فصلنامهٔ پدافند غیرعامل و امنیت (پژوهشی)
سال سیزدهم: شمارهٔ ۵۱ - تابستان ۱۴۰۴
صص: ۱۱۹ - ۱۴۹

Quarterly of Passive Defense & Security
Vol.13, No.51,Summer 2025
P-P: 119 - 149

مدیریت اطلاعاتی در شبکه زیرساخت‌های حیاتی با تمرکز بر ارائه راهبرد

(مطالعه موردی: سد لتیان)

سعید مددی[۱]
محسن مبینی[۲]
عبدالله جلالی‌نسب[۳]

چکیده

زیرساخت‌های حیاتی و دارایی‌های کلیدی، شریان‌های اساسی توسعه و پایداری جوامع هستند که تضمین‌کننده امنیت، رفاه و عملکرد بهینه نظام‌های اجتماعی و اقتصادی به شمار می‌روند. ارزیابی خطرپذیری اطلاعاتی به‌عنوان یکی از کارویژه‌های سازمان‌های اطلاعاتی، گامی اساسی در تضمین تاب‌آوری و پایداری زیرساخت‌های حیاتی و دارایی‌های کلیدی محسوب می‌شود.

این پژوهش با هدف ارزیابی خطرپذیری اطلاعاتی و تدوین راهبردهای مدیریت اطلاعاتی سد لتیان شکل گرفته است. جمع‌آوری اطلاعات موردنیاز پژوهش به روش مطالعه اسنادی، بررسی سوابق، انجام بازدید میدانی و مصاحبه تخصصی نیمه‌ساختاریافته انجام شده است و اطلاعات به‌دست‌آمده با محوریت روش متاسوات و در محیط نرم‌افزار اختصاصی آن، مورد تجزیه‌وتحلیل قرار گرفت. در فرایند تحقیق، در مجموع تعداد ۱۹ آسیب‌پذیری و تهدید اطلاعاتی در پنج بعد اسناد و مدارک، نیروی انسانی، حفاظت فیزیکی و تأسیسات، اطلاعات و ارتباطات و قوانین و فرایندها احصاء و با استفاده از ماتریس خطرپذیری مورد ارزیابی قرار گرفت که نتایج به‌دست‌آمده حاکی از خطرپذیری اطلاعاتی سد لتیان با درجه متوسط است. در ادامه مراحل پیاده‌سازی متاسوات، تعداد هشت کلان‌روند مؤثر در مدیریت اطلاعاتی سد لتیان با رویکرد پستل

---

۱. نویسنده مسئول، دانشجوی دکتری تخصصی رشته حفاظت ملی، دانشگاه اطلاعات و امنیت ملی
۲. عضو هیئت‌علمی، وزارت علوم، تحقیقات و فناوری
۳. استادیار دانشگاه فرماندهی و ستاد آجا

شناسایی و تناسب آن‌ها با اهداف تعریف شده و خطرپذیری‌های احصاشده برمبنای چهار عامل وزن، تأثیر، احتمال افزایش و درجه اضطرار مورد ارزیابی قرار گرفت و نقشه راهبردی قدرت و تناسب عوامل به دست آمد. در پایان برمبنای سه عامل نزدیکی آسیب‌پذیری‌ها و تهدیدات به کلان‌روندها، مختصات هر یک از عوامل و اندازه حباب‌ها، راهبردهای مدیریت اطلاعاتی سد لتیان تدوین و ارائه شد.

کلمات کلیدی: مدیریت اطلاعاتی، خطرپذیری، آسیب‌پذیری، تهدید، زیرساخت حیاتی

۱- مقدمه و بیان مسئله

زیرساخت‌های هر کشور، بستر مهم حیات، رشد و پویایی آن به شمار می‌رود، برخی از زیرساخت‌ها نقشی حیاتی در حفظ منافع ملی دارند و به‌عنوان یکی از ارکان مهم پیشرفت، اختلال هرچند کوتاه‌مدت در عملکرد آن‌ها می‌تواند منجر به آسیب جدی در اقتصاد و امنیت ملی شود؛ زیرساخت‌ها، جریانی به‌هم‌پیوسته از خدمات و پشتیبانی‌ها را برای تأمین نیازهای اساسی به جامعه ارائه می‌دهند و آسیب یا اختلال در عملکرد و کارکرد آن‌ها می‌تواند قطع خدمات زیرساختی به مردم و جامعه را در پی داشته باشد (طرح راهبردی حفاظت از زیرساخت‌های کشور، ۱۴۰۲). زیرساخت‌های حیاتی، ارائه‌دهنده خدمات اساسی و بنیادی هستند و از این چارچوب اصلی برای پشتیبانی از ساختارهای کلان امنیت ملی کشور و آحاد ملت است (پورشاسب و نظری‌نژاد، ۱۳۹۹: ۲۹۳). ازآنجایی‌که بیشتر عملکردهای جامعه وابستگی شدیدی به عاملیت زیرساخت‌های حیاتی دارد، هرگونه اختلال در کارکرد یکی از زیرساخت‌ها می‌تواند منجر به ایجاد پیامدهای مخرب در سایر زیرساخت‌های وابسته و به‌تبع آن در کل جامعه گردد؛ ازاین‌رو، بحث حفاظت از زیرساخت‌های حیاتی به یکی از اولویت‌های تحقیقاتی قرن بیست‌ویکم تبدیل شده است (میریوسفی و غفارپور، ۱۳۹۹: ۱). زیرساخت‌های حیاتی به‌دلیل اهمیت و نقش حیاتی آن‌ها در امنیت ملی کشورها، همواره یکی از اهداف جذاب برای حملات عمدی فیزیکی، نفوذ، سایبری و تجاوز کشورهای متخاصم بوده است. اقتصاد پایدار و توسعه جوامع، بدون برنامه‌ریزی راهبردی برای حفاظت و تأمین امنیت زیرساخت‌های حیاتی امکان‌پذیر نیست (Petit et al,2018). لذا حفاظت از زیرساخت‌های حیاتی در مقابل انواع

تهدیدات و آسیب‌پذیری‌ها، ضرورتی اجتناب‌ناپذیر است. یکی از حوزه‌های بسیار مهم و کلیدی که همواره از جنبه‌های مختلفی زیرساخت‌های حیاتی را تهدید می‌کند و روزبه‌روز بر ابعاد و گستردگی آن افزوده می‌شود، بعد اطلاعاتی است. درواقع «مدیریت اطلاعاتی دارایی‌های زیرساختی» را به جرئت می‌توان به‌عنوان اصلی‌ترین رسالت سازمان‌های اطلاعاتی در خصوص حفاظت از زیرساخت‌های حیاتی نام برد.

مدیریت یک زیرساخت از نظر اطلاعاتی به‌طور مستقیم از ابعاد مختلفی از قبیل تأسیسات و تجهیزات فنی، حفاظت فیزیکی، اسناد و مدارک، اداری و کارکنانی و غیره بر عملکرد، پایداری و تاب‌آوری آن زیرساخت تأثیر می‌گذارد. هرگونه کوتاهی یا عدم مدیریت صحیح در این حوزه‌ها می‌تواند منجر به عواقب جدی و حتی جبران‌ناپذیری را متوجه زیرساخت نماید. بنابراین یک مدیریت اطلاعاتی جامع و صحیح، اساس یک زیرساخت پایدار را شکل می‌دهد و تداوم عملیات و سرویس‌دهی آن را ضمانت می‌کند. ارزیابی خطرپذیری اطلاعاتی در زیرساخت‌ها باعث می‌شود تا تهدیدات و آسیب‌پذیری‌های اطلاعاتی را شناسایی و اولویت‌بندی کنیم، تدابیر پیشگیرانه مؤثر را پیاده‌سازی کنیم و خطرات ناشی از آن‌ها را کاهش دهیم. این ارزیابی‌ها امکان توسعه برنامه‌های پاسخ به بحران و بازیابی خدمات، پس از بروز اختلال را فراهم می‌آورد و به سازمان‌ها کمک می‌کند تا از تطابق با الزامات قانونی و مقررات اطمینان حاصل کنند. همچنین، ارزیابی خطر، بهبود استراتژی‌های امنیتی و افزایش اعتماد ذینفعان را ممکن می‌سازد و به‌طور کلی از عملکرد پایدار و ایمن زیرساخت‌های حیاتی حمایت می‌کند. یکی از دارایی‌های مهم در زیرساخت‌های کشور سدها هستند که با آسیب‌پذیری‌ها و تهدیدات متنوع و متعددی از بعد اطلاعاتی مواجه هستند. سدها با فراهم‌کردن منابع برای تأمین آب شرب، تولید انرژی، کنترل سیلاب، آبیاری کشاورزی، حفاظت از محیط زیست، ایجاد منابع آب برای صنایع، تفریح و گردشگری کاربردی به توسعه اقتصادی و اجتماعی کشورها کمک کرده و به مدیریت منابع طبیعی و کاهش خطرات زیست‌محیطی کمک می‌کنند(قلی‌زاده و همکاران،۱۳۹۶)، لذا سدها از اهمیت راهبردی برخوردارند و هرگونه اختلال در عملکرد سدها می‌تواند تبعات گسترده اجتماعی، اقتصادی و زیست‌محیطی داشته باشد.

سد لتیان به عنوان یکی از سدهای مهم اطراف تهران، نقش کلیدی در تأمین آب شرب منطقه شرق تهران و پایداری و امنیت انرژی و منابع آبی شهر تهران ایفا می‌کند که از بعد اطلاعاتی، دارای تهدیدات و آسیب‌پذیری‌های مختلفی است که تاکنون مورد ارزیابی قرار نگرفته است. ارزیابی میزان خطرپذیری سد لتیان و مدیریت اطلاعاتی مؤثر آن می‌تواند از وقوع حوادث غیرمترقبه جلوگیری کرده و پایداری و ایمنی سد را تضمین کند. بنابراین سؤال اصلی پژوهش این است که چگونه می‌توان خطرپذیری‌های اطلاعاتی مرتبط با سد لتیان را ارزیابی و راهبردهای مؤثری برای مدیریت اطلاعاتی آن تدوین کرد؟ این پژوهش با هدف ارزیابی خطرپذیری اطلاعاتی و تدوین راهبردهای مدیریت اطلاعاتی سد لتیان شکل گرفته است و اهداف فرعی زیر را دنبال می‌کند:

- شناسایی و دسته‌بندی آسیب‌پذیری‌ها و تهدیدات اطلاعاتی سد لتیان
- تهیه نقشه استراتژی و تدوین راهبردهای مدیریت اطلاعاتی سد لتیان ارزیابی وضعیت فعلی میزان خطرپذیری اطلاعاتی سد لتیان در مقایسه با سایر سدهای اطراف شهر تهران

