سازمان پدافند غیرعامل کشور
مرکز مطالعات فنی و مهندسی سازمان پدافند غیرعامل کشور

حفاظت از زیر ساخت‌های حیاتی

Critical Infrastructure Protection

Research Center of Engineering and Technical Science Magazine
Issue, 1 - December, 2019

نشریه مرکز مطالعات فنی و مهندسی
شماره اول آذرماه ۱۳۹۸

ضرورت ایجاد رشته دانشگاهی
حفاظت از زیرساخت‌های حیاتی CIP

"مقابل شیوه های پیچیده تهاجم دشمنان، پدافند غیرعامل نیز باید کاملاً هوشیار و جدی باشد و به صورت علمی، دقیق و به روز همه جانبه عمل و با هر گونه نفوذ مقابله کند"

مقام معظم رهبری (مدظله العالی)

بسم الله الرحمن الرحیم

صاحب امتیاز:
سازمان پدافند غیر عامل کشور
مرکز مطالعات فنی و مهندسی

مدیر مسئول:
دکتر غلامرضا جلالی فراهانی

سر دبیر:
دکتر منصور باقرصاد

دبیر اجرایی:
دکتر حمید هوشنگی

هئیت تحریریه:
مجتبی عراقی زاده. محمدجنیدی. مهنازمیرزاابراهیم طهرانی. حمید هوشنگی

همکاران علمی:
احمد اکرمی. مصطفی غضنفری. لاله فرهنگ متین. سید فضل الدین جمالیان. محمد جنیدی. محمد علی‌نکویی. هادی کریمی نیسیانی. مهناز میرزا ابراهیم طهرانی، امیدرضا میکائیلی. محمدباقرایزدی

گرافیک و صفحه بندی:
علیرضا سلیمی بنی

نشانی:
تهران خیابان ولیعصر بالاتر از ایستگاه جامی کوچه اردشیر ناظم پلاک ۷ طبقه ۳ مرکز مطالعات فنی و مهندسی

تلفن:
۰۲۱-۶۶۹۷۸۲۲۶
۰۲۱-۶۶۹۷۱۳۰۴

سایت:
www.mafpa.ir

فهرست مطالب

نشریه مرکز مطالعات فنی و مهندسی

دکتر منصور باقرصاد رنانی
ریاست مرکز مطالعات فنی و مهندسی
سازمان پدافند غیرعامل کشور

سخن سر دبیر

خدمت مدیران، فرهیختگان، دانشگاهیان، پژوهشگران و تمام‌کسانی که موضوع پدافند غیر عامل و حفاظت از زیرساخت‌های حیاتی کشور عزیزمان ایران به عنوان یکی از دغدغه‌های اصلی آن‌ها می‌باشد، عرض سلام و احترام دارم. مستحضرید که دشمنان نظام مقدس جمهوری اسلامی ایران با وجود ناکامی‌های خودهیچ گاه دست ازعداوت بر نداشته و با بکارگیری ابزارها و علوم پیشرفته به هر طریقی در پی ضربه زدن به زیر ساخت‌های حیاتی کشور عزیزمان ایران هستند. وظیفه ما در دنیایی مملو از منازعات، مصون‌سازی زیرساخت‌های کشور در حوزه‌های مختلف (سایبری، زیستی، پرتویی، شیمیایی،کالبدی، اقتصادی و مردم محور) از طریق افزایش بازدارندگی، ارتقاء تاب‌آوری وکاهش آسیب‌پذیری در برابر تهدیدات متنوع فراروی نظام جمهوری اسلامی ایران می‌باشد. بر همین اساس سازمان پدافند غیرعامل با تفویض بخشی از اختیارات خود به مرکز مطالعات فنی و مهندسی در امرتهیه و تدوین آیین‌نامه‌ها، دستورالعمل‌ها، الزامات و ملاحظات، مقررات و استانداردهای فنی و مهندسی، اقدامات قابل توجهی در راستای حفاظت از زیرساخت‌های حیاتی کشور انجام داده است. در همین راستا، مرکزمطالعات فنی و مهندسی اهمیت پدافند غیرعامل را در نظر گرفته و بر لزوم انجام تحقیق و پژوهش در موضوعات مختلف این مسئله تاکید دارد.

بدیهی است که تحقق این مهم منوط به استفاده از امکانات بالقوه و توانمندی دستگاه‌های اجرایی و مراکز علمی پژوهشی کشور می‌باشد. بنابراین مرکز مطالعات فنی و مهندسی سازمان پدافند غیرعامل قصد دارد از ظرفیت‌های علمی دستگاه‌های اجرایی و مراکز پژوهشی کشور در جهت حفاظت از زیرساخت‌های حیاتی بهره‌مند گردد. به همین منظور نشریه حاضر با عنوان"حفاظت از زیر ساخت‌های حیاتی (CIP)" جهت معرفی برنامه‌ها و ایجاد ارتباط مستمر با تمامی مدیران، فرهیختگان، دانشگاهیان و پژوهشگران در دستگاه‌های اجرایی، دانشگاه‌ها و مراکز علمی تاسیس گردید. لذا امیدوارم که شماره اول این مجله آغازی در جهت ایجاد همکاری‌های علمی در صیانت از زیرساخت‌های حیاتی نظام مقدس جمهوری اسلامی ایران باشد.

من الله توفیق

- آقای دکتربه طورکلی نحوه تعیین و تشخیص زیرساخت‌های حیاتی درکشورایران و دیگر کشورها را بیان بفرمائید. در واقع پارامترها و شاخص‌های‌موثردرشناسایی یک زیرساخت حیاتی در کشورهای مختلف شامل چه مواردی می‌توانند باشند؟

دردرجه نخست فرمول‌ها یا مولفه‌های تعیین کننده حیاتی بودن زیرساخت‌ها درکشورهای مختلف با هم تفاوت دارند. ضمن اینکه تعریف زیرساخت‌های حیاتی درکشورهای مختلف نیز با هم متفاوتند. این دو تفاوت را اگر باهم در نظر بگیریم، در ادبیات مکتوب غربی ها زیر ساخت (Infrastructure) شامل زیر ساخت های فیزیکی، به اضافه زیرساخت اطلاعاتی یا اطلاعات یا حتی عوامل و منابع انسانی، و حتی پروسه و فرایند کار به عنوان زیرساخت تلقی می‌شوند.

- یعنی خود پروسه هم یک نوع زیرساخت در نظر گرفته می‌شود؟

بله. شما اگر در تعریف دیکشنری آمریکایی ها به نام(DHS Lexicon) (۲۰۱۷) که راجع به مدیریت ریسک(Risk Management)یعنی فرهنگ لغات وزارت امنیت سرزمینی آمریکا، برای واژه(Infrastructure)تعریف وسیعی ارائه می‌دهدکه ممکن است این تعریف در کشور ما خیلی ساری و جاری نباشد. در کشور ما بیشتر در ذهن مسئولین، زیرساخت فیزیکی به عنوان زیرساخت مطرح می‌شود. به طور مثال پل، جاده، ارتباطات، آب، برق، گاز، بندر که به عنوان زیرساخت فیزیکی در نظر گرفته می‌شود. این موضوع تا اندازه‌ای در ادبیات جاری گذشته ما مرسوم بوده است. ولی با توسعه فضای سایبر، تعریف زیرساخت تا اندازه ای متفاوت شده و عناصر سایبری هم جز مولفه های تشکیل دهنده یک زیرساخت محسوب شده‌اند. من جمله، ممکن است پروسه و فرآیند یک مجموعه یا سیستم به اضافه داده‌های تشکیل دهنده آن زیرساخت، مثل بیگ دیتا(big data)یا اطلاعات مبتنی بر فضای سایبر که آن را شکل داده و مدیریت می کند، به عنوان زیرساخت تلقی شده و دنبال شوند. بنابراین خود تعریف زیرساخت یه اندازه‌ای متفاوت است. بعضی ها زیرساخت را در ادبیات مربوطه به چهار قسمت تقسیم بندی می کنند:

۱- حوزه؛ مثلا می‌گویند حوزه انرژی، حوزه آب، حوزه غذا، حوزه نظامی، و حوزه غیرنظامی و ....

۲- بخش یا (Sector)؛ مثلا می گویند حوزه انرژی بخش برق، حوزه انرژی بخش هسته‌ای، حوزه انرژی بخش آب و .....

۳- زیرساخت؛ مثلا زیرساخت آب یعنی مجموعه فرآیندها و زیرساخت های فیزیکی و زیرساخت های انسانی که وظیفه تامین و تولید آب را برای ما انجام می‌دهند.

٤- دارایی یا سرمایه (Asset)؛ یعنی به طور کلی دارایی جزئی از زیرساخت بوده، زیرساخت قسمتی از آن بخش مربوطه است، و آن بخش مربوطه جزئی از حوزه آن زیرمجموعه به شمار می‌رود. این تقسیم بندی چهارگانه را ما باید بهریک تعبیری در نظر بگیریم. مثلا وقتی گفته می‌شود زیرساخت حوزه انرژی، ممکن است تعریف درستی ارائه نکرده باشیم. به عنوان مثال نیروگاه تولید برق

را در واقع زیرساخت بخش برق حوزه انرژی بایستی تعریف و دنبال کنیم که یک مقدار هم به لحاظ ادبی بایستی فرق کند.

نکته دوم این است که اگر زیرساخت را معادل دارایی در نظر بگیریم که باید از آن حفاظت کنیم، آنگاه شش مؤلفه وجود خواهد داشت که کریتیکالیتی (Criticality) یا میزان حیاتی بودن یا میزان بحرانی بودن زیرساخت را تعیین کنیم. این شش مولفه شامل این موارد است:

۱- اهمیت؛ خود اهمیت شامل پنج سطح ویژه، حیاتی، حساس، مهم، و قابل محافظت است.

۲- ماهیت؛ یعنی جنس زیرساخت از چیست؟ که می‌تواند ماهیت آن شامل ۵ دسته زیر باشد:

-فیزیکی؛ یعنی زیرساخت فیزیکال باشد؛ مثل ساختمان، تجهیزات، بندر، پل، جاده، دکل، و ....

-انسانی؛ یعنی جمعیت و منابع انسانی به عنوان زیرساخت یک کشور محسوب می‌شود. یعنی منابع انسانی یک دارایی است. که خود دسته‌بندی می‌شود به جمعیت کلان یعنی حفاظت از جمعیت یک شهر یا افراد خاص مثل فرماندار، استاندار، علما، دانشمندان، نخبگان و فرماندهان نظامی و چیزهایی از این قبیل.

-سایبری؛ یعنی ماهیت بعضی از دارایی‌های ما فیزیکی بوده و بعد تبدیل به سایبری می‌شوند. مثل پول یا سایر اجزایی که در فضای سایبر مطرح می‌شوند.

-غیر فیزیکی یا معنوی؛ که در حوزه‌های مختلف تعاریف مختلفی دارد. در حوزه‌های استراتژیکی پرستیژ ملی ، اقتدار ملی گفته می‌شود، مثل نمادها. در حوزه‌های اقتصادی برند و اعتبار گفته می‌شود. این‌ها هم دارایی است که حالا در بحث‌های قدرت ملی می شود در موردشان بحث کرد.

-ترکیبی؛ که ترکیبی از ۴ مورد فوق هستند. یعنی ممکن است مقداری سایبری، مقداری فیزیکی و مقداری انسانی و چیزهایی از این قبیل باشد.

۳- هوشمند یا غیرهوشمند بودن؛ یعنی هوش از هر نوع آن در زیرساخت وجود دارد یا نه؟ اگر دارایی هوشمند باشد یک جور به آن نگاه می‌کنیم و اگر غیرهوشمند باشد یک جور دیگر. مثلا ماهیت شهر، خانه، و کارخانه در صورت هوشمند بودن یا غیرهوشمند بودن آنها تغییر می‌کند.

٤- سیستمی یا سلولی بودن؛ یعنی ممکن است دارایی متشکل از یک سیستم باشد. مثل سیستم چرخه تولید آب؛ یا یک سلول باشد، مثل یک مخزن آب بر سر یک کوه. در حالت سیستمی باید دید کجای سیستم قرار می‌گیرد. در مرکز سیستم (Core) و یا دامنه سیستم. اگر در مرکز سیستم باشد اهمیت بیشتری پیدا کرده و اگر در گوشه سیستم باشد دارای اهمیت کمتری خواهد بود.

۵- قابلیت تولید خطر؛ یعنی ممکن است کارکرد یک دارایی برای شما اهمیت کمی داشته ولی در عین حال خطر بالایی هم داشته باشد. مثلا اهمیت کارکرد زیرساخت ۲۰ درصد بوده ولی دارای قابلیت تولید خطر ۹۰ درصد باشد. مثل یک مرکز هسته ای، یک مرکز شیمیایی و یا یک مرکز تصفیه آب درون شهرکه فقط آب تصفیه می‌کند و چنانچه گاز کلر تصفیه خانه نشت کند تمامی شهر را به مخاطره خواهد انداخت. به طور کلی قابلیت تولید خطر از نظر میزان سطح خطر به سطوح دارای خطر بسیار شدید، شدید، متوسط، کم و بی خطر، دسته بندی می‌شود.

