد علی صیاد شیرازی، تهران

۱۴. عبداله خانی، علی (۱۳۸۶)، مبانی تروریسم شناسی ، موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران

۱۵. افتخاری، اصغر (۱۳۸۷)، براورد تهدید رویکردی سیستمیک، انتشارات دانشگاه عالی دفاع ملی، تهران

۱۶. جلالی غلامرضا (۱۳۸۹)، جزوه آموزشی بررسی تهدیدات، دانشگاه عالی دفاع ملی، تهران

۱۷. ذوالقدر، محمد (۱۳۸۹)، جزوه آموزشی سناریونویسی، دانشگاه صنعتی مالك اشتر، تهران