۲- مفاهیم نظری و پیشینه تحقیق

مدیریت اطلاعاتی دارایی‌های زیرساختی: مدیریت اطلاعاتی دارایی‌های زیرساختی عبارت است از «به‌کارگیری ظرفیت‌ها، امکانات و منابع سازمان اطلاعاتی جهت رفع تهدیدات و آسیب‌پذیری‌های اطلاعاتی و صیانت از کارکرد دارایی‌های زیرساختی» (مبینی، ۱۴۰۲). چندین رویکرد متفاوت در خصوص مدیریت اطلاعاتی زیرساخت‌های و دارایی‌های کلیدی وجود دارد که عبارتند از:

- مدیریت اطلاعاتی به‌مثابه سازمان (در اطلاعات)
- مدیریت اطلاعاتی به‌مثابه محتوا (با اطلاعات)
- مدیریت اطلاعاتی به‌مثابه هویت (از اطلاعات)
- مدیریت اطلاعاتی به‌مثابه سوژه (بر اطلاعات)

زیرساخت: یک زیرساخت، ساختاری عمومی است که دارای سازمان‌دهی و نظام یکپارچه وسیع است، از ساختاری یکپارچه و کامل (نظام مخدوم) پشتیبانی می‌کند، فضایی را برای ارائه خدمت در یک زمینه مشخص فراهم می‌آورد و چارچوبی را برای

خدمت‌ها به شکل بلوک‌های خدمات ایجاد می‌کند (مجیدی و همکاران، ۸:۱۳۸۶). از منظر سازمان پدافند غیرعامل، به مجموعه‌ای از مراکز و بخش‌های فعال اعم از تجهیزات، امکانات و خدمات در فرایند تولید، تبادل، انتقال، توزیع و انتشار در حوزه‌های مختلف از قبیل «برق»، «مخابرات و ارتباطات راه دور»، «مواد و انرژی هسته‌ای»، «سامانه اطلاعات دولتی و خصوصی»، «حمل‌ونقل اعم از راه‌آهن، بزرگراه، بندرها و راه‌های آبی، فرودگاه‌ها»، «شبکه‌های بهداشت، درمان و سلامت انسان، دام و محیط زیست»، «سامانه‌های کشاورزی» و موارد مشابه، زیرساخت گفته می‌شود که به‌صورت ویژه، حیاتی، حساس، مهم و قابل حفاظت دسته‌بندی می‌شوند (نظام عملیاتی پدافند سایبری کشور،۱۴۰۰).

زیرساخت‌های حیاتی: زیرساخت‌های حیاتی به شبکه‌ها، سامانه‌ها و دارایی‌هایی اطلاق می‌شود که عملکرد صحیح و مداوم آن‌ها برای عملکرد اساسی جامعه، اقتصاد و امنیت ملی ضروری است (Brian,2017). «زیرساخت‌های حیاتی، سازمان‌ها یا امکاناتی که برای منافع ملی اهمیت کلیدی دارند و شکست یا نقص در آن‌ها می‌تواند منجر به کمبود زیان‌آور عرضه، اختلال قابل‌توجه در جامعه یا آثار شدید مشابه شود» (واعظی‌نژاد و مقدس، ۱۳۹۴: ۳). زیرساخت‌های حیاتی کشور حوزه بسیار گسترده‌ای از حوزه‌های فنی گرفته تا سایبری را شامل می‌شود. درواقع زیرساخت‌هایی که به‌نوعی موضوع تداوم تأمین نیازهای اساسی مردم ازجمله آب، برق، گاز، انرژی، حمل‌ونقل، ارتباطات، بهداشت و درمان، غذا، امنیت و غیره راه تأمین می‌کند به‌عنوان زیرساخت حیاتی شناخته می‌شود (عراقی‌زاده و کاملی، ۱۴۰۱: ۲). زیرساخت‌های حیاتی هر سامانه‌ای چه در سطح کلان آن به عنوان یک کشور و چه در سطح منطقه‌ای و محلی، نقشی کلیدی در ادامه جریان حیات و پویایی آن سامانه بر عهده دارند (Liu and Song,2020).

دارایی کلیدی: دارایی کلیدی، یک منبع حیاتی، جزء یا بخشی از زیرساخت ضروری برای عملکرد یک سامانه، سازمان یا کشور است. این دارایی‌ها بسیار با ارزش در نظر گرفته می‌شوند زیرا ازدست‌دادن، آسیب یا اختلال آن‌ها می‌تواند به‌طور قابل‌توجهی بر عملیات، ایمنی، ثبات اقتصادی یا امنیت ملی تأثیر بگذارد. دارایی‌های کلیدی برای اطمینان از ثبات و تداوم خدمات ضروری توسط زیرساخت‌های حیاتی محافظت و مدیریت می‌شوند. شناسایی و حفاظت از دارایی‌های کلیدی اغلب بخشی از استراتژی‌های

مدیریت خطرپذیری و یا بازیابی بلایا در یک شبکه زیرساخت است. دارایی‌های کلیدی شامل عناصری هستند که در صورت خرابی، آسیب یا اختلال در آن‌ها، می‌توانند به اختلالات گسترده در عملکرد جامعه، اقتصاد و امنیت کشورها منجر شوند. این دارایی‌ها از اهمیت حیاتی برخوردارند و شامل تجهیزات فیزیکی، فنّاوری‌ها، سامانه‌های اطلاعاتی و فرایندهای عملیاتی می‌شوند که در بخش‌هایی مثل انرژی، حمل‌ونقل، مخابرات، بهداشت، تأمین آب و امنیت غذایی قرار دارند.

سدها و زیرساخت‌های حیاتی: جایگاه سدها در زیرساخت‌های حیاتی به سه حالت تعریف می‌شود:

- به عنوان بخشی از زیرساخت حیاتی آب و فاضلاب یک کشور محسوب می‌شوند که در این حالت یک دارایی[1] در شبکه زیرساخت‌های حیاتی قلمداد می‌شود.
- به‌طور مستقل از زیرساخت حیاتی آب و فاضلاب، به عنوان یک دارایی کلیدی[2] محسوب می‌شوند.
- به‌تنهایی به عنوان یک زیرساخت حیاتی محسوب می‌شوند برای مثال در ایالات‌متحده آمریکا، سدها به عنوان یکی از زیرساخت‌های ۱۸گانه در وزارت امنیت داخلی تعریف شده‌اند.

در این پژوهش، سدها به‌عنوان بخشی از شبکه زیرساخت حیاتی آب و فاضلاب کشور در نظر گرفته شده است. در طرح راهبردی حفاظت از زیرساخت‌های کشور سازمان پدافند غیرعامل نیز، عنوان سدها مشخصاً قید نشده است ولی از زیرساخت حیاتی آب، به عنوان حوزه‌های با اهمیت بالا یاد شده است. در تقسیم‌بندی سازمان پدافند غیرعامل از منظر مراکز حیاتی، حساس، مهم و قابل حفاظت نیز از سدها به‌عنوان یک مرکز مهم یاد شده است.

آسیب‌پذیری[3] و تهدید[4]: طبق تعریف مؤسسه ملی استانداردها و فنّاوری آمریکا (NIST[5])، آسیب‌پذیری به عنوان «ضعف در یک سامانه یا دارایی که ممکن است توسط

1. Property
2. Key asset
3. Vulnerability
4. Threat
5. NIST: National Institute of Standard and technology

یک تهدید مورد سوءاستفاده قرار گیرد» تعریف شده است (NIST,2012). در استاندارد ISO/IEC 27005نیز آسیب‌پذیری به عنوان هر ضعف داخلی در یک سازمان یا سامانه که می‌تواند احتمال بهره‌برداری توسط یک تهدید را افزایش دهد، تعریف شده است (ISO,2018). از ویژگی‌های کلیدی آسیب‌پذیری می‌توان به ذاتی یا داخلی بودن و پتانسیل برای بهره‌برداری اشاره نمود. مؤسسه ملی استانداردها و فنّاوری آمریکا (NIST)، تهدید را به‌عنوان «هر ظرفیتی که به‌طور بالقوه می‌تواند به یک سامانه یا داده آسیب برساند» تعریف می‌کند. تهدید به‌صورت کلی یک عنصر یا رویداد خارجی است که قصد یا امکان سوءاستفاده از ضعف‌های یک سامانه را دارد (NIST,2012). در استاندارد/ISO IEC 27005نیز تهدید به‌عنوان «رویداد یا موجودیتی که ممکن است به سامانه آسیب بزند و از آسیب‌پذیری‌ها سوءاستفاده کند» تعریف شده است. از ویژگی‌های کلیدی تهدید می‌توان به خارج از سامانه بودن یا به‌صورت رویدادی بودن و بهره‌برداری از آسیب‌پذیری اشاره نمود. به‌طور کلی تفاوت بین آسیب‌پذیری و تهدید را در دو بعد به شرح ذیل می‌توان خلاصه نمود:

- ماهیت: آسیب‌پذیری یک ضعف یا نقص در سامانه است، درحالی‌که تهدید یک عامل خارجی یا رویداد است که ممکن است از این ضعف بهره‌برداری کند.
- تعامل با یکدیگر: آسیب‌پذیری بدون تهدید به‌تنهایی خطر ایجاد نمی‌کند. تهدید نیاز به وجود آسیب‌پذیری برای سوءاستفاده دارد. درواقع وقتی یک تهدید از یک آسیب‌پذیری استفاده کند، خطر ایجاد می‌شود. بنابراین ترکیب این دو می‌تواند منجر به بروز خطر امنیتی و اطلاعاتی گردد.

خطرپذیری[1]: واژه خطرپذیری از واژه ایتالیایی یسیکار[2] مشتق که به معنای «جرئت کردن» است. خطرپذیری مفهومی است که بشر در طول تاریخ همواره با آن سروکار داشته است. خطرپذیری به‌عنوان فرصت ایراد خسارت به یک شخص یا یک دارایی باارزش از طریق وقع یک حادثه یا اقدام خصمانه است (Woodruff, 2005). خطرپذیری احتمال رخداد یک خطر در خلال یک دورهٔ زمانی مشخص است (Godschalk et al, 1998). به‌طور کلی خطرپذیری برابر است با حاصل‌ضرب احتمال در پیامد یا تأثیر یک رویداد (Ansell and Wharton, 1992).

1. Risk
2. Risicare

خطرپذیری = احتمال وقوع * شدت یا تأثیر یک رویداد

در حوزه پیشینه تحقیق، به‌طور کلی در حوزه مطالعات مربوط به ارزیابی خطرپذیری اطلاعاتی، ادبیات بسیار ضعیفی وجود دارد. در مطالعات داخلی مرتبط می‌توان به پژوهش اسدالله‌فردی و همکاران با عنوان «ارزیابی آسیب‌پذیری تأسیسات آب‌رسانی با روش تلفیقی AHP وRAMCAP » اشاره نمود که در پژوهش مذکور، گروه پژوهشی زیرساخت‌های آبی شهر تهران شامل سدها، تصفیه‌خانه‌ها، مخازن ذخیره، چاه‌ها، تلمبه‌خانه‌ها و شبکه برق از بعد آسیب‌پذیری بر اساس شاخص‌های قابلیت کشف، دسترسی به هدف، ضعف بخش، قابلیت بازسازی، آسیب‌های ثانویه و شاخص اثرات آسیب‌پذیری موردبررسی قرار داده بودند (اسدالله‌فردی و همکاران، ۱۳۹۹). سایر مطالعات مهم داخلی در جدول(۱) آورده شده است.