٦- دارایی از نظر نوع کارکرد؛ به عنوان مثال وقتی صحبت از زیرساخت آب است، کارکرد از نوع تامین آب مورد نظر است. در این حالت چنانچه دشمن در استراتژی‌های خود قصد حذف آب را داشته باشد، در چرخه زیرساخت آب به دنبال این خواهد بود که کدام دارایی نقش کلیدی در تامین آب داشته و آن را حذف می‌کند. یا مواردی دیگر نظیر ارتباطات، گرمایش، سرمایش و انرژی و یا چیزهایی از این قبیل که نوع کارکردشان اهمیت دارد.

بنابراین این ۶ عامل فوق با ضرایب مختص به خود و قرارگیری در فرمول‌ها و محاسبات مربوطه، می توانند میزان اهمیت یک زیرساخت را ارائه کنند. در واقع اگر فرض شود که عدد محاسبه شده در بازه۱۰۰-۹۰ قرار گیرد آن زیرساخت دارای سطح اهمیت ویژه، ۹۰-۸۰ حیاتی، ۸۰-۷۰ حساس، ۶۰-۴۰ مهم، و زیر ۴۰ قابل حفاظت خواهد بود.

- در کشور ما با همین روش میزان اهمیت زیرساخت ها تعیین و درجه بندی می‌شوند؟

ما الان از ۶ مولفه‌ای که بیان شد روی ۳ مولفه آن حساس هستیم. به این دلیل که طبقه‌بندی حفاظت از زیرساخت‌ها در کشور ما از مناظر مختلف اتفاق می‌افتد. یک جا منظر امنیتی مورد نظر است و شورای امنیت کشور تعیین می کند که چه میزان حفاظت نیاز است؛ مانند سفارتخانه‌ها. یک جا پدافند غیرعامل تعیین می‌کند که نقشش در پایداری کشور در برابر تهدیدات چقدر است. در این حالت ما ۳ مولفه اساسی را برای طبقه بندی در نظر می‌گیریم که شامل کارکرد، اهمیت، و پیامد نبود زیرساخت می‌باشند. آن وقت می‌توانیم سطح آنها را اندازه گیری کرده و این سه مولفه را از درونشان استخراج کنیم.

- با توجه به پویا بودن جوامع بشری این امکان وجود دارد که در آینده، زیرساخت های جدیدی به فهرست زیرساخت های کنونی اضافه شود؟

ببینید مبنای ما تهدید انسان ساخت است. تهدید انسان ساخت دو مولفه دارد؛ یکی تحولات علمی ناشی از تلاش علمی انسان، که می‌شود فناوری ها و صنعت و

محصولات آن، و یکی دیگر استراتژی‌ها و رویکردهایی که انسان در بکارگیری آن فناوری‌ها دارد. این دو مولفه برای ما مهم است. هر دو مولفه روی هم اثر می‌گذارن دمولفه اصلی اول که تغییرات فناورانه است مولفه بسیار اساسی بوده و بصورت پویا و متغیر به سرعت در حال تغییر می‌باشد.

ما در موضوعات پدافند غیر عامل تلاش زیادی می‌کنیم که این‌ها را بشناسیم؛ به طوری که هم ماهیت پدیده، هم میزان کاربرد و کارکرد آن، هم میزان آسیب پذیری و ضعف های آن و اثرات آن بر ما، و همچنین تهدیداتشان را کشف و احصاء کنیم. سپس در یک تجزیه و تحلیلی، رویکردی اتخاذ کنیم که بتوانیم از منافع آن بهره بردار شده، درگیر آسیب پذیری‌های آن نشده و با تهدیداتشان نیز مقابله کنیم. این رویکرد کلان ما نسبت به این موضوع بوده و طبیعتاً پاسخ سوال شما مثبت است. یعنی حتماً احتمال چنین اتفاقی وجود دارد.

- از نظر جنابعالی عمده ترین دلایل آسیب پذیری حال زیرساخت‌های حیاتی با توجه به شرایط حساس کشورمان چه مواردی می‌توانند باشند؟

یک عنصر اساسی در این مورد، تحول در تهدیدات و فناوری‌ها و به وجود آمدن قابلیت‌ها و حوزه‌های جدید فناورانه در زیرساخت‌ها است. دوم اینکه این فناوری‌ها به دلیل پیچیدگی و پیشرفتی که دارند، در درونشان منبع و قابلیتی از تهدید و آسیب استتار شده است. یعنی فناوریی که شما استفاده می‌کنید در ذاتش تهدید و آسیب بوجود آمده است. مثلا شما فناوری اطلاعات یا فضای سایبری که استفاده می‌کنید، ناخودآگاه تحت اشراف صاحب فناوری قرار می‌گیرید. یعنی اشراف اطلاعاتی بخشی از آن قابلیت تهدیدزایی است که درون آن فناوری بوجود آمده است.

بنابراین بخشی از آن قابلیت تهدید زایی است که درون آن فناوری به وجودآمده است بنابراین می توانیم بگوییم که تهدید و فرصت در ذات فناوری باهم اختلاط پیدا کرده اند. باید شما با تلاش زیاد آن ها را شناخته و از هم دیگر تفکیک کنید که کدام تهدید و کدام فرصت است. در عین حال چگونه از آن استفاده کنید که درگیر تهدیدات نشده و بتوانید از فرصت های آن استفاده لازم را ببرید

بنابراین یک نگاه هوشمندانه در استفاده وبهره مندی ازفناوری‌های نو راه چاره بوده که بهره گیری از فرصت ها و خدمات مقابله با آسیب ها و تهدیدات برای هر فناوری را به ما دیکته می‌کند و ما باید این مسئله را مدنظر داشته باشیم.

- آقای دکتر بنده اخیراً در خبری خواندم که آمریکایی ها مدیریت شبکه‌های برق خودشان را به حالت سنتی و دستی تبدیل می‌کنند که از تهدیدات سایبری در امان بمانند. نظر شما در این خصوص چیست؟

احساس آمریکایی ها این است که هر چقدر زیرساخت ها به سمت هوشمند شدن و ارجاع در فضای مجازی پیش بروند احتمال بکارگیری همین سیستم علیه خودشان بوجود می‌آید. بنابراین توصیه راهبردی آنها این است که سه کار انجام بدهند؛ یکی امکان دستی سازی (Manually) را در کنار آنها پیش بینی کنند. یعنی امکان انتقال به حوزه کنترل دستی زیرساخت فراهم شود. دوم اینکه سیستم کیل سوئیچ (Kill Switch) یا سوئیچ خودکشی در آنها تعبیه شود.

یعنی اینکه اگر یک سلاحی را آمریکایی‌ها ساختند مثلا فرض کنید یک موشک و آن موشک به نحوی در اختیار دشمن آمریکا قرار گرفت، بتوانند یک فرمول و یک مدلی پیش بینی کنند که دشمن آنها نتواند آن موشک را علیه سازنده به کار بگیرد. این موضوع جزء استراتژی‌های آن‌ها است. سوم اینکه راهبرد شبکه‌ای سلولی یا آیلندنتورکینگ(IslandNetworkin)را پیاده‌سازی کنند. یعنی درعین حال که سیستم شبکه‌ای است قابلیت سلولی شدن هم داشته باشد.

- آقای دکتر این راهبردها مورد تایید شما نیز قرار دارد؟

بله این راهبردها، راهبردهای عاقلانه‌ای است.

- به طور خلاصه برنامه‌های علمی سازمان پدافند غیرعامل درحداقل نمودن و یاحذف آسیب پذیری زیرساخت‌های حیاتی و حفاظت از آن‌ها را بیان فرمائید.

به صورت کلی ما معتقدیم که بایستی با یک تحقیق و پژوهش نظام مصون سازی زیرساخت‌های کشور با قابلیت بروزرسانی و روزآمدی از نظر فناوری را دنبال کنیم. به شکلی که بتوانیم هم فناوری‌ها به صورت روزآمد به کار گرفته شود و هم به سمتی که این فناوری‌ها در اختیار ما بوده و مصون باشند، پیش برویم. به عنوان مثال وقتی هوشمندی در شهر مطرح می‌شود، ما نمی‌توانیم شهرها را بصورت سنتی و کلاسیک مانند گذشته اداره کنیم. بلکه از هوشمندی استفاده می‌کنیم منتها باید به سمتی حرکت کنیم که از مقولات مفید آن بهره مند شده و آنها را در اختیار بگیریم. نکته دوم اینکه یک جهاد دانشی و علمی در این حوزه شکل گرفته و ما رویکردهای جدید پدافند غیر عامل را مبتنی بر فناوری‌های جدید ایجاد کنیم. به شکلی که آن چارچوب کلی بهره مندی از فرصت و خدمت و مقابله با آسیب و تهدید در هر فناوری را بتوانیم داشته باشیم. نکته سوم اینکه اختلاط فرصت و تهدید را در فناوری‌های نو یک اصل بدانیم. به طوری که نگاه فرصت محور محض یا تهدید محور محض نداشته باشیم. نکته چهارم اینکه یک نگاه پیش دستانه داشته باشیم. به‌طوری که پدافند غیر عامل تبدیل به یک مانع برای پیشرفت نشده و بتواند از پیش فناوری ها را قبل از اینکه داخل کشور بیاد و مستقر بشود رصد کرده و احصاء تهدید و فرصت را پیش دستانه انجام بدهد. در نتیجه ما از قبل می‌توانیم تشخیص دهیم که این فناوری دارای چه تهدیدی بوده و چه بهره‌مندی برای ما خواهد داشت.

- ارتباط دستگاه های اجرایی با سازمان پدافند غیرعامل در امر حفاظت از زیرساخت های حیاتی را چگونه ارزیابی می کنید؟

ببینید دستگاه های اجرایی در سطوح استانی و در سطوح تخصصی به نظرم فهم خوبی نسبت به موضوع پدافند غیر عامل دارند و تلاش خوبی انجام می‌دهند منتها آیا اینکه به سطح رضایت‌مندی و هدف ما رسیده است یا خیر، طبیعتاً نرسیده است. به دلیل اینکه آن سقفی که مقام معظم رهبری برای ما تعریف کرده به عنوان افقی که باید به آن برسیم افق خیلی بلند و مصونیت کامل در برابر تهدید است که خوب طبیعتاً ما به آن سقف هنوز نرسیده‌ایم.

- در واقع خیلی ایده آل است؟

بله. چون در واقع یک هدف بلند مدتی در نظر گرفته شده تا مشخص شود باید به کدام طرف حرکت کنیم. مثلا اگر چهار اقدام اولیه انجام دادیم فکر نکنیم همه چیز تمام و حل وفصل شده‌است.

بنابراین‌دستگاه‌هادراین سطوحی که اشاره شد، هماهنگ و خوب پیش می‌روند ولی به سطح ایده آل هنوز نرسیده‌اند و این یک موضوع کاملا اساسی است که ما باید به آن سطح برسیم.

برای رسیدن به سطح ایده آل در زمینه مصونیت کامل راه زیادی مانده و تلاش همه جانبه و مضاعف رامی‌طلبد.

- آقای دکتر چه برنامه‌هایی برای افزایش این هم کاری‌ها در نظر گرفته شده‌است؟

همه برنامه‌هایی که ما در طول سال برای سازمان پدافند غیر عامل تنظیم می‌کنیم به شکلی است که ما بتوانیم به این سطح از همکاری برسیم. طبیعتاً این برنامه را به صورت سالانه جلو می‌بریم و پیشرفت حاصله هم بد نبوده ولی خوب کفایت نمی‌کند.

- آقای دکتر اخیراً کارگروهی بنام کارگروه حفاظت از زیرساخت‌های حیاتی با مدیریت جنابعالی در محل سازمان پدافند غیر عامل راه اندازی شده است.
در مورد اهداف این کارگروه و دستاوردهای مورد انتظار آن نکته ای اگر وجود دارد بفرمائید.

عرض کنم که جمع بندی ما بصورت کلی این بوده است که در حوزه CIP یا همان حفاظت از زیرساخت‌های حیاتی، اول مشکلی که داریم از جنس دانش و تکنولوژی است .به دلیل اینکه طبیعتاً تکنولوژی‌های مختلفی در زیرساخت‌ها بکارگیری می‌شوند و رویکردی که اشاره کردم در نوع کنترل تکنولوژی، تهدیدات ناشی از تکنولوژی، و نوع بهره برداری آن به شکلی که عملا در برابر تهدیدات آسیب ندیده و مصون بماند، نیازمند آن است که تکنولوژی و حوزه مربوطه کاملاً شناخته شده باشد. علاوه بر آن روش‌های مقابله و مصون سازی هم شناسایی شوند. خوب این سه قلم را چنانچه با هم در نظر بگیریم در واقع همان حفاظت از زیرساخت شکل خواهد گرفت که مستلزم آن است که هم فناوری و هم کارکرد سیستم را بشناسید و هم بدانید که چگونه از آن حفاظت و دفاع کنید. بنابراین اینجا چون عرصه ها متفاوت هستند یک بررسی کردیم و دیدیم در دنیا بعضی کشورهایی هستند که این رشته را درست کردند (رشته حفاظت از زیرساخت های حیاتی). ولی در داخل کشور ما نه رشته آن و نه گرایشات آن وجود دارد. البته بعضی از موضوعات در این مباحث در بعضی از رشته‌ها به صورت منفرد پرداخته می‌شود ولی بصورت یکپارچه دیده نمی‌شود.