جدول(۱) مطالعات داخلی مرتبط با بررسی خطرپذیری زیرساخت‌های آبی

ردیف	عنوان پژوهش	پژوهشگر	سال	نتایج
۱	ارزیابی و اولویت‌بندی خطر سدها با استفاده از روش ترکیبی DEMATEL-ANP	راضیه خسروی‌طائمه و همکاران	۱۴۰۲	در این پژوهش خطرهای سه سد طالقان، ماملولار از چهار بعد اجتماعی، اقتصادی، فنی-مدیریتی و زیست‌محیطی با ۴۲ معیار مورد ارزیابی قرار گرفتند.
۲	ارزیابی آسیب‌پذیری تأسیسات آب‌رسانی با روش تلفیقی AHP وRAMCAP	غلامرضا اسدالله‌فردی و همکاران	۱۳۹۹	در این پژوهش زیرساخت‌های آبی شهر تهران شامل سدها، تصفیه‌خانه‌ها، مخازن ذخیره، چاه‌ها، تلمبه‌خانه‌ها و شبکه برق از بعد آسیب‌پذیری بر اساس شاخص‌هایی از قبیل قابلیت کشف، دسترسی به هدف و ضعف بخش و غیره موردبررسی قرار گرفته است.
۳	تحلیل خطر در ضداطلاعات با استفاده از ماتریس خطر	غلامرضا سادات	۱۳۹۸	در این پژوهش یک مارتیس کیفی-کمی برای خطرهای ضداطلاعاتی ارائه شده است.
۴	تحلیل آسیب‌پذیری عناصر زیرساخت آب شهری در مقابل تهدیدات تروریستی	فاطمه بخشی شادمهری و همکاران	۱۳۹۸	در این پژوهش نشان دادند که همه دارایی‌ها به‌جز چشمه آسیب‌پذیری بالایی دارند و بیش‌ترین آسیب اقدامات تروریستی به لوله‌های توزیع آب و مخازن زمینی، بیوتروریسم به سدها و ایستگاه پمپاژ، تروریست سایبری به سدها و تصفیه‌خانه‌هااست.

در حوزه مطالعات بین‌المللی، غالب مطالعات انجام شده بیشتر متمرکز بر ارزیابی خطرپذیری‌های ایمنی و امنیتی سدها است که غالباً نیز رویکرد فنی و کمی دارند که به دو نمونه از آن‌ها در جدول (۲) اشاره شده است.

جدول(۲) مطالعات خارجی مرتبط با بررسی خطرپذیری زیرساخت‌های آبی

ردیف	عنوان پژوهش	پژوهشگر	سال پژوهش	نتایج
۱	Risk assessment and risk management for dams	Michael Harrington	۲۰۲۲	این پژوهش یک چارچوب کلی و عملی را برای انجام تجزیه‌وتحلیل خطر یک سد ارائه نموده و روش‌های کمی را ارزیابی و مدیریت خطر و همچنین برنامه‌ریزی برای آمادگی سد برای واکنش اضطراری با تمرکز بر سدهای کشور نروژ پیشنهاد داده است.
۲	Assessing and managing safety risks	Camila and et al	۲۰۲۴	این مطالعه با هدف درک چگونگی آسیب‌پذیری ایمنی سدها و پیامدهای آن برای جوامع پایین‌دستی آن در کشور برزیل انجام شده است. این پژوهش روش‌های مختلف را برای ارزیابی خطر بکار گرفته و نشان داده است که قوانین و استانداردهای موجود، هنوز مرجع مناسبی برای تضمین ایمنی زیست‌محیطی سدها نیستند.
۳	A Review of Research and Practice on the Theory and Technology of Reservoir Dam Risk Assessment	Zhang and et al	۲۰۲۳	این تحقیق به بررسی روش‌های رایج ارزیابی خطر سدها می‌پردازد. این مقاله روش‌های متداولی مانند ارزیابی خطر احتمالی (PRA)، تحلیل حالات خرابی و اثرات (FMEA) و تحلیل درخت رویداد (ETA) را تحلیل می‌کند و نقاط قوت و ضعف آن‌ها را برجسته می‌کند. نویسندگان به این موضوع اشاره دارند که این روش‌ها معمولاً تمام عدم‌قطعیت‌ها و وابستگی‌های موجود در سامانه‌های سد را به‌طور کامل در نظر نمی‌گیرند. مقاله بر لزوم استفاده از نظریه سامانه‌ها و تکنیک‌های پیشرفته مدل‌سازی برای بهبود دقت ارزیابی‌های خطر تأکید می‌کند و خواستار اصلاح چارچوب‌های قانونی برای هم‌راستاسازی بهتر مدیریت خطر با چالش‌های واقعی می‌شود.

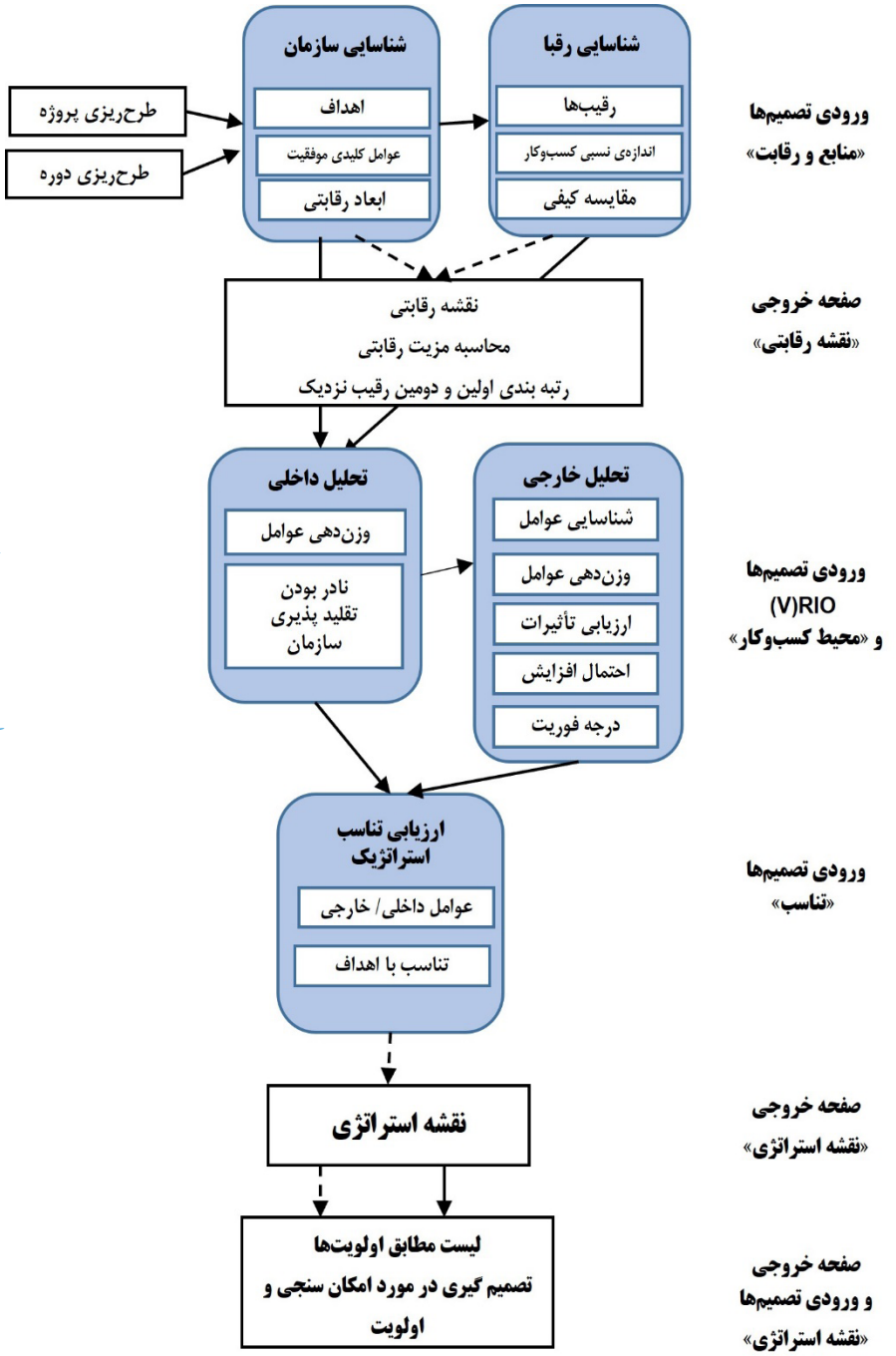
وجه تمایز و نوآوری این پژوهش، دارای دو جنبه است. بعد اول ناظر بر تعریف و به‌کارگیری اصطلاحات جدید و تولید ادبیات پژوهشی جدید و بعد دوم ناظر بر طرح روش‌های جدید یا توسعه و بهینه نمودن روش‌های موجود به منظور به‌کارگیری درزمینهٔ

ارزیابی خطرپذیری اطلاعاتی است. در این پژوهش مفاهیمی از قبیل «مدیریت اطلاعاتی دارایی‌های زیرساختی» و «ارزیابی خطرپذیری اطلاعاتی» مطرح شده است که جزء مطالعات اولیه در این حوزه است که تاکنون ادبیات چندانی در این حوزه تولید نشده است. جنبه دوم نوآوری استفاده از روش متاسوات در ارزیابی خطرپذیری اطلاعاتی است که به نظر می‌رسد این روش نوآورانه به‌ویژه در ارزیابی خطرهای اطلاعاتی مفید بوده و می‌تواند به مدیران و مسئولین در حوزه سدها کمک می‌کند تا با شفافیت بیشتری به ارزیابی و تصمیم‌گیری در مواجهه با تهدیدات اطلاعاتی بپردازند.