بنابراین ما تلاش کردیم که یک گروهی از اساتید و دانشجویانی که در این زمینه علاقه مند هستند را دور هم جمع کنیم و در قالب یک کارگروه علمی و پژوهشی موضوعات مربوط به حفاظت از زیرساخت‌ها را باهم بحث کنیم.

به طوری که با مطالعه ادبیات آن و هم اندیشی‌هایی در این زمینه صورت می‌گیرد بتوانیم تولیدات موجود در کشور را شناسایی نماییم. دوم عناصری که در این زمینه فعالیت دارند مانند اساتید، دانشجویان و همچنین پایان نامه‌های مرتبط را شناسایی کنیم. سوم سطوح علمی پیشرفت در حوزه‌های مختلفدر دنیا را شناسایی نموده و مشخص نماییم که کدام کشورها در چه حوزه هایی کار کرده‌اند. چهارم ادبیات علمی حوزه‌ها را شناسایی و تبیین کنیم. به طوری که در نهایت بتوانیم به چند تا هدف برسیم.ایجاد رشته دانشگاهی حفاظت از زیر ساخت ه یک ضرورت دفاعی است. باید رشته ای به نام CIP در گرایش های مختلف برای کشورمان تولید و راه اندازی کنیم ، محتوای دروس و کتاب ها را آماده کنیم ، اساتید مربوطه را تربیت و دانشجو پذیرش کنیم ، از وزارت علوم انتظار مساعدات جهادی داریم

۱- رشته ای بنام CIP در گرایش های مختلف برای کشورمان تولید و راه اندازی کنیم.
۲- محتوای دروس و کتاب ها را آماده کنیم.
۳- اساتید مربوطه را تربیت کنیم.
۴- دانشجو پذیرش کنیم.

در واقع نیروی انسانی متخصصی تربیت کنیم که در هر حوزه‌ای مثل نفت، گاز، برق، شیمیایی، هسته‌ای، سایبری و بقیه ضمن اینکه برنامه توسعه کشور را جلو می‌برد، امنیت و پایداری سیستم را هم بتواند تضمین کند.

باید رشته ای به نام CIP در گرایش های مختلف برای کشورمان تولید و راه اندازی کنیم ، محتوای دروس و کتاب ها را آماده کنیم ، اساتید مربوطه راتربیت و دانشجو پذیرش کنیم ، از وزارت علوم انتظار مساعدات جهادی داریم

-با توجه به اینکه مخاطب این ویژه نامه، بخش دستگاه‌های اجرایی، دانشگاهیان، و بخش خصوصی می‌باشد، چنانچه توصیه و یا هر مطلب دیگری در خصوص حفاظت از زیرساخت‌های حیاتی مورد نظرتان است، بفرمائید.

اساسی ترین توصیه ما این است که موضوع حفاظت از زیرساخت‌ها، از نظر ما موضوعی علمی و تخصصی بوده و در آن بایستی نگاه دفاعی و پدافندی و نگاه امنیت افزایی در خلال و در ذات برنامه توسعه و پیشرفت هر دستگاهی دیده بشود. در واقع همه ملاحظاتی که می‌تواند پایداری، تاب آوری، ضریب اعتماد کارکرد دستگاه در شرایط و سناریوهای مختلف را افزایش بدهد بایستی در ذات طراحی و در حین طرح دیده شود.

طبیعتاً چون در بخش های صنعتی یک اندازه ای طرح‌ها و برنامه‌های زیرساخت‌های ما از کشورهای خارجی گرفته می‌شود

و کشورهای خارجی بعضاً با شرایط امنیتی و اقلیمی خودشان کار برنامه‌ریزی می‌کنند، ممکن است شرایط اقلیمی و امنیتی آن‌ها متناسب و سازگار با شرایط ما نباشد. به عنوان مثال یک کشوری صرفاً با لحاظ ضریب ایمنی یک صنعتی را توسعه می‌دهد، خوب ضریب ایمنی تنها در منطقه ما کفایت نمی‌کند.

ما باید حتما علاوه بر آن ضریب امنیتی و ضریب پدافندی (دفاعی) را نیز در نظر داشته باشیم. بنابراین با این رویکرد ممکن است نقشه‌ها و برنامه‌های آن زیرساخت به طور کلی تغییر کند.

خواهش من از دستگاه‌های اجرایی این است که حتما سه لایه ایمنی، امنیتی و پدافند (دفاع) را مجزا از هم در نظر بگیرند. این که فکر کنیم ضوابط ایمنی کفایت از ضوابط امنیت و ضوابط دفاعی می‌کند یک اشتباه است.

الان ببینید در حوادثی مثل حمله به آرامکو، ضرایب ایمنی در سطح خوبی هم در نظر گرفته شده بود ولی وقتی که یکی از مخازن یک مجموعه مورد اصابت واقع شد آتش گرفت، آتش آن مخزن دیگر مخازن را هم در معرض آتش قرار داد. این موضوع نشان می‌دهد که ضوابط ایمنی صرفاً برای شرایط صنعتی و فارغ از هر نوع تهدید دیده شده است. بنابراین اگر یک منطقه ای ضریب تهدید داشت مثل منطقه غرب آسیا یا خاورمیانه که ضریب تهدید در آن وجود دارد، بنابراین ضوابط ایمنی اولیه کفایت از استقلال طرح را نمی‌کند و این موضوعی است که همه باید متوجه آن باشند. اینکه به عنوان مثال چنانچه ما در ساخت یک پالایشگاه، در تعیین فاصله بین یک مخزن تا مخزن دیگر، صرفاً تاثیر حوادث صنعتی و سلامت کارکرد را ببینیم، یک حداقل بوده و حتما حادثه امنیتی را نیز در کنار آن باید در نظر بگیریم. فرض کنیم که یکی از مخازن به هر دلیلی دچار حریق شد، باید جوری طرح ریزی کنیم که حریق این مخزن، مخازن دیگر را به حریق نکشاند. یا چنانچه ما در یک منطقه نیمه کوهستانی و یا در دامنه یک کوه پالایشگاهی بسازیم که فرضاً مخازن و فلرها (Flare) بالادست باشند. بعد یکی از مخازن به هر دلیلی نشت کند، در این حالت طبیعتا الزامات ایمنی کفایت نکرده و باید الزامات حفاظتی را نیز در نظر داشته باشیم. به عنوان نمونه امکان اصابت سلاح و امکان جاری شدن مواد مایع وجود نداشته باشد. بنابراین ما باید نگاه جامع تر به این مسئله داشته و ملاحظات خاص خودمان را در نظر بگیریم. این نگاه جامع از نظر ما همان موضوع حفاظت از زیرساخت است که هم بهره‌مندی و هم سایر مقولات را تامین نماید. یا از یک نگاه دیگر، ممکن است مخزن با سلاح مورد هدف قرار داده شده و منفجر شود و مایع آتش زا با آتش شروع به حرکت کند. خوب باید به نحوی مانع حرکت آن شد که به عنوان مثال با باند وال (BundWall) می‌توان این کار را انجام داد. جالب توجه است که در حوزه ایمنی باند وال‌ها وجود ندارند. به طور کلی در ضوابط مربوط به ایمنی مواردی نظیر حملات با سلاح تعریف نشده اند. پس چنانچه در منطقه ای احتمال وجود حملاتی از این جنس وجود دارد بایستی این موضوع را در نظر گرفت. در این صورت ممکن است فواصل مخازن با هم فرق داشته، همه مخازن روی زمین نبوده و بخشی از آنها به زیر زمین منتقل شده و مدفون باشند، یا شکل ظاهری مخزن عوض شده و تمهیدات از این قبیل در نظر گرفته شود. خوب همه این موارد بحث هایی است که در اینجا راجع به آنها مطالعه و بررسی می شوند.

– آقای دکتر ارتباط بین سه لایه ایمنی، امنیت و دفاع را چگونه می توان برقرار نمود به طوری که تعارضی بین آنها شکل نگیرد؟

در پدافند غیر عامل تلاش بر این است که این سه لایه را به صورت هماهنگ باهم ببینیم و اثرات آنها را حفظ کنیم. اگر در جایی این سه لایه باهم هماهنگ نبوده و ضعفی وجود داشته باشد، آن ضعف ها را کاهش داده و به نتیجه درستی برسانیم ان شاء الله.

تهیه و تنظیم کننده : دکتر حمید هوشنگی

مروری کوتاه بر پیشینه حفاظت از زیر ساخت‌های حیاتی

زیرساخت به مجموعه عناصر ساختاری به هم پیوسته ای اطلاق می شود که یک سیستم بزرگ را تشکیل داده و دارای ابعاد فنی-تکنولوژی گسترده ای است و در صورت عملکرد صحیح همه بخش‌های آن، می‌توان عرضه خدمات را به نحو مطلوبی انتظار داشت. در یک تقسیم بندی کلی، می‌توان زیر ساخت ها را به دو نوع زیرساخت حیاتی و غیرحیاتی طبقه بندی کرد.

بطور کلی زیرساخت‌های حیاتی، شامل زیرساخت‌هایی می‌شوند که انهدام و از کارافتادگی آن‌ها، تأثیر مخربی بر روی دفاع یا امنیت اقتصادی کشور خواهد داشته و در صورت فقدان و قطع خدمات ضروری زیرساخت مورد نظر، تداوم و حفظ حکومت یک کشور، به خطر می‌افتد.

بنابراین لزوم پرداختن به موضوع حفاظت از زیر ساخت‌های حیاتی نقش کلیدی در پایداری و تاب آوری کشورها دارد.

امروزه"حفاظت از زیرساخت‌های حیاتی" یا Critical Infrastructure Protection (CIP) بصورت یک شاخه علمی درآمده و از جمله اهداف کلیدی آن، تامین و افزایش ایمنی، امنیت و تاب‌آوری از طریق تقویت توانمندی حفاظت از سرمایه‌های ملی به‌منظور جلوگیری، بازدارندگی، خنثی سازی و یا کاهش اثر تهدیدات انسان ساخت می‌باشد. موضوع CIP و حفاظت از زیرساخت ها در برابر تهدیدات انسان‌ساخت بطور گسترده پس از حملات یازدهم سپتامبر ۲۰۰۱، در کشور آمریکا و دنیا مطرح گردید.بطوریکه پس از وقوع این حادثه، برخی سیاست گزاران در دنیا بدنبال طراحی سیاست هایی بودند که منجر به ایجاد یک استراتژی برای تامین امنیت ملی گرددکه بخش اصلی آن براساس CIP می‌باشد.

در کشور جمهوری اسلامی ایران نیز با پیشرفت علم و دانش در زمینه مهندسی پدافند غیرعامل، موضوع حفاظت از زیرساخت‌های حیاتی مطرح شده و در حال حاضر کارگروه‌های تخصصی نیز توسط سازمان پدافند غیرعامل تشکیل و بصورت تخصصی به این موضوع می‌پردازد.

در کشورهای مختلف دنیا از جمله ایالات متحده آمریکا، آلمان و انگلستان و جمهوری اسلامی ایران زیر ساخت حیاتی تعاریف مختلفی داشته که در این بخش به آن پرداخته شده‌است

آمریکا:

۱- مؤسسه استاندارد و فناوری آمریکا(NIST) زیرساخت حیاتی را اینچنین تعریف مینماید: " زیرساخت حیاتی عبارت است از سیستم ها و دارایی های حیاتی کشور، اعم از فیزیکی یا مجازی که تضعیف یا نابودی آنها موجب اثرات منفی بر امنیت، امنیت اقتصاد ملی، سلامت عمومی ملی یا ایمنی یا ترکیبی از این مواردشود".در یک گزارش به کنگره آمریکا، در تعریف زیرساخت حیاتی آمده است که "ساختارهایی که اختلال طولانی مدت در آنها میتواند موجب آسیب اقتصادی یا نظامی شود".

آلمان:

۲- اداره فدرال امنیت اطلاعات آلمان (BSI) زیرساخت حیاتی را چنین تعریف نموده است: " سازمانها یا امکاناتی که برای منافع ملی اهمیت کلیدی دارند و شکست یا نقص در آنها می تواند منجر به کمبود زیان آور عرضه، اختلال قابل توجه در جامعهیا آثار شدید مشابه شود".

انگلستان:

۳- زیرساخت حیاتی در انگلستان چنین تعریف می شود: " یکزیرساخت حیاتی شامل آن دسته تسهیلات، شبکه ها، خدماتو دارایی های فیزیکی و فناوری اطلاعات است که اختلال یا خرابی آنها، تأثیر جدی بر سلامت، ایمنی، امنیت یا رفاه اقتصادی شهروندان یا عملکرد مؤثر دولت خواهد داشت".