۳- روش‌شناسی

این پژوهش با توجه به ماهیت آن، توصیفی- تحلیلی است. برای تدوین چارچوب نظری و مرور پیشینه تحقیقات، از روش کتابخانه‌ای (اسنادی) بهره گرفته شد. جمع‌آوری اطلاعات در این پژوهش به‌صورت میدانی و انجام مصاحبه تخصصی صورت گرفته است. در فرایند پژوهش، یک گروه کارشناسی ۵نفره به‌صورت میدانی و دوره‌ای از کلیه سدهای اطراف تهران شامل سد لتیان و سدهای ماملو، امیرکبیر، طالقان و لار بازدید و ارزیابی تخصصی به عمل آوردند و از کارشناسان بخش‌های مختلف سدهای مذکور، مصاحبه‌های تخصصی نیمه‌ساختاریافته به عمل آورند. روش تحقیق، کیفی و میدانی و نوع پژوهش کاربردی است. جامعه آماری نیز شامل مسئولین، حراست و کارشناسان سد هستند که اطلاعات لازم در خصوص ارزیابی آسیب‌پذیری اطلاعاتی سد را ارائه نمودند. روش نمونه‌گیری غیرتصادفی هدفمند است و افراد بر اساس تجربه، تخصص و نقش آن‌ها در مدیریت، بهره‌برداری و حراست از سد انتخاب شده‌اند و بازدید میدانی نیز از بخش‌های مهم و کلیدی سد بر اساس اهداف تحقیق به‌صورت هدفمند گردید. حجم نمونه نیز شامل تعداد شش نفر از کارشناسان و مسئولین حراست سد است.محوریت روش تجزیه‌وتحلیل داده‌ها در پژوهش، روش متاسوات[1] است که مراحل کلی پیاده‌سازی در شکل (۱) نشان‌داده‌شده است. ازآنجایی‌که این روش بر اساس رهیافت داخل به خارج[2] و به‌نوعی بر دیدگاه مبتنی بر منابع[3] استوار است؛ لذا به منظور بهره‌گیری از این

1. Meta-SWOT
2. Inside-out
3. Resource Based View (RBV)



شکل(۱) فرایند پیاده‌سازی روش متاسوات (Ravi,2015:17)

شناسایی و ارزیابی آسیب‌پذیری و تهدیدات اطلاعاتی که در مرحله اول متاسوات یعنی شناسایی سازمان و زیرمرحله دوم یعنی عوامل کلیدی موفقیت صورت گرفته است، در سه گام زیر و با استفاده از روش تحلیل خطرپذیری با استفاده از ماتریس خطر انجام شده است (سادات، ۱۳۹۸).

- گام اول: مراجعه به جدول شماره ۳ برای تعیین احتمال خطر.

جدول(۳) احتمال خطر

رتبه	احتمال	شرح
۵	تقریباً حتمی	انتظار وقوع در اغلب اوقات می رود. به‌طور موقت واقع خواهد شد مگر آن‌که اقدامات برای تغییر به انجام برسد.
۴	احتمالاً	احتمالاً بعضی وقت‌ها به وقوع می پیوندد. انتظار می‌رود در بیش از ۵۰ درصد مواقع رخ دهد.
۳	گاهی اوقات	گاهی اوقات تحت یک شرایط خاص اتفاق می افتد. غیرمحتمل اما امکان وقوع وجود دارد.
۲	غیرمحتمل	تحت شرایطی امکان وقوع وجود دارد. احتمال وقوع به‌شدت پایین است. وقوع آن تاکنون دیده نشده است.
۱	به‌ندرت	تنها در شرایط استثنایی به وقوع می پیوندد. احتمال وقوع تقریباً وجود ندارد.

○ گام دوم: مراجعه به جدول شماره ۴ برای تعیین پیامد خطر.

جدول(۴) پیامد خطر

رتبه	پیامد	شرح
۱	ناچیز	تأثیر اندک یا بی اهمیت یا قابل چشم‌پوشی دارد.
۲	کم (اندک)	میزان پایینی از تأثیر برجای می‌گذارد. تأثیر برجای‌مانده سطحی است.
۳	متوسط (چشم‌گیر)	تأثر زیادی دارد. زیان ملموسی برجای می‌گذارد.
۴	عمده (زیان‌بخش)	تأثیر قابل توجهی بر وظایف، حفاظت یا توان رقابتی برجا می‌گذارد.
۵	فاجعه‌بار	منجر به از دست رفتن توانایی ها، اقدامات عملیاتی شده و تأثیر غیرقابل جبرانی برجای می‌گذارد.

○ گام سوم: واردکردن نتایج در جدول ماتریس خطر (شکل شماره ۲)

شدت	فاجعه‌بار (۵)					
	عمده (۴)					
	متوسط (۳)					
	کم (۲)					
	ناچیز (۱)					
نقشه حرارتی خطرپذیری		نادر (۱)	غیرمحتمل (۲)	امکان‌پذیر (۳)	احتمالاً (۴)	تقریباً حتمی (۵)
		احتمال				

شکل (۲) ماتریس حرارتی خطرپذیری (میرزارمضانی، ۱۴۰۲)

○ گام چهارم: مقایسه نتایج به‌دست‌آمده از جدول ماتریس خطر با استانداردهای ارائه شده در جدول (۵)

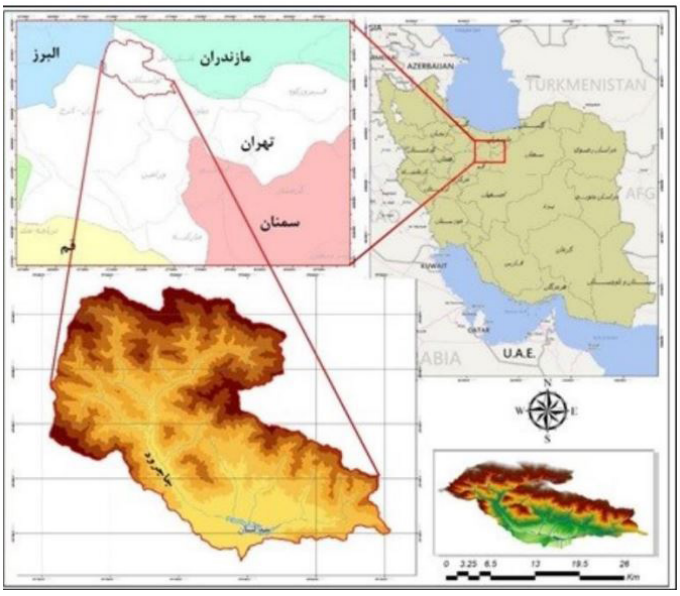
جدول(۵) راهنمای جدول ماتریس حرارتی خطرپذیری

رنگ	میزان خطرپذیری
	خطرپذیری با درجه بحرانی
	خطرپذیری با درجه بالا
	خطرپذیری با درجه متوسط
	خطرپذیری با درجه کم

معرفی منطقه موردمطالعه:

سد لتیان در جنوب شرق استان تهران و بخش مرکزی شهرستان لواسانات واقع شده است. سد لتیان با ارتفاع ۱۰۷ متر و پهنای ۴۵۰ متر و عمق ۹۹ متر به‌عنوان یکی از بزرگ‌ترین سدهای استان تهران بر روی رودخانه «جاجرود» با سطح حوضه آبریزی به مساحت ۶۹۸۰۰ کیلومترمربع و با متوسط جریان آب سالانه به میزان ۳۵۰ میلیون مترمکعب در

استان تهران و در فاصله ۳۵ کیلومتری شمال شرقی تهران و ۵ کیلومتری بخش جاجرود قرار دارد. مطالعات برای ساخت این سد در سال ۱۳۳۸ آغاز گردید و در سال ۱۳۴۲ عملیات احداث آن شروع و در سال ۱۳۴۶ به بهره‌برداری رسید. اهداف ساخت این سد ، تأمین آب شرب تهران به میزان ۲۹۰ میلیون مترمکعب از طریق تونل ۹٫۵ کیلومتری به تصفیه‌خانه تهران‌پارس، تأمین آب زراعی دشت ورامین به میزان متوسط ۱۶۰ میلیون مترمکعب و همچنین تولید متوسط سالانه ۷۰۰۰۰ مگاوات ساعت انرژی برق – آبی شبکه سراسری ایران است. در ادامه توسعه منابع آب شرب برای مصرف روزافزون تهران بزرگ، از سال ۱۳۶۷ نیز سالانه به‌طور متوسط ۱۴۰ میلیون مترمکعب آب از سد لار، از طریق تونل انتقال لار–کلان به طول ۲۰ کیلومتر به نیروگاه کلان و ازآنجا به مخزن سد لتیان انتقال داده شده است که این توسعه باعث بالارفتن حجم آب قابل تنظیم سد لتیان به میزان ۴۱۰ میلیون مترمکعب شده است. علاوه بر رودخانهٔ جاجرود که اصلی‌ترین رود این سد به شمار می‌آید رودهای کوچک‌تر دیگری همچون کُندرود، افچه، برجهان نیز به آن می‌ریزند (برنا و صحرایی‌نژاد، ۱۴۰۳: ۱۰۵). گفتنی است در این پژوهش سد لتیان به‌عنوان یک دارایی کلیدی در شبکه دارایی‌های زیرساختی آب و فاضلاب در نظر گرفته شده است.



شکل(۲) موقعیت جغرافیایی سد لتیان

۴- ارزیابی خطرپذیری و تدوین راهبردهای مدیریت اطلاعاتی سد لتیان برمبنای روش متاسوات

در گام نخست عنوان دقیق پروژه باید تعریف و دوره زمانی موردنظر مشخص گردد که عبارتند از:

برنامه‌ریزی راهبردی به منظور: مدیریت اطلاعاتی سد لتیان

دوره زمانی برنامه‌ریزی: ازآنجایی‌که یکی از اهداف مهم این پژوهش، تدوین راهبردهای مدیریت اطلاعاتی دارایی موردمطالعه است، لذا قلمرو زمانی این مطالعه برای بازه زمانی ۵ ساله در نظر گرفته شده است.

۴-۱- شناسایی سازمان

شناسایی سازمان شامل تعریف اهداف سازمانی، تعریف عوامل کلیدی موفقیت و تعریف ابعاد رقابتی است؛ به‌عبارت‌دیگر در این مرحله خطرپذیری اطلاعاتی، شناسایی و مورد ارزیابی قرارمی‌گیرد و در مراحل بعدی فرایند تدوین راهبردها برمبنای نتایج به‌دست‌آمده از این مرحله انجام می‌گیرد.

اهداف سازمانی: اهداف ارزیابی خطرپذیری اطلاعاتی نیز در جدول (۶) آورده شده است.

جدول(۶) اهداف و اولویت‌بندی آنان در مدیریت اطلاعاتی سد لتیان

کد	هدف	اولویت
G1	دستیابی به بیش‌ترین تاب‌آوری	اولویت بالا
G2	دستیابی به کمترین آسیب‌پذیری	اولویت بالا
G3	اشراف و صیانت اطلاعاتی	اولویت متوسط
G4	تحلیل و برآورد اطلاعاتی	اولویت متوسط
G5	هم‌افزایی اطلاعاتی-امنیتی	اولویت پایین
G6	معماری و مهندسی اطلاعاتی	اولویت پایین

برابر منطق تعریف شده در روش متاسوات، در این مرحله می‌بایست منابع و قابلیت‌های سازمانی شناسایی و با یکی از روش‌های موجود وزن‌دهی شوند به‌طوری‌که مجموع اوزان اختصاص یافته به موارد شناسایی‌شده ۱۰۰ باشد. ازآنجایی‌که هدف

این پژوهش از به‌کارگیری روش متاسوات، ارزیابی خطرپذیری اطلاعاتی و تدوین راهبردهای مدیریت اطلاعاتی یک زیرساخت است و محوریت تحلیل اطلاعاتی یک زیرساخت آسیب‌پذیری و تهدیدات اطلاعاتی است، لذا در این پژوهش بجای منابع از آسیب‌پذیری اطلاعاتی و بجای قابلیت از تهدیدات اطلاعاتی استفاده شده است.

برای احصاء آسیب‌پذیری‌ها و تهدیدات اطلاعاتی سد لتیان به‌دلیل نبود مرجع و استاندارد از قبل تعریف شده، از روش استقرایی یا محقق‌ساخته استفاده گردید. ابعاد و گویه‌های احصاشده نتیجه از تلفیق و ترکیب اطلاعات به‌دست‌آمده از سه منبع شامل اسناد موجود شامل منابع علمی و برخی چک‌لیست‌های مشابه موجود، پانل خبرگی شامل گروه بازدیدکننده و انجام مصاحبه‌های تخصصی نیمه‌ساختاریافته با کارشناسان سدهای مورد بازدید و همچنین اطلاعات به‌دست‌آمده از بازدید و بررسی‌های میدانی سدها است. در استخراج ابعاد و گویه‌ها سعی گردیده است موارد و مصادیق، به‌طور خلاصه ارائه شوند و تا حد امکان گویه‌های همسان و هم‌پوشان ادغام شود. جدول(۷) ابعاد و گویه‌های استخراج‌شده در آسیب‌پذیری‌ها و تهدیدات اطلاعاتی سد لتیان را نشان می‌دهد.

جدول(۷) ابعاد و گویه‌های آسیب‌پذیری‌ها و تهدیدات اطلاعاتی سد لتیان

ابعاد	کد	آسیب‌پذیری و تهدیدات
اسناد و مدارک	R1	عدم رعایت حیطه‌بندی، دست‌کاری و تغییر غیرمجاز اسناد توسط کارکنان سد
	R2	دسترسی غیرمجاز، ربایش، تخریب و افشای اطلاعات حساس سد توسط عوامل بیرونی
نیروی انسانی	R3	نشست اطلاعات حساس سد توسط عوامل داخلی با انگیزه‌های مختلف
	R4	ایجاد اختلال در فعالیت سد به‌دلیل عدم جذب نیروی‌های نخبه و کیفی، عدم احراز صلاحیت امنیتی و مهارتی کارکنان
	R5	انجام خرابکاری توسط شرکت‌های پیمانکاری، عوامل نفوذی، کارکنان مستعفی و منفک شده
حفاظت فیزیکی و تأسیسات	R6	اختلال در عملکرد سد به‌دلیل فرسودگی تأسیسات و سازه‌های فنی سد و یا استفاده از تجهیزات کهنه و تقلبی
	R7	آسیب‌دیدن سد به‌دلیل عدم بهره‌گیری از تجهیزات مناسب و به‌روز بازرسی، نظارتی و مراقبتی
	R8	ایجاد اختلال در عملکرد سد به‌دلیل اثرات آبشاری وابستگی سد به زیرساخت‌های شهری

ابعاد	کد	آسیب‌پذیری و تهدیدات
	R9	حملات تروریستی به سد و خطوط انتقال آب
اطلاعات و ارتباطات	R10	لورفتن اطلاعات به‌دلیل ضعف شبکه ارتباطی، به‌روز نبودن سامانه‌های سخت‌افزاری و نرم‌افزاری
	R11	ازبین‌رفتن اطلاعات حساس و طبقه‌بندی‌شده به‌دلیل نقص در سامانه‌های پشتیبان‌گیری و بازیابی اطلاعات
	R12	تبادل اطلاعات حفاظت نشده با ذینفعان از قبیل شرکت‌های پیمانکاری و غیره
	R13	حملات سایبری به سامانه‌های کنترل صنعتی سد
	R14	نشست اطلاعات طبقه‌بندی‌شده سد از طریق تلفن همراه، رسانه‌ها و فنّاوری‌های نوظهور
قوانین و فرایندها	R15	خلأ نظام شناسایی، ارزیابی و مدیریت اطلاعاتی سد
	R16	اختلال در عملکرد و حفظ امنیت اطلاعات سد به‌دلیل عدم تعامل مناسب با بخش خصوصی
	R17	کاهش تاب‌آوری اطلاعاتی سد در بلندمدت به‌دلیل نبود برنامه‌ریزی راهبردی مدیریت شبکه سدهای آبی
	R18	عدم تخصیص اعتبارات لازم برای رفع خلأهای اطلاعاتی سد
	R19	سوء مدیریت در بهینه‌سازی فرایندهای مدیریت اطلاعاتی سد به‌دلیل انتصابات غیرتخصصی در سطوح بالای سازمانی

در این مرحله به ارزیابی خطرپذیری وزن‌دهی به هر یک از گویه‌های استخراج‌شده به شرح ذیل پرداخته شد:

الف- به منظور ارزیابی احتمال وقوع و شدت یا تأثیر وقوع رویداد از جداول ۷ و ۸ برمبنای نظر خبرگان استفاده گردید و میانگین حسابی اوزان اختصاص داده شده به هر یک از کدها به عنوان عدد نهایی در نظر گرفته شد.

ب- میزان خطرپذیری برابر فرمول ارائه شده در بخش مفاهیم از حاصل‌ضرب احتمال درشدت/تأثیر هر کد محاسبه شده است.

پ- محاسبه درصد فراوانی نسبی گویه: ازآنجایی‌که مجموع اوزان عوامل کلیدی شناسایی‌شده در روش متاسوات می‌بایست ۱۰۰ باشد لذا در این مرحله درصد فراوانی

نسبی خطرپذیری، با تقسیم خطرپذیری هر کد بر مجموع کل خطرپذیری‌ها و ضرب عدد حاصل به ۱۰۰ محاسبه و در ستونی تحت عنوان در فراوانی نسبی درج گردید تا در مرحله بعدی جهت ورود به نرم‌افزار متاسوات آماده باشد.

جدول(۸) میزان خطرپذیری هر یک از ابعاد و گویه‌های آسیب‌پذیری‌ها و تهدیدات اطلاعاتی سد لتیان

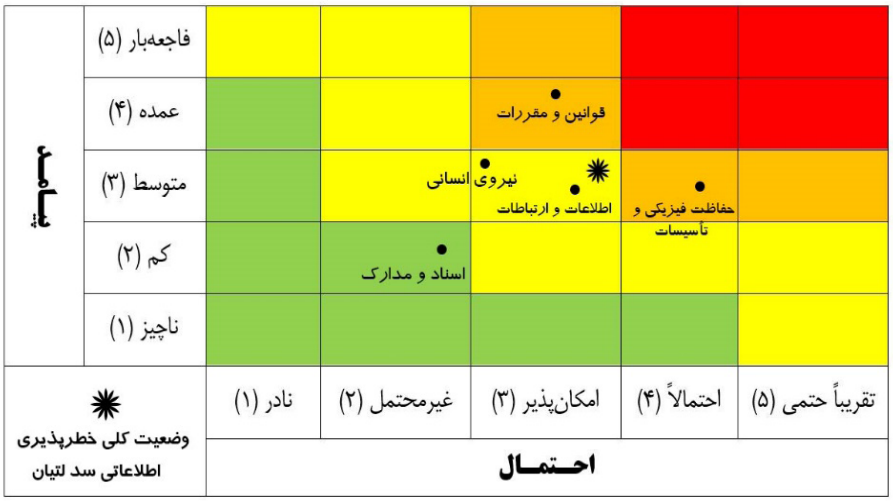
ابعاد	کد	احتمال (۱-۵)	شدت/تأثیر(۱-۵)	خطرپذیری (۱-۲۵)	درصد فراوانی نسبی
اسناد و مدارک	R1	۲٫۲	۱٫۵	۳٫۵	۲
	R2	۱٫۶	۱٫۹	۳٫۰۴	۲
نیروی انسانی	R3	۱٫۶	۲٫۳	۳٫۶۸	۲
	R4	۲٫۱	۲٫۴	۵٫۰۴	۳
	R5	۲٫۹	۳٫۷	۱۰٫۷۳	۶
حفاظت فیزیکی و تأسیسات	R6	۳٫۱	۴٫۳	۱۳٫۳۳	۸
	R7	۳٫۸	۳٫۴	۱۲٫۹۲	۷
	R8	۳٫۲	۳	۹٫۶	۶
	R9	۳٫۹	۴٫۱	۱۵٫۹۹	۹
اطلاعات و ارتباطات	R10	۲٫۲	۱٫۸	۳٫۹۶	۲
	R11	۲٫۰	۲٫۲	۴٫۴	۳
	R12	۳٫۸	۲٫۹	۱۱٫۰۲	۶
	R13	۲٫۳	۲٫۰	۴٫۶	۳
	R14	۲٫۷	۳٫۱	۸٫۳۷	۵
قوانین و فرایندها	R15	۴٫۲	۳٫۷	۱۵٫۵۴	۹
	R16	۳٫۹	۳٫۱	۱۲٫۰۹	۷
	R17	۳٫۳	۳٫۹	۱۲٫۸۷	۷
	R18	۳٫۷	۳٫۰	۱۱٫۱	۶
	R19	۳٫۹	۳٫۳	۱۲٫۸۷	۷
مجموع درصد فراوانی نسبی					۱۰۰

جدول(۹) و شکل (۳) وضعیت کلی خطرپذیری اطلاعاتی سد لتیان را به تفکیک هر یک از ابعاد پنج‌گانه اسناد و مدارک، نیروی انسانی، حفاظت فیزیکی و تأسیسات، اطلاعات و

ارتباطات و قوانین و فرایندها و همچنین خطرپذیری کلی سد را نشان می‌دهد. برابر نتایج حاصله، بعد اسناد و مدارک با مختصات (۱٫۷-۱٫۹) در خانه‌های سبز دارای خطرپذیری با درجه کم، بعد نیروی انسانی با مختصات (۲٫۸-۲٫۲) در خانه‌های زرد دارای خطرپذیری با درجه متوسط، بعد حفاظت فیزیکی و تأسیسات با مختصات (۳٫۸-۳٫۵) در خانه‌های زرد دارای خطرپذیری با درجه متوسط، بعد اطلاعات و ارتباطات با مختصات (۲٫۴-۲٫۶) در خانه‌های نارنجی دارای خطرپذیری با درجه بالا و بعد قوانین و فرایندها با مختصات (۳٫۸-۳٫۴) در خانه‌های نارنجی دارای خطرپذیری با درجه بالا است. نتایج به‌دست‌آمده همچنین نشان می‌دهد در مجموع سد لتیان از نظر خطرپذیری اطلاعاتی در ماتریس نقشه حرارتی خطرپذیری در موقعیت (۲٫۹-۲٫۷) و در خانه‌های زردرنگ قرار دارد که این موقعیت نشان‌دهنده خطرپذیری اطلاعاتی سد لتیان با درجه متوسط است.