جمهوری اسلامی ایران:

در طرح جامع امن سازی زیرساختهای حیاتی کشور که توسط مرکز مدیریت راهبردی افتای (امنیت فضای تولید و تبادل اطلاعات و ارتباطات) کشورمان تهیه شده است، زیرساخت حیاتی چنین تعریف می‌شود:

"زیرساختی حیاتی است که در صورت اختلال یا تخریب، مؤلفه های امنیت ملی را تحت تأثیر قرار داده و امنیت ملی کشور را به خطر می‌اندازد".

در سند راهبردی پدافند سایبری کشور که توسط قرارگاه پدافند سایبری(وابسته به سازمان پدافند غیرعامل)تدوین شده است، **"زیرساخت حیاتی به مراکزی گفته می شود که در صورت انهدام کامل یا قسمتی از آن ها، موجب بروز بحران، آسیب و صدمات جدی و مخاطره آمیز در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصاد، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و یا دفاعی با سطح تأثیرگذاری سراسری در کشور شود".**

زیرساخت‌حیاتی درسایر کشورها

کشورهای مختلف، زیرساخت‌های حیاتی خاص خود را دارند. به طور معمول، زیرساخت‌های مربوط به **کشاورزی و غذا، آب، ایمنی و بهداشت، خدمات امداد و اضطرار، خدمات دولتی، صنایع دفاعی، فناوری اطلاعات و ارتباطات، انرژی، حمل و نقل، مالی و بانکداری، صنعت و تولید، پست و غیره** در کشورهای مختلف در مصادیق زیرساخت‌های حیاتی گنجانده شده‌است و هر یک از این‌ها نیز زیر ساخت‌های خُردتر مخصوص به خود را دارند مانند آزادراه، نیروگاه برق و غیره.

زیرساخت‌هایی مانند حمل و نقل، انرژی، مواد خطرناک، ارتباطات مخابراتی، امور مالی و بیمه و خدماتی مانند مدیریت فاضلاب، آب و غذا، حفاظت شهری و بهداشت را نیز می‌توان در زمره زیرساخت‌های حیاتی قرار داد. در برنامه حفاظت از زیرساخت‌های حیاتی اروپا هم زیرساخت‌های انرژی، اطلاعات صنعت هسته‌ای، فناوری‌های ارتباطات، آب، غذا، بهداشت، خدمات مالی، حمل و نقل، صنعت شیمیایی، فضا و امکانات تحقیق، به عنوان بخش‌های حیاتی در نظر گرفته شده‌اند.

تعیین زیرساخت‌های حیاتی در کشورهای مختلف، با شرایط و اولویت‌ها و سطح نیازهای آنها ارتباط تنگاتنگ دارد. به عنوان مثال، در بعضی از کشورها ممکن است امکانات و زیر ساخت‌های پژوهش و آموزش، به همراه زیرساخت‌های فیزیکی و سخت افزاری، جزء زیرساخت‌های حیاتی تعریف شوند. در یک مثال دیگر، اوباما پس از حمله های سایبری تاریخ ۲۴ مه ۲۰۰۹ میلادی، از زیرساخت‌های فناوری اطلاعات به عنوان یک دارایی راهبردی ملی نام می‌برد و حفاظت از آن‌ها را در زمره یک اولویت در امنیت ملی دانسته و می‌گوید: "ما اطمینان می‌دهیم که این شبکه‌ها امن، مورد اعتماد و قوی باشند. ما از آن‌ها در برابر هر گونه حمله‌ای، دفاع و از آن صیانت می‌کنیم و در صورت ورود هر نوع اختلال یا لطمه، آن را به سرعت برطرف می‌کنیم".

بنابراین همانطور که در بالا به نمونه‌هایی از آن اشاره شد، کشورهای مختلف با توجه به ضرورت‌ها و اولویت‌های خود، تعریف‌های متنوعی از زیرساخت‌های حیاتی ارائه می‌کنند. این تعاریف مختلف، مصادیق مختلفی را نیز شامل می‌شوند. به عنوان مثال، چنانچه گفته شد، امکانات و تجهیزات آموزش و پرورش یا فناوری فضا ممکن است در یک کشور جزء زیرساخت‌های مهم و حیاتی به شمار بیاید اما در کشور دیگری، در این تعریف قرار نگیرد. به همین منظور، برای انجام مطالعات، برگزیدن سیاستها و اعمال روش‌هایی برای مدیریت، نگهداری و حفاظت از زیرساخت‌ها لازم است که در هر کشوری تعریف جامعی از این زیرساخت‌ها ارائه شود. شناخت صحیح زیرساخت‌های حیاتی علاوه بر بررسی تأثیرات اقتصادی، ارزیابی عملکرد و برنامه‌ریزی مناسب در شرایط بحرانی، موجب درک بهتر سیستم‌های زیرساختی حیاتی، وابستگی زیرسیستم‌های موجود در این سیستم‌ها در تأسیسات زیربنایی ملی، تجزیه و تحلیل آسیب پذیری‌ها و پیامدهای ناشی از انتشار این آسیب پذیری‌ها و همچنین لزوم به کارگیری الزام‌های امنیتی در آن‌ها خواهد شد.

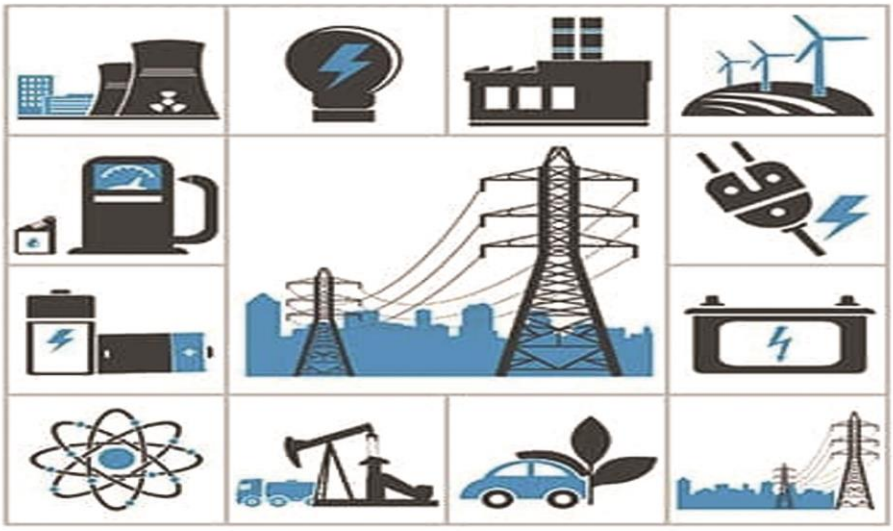
مؤسسه استاندارد و فناوری آمریکا با کمک وزارت امنیت داخلی(DHS) این کشور، در سال ۲۰۱۳ اقدام به شناسایی و معرفی اجزای زیرساخت‌های حیاتی در آمریکا کرده‌است. این زیر ساخت‌های حیاتی و منابع کلیدی که در ۱۸ بخش، به صورت کلی معرفی شده اند، شامل موارد زیر هستند:

۱- **کشاورزی و غذا:** شامل حیوانات، محصولات حیوانی، فرایندهای تولید محصول، بذر و کود که به دلیل حضور در زنجیره تأمین غذای شهروندان از اهمیت بالایی برخوردار هستند. فرآیندهای پس از برداشت محصول که، همچون تفکیک و بسته بندی، ذخیره‌سازی و توزیع نهایی آنها به مراکز خرده فروشی، خدمات مواد غذایی، رستوران‌ها و در نهایت، مصرف‌کنندگان خانگی نیز در این بخش قرار دارند.

۲- **بانکداری و امور مالی:** این بخش شامل مؤسسه‌هایی است که خدمات سپرده‌گذاری، اعتبارسنجی مشتریان، سیستم‌های پرداخت، اعتبار و نقدینگی، خدمات سرمایه گذاری و امور مربوط به بیمه آن‌ها را آنجا می‌دهند.

۳- **مواد شیمیایی:** این بخش شامل مواد شیمیایی اساسی، مواد شیمیایی خاص، مواد شیمیایی کشاورزی، داروسازی و مصرف کننده نهایی این محصول است.

۴- **امکانات تجاری:** این بخش شامل ۸ قسمت است که عبارتند از: اماکن تجمع عمومی)به عنوان مثال استادیوم‌ها، میدان‌های مسابقه، ورزشگاه‌ها، آکواریوم‌ها، باغ وحش‌ها، موزه‌ها و انجمن‌ها(، لیگ‌های ورزشی)به عنوان مثال لیگ‌های ورزشی حرفه‌ای و فدراسیون‌ها(، تفرجگاه‌ها،



محل‌های سکونت)به عنوان مثال هتل‌ها، متل‌ها و مراکز کنفرانس(، فضاهای عمومی باز)به عنوان مثال مراکز تفریحی، پارک‌ها، نمایشگاه‌ها، اردوگاه‌ها و راهپیمایی‌ها (سرگرمی و رسانه)به عنوان مثال استودیوهای فیلم و رسانه‌های تصویری(املاک و مستغلات)به عنوان مثال دفاتر و آپارتمان‌ها(، خرده فروشی)به عنوان مثال مراکز خرده فروشی و مراکز خرید).

۵- **ارتباطات:** این بخش شامل اجزای فیزیکی همچون خطوط سیمی، زیرساخت‌های بی سیم، ماهواره‌ای، کابلی، رادیو تلویزیون و همچنین قسمت‌های خدماتی مانند خدمات اینترنتی، اطلاعاتی و شبکه‌های تلویزیون کابلی است.

۶-**کارخانه‌های حیاتی:** این بخش شامل تولیدکنندگانی است که در طراحی، تولید و توزیع محصولات بخش‌های دیگر پوشش داده نمی‌شوند، همچون فلزات اولیه (به عنوان مثال کارخانه‌های ساخت و تولید آهن و فولاد و آلیاژهای آن‌ها)، تولید و فرآوری آلومینیوم و آلومینا، تولید فلزات غیرآهنی (به جز آلومینیوم)، ماشین آلات (به عنوان مثال موتور، توربین و تجهیزات انتقال قدرت)، تجهیزات الکتریکی، لوازم و تجهیزات حمل و نقل (به عنوان مثال وسایل نقلیه موتوری) محصولات و قطعات هوافضا، ریل‌های راه آهن و دیگر تجهیزات حمل و نقل).

۷- **سدها:** این بخش شامل دارایی‌ها، سیستم‌ها، شبکه‌ها و دیگر اجزای مربوط به پروژه‌های سدها، ناوبری، خاکریزها، موانع طوفان، آبگیرها، معادن و دیگر موارد مرتبط به همراهتجهیزات کنترلی آن‌ها است. همچنین طیف گسترده‌ای از مواردی که دارای منافع اقتصادی، زیست محیطی و اجتماعی هستند (شامل نیروگاه‌های برق آبی، رودخانه‌ها، آب، زیستگاه‌های حیات وحش، مدیریت مواد زاید و پسماندها و کنترل سیل) را نیز دربر می‌گیرد.

۸- **صنایع دفاعی:** این بخش شامل قسمت ها و واحدهایی است که در نهایت به تولید سلاح، قطعات و هزینه‌های سرمایه‌گذاری در آن مربوط می‌شود که بخش‌های عمده آن عبارتند از: موشک‌ها، هواپیما، پشتیبانی از نیروهای مسلحتجهیزات فضایی، خودروهای جنگی، مهمات، اسلحه‌ها، کشتی‌سازی، فناوری اطلاعات نظامی و الکترونیک.

۹- **خدمات اضطراری:** این بخش شامل یک سیستم مقابله و بازسازی است که اولین خط دفاعی کشور در مواجهه با حملات تروریستی و همچنین پیشگیری و کاهش پیامدهای ناشی از آن محسوب می‌شود. این بخش، از کارمندان آموزش دیده، سیستم‌ها، موافقت نامه‌ها و معاهده‌هایی تشکیل شده‌است که خدمات ایمنی زندگی را به شهروندان ارائه می‌کنند و شامل مدیریت اضطراری، خدمات اورژانس پزشکی، آتش نشانی، مواد خطرناک بمب گذاری‌ها، تیم‌های عملیات‌های تاکتیکی، گروه‌های اجرای قانون، تیم سلاح های ویژه، تیم‌های جستجو و نجات است.

۱۰- **انرژی:** زیرساخت‌های انرژی به ۳ بخش عمده تقسیم می‌شوند که شام برق، نفت و گاز طبیعی است.

۱۱- **امکانات دولتی:** این بخش دربرگیرنده طیف گسترده ای از ساختمان‌هایی است که تحت مالکیت یا اجاره دولت آمریکا در داخل یا خارج از این کشور قرار دارند که شامل ساختمان‌های اداری، تأسیسات خاص نظامی، سفارتخانه‌ها، دادگاه ها، آزمایشگاه های ملی و سازه هایی است که ممکن است در آنجا تجهیزات حیاتی، سیستم ها، شبکه‌ها و سایر موارد مرتبط وجود داشته باشد.

۱۲- **بهداشت و درمان:** این بخش شامل دولت و بخش‌های محلی بهداشت، بیمارستان‌ها، کلینیک‌های بهداشتی، مراکز بهداشت روان، خانه‌های سالمندان، مکان‌های نگهداری خون و فراورده‌های آن، آزمایشگاه‌ها، سردخانه‌ها و انبارهای دارویی است.

۱۳- **فناوری اطلاعات:** این بخش شامل قسمت‌های مجازی و فیزیکی توزیعی ارایه محصولات و خدمات فناوری اطلاعات از جمله سخت افزار، نرم افزار، سیستم‌های فناوری اطلاعات و خدمات آن است.

۱۴- **نمادها و آثار ملی:** این بخش شامل اماکن و ابنیه‌های ملی و تاریخی است که عبارتند از: بناهای تاریخی، ساختار فیزیکی و اشیای ملی و بین المللی به رسمیت شناخته شده که بیانگر میراث ملت‌ها، سنت‌ها و ارزش‌های مرتبط با آن و همچنین دارای اهمیت فرهنگی، مذهبی، تاریخی، سیاسی و ملی هستند و برای بازدید کنندگان و فعالیت های آموزشی مورد توجه قرار دارند.

۱۵- **راکتورهای هسته‌ای، مواد و ضایعات آن:** این بخش شامل نیروگاه‌های هسته‌ای حرارتی، نیروگاه‌های غیر حرارتی مورداستفاده درتحقیقات، آزمون و آموزش مواد هسته‌ای مورد استفاده در مصارف پزشکی، صنعتی و دانشگاهی، امکانات مورد تولید سوخت هسته‌ای راکتورهای انهدام، حمل و نقل، ذخیره سازی و دفع مواد هسته‌ای و زباله‌های آن است.

۱۶- **پست و حمل و نقل مرسوله:** با توجه به انتقال روزانه بیش از ۷۲۱ میلیون پیام، محصول و معاملات مالی در آمریکا، فعالیت‌های پستی و حمل و نقل مرسوله از اهمیت ویژه ای برخوردارند. این بخش شامل دارایی‌هایی همچون امکانات پردازش خودکار، واحدهای تحویل محلی، جمع آوری، پذیرش، عملیات خرده فروشی و همچنین وسایط حمل و نقل از جمله وانت، کامیون، تریلر، هواپیما و شبکه‌های اطلاعات و ارتباطات است. مواردی همچون مراکز بسته بندی، توزیع و دیگر امور مربوط به مرسوله‌ها نیز شامل این بخش هستند.

۱۷- **سیستمهای حمل و نقل:** شامل تمام انواع حمل و نقل همچون حمل و نقل هوایی، دریایی، حمل و نقل عمومی، بزرگراه‌ها، راه آهن، خطوط لوله و سیستم‌های شبکه‌ای به هم وابسته وسیع است که هر ساله میلیون‌ها نفر از مسافران و همچنین میلیون‌ها تن بار از طریق آن‌ها انتقال می‌یابند.

۱۸- **آب:** این بخش، شامل تأسیسات و سیستم‌های آب آشامیدنی و فاضلاب است.

گردآورنده: مهندس محمد جنیدی

مطالبی که ارائه می‌گردد از منابع مربوطه استخراج شده است.

سرفصل‌ها و برنامه‌های رشته CIP در برخی دانشگاه‌های خارجی و داخلی

حفاظت از زیر ساخت‌های حیاتی(CIP)، امروزه به صورت یک رشته مهندسی در مراکز علمی دنیا در آمده و شامل سرفصل‌های مختلفی می‌باشد.
در کشور ایران نیز با توجه به اهمیت موضوع CIP ، رشته مهندسی مرتبط با همین موضوع در مراکز علمی در دست بررسی است.
در این بخش به سرفصل‌های پیشنهادی این رشته درکشورهای مختلف اشاره شده است:

الف) دانشگاه‌های خارج از کشور

۱ دانشگاه جورج میسون (GeorgeMason University) آمریکا

یکی از مهمترین دانشگاه‌های جهان در حوزه حفاظت از زیرساخت‌های حساس، دانشگاه جورج میسون آمریکا می‌باشد. این دانشگاه به‌همراه پنج دانشگاه دیگر، کنسرسیونی تشکیل داده و مسئولیت راهبری علمی این مسئله را در آمریکا بر عهده دارد. دوره تحصیلات عالی که در این دانشگاه ارائه می‌شود، ۱۳ سرفصل کلی را مورد پوشش قرار می‌دهد که عبارتند از:

۱- مقدمه‌ای بر امنیت و تاب‌آوری زیرساخت‌های حساس
۲- تعریف و دستیابی به تاب‌آوری در زیرساخت‌های حساس
۳- آزمودن تاب‌آوری و امنیت زیرساخت‌های حساس (Critical Infrastructure Security and Resiliency) در محیط تهدیدات قرن ۲۱
۴- آزمودن توانایی‌ها، نقش‌ها و مسئولیت‌های CISR در سطوح: فدرال،(State, Local,Tribal and Territorial) SLTT وبخش‌های خصوصی
۵- سازماندهی و مشارکت برای تبادل اطلاعات
۶- ارزیابی ریسک زیرساخت‌های حساس در جهانی وابسته
۷- توانمندسازی امنیت و تاب‌آوری زیرساخت‌های حساس، مدیریت ریسک و سنجش عملکرد: رویکرد انتخابی
۸- توانمندسازی امنیت و تاب‌آوری زیرساخت‌های حساس، مدیریت ریسک و سنجش عملکرد: رویکرد قانونی و اجباری
۹- تهدید نفوذگرها و امنیت سایبری و آسیب‌پذیری‌های اسکادا
۱۰- امنیت وتاب‌آوری زیرساخت‌های حساس: ابعاد بین‌المللی
۱۱- مدیریت اثرات بر زیرساخت‌های حساس در یک محیط تمام‌تهدیداتی
۱۲- تمرین مدیریت امنیت و تاب‌آوری زیرساخت‌ها (فعالیت دانشجویی)
۱۳- شناخت، برنامه‌ریزی و حل ریسک‌های بلندمدت و مانا در زیرساخت‌های حساس و تمام دوره

دانشگاه کارلتون
(Carleton University)
کانادا

۲

رشته اول، مدیریت زیرساخت و امنیت بین الملل در دانشگاه کارلتون کانادا می‌باشد. این رشته در مقطع کارشناسی و کارشناسی ارشد ارائه گردیده است. جالب‌تر اینجاست که در مقطع کارشناسی ارشد دو مدل گرایش یکی کارشناسی ارشد (راهبردی) M.IPIS و کارشناسی ارشد مهندسی حفاظت از زیرساخت و امنیت بین الملل M.Eng in IPIS می‌باشد که در ادامه واحدهای هریک نیز مورد بررسی قرار می‌گیرد.

رشته حفاظت از زیرساخت و امنیت بین الملل سعی نموده ترکیبی علمی از سه دانشکده عمران، مهندسی محیط‌زیست و روابط بین الملل را ترکیب نموده و برنامه‌ای را طرح ریزی کنند که با ساختاری چند موضوعی به اصول مدیریت زیرساخت و ارزیابی تهدیدات چندلایه بپردازد. بدین منظور ایجاد چارچوب هشداردهی، عملیات پاسخ گرودارن امنیت و شناسایی سیاست‌های ایجاد کننده امنیت شهری از اهم دستاوردهای مد نظر در انتهای این پروژه می‌باشد. هدف این برنامه ایجاد فارغ التحصیلانی است که بتوانند به جامعه در زمان مناسب پاسخی چند بعدی بر اساس نیاز جامعه ارائه دهند. آن‌ها باید به راهکاری مستحکم، اقتصادی، جامعه پسند جهت ایجاد جامعه و شهری امن و تاب آور با ایجاد زیر ساخت‌های ایمن و تاب آور برسند.

از سوی دیگر دانشگاه کارلتون بر اساس موقعیت جغرافیایی خود که در اوتاوا قرار گرفته است مرکزیت را عامل فایده ایجاد این رشته می‌داند چرا که اکثر گرودارن اصلی بحران ساکن مرکز یا بهتر بگوییم پایتخت می‌باشند. تمام برنامه‌ها و مراکز هدایت و سیاست گذاری ۱۰ زیرساخت حیاتی ملی کانادا در پایتخت مستقر می‌باشند که خود باعث دسترسی حتی دانشجویان به مدیران زیرساخت و همچنین صنایع دولتی و غیردولتی می‌گردد. دانشگاه کارلتون سعی دارد با استفاده از این رشته و کار بروی حفاظت از زیرساخت‌ها پیوند محکمی را با این بخش حیاتی کشور ایجاد نماید. فارغ التحصیلان این رشته شانس استخدام در دپارتمان‌های دولتی کانادا در بخش زیرساخت‌های حیاتی ملی خواهند داشت مثل دپارتمان‌های انرژی، حمل و نقل، فن آوری اطلاعات، مخابرات، سلامت، سرمایه و ایمنی.

حیطه تخصصی:

- امنیت
- مهندسی
- توسعه سیاسی (علوم سیاسی)

زمینه‌های پررنگ تحقیقاتی در دانشکده:

- حفاظت از دارایی و زیرساخت حیاتی
- مدیریت ریسک امنیتی
- سیاست‌های امنیت ملی، حفاظت اطلاعات و تروریسم
- سازه‌های مقاوم طراحی شده در برابر انفجار
- ارزیابی تهدید و آسیب پذیری زیرساخت‌های حیاتی

سرفصل‌های دروس:

۱. استراتژی‌ها و مسائل در محافظت از زیرساخت‌های حیاتی
۲. اصول مهندسی زیرساخت
۳. ارزیابی ریسک در زیرساخت‌های حیاتی
۴. مدیریت زیرساخت‌های حیاتی
۵. تروریسم و امنیت بین الملل
۶. کاهش و کنترل تسلیحات و محدودسازی زرادخانه‌های نظامی و هسته‌ای
۷. امنیت بین المللی معاصر
۸. اطلاعات و امور بین الملل
۹. اطلاعات و امنیت ملی
۱۰. قوانین و سیاست‌های امنیت ملی
۱۱. موضوعات خاص در سیاست‌های امنیت زیرساخت
۱۲. امنیت حمل ونقل هوای و زمینی
۱۳. اصول و مبانی ایمنی حریق
۱۴. بحران‌های طبیعی در کانادا: ریسک و آثار
۱۵. تحلیل انفجار بر سازه‌ها
۱۶. مقدمه‌ای بر انفجار و مواد انفجاری مرتبط با زیرساخت‌ها و اجزای آن
۱۷. موضوعات انتخابی در مهندسی زیرساخت‌های حیاتی

پروژه کارشناسی ارشد:

به دانشجویان اجازه داده خواهد شد در زمینه حفاظت و امنیت زیرساخت‌ها تحت نظر یک مجموعه مهندسی زیرساخت پایان نامه خود را با نظر گروه اخذ و انجام دهند.

۳ دانشگاه آپریون کراکف– لهستان

٤ دانشگاه یو مس لوول آمریکا

رشته حفاظت از زیرساخت‌های حیاتی تحت عنوان امنیت مدیریت سیستم‌ها و حفاظت از زیرساخت‌های حیاتی (administration of security systems and critical infrastructure protection) در این دانشگاه ارائه گردیده است. هدف از این رشته مدیریت سیستم‌ها، امنیت و حفاظت از زیرساخت‌های حیاتی می‌باشد که بتواند فارغ التحصیلانی توانمند در این زمینه برای موقعیت‌های دولتی و اقتصادی مرتبط در جهت حفاظت از مردم و دارایی‌ها ایجاد نماید.

فرایند آموزش به گونه‌ای است که بستر دانشی را در جهت آشنایی با ارزیابی و مدیریت ریسک و حیطه‌های حفاظتی زیرساخت فراهم نماید.

جامعه هدف در این رشته افرادی هستند که در موقعیت‌های مرتبط با تیم‌های مدیریتی در سامانه‌های خصوصی و دولتی که در امور حفاظتی مشارکت دارند. همچنین تمامی افراد مرتبط با ساخت و ساز، تجهیزات، نصب و خدمات که نقش مهمی را در امنیت شهر و شهروندان ایفا نمایند جزو جامعه هدف می‌باشند. گروه‌های امنیتی، پلیس، امور زندانها، ارتش، گاردهای مرزی، آتش نشانی، گمرک، امنیت شبکه ریلی، شهرداری‌ها و آژانس‌های امنیتی جامعه هدف اصلی این مجموعه می‌باشد.

زیرساخت‌های مورد تحقیق در این رشته به شرح ذیل می‌باشد:

- تأمین انرژی و سوخت
- شبکه و ارتباطات
- مدیریت مالی
- مدیریت تأمین آب و غذا
- سلامت
- مدیریت امنیت راه و ارتباطات
- امداد و نجات
- تداوم فعالیت زیرساختهای عمومی و خدمت رسان
- تولید، ذخیره سازی، استفاده از مواد شیمیایی و رادیواکتیو و شبکه انتقال آن‌ها مثل خطوط لوله انتقال

در این دانشگاه نیز رشته حفاظت از زیرساخت در مقطع کارشناسی ارشد ارائه گردیده است. دانشجویان این رشته تلاش بر ارتقای مهارت‌هایشان در زمینه امنیت سیستم‌های پیچیده در نواحی شهری و همچنین فرودگاه‌های بین المللی، شبکه ریلی، سامانه‌های بندری، مسیرهای حمل و نقل جاده‌ای دارند. تکنولوژی سنسورها، امنیت حمل و نقل، مهندسی سامانه‌ها، علوم اجتماعی، و آنالیز اطلاعات و امنیت اطلاعات جزو اصلی‌ترین آموزه‌های رشته می‌باشد.