جدول (۹) میانگین احتمال، شدت و خطرپذیری اطلاعاتی هر یک از ابعاد پنج‌گانه

ابعاد	احتمال	شدت/تأثیر	خطرپذیری
اسناد و مدارک	۱٫۹	۱٫۷	۳٫۲۳
نیروی انسانی	۲٫۲	۲٫۸	۶٫۱۶
حفاظت فیزیکی و تأسیسات	۳٫۵	۳٫۸	۱۳٫۳
اطلاعات و ارتباطات	۲٫۶	۲٫۴	۶٫۲۴
قوانین و فرایندها	۳٫۴	۳٫۸	۱۲٫۹۲
میانگین کل	۲٫۹	۲٫۷	۸٫۳۷



شکل(۳) ماتریس حرارتی خطرپذیری اطلاعاتی سد لتیان در ابعاد پنج‌گانه

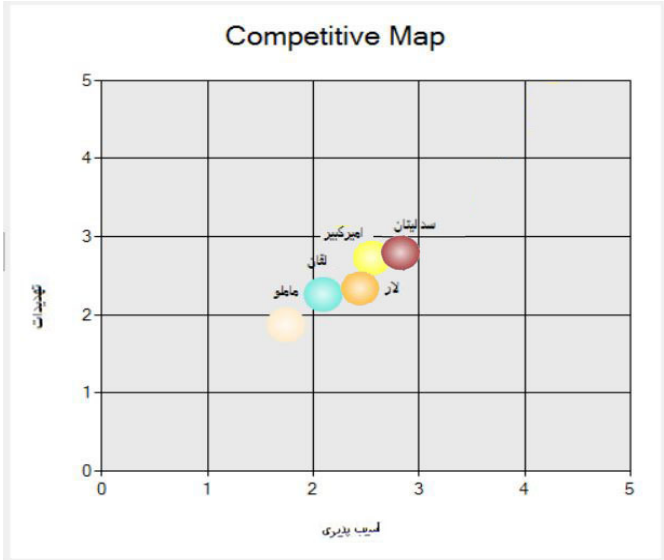
۲-۴- شناسایی رقبا

شناسایی ابعاد رقابتی[1]: ابعاد رقابتی در مدیریت اطلاعاتی یک زیرساخت یا دارایی کلیدی، میزان آسیب‌پذیری و تهدیدات اطلاعاتی آن‌ها است.

شناسایی رقبا و مقایسه آن با زیرساخت موردمطالعه از نظر آسیب‌پذیری اطلاعاتی: منظور از رقبا در بافتار ارزیابی خطرپذیری اطلاعاتی، یعنی دارایی‌های کلیدی که در شبکه مدیریت زیرساخت‌ها با دارایی کلیدی موردمطالعه هم‌وند هستند. با این تفسیر، رقبای اصلی سد لتیان، سایر سدهای اطراف شهر تهران هستند و همان‌طور که پیش‌تر بیان شده عبارتند از: سدهای لار، ماملو، امیرکبیر و طالقان. در گام بعدی، سد لتیان با کلیه رقبای خود از نظر آسیب‌پذیری و تهدیدات احصاشده در مرحله اول در یک مقیاس پنج‌گزینه‌ای شامل بسیار فراتر، فراتر، تقریباً برابر، پایین‌تر و بسیار پایین‌تر مقایسه شده است بدین‌معنا که سدهای دیگر از نظر میزان خطرپذیری با سد لتیان مقایسه شدند. ازآنجاکه محوریت سرویس‌دهی و ارائه خدمات در موضوع زیرساخت‌ها، شبکه است، لذا این مقایسه می‌تواند اطلاعات دقیق‌تری از وضعیت شبکه دارایی‌ها در اختیار ما قرار دهد. نرم‌افزار متاسوات به‌طور سامانه‌ای برمبنای مقایسه انجام شده،

1. Identification of Competitive Dimensions

نقشه رقابتی موقعیت موردمطالعه با رقبای خود را ارائه می‌دهد. شکل (۵) موقعیت سد لتیان در شبکه سدهای اطراف تهران از نظر خطرپذیری اطلاعاتی را نشان می‌دهد. از خروجی‌های نرم‌افزار دو نکته مهم را می‌توان برداشت نمود، اولاً ازآنجایی‌که تهدید عاملی است که در پیامد تأثیرگذار است و آسیب‌پذیری در احتمال وقوع یک حادثه. لذا محور احتمال خروجی نرم‌افزار متاسوات را می‌توان تقریباً با محور احتمال ماتریس حرارتی و محور احتمال خروجی نرم‌افزار متاسوات را می‌توان تقریباً با محور پیامد ماتریس حرارتی معادل‌سازی نمود از این منظر موقعیت کلی خطرپذیری اطلاعاتی سد لتیان که در مرحله اول محاسبه گردید با موقعیت به‌دست‌آمده در این مرحله تقریباً برابر است. با توجه به اینکه این دو نتیجه از دو روش متفاوت به‌دست‌آمده‌اند، این شباهت مؤید کارایی روش متاسوات در ارزیابی خطرپذیری اطلاعاتی است. دومین نکته وضعیت و رتبه‌بندی خطرپذیری اطلاعاتی سایر سدها نسبت به سد لتیان است که در شکل(۴) و جدول(۱۰) با دقت دو رقم نشان‌داده‌شده است.



شکل(۴) نقشه رقابتی سد لتیان با رقبای خود برمبنای گویه‌های خطرپذیری اطلاعاتی

جدول(۱۰) وزن مطلق و نرمال‌شده و رتبه‌بندی خطرپذیری اطلاعاتی سدها

ابعاد رقابتی نام سد	آسیب‌پذیری		تهدیدات		مجموع		رتبه‌بندی
	مطلق	نرمال‌شده	مطلق	نرمال‌شده	مطلق	نرمال‌شده	
لار	۱٫۸۶	۰٫۵۹	۱٫۸۰	۰٫۵۹	۳٫۶۶	۱٫۱۸	۳
طالقان	۲٫۱۷	۰٫۶۹	۲٫۲۳	۰٫۷۳	۴٫۴۰	۱٫۴۲	۲
ماملو	۲٫۲۵	۰٫۶۱	۲٫۴۹	۰٫۸۲	۴٫۷۴	۱٫۵۳	۱
امیرکبیر	۲٫۶۴	۰٫۸۴	۲٫۷۵	۰٫۹۰	۵٫۳۹	۱٫۷۴	۴

۳-۴- تحلیل عوامل داخلی

در بافتار ارزیابی خطرپذیری اطلاعاتی با روش متاسوات، منظور از ارزیابی عوامل داخلی، ارزیابی هر یک از آسیب‌پذیری‌ها و تهدیدات اطلاعاتی بر اساس نظریه مبتنی بر منابع در چهار بعد زیر است که عبارتند از:

- ❖ باارزش بودن[1]: میزان اهمیت گویه در بین همه گویه‌های شناسایی‌شده (درصد فراوانی نسبی گویه)
- ❖ کمیابی[2]: میزان نادر بودن گویه موردنظر در این سد
- ❖ تقلیدناپذیری[3]: میزان قدرت گویه برای دارابودن منابع مشابه
- ❖ غیرقابل‌جایگزینی[4]: بررسی اینکه گویه‌های دیگر قابل جایگزین با این گویه هستند یا نه

ازآنجایی‌که میزان وزن نسبی هر یک گویه‌ها با عنوان درصد فراوانی نسبی در جدول (۸) محاسبه گردید لذا در این مرحله هر یک از گویه‌های ۱۹گانه شناسایی‌شده در سه بعد باقیمانده و در پنج طیف کاملاً موافقم، موافقم، نظری ندارم، مخالفم و کاملاً مخالفم مورد ارزیابی قرار گرفتند که نتایج آن در شکل(۵) آورده شده است.

1. weighting
2. Rarity
3. Inimitable
4. Organization

Identification Consider these resources and capabilities of our business and add new ones of relevance.	Weighting How important are these in comparison with each other?	Rarity Our competitors... do not have this	Imitability Our competitors cannot easily develop this	Organization We benefit from this factor through our approach to decision making
R-1	2 %	Neutral	Neutral	Agree
R-2	2 %	Agree	Agree	Neutral
R-3	2 %	Neutral	Neutral	Neutral
R-4	3 %	Neutral	Neutral	Agree
R-5	6 %	Agree	Agree	Agree
R-6	8 %	Strongly Agree	Agree	Agree
R-7	7 %	Strongly Agree	Strongly Agree	Agree
R-8	6 %	Agree	Strongly Agree	Neutral
R-9	9 %	Strongly Agree	Neutral	Strongly Agree
R-10	2 %	Neutral	Neutral	Neutral
R-11	3 %	Neutral	Neutral	Neutral
R-12	6 %	Neutral	Neutral	Neutral
R-13	3 %	Neutral	Neutral	Neutral
R-14	5 %	Neutral	Neutral	Neutral
R-15	9 %	Strongly Agree	Agree	Neutral
R-16	7 %	Strongly Agree	Agree	Agree
R-17	7 %	Strongly Agree	Strongly Agree	Neutral
R-18	6 %	Neutral	Agree	Neutral
R-19	7 %	Neutral	Neutral	Neutral

شکل(۵) ارزیابی گویه‌های ۱۹گانه خطرپذیری اطلاعاتی بر اساس نظریه مبتنی بر منابع

۴-۴- تحلیل محیط خارجی

در این مرحله کلان‌روندهایی که می‌توانند بر خطرپذیری اطلاعاتی سد لتیان اثرگذار باشند، برمبنای نظر خبرگی و رویکرد پستل[1] شناسایی شدند. گفتنی است تحلیل پستل یک ابزار راهبردی برای ارزیابی تأثیر عوامل عمده بیرونی بر محیط کسب‌وکار است. این تحلیل شش عامل سیاسی، اقتصادی، اجتماعی، فنّاورانه، زیست‌محیطی و قانونی را بررسی می‌کند تا به درک بهتر فرصت‌ها و تهدیدهای محیطی کمک کند. عوامل عمده بیرونی شناسایی‌شده در این مرحله عبارتند از:

- ❖ رشد شتابان فنّاوری
- ❖ عدم تنظیم گری مناسب بین بخش خصوصی و بخش دولتی
- ❖ تحریم‌های اقتصادی
- ❖ مشکلات ساختاری کلان در حوزه مدیریت شبکه زیرساخت‌های کشور

1. PESTEL: Political, Economic, Social, Technological, Legal, Environment

- ❖ خشک‌سالی و بلایای طبیعی
- ❖ عدم تدوین چشم‌انداز و نقشه راه
- ❖ چالش‌های مدیریت سرمایه انسانی

درگام بعدی کلیه کلان‌روندهای شناسایی‌شده برمبنای چهار عامل وزن[1]، تأثیر[2]، احتمال افزایش[3] و درجه اضطرار[4] مورد ارزیابی قرار گرفتند که نتیجه آن در شکل(۶) آورده شده است.