دروس اصلی:

- آموزه‌های امنیتی معاصر
- آنالیز امنیت اطلاعات: سیاست‌ها و آموزه‌ها
- ابعاد تخصصی و علمی و فن آورانه امنیت ملی
- روش تحقیق
- مقالات و تحقیقات امنیت زیرساخت

دروس انتخابی (۵ درس):

- پایش و بازرسی زیرساخت شهری
- نگاهی بر امنیت میهنی
- ایمنی و امنیت حمل و نقل
- ارزیابی تهدید و مدیریت ریسک
- امنیت سایبری و جرائم سایبری
- در معرض بودن و ارزیابی ریسک
- بازرسی و امنیت سیستمها
- درک طرح آینده پژوهی ایالت ماساچوست
- مدیریت بحران و حادثه
- آمار توصیفی و استنباطی
- سلاح‌های کشتار جمعی

ب) دانشگاه‌های داخل کشور

در کشور ایران در حال حاضر رشته مهندسی پدافند غیرعامل در دو مقطع کارشناسی ارشد و مقطع دکتری در تعدادی از دانشگاه‌های خاص، مورد توجه قرار گرفته شده است. اخیراً با تشکیل کمیته‌ای مشترک میان دانشگاه صنعتی مالک اشتر و شخص ریاست محترم سازمان پدافند غیرعامل کشور از سال ۱۳۹۵ فرآیند تدوین رشته حفاظت از زیرساخت‌های حیاتی کشور در مقطع دکتری و کارشناسی ارشد آغاز گردید. طی فرآیندی چند ماهه سرفصل‌ها، منابع و اطلاعات مورد نیاز جهت دست یافتن به این مهم صورت پذیرفت.

سپس به منظور تسریع در به ثمر رسیدن نتیجه محتوای طراحی شده برای رشته حفاظت از زیرساخت‌های حیاتی جایگزین محتوای رشته مهندسی طراحی صنعتی از منظر پدافند غیرعامل گردید. پس از طی فرآیندهای علمی و اداری این تغییر به تائید وزارت علوم، تحقیقات و فناوری رسید. به عبارت دیگر در سال ۱۳۹۶ مقطع کارشناسی ارشد این رشته امکان جذب دانشجو را پس از ابلاغ به دانشگاه صنعتی مالک اشتر دارا می‌باشد. در مقطع دکتری نیز تشکیل چنین رشته‌ای به تائید کمیته نظامی-انتظامی وزارت علوم، تحقیقات و فناوری رسیده و یکی از دانشگاه‌های دفاعی کشور باید آمادگی خود را جهت جذب دانشجو اعلام نماید.

دروس جبرانی و تخصصی الزامی در این رشته، شامل عناوین زیر بوده که عبارتند از:

دروس جبرانی

۱-طرح ریزی واحدهای صنعتی
۲-طراحی ایجاد صنایع
۳-سیستم‌های آسیب پذیر
۴-روش‌های ارزیابی ریسک
۵-بازگشت پذیری و تاب‌آوری
۶-مهندسی ارزش در حفاظت از زیرساخت‌های حیاتی

یکی از مهمترین دروس تخصصی الزامی، بازگشت پذیری و تاب‌آوری سیستم بوده که خود شامل سرفصل‌هایی به شرح زیر است:

- تاریخچه رویکرد تاب‌آوری و برگشت پذیری در حفاظت از زیرساخت‌ها
- گرودارن در زیرساخت و مفهوم کارایی و نحوه سنجش کارایی زیرساخت‌ها
- مدل‌های تاب‌آوری بر اساس تاب‌آوری در برابر زلزله
- مدل تاب‌آوری اقتصادی
- روش‌های ارزیابی ریسک برگشت‌پذیری در زیرساخت‌های بحرانی
- ظرفیت‌ها و زیرظرفیت‌های تاب‌آوری در زیرساخت‌ها
- ارزیابی برگشت‌پذیری موضوعی زیرساخت آب، انرژی و سایبری

با توجه به اینکه تاکنون و با توجه به گرایش‌های موجود، با این جامعیت (با توجه به دروس و سرفصل‌های پیشنهادی)، بدین صورت تخصصی به زیرساخت‌های حیاتی در حوزه دانشگاهی پرداخته نشده است، با تصویب این گرایش در وزارت علوم، گام بسیار مهمی در خصوص حفاظت از زیر ساخت‌های حیاتی برداشته‌خواهد شد.

گردآورندگان : -دکتر محمد علی نکویی - مهندس مجتبی عراقی زاده

طرح‌ها و برنامه‌های حفاظت از زیر ساخت‌های حیاتی در کشورهای مختلف

کارکرد پیوسته و مطمئن زیرساخت‌های حیاتی نقش کلیدی در تأمین رفاه اجتماعی، بهره اقتصادی و امنیت ملی برای کشورها دارد. مسئله تأمین امنیت زیرساخت‌های حیاتی در سال‌های اخیر با توجه به افزایش فعالیت گروه‌های تروریستی، توجه زیادی را از طرف کشورهای مختلف به خود معطوف کرده است. به طوری که‌این کشورها برای دفاع از زیرساخت‌های حیاتی خود در برابر تهدیدات برنامه‌های متنوعی را آماده کرده‌اند که از جمله می‌توان به طرح ملی حفاظت از زیرساخت‌های‌ایالت متحده و برنامه اتحادیه اروپا برای حفاظت از زیرساخت‌های بحرانی اشاره کرد.این برنامه‌ها شامل فازهای مستقل و معمولاً بلند مدتی برای مقابله با تهدیدات ناشی از حملات عامدانه و یا بلایای طبیعی علیه زیرساخت‌ها هستند. با وجوداینکه ممکن است تعاریف و اصطلاحات به کار رفته دراین برنامه‌ها با هم متفاوت باشند، تمامی‌این برنامه‌ها شامل سه فراز اصلی آمادگی‌های قبل از وقوع بحران، اقدامات حین وقوع بحران و اقدامات پس از وقوع بحران ناشی از حمله یا بلایای طبیعی هستند.

به طور کلی در پدافند غیرعامل، آمادگی‌ها و اقدامات قبل از شروع بحران شامل سه مرحله پیش بینی، پیشگیری و هشدار است. مرحله پیش بینی بحران عبارت است از شناسایی، رصد و تشخیص تهدیدات علیه تأسیسات و زیرساخت‌ها که با توجه به ویژگی‌ها و مشخصات محیطی و محاطی‌این تأسیسات و تهدیداتی که علیه آن‌ها مطرح است، صورت می‌پذیرد. مرحله پیشگیری عبارت است از خنثی کردن تهدیدات از اولین مرحله شکل گیری تا مرحله قبل از وقوع بحران. به عنوان مثال فرض کنید حمله یک گروه تروریستی خارجی به عنوان یک تهدید علیه یک زیرساخت در داخل یک کشور شناسایی می‌شود. دراین حالت اولین مرحله پیشگیری امن کردن مرزها جهت جلوگیری از ورود مهاجمین به داخل کشور است. با فرض عدم موفقیت اولین مراحل پیشگیری، حفاظت فیزیکی مناسب از تأسیسات مورد نظر به عنوان آخرین مرحله پیشگیری از وقوع بحران شناخته می‌شود.

در نتیجه یکی از مهم ترین اقدامات جهت آمادگی قبل از وقوع بحران، حفاظت فیزیکی و یا مستحکم سازی تأسیسات‌است. حفاظت فیزیکی مناسب از تأسیسات سبب می‌شود که احتمال موفقیت آمیز بودن حمله به زیر ساخت‌ها به میزان چشمگیری کاهش یابد. تمامی‌برنامه‌هایی که به پدافند زیرساخت‌ها می‌پردازند به حفاظت فیزیکی و نقش آن توجه ویژه دارند. مرحله هشدار نیز به منظور کسب آخرین آمادگی‌ها جهت مقابله با وقوع بحران انجام می‌پذیرد .مقابله با وقوع بحران با آمادگی کامل سبب کاهش خسارت ناشی از بحران می‌شود.

با توجه به محدود بودن منابع پدافند غیرعامل و همچنین تعددانگونه از تأسیسات، گام اول در تمامی‌برنامه‌های دفاع غیرعامل از زیرساخت‌های حیاتی در کشورهای دنیا در قالب قوانین و دستورالعمل، شناسایی تأسیسات حیاتی سامانه به منظور قرار گرفتن در اولویت مستحکم سازی است. بدین منظور از روش‌هایی تحت عنوان ارزیابی آسیب پذیری و ارزیابی ریسک سامانه استفاده می‌شود. دراین روش‌ها، به کمی‌سازی تحلیل‌ها نیاز است تا رابطه ریاضی میان حفاظت فیزیکی از تأسیسات حیاتی و احتمال موفقیت آمیز بودن حمله به آن‌ها تعیین گردد.

زیرساخت‌های حیاتی تبدیل به سیستم عصبی مرکزی برای اقتصاد در تمامی‌کشورها شده است. اگر عملکرد شبکه زیرساختی‌این زیر ساخت‌ها در معرض خطر یا آسیب پذیری باشند، امکان دستیابی به اهداف پایدار انرژی، توسعه اقتصادی و اجتماعی وجود ندارد. در سال‌های اخیر، کمیسیون اروپا (EC)وزارت امنیت سرزمینی ایالات متحده آمریکا (US) و دیگران، به دلیل تهدیدات بین المللی جدید، نگران امنیت زیرساخت‌های کشورشان بوده و طرح‌هایی را برای حفاظت از آنها ارائه کرده اند.

طرح حفاظت از زیرساخت‌ها:

در تعریف زیرساخت‌های حیاتی به عنوان زیرساختی که قطع دسترسی به آن ممکن است باعث از دست دادن زندگی، تاثیرات جدی یا شدید بر سلامت،ایمنی و یا اقتصاد شهروندان شود، توافق وسیعی وجود دارد. اگر چه امکان حمله سایبری به زیرساخت‌های حیاتی در اواخر دهه ۱۹۹۰ مشخص شد، اما خطرات بر زیرساخت‌های انرژی به عنوان پیامدی از رویدادهای قرن بیست و یکم (حملات تروریستی و بلایای طبیعی) برجسته تر شده است و به طور ویژه‌ای افکار عمومی‌را تحت تاثیر قرار داده و مشخصات مسائل مربوط به زیرساخت‌های حیاتی را مطرح کرده است. علاوه براین، سانحه در نیروگاه هسته‌ای فوکوشیما در ژاپن در ماه مارس ۲۰۱۱، مسائل مربوط به زیرساخت‌های انرژی حیاتی را در برنامه‌های سیاسی در اهمیت بالایی قرار داده است.

۱ طرح حفاظت از زیرساخت‌های ملی ایالت متحده آمریکا

ایالات متحده آمریکا و همه کشورهای عضو اتحادیه اروپا، کمیته‌ها و کارگروه‌هایی را برای پیشگیری، آمادگی، واکنش به حملات تروریستی و برنامه‌های همبستگی درمورد پیامدهای تهدیدات تروریستی تشکیل داده‌اند. در نتیجه کمیسیون اروپا در سال ۲۰۰۵ اوراق سبزی درمورد "برنامه اروپایی برای حفاظت از زیرساخت‌های حیاتی" را تصویب کرد (EC، ۲۰۰۵). پس از آن، در دسامبر ۲۰۰۸این شورا دستورالعمل ۰۸/۱۱۴ (CEU، ۲۰۰۸) را به تصویب رساند. در سال ۲۰۰۹،ایالات متحده طرح حفاظت از زیرساخت‌های ملی خود را تصویب کرد (NIPP، ۲۰۰۹). هر دو برنامه پیشین در جهان، NIPP و دستورالعمل EC/۰۸/۱۱۴، ناحیه‌هایی حیاتی را تعیین می‌کنند که در آن ناحیه‌ها تلاش‌ها باید به پیشگیری و حفاظت از زیرساخت‌ها متمرکز شوند.

این برنامه‌ها فرصتی برای تعریف دقیق تر سیستم‌های هشدار دهنده برای حفاظت از زیرساخت‌های حیاتی، شامل برنامه ریزی و اجرای فعالیت‌ها جهت اطمینان از تداوم و قابلیت اطمینان‌این زیرساخت‌ها را فراهم می‌کند.این قبیل طرح‌های حفاظتی زیرساختی عمدتاً در بخش‌های انرژی، حمل و نقل، فناوری اطلاعات و ارتباطات تمرکز می‌کنند.

چشم اندازی وسیع تر توسط NIPP مشخص می‌شود، بطوریکه بخش‌های بیشتری را پوشش می‌دهد که در آن زیرساخت‌های حیاتی را شناسایی می‌کند. اگرچه رویکرد ارائه شده توسط اوراق سبز کمیسیون اروپا (EC، ۲۰۰۵) در ابتدا هدف تحت پوشش قرار دادن هر چه بیشتر زیرساخت ها را داشت، در نهایت،این دستورالعمل (CEU، ۲۰۰۸) عمدتاً در بخش‌های انرژی و حمل و نقل، همچنین شامل زنجیره ارزش و عرضه، قابل قبول است. در ادامه به صورت مختصر در خصوص طرح‌های حفاظتی زیرساخت‌ها ارائه شده توسط کشورهای مختلف مورد بررسی قرار می‌گیرد:

یکی از مهترین دستورالعمل‌ها و قوانین موجود در خصوص زیرساخت‌ها، مربوط به کشور آمریکا بوده است. طرح ملی حفاظت از زیرساخت‌های حیاتی و منابع کلیدی طرحی در ابعاد بزرگ و یکپارچه است که اهداف، رویدادهای مهم و ابتکارات کلیدی را تعیین می‌کند.این طرح چارچوبی جامع و یکپارچه برای حفاظت از زیرساخت‌های حیاتی و منابع کلیدی (CI / KR) از طریق بخش فدرال،ایالتی، منطقه‌ای، محلی، قبیله ای و خصوصی (وزارت امنیت میهن‌ایالات متحده آمریکا ، ۲۰۰۳) فراهم می‌کند. طرح ملی حفاظت از زیرساخت‌های حیاتی سه حوزه خاص را شناسایی می‌کند: وابستگی متقابل بین بخش‌ها، امنیت سایبری و ماهیت بین المللی تهدیدات زیرساخت‌های حیاتی (Consolini، ۲۰۰۹).

چارچوب مدیریت ریسک طرح ملی حفاظت از زیرساخت‌های حیاتی (NIPP) شامل ۵ مرحله است که عبارتند از:

۱- تعیین اهداف امنیتی؛
۲- شناسایی دارایی‌ها، سیستم‌ها، شبکه‌ها و عملکردها؛
۳- ارزیابی ریسک؛ (پیامدها، آسیب پذیری‌ها و تهدیدات)
۴- اجرای عملیات مدیریت ریسک و اولویت بندی اقدامات؛
۵- سنجش اثربخشی.

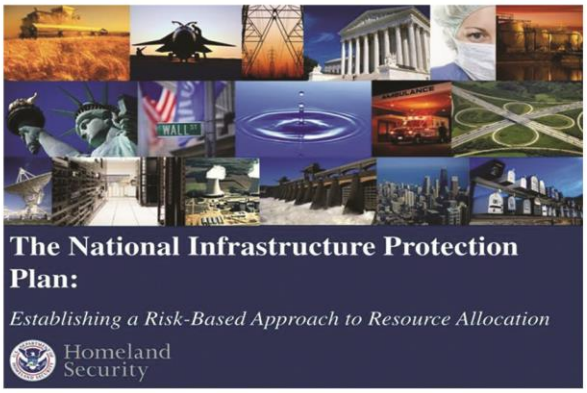
علاوه براین، چارچوبی برای بازخورد و بهبود مستمر در یک رویکرد انعطاف پذیر را ارائه می‌دهد. طرح کلی‌این طرح در شکل زیر نشان داده شده است.

از دیدگاه صنعت و در چارچوب مدیریت ریسک، اولین گام ایجاد اهداف‌ایمنی است. مسائل مهمی‌مانند از دست دادن زندگی، تاثیر اقتصادی و تاثیر امنیت ملی باید در فرمول بندی اهداف ایمنی در نظر گرفته شوند.

مرحله دوم، شناسایی منابع، سیستم‌ها، شبکه‌ها و عملکردها، نیاز به توسعه فهرستی کامل، حاوی اطلاعات اولیه در مورد منابع، سیستم‌ها و شبکه‌ها در کشور و شامل کالاهای مادی، ویژگی‌های انسانی و اطلاعات سیستم، می‌باشد.این اولین گام برای اطمینان از انعطاف پذیری است.

این روش شناسی‌ها در مرحله ارزیابی ریسک، نتایجی کامل و منطقی را با استفاده از فرایندهای کمی، سیستماتیک و خیلی دقیق ارائه می‌دهند.

برای مرحله اولویت بندی اقدامات، وزارت امنیت ملی‌ایالات متحده با شرکای امنیتی برای‌ایجاد اولویت‌های ارزیابی ریسک، اقدامات مشترکی را انجام می‌دهد.این همکاری برایشناسایی راهکارهایی به منظور کاهش خطر بوده و سپس اقدامات حفاظتی که می‌بایست لحاظ شود را تعیین کند.این مورد نیاز به مقایسه سطوح نسبی خطر و بخش‌های منابع همراه با گزینه‌هایی برای دستیابی به اهداف امنیتی دارد. بنابراین، در صورت امکان اقدامات حفاظتی به منظور کاهش خطر امنیتی اعمال می‌شود، که نتیجه آن یک تصمیم مقرون به صرفه است. در مرحله اجرای برنامه‌های حفاظتی، اقدامات حفاظتی با هدف کاهش خطر انجام می‌شود.



مرحله اندازه گیری اثربخشی از یک سیستم شاخص برای ایجاد اطلاعات در مورد دستیابی به اهداف خاص امنیتی تشکیل شده است که در NIPP (۲۰۰۹) تعریف شده است. شاخص‌های چنین نتیجه‌ای توصیفی و مبتنی بر فرایند هستند. به منظور حفاظت از زیرساخت‌ها، وزارت امنیت داخلی آمریکا، ساختاری را معرفی نموده است.

۲ برنامه اروپا برای حفاظت از زیرساخت‌های حیاتی (EPCIP)

در سال ۲۰۰۵، کمیسیون اروپایی "اوراق سبزی" با عنوان "برنامه اروپایی برای حفاظت از زیرساخت‌های بحرانی" منتشر کرد. در سال ۲۰۰۸، شورای اروپا دستورالعمل EC/۰۸/۱۱۴ به تصویب رساند، که برنامه اروپایی حفاظت از زیرساخت‌های بحرانی (EPCIP) راایجاد کرد. EPCIP به وضوح بر روی زمینه‌هایی به منظور توسعه برنامه‌های پیشگیری از تهدید و حمایت از زیرساخت‌ها، متمرکز شده واین زمینه‌ها را تعیین می‌کند.

چارچوب‌هایی که توسط دستورالعمل EC/۰۸/۱۱۴ ایجاد شده، را می‌توان از لحاظ طرح مدیریت ریسک که شامل شش مرحله است خلاصه کرد:

۱- ایجاد اهداف‌ایمنی؛

۲- شناسایی منابع و خطرات؛

• این مرحله شامل‌ایجاد فهرستی از منابع، دارایی‌ها، سیستم‌ها و شبکه‌ها در زنجیره ارزش زیرساخت می‌باشد. این گام همچنین شامل شناسایی خطرات موثر بر انعطاف پذیری سیستم است که نیاز به توسعه و نگهداری از فهرست دارایی‌های زیرساختی فیزیکی که شامل اموال، سیستم‌های اطلاعاتی می‌باشد، است و همچنین نیاز به در نظر گرفتن تهدیدات فنی و غیر فنی نیز می‌باشد.

۳- ارزیابی ریسک و خطرات؛

• تکنیکی است که به طور گسترده‌ای مورد استفاده قرار گرفته و پذیرفته شده است که شامل ارزیابی کیفی ریسک با استفاده از ماتریس‌های ارزیابی ریسک می‌باشد که به احتمال و پیامدهای هر ریسک توجه می‌کند. ماتریس خطر با ورودی از طریق مصاحبه و تکنیک‌های دلفی ایجاد می‌شود. ارزیابی ریسک کمی با استفاده از داده‌ها و متغیرهایی صورت می‌گیرد که مدل سازی آماری را امکان می‌سازد. ارزیابی ریسک کمی معمولا بر روی خطرات خاص، به ویژه خطراتی که می‌تواند عواقب جدی ایجاد کند، متمرکز می‌شود.

۴- اولویت بندی اقدامات و اجرای برنامه؛

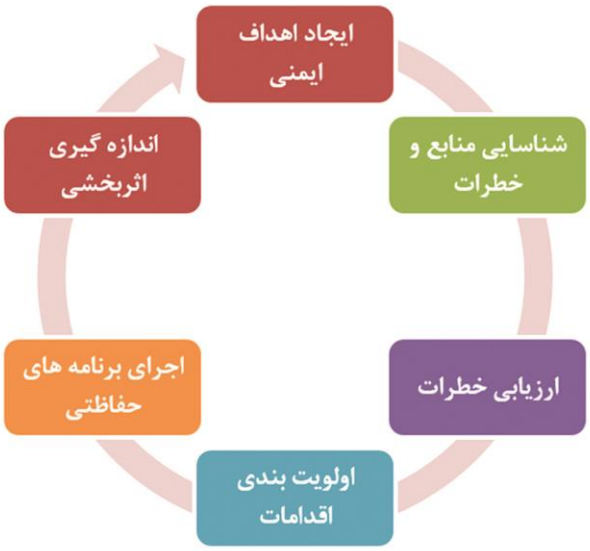
• این مرحله شامل مقایسه سطوح نسبی ریسک و گزینه‌هایی برای دستیابی به اهداف ایمنی است. اقدامات حفاظتی در صورت امکان به منظور کاهش خطرات امنیتی در یک روش مقرون به صرفه اعمال می‌شود.

۵- اجرای برنامه‌های حفاظتی؛

۶- اندازه گیری و نظارت بر اثربخشی.

• این مرحله فعالیت‌های نظارتی را به عنوان وسیله‌ای برای دستیابی به نظارت منظم، از جمله ایجاد شاخص‌های عملکرد، به کار می‌گیرد. بسیاری از فرصت‌ها برای تغییر و بهبود در این مرحله می‌توانند شناخته شوند.

بازخورد و بهبود مستمر نیز بخشی از این چارچوب هستند. شکل زیر یک طرح مدیریت خطر برای حفاظت از زیرساخت های بحرانی را ارائه می‌دهد که بااین چارچوب سازگار است. طرح‌های حفاظت از زیرساخت‌ها، استفاده از مدل های مدیریت ریسک‌کراکه‌استراتژی هایی برای افزایش اعتماد و اطمینان به وسیله گردآوری جامع و توجه به داده‌های دارایی‌های زیرساخت‌ها و ارتباطات زیرساخت‌ها ترکیب می‌کند، گسترش می‌دهند. همچنین برنامه‌های حفاظت از زیرساخت، رویکردهایی را برای دستیابی ذی نفعان و سهامداران مختلف به زنجیره ارزش زیربنایی حیاتی پیشنهاد می‌دهد.



هدف کلی EPCIP، تقویت حفاظت از زیرساخت‌های حیاتی در اتحادیه اروپا است. این کار از طریق اجرای قوانین اروپا به عنوان دستورالعمل‌ها و توصیه‌های منتشر شده توسط کمیسیون اروپا به دست خواهد آمد (Costantini et al.، ۲۰۰۷). چارچوب قانونی EPCIP شامل عناصر زیر می‌باشد (EC، ۲۰۰۵):

– روشی برای شناسایی و تعیین زیرساخت‌های بحرانی اروپا (ECI) و رویکردی مشترک برای ارزیابی نیاز به بهبود ایمنی آنها، که دومی توسط یک دستورالعمل ایجاد شده است.

– اقداماتی برای تسهیل در بهبود EPCIP که شامل یک طرح عملیاتی، یک سیستم هشدار در زیرساخت‌های حیاتی (CIWIN)، با

۳ استانداردهای تداوم فعالیت در بریتانیا

استفاده از ایجاد میز شور بر روی حفاظت از زیرساخت‌های بحرانی (CIP) در سطح اتحادیه اروپا، روش‌های به اشتراک گذاری اطلاعات در مورد CIP، شناسایی و تجزیه و تحلیل وابستگی متقابل.
- کمک به کشورهای عضو (MS) برای بهبود امنیت زیر ساخت‌های حیاتی ملی (CNI) و برنامه‌های مداخله (EC، ۲۰۱۱).
- برنامه‌های مالی تکمیلی و به ویژه برنامه ویژه "مدیریت پیشگیری، آمادگی و پیامد پس از وقوع تروریسم و سایر خطرات امنیتی" در دوره زمانی ۲۰۰۷ الی۲۰۱۳، که باعث شد اقدامات تامین مالی جدید برای حمایت از زیرساخت‌های حیاتی صورت پذیرد.

بخش انرژی اروپا توجه بیشتری به حفاظت از زیرساخت‌های بزرگ انرژی و تاسیسات آن‌ها دارد. همچنین شبکه‌ای از اپراتورهای زیرساخت حیاتی انرژی از بخش‌های برق، گاز و نفت برای تبادل تجربه در سطح اروپا در زمینه مسائل امنیتی (EC، ۲۰۱۱)ایجاد شده است.