Identification Which factors that our business cannot directly control are critical for achieving its purpose? Consider political, economic, socio-cultural, technological, ecological, legal, and competitive issues.	Weighting How important are these in comparison with the average business challenge?	Impact How strong would the impact of this factor be on the success of our organization?	Probability of Increase The likelihood of this factor increasing over the planning period is ...	Degree of Urgency Our organization needs to address this issue ...
رشد شتابان فناوری	Average	Medium	High	Soon
عدم تنظیم گری مناسب بین بخش خصوصی و بخش دولتی	More Important	Strong	High	Soon
تحریم های اقتصادی	More Important	Medium	Medium	Soon
مشکلات ساختاری کلان در حوزه مدیریت شبکه زیرساخت های کشور	Much More Important	Strong	High	Not so soon
خشکسالی و بلایای طبیعی	Average	Strong	Medium	Soon
عدم تدوین چشم انداز و نقشه راه	More Important	Strong	Medium	Not so soon
چالش‌های مدیریت سرمایه انسانی	More Important	Strong	High	Not so soon

شکل(۶) ارزیابی کلان‌روندهای مؤثر در خطرپذیری اطلاعاتی

۵-۴- ارزیابی تناسب راهبردی

ارزیابی تناسب راهبردی شامل ارزیابی میزان تأثیرپذیری آسیب‌پذیری‌ها و تهدیدات شناسایی از کلان‌روندهای شناسایی‌شده و همچنین ارزیابی تناسب گویه‌های شناسایی‌شده با اهداف تعریف شده است. تأثیرپذیری آسیب‌پذیری‌ها و تهدیدات شناسایی از کلان‌روندهای شناسایی‌شده در یک طیف ۵تایی شامل بسیار قوی، قوی تا حدودی، ضعیف و بسیار ضعیف مورد ارزیابی قرار گرفت که نتیجه آن در شکل(۷) نشان‌داده‌شده است.

1. Weighting
2. Impact
3. Probability of increase
4. Degree of Urgency

	رشد شتابان فناوری	عدم تنظیم گری مناسب بین بخش خصوصی و بخش دولتی	تحریم های اقتصادی	مشکلات ساختاری کلان در حوزه مدیریت شبکه زیرساخت	خشکسالی و بلایای طبیعی	عدم تدوین چشم انداز و نقشه راه	چالش‌های مدیریت سرمایه انسانی
R-1	Strongly	Very Weakly	Very Weakly	Very Weakly	Very Weakly	Very Weakly	Very Strongly
R-2	Somewhat	Somewhat	Very Weakly	Very Weakly	Very Weakly	Very Weakly	Somewhat
R-3	Somewhat	Very Weakly	Very Weakly	Somewhat	Very Weakly	Very Weakly	Very Strongly
R-4	Weakly	Very Weakly	Very Weakly	Somewhat	Very Weakly	Strongly	Very Strongly
R-5	Weakly	Strongly	Somewhat	Weakly	Very Weakly	Very Weakly	Somewhat
R-6	Weakly	Somewhat	Very Strongly	Weakly	Weakly	Strongly	Weakly
R-7	Strongly	Weakly	Somewhat	Somewhat	Very Weakly	Weakly	Weakly
R-8	Weakly	Very Weakly	Very Weakly	Somewhat	Very Weakly	Somewhat	Very Weakly
R-9	Strongly	Very Weakly	Very Weakly	Weakly	Very Weakly	Weakly	Very Weakly
R-10	Very Strongly	Very Weakly	Very Weakly	Very Weakly	Very Weakly	Weakly	Very Weakly
R-11	Very Weakly	Very Weakly	Very Weakly	Very Weakly	Very Weakly	Very Weakly	Very Weakly
R-12	Somewhat	Very Strongly	Very Weakly	Weakly	Very Weakly	Very Weakly	Very Weakly
R-13	Very Strongly	Very Weakly	Very Weakly	Weakly	Very Weakly	Very Weakly	Very Weakly
R-14	Very Strongly	Very Weakly	Very Weakly	Very Weakly	Very Weakly	Very Weakly	Very Weakly
R-15	Very Weakly	Very Weakly	Very Weakly	Very Strongly	Very Weakly	Strongly	Very Weakly
R-16	Very Weakly	Very Strongly	Very Weakly	Weakly	Very Weakly	Very Weakly	Very Weakly
R-17	Very Weakly	Very Weakly	Very Weakly	Strongly	Very Weakly	Very Strongly	Very Weakly
R-18	Very Weakly	Somewhat	Somewhat	Very Strongly	Very Weakly	Strongly	Very Weakly
R-19	Very Weakly	Very Weakly	Very Weakly	Weakly	Very Weakly	Weakly	Very Strongly

شکل(۷) ارزیابی میزان تأثیرپذیری گویه‌های ۱۹گانه از کلان‌روندهای شناسایی‌شده

ارزیابی تناسب گویه‌های شناسایی‌شده با اهداف تعریف شده نیز در یک در یک طیف ۵تایی شامل بسیار قوی، قوی تا حدودی، ضعیف و بسیار ضعیف انجام شده است که نتیجه آن در شکل(۸) نشان‌داده‌شده است.

	دستیابی به بیشترین تاب	دستیابی به کمترین آسیب پذیری	اشراف و صیانت اطلاعاتی	تحلیل و برآورد اطلاعاتی	هم افزایی اطلاعاتی- امنیتی	معماری و مهندسی اطلاعاتی
R-1	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-2	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat	Somewhat
R-3	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-4	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-5	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat	Somewhat
R-6	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-7	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-8	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat	Somewhat
R-9	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat	Somewhat
R-10	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-11	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-12	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-13	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat	Somewhat
R-14	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-15	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-16	Somewhat	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat
R-17	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat	Somewhat
R-18	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat	Somewhat
R-19	Very Strongly	Somewhat	Strongly	Somewhat	Somewhat	Somewhat

شکل(۸) ارزیابی میزان تناسب گویه‌های ۱۹گانه با اهداف تعریف شده

۶-۴- نقشه استراتژی

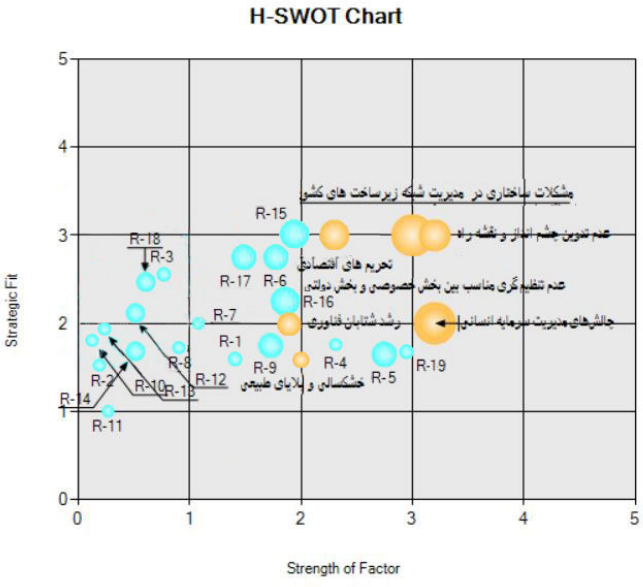
در این مرحله نقشه راهبردی به‌عنوان یکی از خروجی‌های مهم مدل متاسوات به دست می‌آید که در شکل(۹) آورده شده است. در نقشه راهبردی آسیب‌پذیری‌ها و

تهدیدات و همچنین کلان‌روندهای شناسایی‌شده برمبنای سه معیار مورد تحلیل قرار می‌گیرند که عبارتند از:

- ❖ نزدیکی آسیب‌پذیری‌ها و تهدیدات به کلان‌روندها
- ❖ موقعیت یا همان مختصات هر یک از عوامل
- ❖ اندازه حباب‌ها

میزان نزدیکی آسیب‌پذیری‌ها و تهدیدات به کلان‌روندها، نشانگر ارتباط آن‌ها با کلان‌روندها و پتانسیل بیشتر آن‌ها برای تدوین راهبرد است. در نقشه استراتژی محور افقی میزان قدرت هر عامل است که از سه ویژگی کمیابی، تقلیدناپذیری و تناسب سازمانی تأثیر می‌پذیرد و محور عمودی هم میزان و درجه تناسب راهبردی هر یک از عوامل نشان می‌دهد. همچنین اندازه حباب‌ها میزان تناسب با اهداف را مشخص می‌نماید.

شکل(۹) نقشه استراتژی مدیریت اطلاعاتی سد لتیان



نقشه استراتژی مدیریت اطلاعاتی سد لتیان نشان می‌دهد که عامل «مشکلات ساختاری کلان در حوزه مدیریت شبکه زیرساخت‌های کشور» با مختصات (۳-۳) و اندازه حباب ۴، دومین قدرت و اولین تناسب و همچنین بیش‌ترین اضطرار را به منظور تدوین

استراتژی مدیریت اطلاعاتی را دارد. عدم تدوین چشم‌انداز و نقشه راه با مختصات (۳-۳٫۲) اولین قدرت و تناسب را برای تدوین استراتژی را دارد ولی درجه اضطرار پایین‌تری دارد. عامل «عدم تنظیم‌گری مناسب بین بخش خصوصی و بخش دولتی» قدرت بسیار خوب ولی تناسب کمتری در مقایسه با عوامل ساختار و تدوین چشم‌انداز دارد ولی میزان اضطرار آن با عامل ساختاری برابر است. قرارگرفتن R-16 هم با عنوان اختلال در عملکرد و حفظ امنیت اطلاعات سد به‌دلیل عدم تعامل مناسب با بخش خصوصی با مختصات (۲٫۳-۱٫۹) در فاصله نه‌چندانی دوری از این عامل، مؤید پتانسیل بسیار بالای آن برای تدوین راهبرد است. عامل تحریم‌های اقتصادی با مختصات (۳-۲٫۳) و اندازه حباب ۳ و نزدیکی آن با R-15 با عنوان «اختلال در عملکرد سد به‌دلیل فرسودگی تأسیسات و سازه‌های فنی سد و یا استفاده از تجهیزات کهنه و تقلبی» حاکی از ارتباط بین این دو عامل و پتانسیل آن‌ها برای طراحی راهبردهای متناسب به منظور مدیریت خطرپذیری اطلاعاتی ناشی از این عوامل است. موقعیت سایر عوامل و آسیب‌پذیری و تهدیدات اطلاعاتی متناسب با آن‌ها نیز تا حدود قابل‌توجهی معنادار است که راهبردهای ارائه شده در بخش نتیجه‌گیری از آن‌ها منتج می‌گردد. عامل خشک‌سالی و بلایای طبیعی نیز با مختصات (۲-۱٫۵) و اندازه حباب ۱ کمترین قدرت و تناسب و همچنین اضطرار را به منظور تدوین راهبردهای مدیریت اطلاعاتی به خود اختصاص داده است.

۵- تجزیه‌وتحلیل و نتیجه‌گیری

این پژوهش با هدف ارزیابی خطرپذیری اطلاعاتی، تدوین راهبردهای مدیریت اطلاعاتی سد لتیان و کاربرد یک روش جدید به این منظور شکل گرفت. تلاش گردید تا نتیجه یک کار پژوهشی، تیمی و میدانی به نحو مطلوبی در قالب یک روش جدید پیاده‌سازی و ارائه گردد. در این راستا پس از شناسایی ادبیات تحقیق و مرور پیشینه تحقیق، کلیه مراحل تحقیق متاسوات با تغییرات جزئی در بخش منابع و قابلیت‌ها که بجای آن‌ها از آسیب‌پذیری‌ها و تهدیدات اطلاعاتی استفاده شد، پیاده‌سازی گردید. برای ارزیابی خطرپذیری اطلاعاتی سد لتیان نیز از روش تحلیل خطرپذیری ماتریس خطر استفاده شد. نتایج به‌دست‌آمده نشان می‌دهد که سد لتیان به عنوان یکی از مراکز حساس تأمین آب شهر تهران، با چالش‌های اطلاعاتی متعددی روبه‌رو است که باید با

رویکردی چندجانبه مدیریت شود. روش متاسوات نیز به‌عنوان ابزاری کارآمد، می‌تواند به شناسایی و ارزیابی خطرپذیری اطلاعاتی کمک نماید.این تحلیل به ما کمک کرد تا ابعاد مختلف خطرپذیری اطلاعاتی سد را از زوایای مختلف شناسایی و برنامه‌ریزی‌های راهبردی برای مدیریت اطلاعاتی و بهبود شرایط را به عمل آوریم. یافته‌های تحقیق نشان می‌دهد که سد لتیان در میان سدهای اطراف تهران بیش‌ترین خطرپذیری اطلاعاتی را دارد و پس از به ترتیب سد امیرکبیر، سد لار، سد طالقان و کمترین خطرپذیری اطلاعاتی متعلق به سد ماملو است. با توجه به نتایج به‌دست‌آمده و ارزیابی تناسب آسیب‌پذیری‌ها و تهدیدات اطلاعاتی با عوامل خارجی شناسایی‌شده و اهداف تعریف شده، راهبردهای ذیل به ترتیب می‌توانند در مدیریت اطلاعاتی سد لتیان سودمند واقع شوند:

- اصلاح ساختار مدیریتی و یکپارچه‌سازی مدیریت راهبردی شبکه‌های زیرساختی سدهای اطراف تهران

- تنظیم چارچوب‌های همکاری شفاف بین بخش دولتی و خصوصی در مدیریت سد لتیان، با تأکید بر مشارکت بخش خصوصی و ایجاد سازوکارهای نظارتی مشترک برای تضمین منافع هر دو بخش

- تدوین یک نقشه راه و چشم‌انداز با مشارکت ذینفعان کلیدی سد لتیان، مبتنی بر اهداف بلندمدت و تحلیل خطرپذیری‌های اطلاعاتی همراه با پایش دوره‌ای و بازنگری مستمر برای تضمین تاب‌آوری سد در شرایط و موقعیت‌های مختلف

- پیگیری مستمر تأمین پایدار قطعات حیاتی موردنیاز سد از طریق شرکت‌های دانش‌بنیان و یا از طریق کشورهای همسایه و غیرتحریمی

- استفاده از فنّاوری‌های نوین، حسگرهای هوشمند و سامانه‌های هوش مصنوعی برای پایش مداوم و تحلیل داده‌های محیطی سد به منظور شناسایی به‌موقع تهدیدات بیوتروریستی و آلودگی‌های محیطی

- ارتقای زیرساخت‌های اطلاعاتی و توسعه چارچوب‌های امنیت سایبری سد

- پیاده‌سازی یک سامانه مدیریت منابع انسانی هوشمند مبتنی بر اهداف بلندمدت و نیاز سد به منظور تربیت، صیانت، همتاسازی، مدیریت دانش و تجربه کارکنان

- بهره‌گیری از مدل‌های پیش‌بینی هوشمند برای شناسایی الگوهای خشک‌سالی و بلایای طبیعی به منظور احراز آمادگی برای مقابله با بحران‌ها و مدیریت پایدار منابع آب

منابع

۱- اسدالله‌فردی، غلامرضا؛ شیخ‌علی، مجید و امامزاده، سیدشهاب. (۱۳۹۹). ارزیابی آسیب‌پذیری تأسیسات آب‌رسانی با روش تلفیقی AHP وRAMCAP ، نشریه مهندسی عمران، دوره۵۲، شماره۵، ۱-۱۵.

۲- بخشی‌شادمهری، فاطمه؛ زرقانی، سیدهادی و خوارزمی، امیدعالی. (۱۳۹۸). تحلیل آسیب‌پذیری عناصر زیرساخت آب شهری در مقابل تهدیدات تروریستی، فصلنامه ژئوپلیتیک، سال۱۶، شماره ۲، ۳۲-۵۷.

۳- برنا، حسن و صحرایی‌نژاد، نسیم. (۱۴۰۳). مکان‌یابی و ساماندهی منظر پیرامون سد لتیان تهران با رویکرد گردشگری پایدار، نشریه علمی پدافند غیرعامل، سال پانزدهم، شماره۲، ۱۰۱-۱۱۱.

۴- پورشاسب، عبدالعلی و نظری‌نژاد، احمدعلی. (۱۳۹۹). تدابیر و راهکارهای پدافند غیرعامل در حفاظت از زیرساخت‌های حیاتی ج.ا.ایران، فصلنامه مطالعات دفاعی راهبردی، ۸۲، ۲۸۹-۳۱۲.

۵- خسروی‌طائمه، راضیه؛ سامانی، محمدولی و رضوی طوسی، سیده‌لیلا. (۱۴۰۲). ارزیابی و اولویت‌بندی خطر سدها با استفاده از روش ترکیبیDEMATEL-ANP ، نشریه مدیریت آب و آبیاری، دوره ۱۳، شماره۴، ۱۰۵۳-۱۰۶۹.

۶- رضایی، محمدرضا؛ اروجی، حسن و عزیزی، حسین. (۱۴۰۲). واکاوی توسعه گردشگری شهر شیراز با رویکرد تاب‌آوری با استفاده از مدل متاسوات، فصلنامه گردشگری و اوقات فراغت، ۸ (۱۵).

۷- سادات، غلامرضا. (۱۳۹۸). تحلیل خطر در ضداطلاعات با استفاده از ماتریس خطر، دومین همایش ملی روش‌های تحلیل اطلاعات.

۸- عراقی‌زاده، مجتبی و کاملی، بهروز. (۱۴۰۱). رسیم قلمرو خوشه‌بندی پژوهش‌های بین‌المللی در حوزه حفاظت از زیرساخت‌های حیاتی بر اساس تحلیل هم‌واژگانی مقالات نمایه شده در پایگاهScience of Web، دوفصلنامه علمی-پژوهشی مدیریت بحران، شماره ۲۲.

۹- قلی‌زاده، سعید؛ نکویی، محمدعلی و فخرایی، حسین. (۱۳۹۶). بررسی و ارزیابی تهدیدات دارایی‌های پایین‌دست سدها با رویکرد پدافند غیرعامل (مطالعه موردی: سد شیرین‌دره)، فصلنامه پدافند غیرعامل، سال هشتم، شماره۱ (۲۹)، ۲۵-۳۴.

۱۰- مجیدی، اردوان و درخشان، رضا. (۱۳۸۶). یک معماری کلان برای سازمان‌دهی زیرساخت‌های خدمات در شهر الکترونیک، اولین کنفرانس بین‌المللی شهر الکترونیک.

۱۱- میرزارمضانی، ابوالفضل. (۱۴۰۲). روش‌های ارزیابی خطر با استفاده از احتمال و تأثیر، گروه تخصصی دیجیتال ساینس:

https://digital-science.ir/use-of-probability-and-impact-of-risk-in-risk-assessment

۱۲- میربوسفی، سیدمحسن و غفارپور، رضا. (۱۳۹۹). راهبردهای نوین حفاظت از زیرساخت‌های حیاتی، مجله پدافند غیرعامل، ۳ (۴۳)، ۱-۱۴.

۱۳- نظام عملیاتی پدافند سایبری کشور. (۱۴۰۰). قرارگاه پدافند سایبری، سازمان پدافند غیرعامل کشور.

۱۴- نعمت‌پور، اردشیر؛ تقی‌زاده انصاری، مصطفی و ببری‌گنبدی، سکینه. (۱۴۰۲). مسئولیت دولت‌ها در مقابله با حملات تروریستی به زیرساخت‌های حیاتی یک کشور، فصلنامه مطالعات بین‌المللی، سال۱۹، شماره ۴ (۷۶).

۱۵- واعظی‌نژاد، محمدمهدی و مقدس، محمدرضا. (۱۳۹۴). راهبردهای امن‌سازی زیرساخت‌های حیاتی کشور در حوزه فنّاوری:
https://mvaezi.ir/files/eBooks/Infra%20Security)20%Vaezi(.pdf

16- Ansell, J. and F. Wharton, 1992, "Risk: Analysis, Assessment, and Management," Chichester: John Wiley & Sons.

17- Brian R. McDonald, 2017, "Critical Infrastructure Protection: A Comprehensive Review," Computers & Security.

18- Camila A., De Paiva, Cesar F. Barella, Alberto Fonseca, 2024, Assessing and managing safety risks to downstream communities)in hindsight:(What went wrong in the licensing and impact assessment procedures of Brazil's deadliest dam breaks, Environmental Impact Assessment Review, Volume 106.

19- Godschalk, David R., Edward Kaiser, and Philip Berke, 1998, "Integrating Hazard Mitigation and Local Land Use Planning." Chapter four in Cooperating with Nature, edited by Raymond Burby, National Academy Press, Joseph Henry Press, Washington, DC.

20- ISO/IEC 27005, Information security risk management, 2018, International Electrotechnical Commission, Information technology, Security techniques.

21- Lacasse., Suzanne, 2022, Risk assessment and risk management for dams, Norwegian Geotechnical Institute, 0828-01-R.

22- Liu, W. and Song, Z., 2020. Review of studies on the resilience of urban critical infrastructure networks, Reliability Engineering and System Safety: 193, 106617. https://doi.org/10.1016/j.ress.2019.106617.

23- NIST: National Institude of Standard and technology, 2021, Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1, U.S. Department of Commerce.

24- Petit.F., D. Verner, D., J. Phillips, and L. P. Lewis, 2018, "Critical Infrastructure Protection and Resilience Integrating Interdependencies," In Security by Design, A. J. Masys, Ed., Cham., Switzerland: Springer.

25- Ravi Agarwal, Wolfgang Grassl, Joy Pahl, 2015,"Meta-SWOT: introducing a new strategic planning tool," Journal of Business Strategy, Vol. 33 Iss: 2 pp. 12 .21 –

26- Woodruff, J. M, 2005, "Consequence and likelihood in risk estimation: a matter of balance in UK health and safety risk assessment practice." Safety Science,43(5e6 ,(345e353.

27- Zhang, S., Hou, W., Yin, J., & Lin, Z. .(2023) A review of research and practice on the theory and technology of reservoir dam risk assessment. Sustainability, 15(14), 11004. https://doi.org/10.3390/su142214984