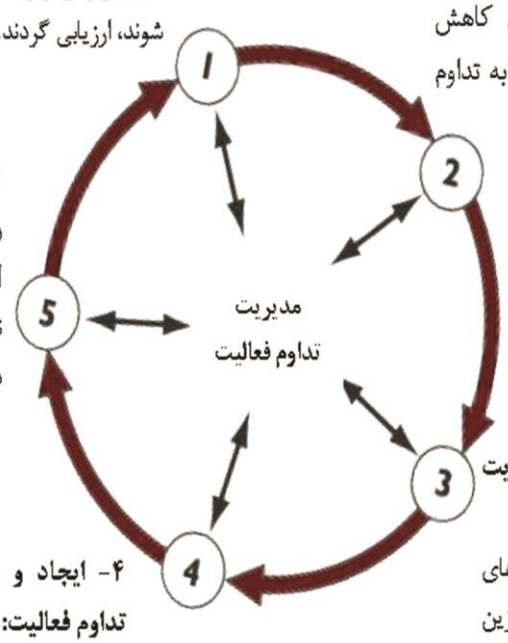
مؤسسه تدوین استانداردهای بریتانیا در مورد چگونگی مدیریت ادامه فعالیت‌ها در شرایط اضطراری استانداردی تدوین نموده است. این استاندارد BS ۲۵۹۹۹ نام دارد و در سال ۲۰۰۶ تصویب شده و با نگرشی بر اجزای کلیدی و مؤثر در برنامه‌های تداوم فعالیت در شرایط اضطراری تصویب شده است. در این رابطه چیزی شبیه چرخه زندگی یا چرخه دوام ارائه می‌دهد که شامل پنج جزء است:

۱- شناخت سازمان:

ابزارهای اندازه‌گیری ریسک و اثرات فعالیت، در تشخیص عوامل ایجادکنندهٔ شرایط اضطراری استفاده شود. اولویت-های بازتوانی و ریسک که می‌توانند منجر به توقف فعالیت شوند، ارزیابی گردند.

۲- راهبردهای مدیریت تداوم فعالیت:

تعیین مجموعهٔ راهبردهایی برای کاهش خسارت، ارزیابی معیارهای مربوط به تداوم و کارایی فعالیت‌های حیاتی



۳- اجرا و توسعهٔ واکنش‌های مدیریت تداوم فعالیت:

ایجاد ماتریس ریسک در مورد فرآیندهای عملیاتی. اجرایی سازی راهبردهای جایگزین سازی فعالیت با استفاده از معیارهای مالی ریسک و برنامه‌های تداوم فعالیت

۴- ایجاد و فرهنگ‌سازی استفاده از مدیریت تداوم فعالیت:

معرفی فرآیند مدیریت تداوم فعالیت از طریق نظام آموزشی و مسئولین و سرمایه‌گذاران، مشتری‌ها، کارکنان و ... .

۵- تمرین، بازنگری و حمایت از روش:

آزمایش برنامه، حسابرسی و تغییر نحوهٔ مدیریت فرآیند تداوم فعالیت در دستور کار قرار گیرد.

- شناخت سازمان
- شناخت راهبردهای مدیریت تداوم فعالیت
- اجرا و توسعه واکنش‌های مدیریت تداوم فعالیت
-ایجاد و فرهنگ سازی استفاده از مدیریت تداوم فعالیت
- تمرین، بازنگری و حمایت از استانداردهای مدیریت تداوم فعالیت

اگرچه رویکردها و روش‌های دیگری برای برنامه ریزی مدیریت تداوم فعالیت وجود دارد اما با این وجود، این استاندارد قابل مقایسه با توانمندی‌های دیگر روشها است. شکل صفحه قبل، مدلی برای برنامه ریزی تداوم فعالیت نشان می دهد که با استاندارد BS ۲۵۹۹۹ نیز هماهنگی دارد. باید گفت در بریتانیا بیشتر سازمان های دولتی در تشویق انواع کسب و کارها به اجرا و استفاده از برنامه‌های تداوم فعالیت نقش فعالی بازی می‌نمایند.

٤ اقدامات امنیتی و حفاظتی برای مقابله با تهدیدات در زیرساخت حیاتی حوزه مهندسی آب توسط سازمان امنیت منابع آب در آمریکا

امنیت منابع آب در آمریکا بعد از وقوع حادثه ۱۱ سپتامبر و ارسال پاکت‌های حاوی باکتری سیاه زخم، زیرساخت آب را مورد توجه خاص قرار داده و برای این منظور دو موسسه جدید به نام‌هایNHSRCو WSD of US EP تاسیس گردیده‌اند. بعد از حادثه ۱۱ سپتامبر، در کشور آمریکا مقرر شد وضعیت حفاظتی و آسیب پذیری منابع و سیستم‌های آبرسانی، سیستم‌های تصفیه، محل‌های ذخیره مواد شیمیائی، فرآیند گندزدائی، سیستم‌های کنترل الکترونیکی، مخازن ذخیره و شبکه توزیع آب و شبکه جمع آوری و تاسیسات تصفیه فاضلاب با شعار حفاظت همیشگی آب برای زندگی(protect water for life) مورد ارزیابی قرار گیرد. علاوه بر اصلاح قانون آب آشامیدنی سالم، طرح اصلاحی اضطراری مورد نیاز برای زیرساخت آب، تنظیم و ارائه شد تا با انجام اصلاحات، میزان آسیب پذیری‌این زیرساخت تا حد لازم کاهش یابد. دراین طرح اضطراری هشت عامل مهم و موثر مورد توجه قرار گرفت که عبارتند از:

- تهیه اطلاعات ویژه سیستم‌های آبرسانی(اطلاعات پایه شامل جمعیت تحت پوشش و نقشه)
- تعیین وضعیت موجود سیستم‌های آبرسانی و مسئولیت‌ها (تعیین نقش‌ها و مسئولیت‌های هر فرد)
- تعیین روش‌های ارتباطی: چه کسی؟ چه کار؟ چه وقت؟ (برای هرنفر از اعضای تیم مسئول اقدامات اضطراری)
- امنیت و ایمنی کارکنان (طرح تخلیه اضطراری، آموزش کارکنان، فراهم نمودن تجهیزات وکمک‌های اولیه)
- شناسائی منابع آب جایگزین (منابع آب نزدیک محل و ظرفیت آن‌ها، شناسائی صنایع توانمند در تهیه آب بطری شده)
- تجهیزات جایگزین و تهیه مواد شیمیائی (ازقبیل پمپ‌ها و دمنده‌ها برای مواقع اضطراری و تعمیرات)
- حفاظت ویژه (برای جلوگیری از دسترسی سایرین)
- نمونه برداری آب و کنترل (برای شناسائی بموقع آلودگی بالقوه وارد شده احتمالی)

با توجه به موارد فوق آمریکائی‌ها برای افزایش امنیت اساسی منابع آب، بودجه قابل توجهی به منظور انجام اقدامات زیر اختصاص دادند.

- خریداری و نصب تجهیزات فیزیکی، دریچه، پروژکتور یا دوربین‌های مدار بسته امنیتی.
- خریداری و نصب تجهیزات مناسب برای شناسایی متخلفان.
- غیر قابل دستکاری بودن پوشش‌های دریچه آدم رو، کپسول‌های آتش نشانی و اتاقک‌های شیر فلکه.
- دو قفله کردن درب‌ها و قفل‌ها.
- بهبود و اصلاح سیستم‌های الکترونیک، رایانه‌ای یا دیگر سیستم‌های اتوماتیک و سیستم‌های امنیتی کوچک.
- شرکت در برنامه‌های آموزشی و تهیه رهنمودهای آموزشی در خصوص موادی که به نحوی با مسئله امنیت آب ارتباط دارند، برای کسب آمادگی جهت مقابله با حملات تروریستی.
- توسعه و اصلاح نحوه استفاده، ذخیره سازی، یا حمل ونقل انواع مواد شیمیایی.
- اطمینان خاطر از انتخاب مناسب و صحیح و گزینش درست مستخدمین یا کارگران خدماتی.

۵ اقدامات امنیتی و حفاظتی برای مقابله با تهدیدات در زیرساخت حیاتی در کشور استرالیا

در کشور استرالیا سه وزارتخانه دفاع، دادگستری و ارتباطات در حوزه سیاست گذاری و اجرای برنامه‌های حفاظت از زیر ساخت‌های حیاتی فعالیت داشته که در این میان وزارت ارتباطات بیشتر وظیفه اجرای سیاست‌ها را بر عهده دارد.

وزارت دفاع استرالیا در زیر مجموعه خود اداره‌ای به نام سیگنال‌های دفاعی(DSD) داشته که وظیفه اصلی آن حفاظت از زیرساخت‌های رایانه‌ای و شبکه‌ای را بر عهده دارد. همچنین درکشور استرالیا سازمان مدیریت اطلاعات دولت، بخش دیگری از وظایف مربوط به امنیت در فضای اطلاعاتی را برعهده داشته و ذیل نظر وزارت ارتباطات قرار گرفته است.

در وزارت دادگستری نیز گروه حفاظت از زیرساخت‌های حیاتی قرار گرفته که وظیفه اصلی آن تشخیص مخاطرات، تعیین و ارزیابی آسیب پذیری در بخش‌های مختلف اعم از برق، حمل و نقل، موسسات مالی و مخابرات است. کشور استرالیا همچنین از یک شبکه اشتراک امن اطلاعاتی برای جریان داده‌های مربوط به حفاظت از زیرساخت‌های حیاتی خود بهره می‌برد.

گردآورنده : مهندس محمد جنیدی

یادداشت اعضا کارگروه CIP

سازمان پدافند غیرعامل جهت حفاظت از زیرساخت‌های حیاتی کشور کارگروهی متشکل از اساتید، دانشجویان و پژوهشگران علاقه‌مند به موضوع CIP تشکیل داده است. در کارگروه CIP با شکل گیری کمیته‌های توانمند در حوزه‌های مختلف زیرساختی مطالعات وپژوهش‌های قابل توجهی درجهت بومی سازی این موضوع انجام یافته است. در این مجله چندی از یادداشت های اعضا کارگروه در حوزه‌های مختلف ارائه می‌گردد.

حفاظت از زیرساخت‌های حیاتی شیمیایی

دکتر احمد اکرمی

مقدمه:

یک زیرساخت، چارچوبی از سیستم‌ها و شبکه های وابسته به یکدیگر شامل صنایع، موسسات و فعالیت‌های تجاری و مالی که فراهم کننده محصولات و سرویس‌های ضروری مورد نیاز برای برقراری امنیت اقتصادی و دفاعی کشور همراه با ادامه عملکرد مطلوب در تمام سطوح دولت و جامعه است. واژه زیر ساخت حیاتی به زیرساخت‌هایی اطلاق می‌شودکه تخریب و یا اختلال در عملکرد آن‌ها تاثیرات جبران ناپذیری از جنبه امنیت ملی، اقتصادی و روانشناسی برای یک کشور خواهدداشت.زیرساخت‌های‌حیاتی‌به‌علت‌سرویس‌ها، عملکردها و نقش‌هایی که در کشور ایفا می‌کنند به شدت پراهمیت هستند. این زیرساخت‌ها همچنین به علت متشکل بودن از مراکز پیچیده و وابسته به یکدیگر از اهمیت بالایی برخوردارند به گونه ای که، هرگونه حمله بر روی آن ها می‌تواند به مراتب فراتر از هدفی که مورد حمله قرار گرفته است انتشار و گسترش یابد و خسارت های ناشی از آن نه تنها در زمان حادثه بلکه بعد از آن نیز برای مدت طولانی پابرجا خواهد بود. حفاظت از زیرساخت‌های حیاتی (CIP) به مجموعه عملیات‌های مرتبط با آگاهی و پاسخ در مقابل حوادث ناگهانی درگیر کننده زیرساخت‌های حیاتی اطلاق می‌شود.

زیرساخت های حیاتی شیمیایی:

در تقسیم بندی زیرساخت‌های حیاتی، مواد و تاسیسات شیمیایی به طور رسمی به عنوان یک زیرساخت‌های حیاتی پذیرفته شده است. زیرساخت های حیاتی شیمیایی بخشی جدایی ناپذیر از اقتصاد کشور است که متشکل از چند صد هزار مرکز شیمیایی که به صورت یک مجموعه با یکدیگر در تعامل بوده و وظیفه تولید، ذخیره، انتقال و استفاده از مواد شیمیایی که عملکرد طیف گسترده ای از زیر ساخت‌ها بر اساس آن است را بر عهده دارد. برقراری امنیت در زیرساخت‌های شیمیایی نیازمند هوشیاری و مراقبت بخش دولتی و خصوصی در مقابل تهدیدات موجود و روبه رشد می‌باشد.

مواد و تاسیسات شیمیایی:

براساس محصول نهایی تولید شده زیر ساخت‌های شیمیایی را می‌توان به ۶ دسته شامل:

۱- زیرساخت‌های تولید کننده موادشیمیایی مرتبط با محصولات پالایشگاهی، پتروشیمی و سوخت‌های فسیلی،
۲- مواد معدنی و کودهای شیمیایی،
۳- گازهای صنعتی،
۴- مواد شیمیایی ویژه،
۵- مواد دارویی
۶- مواد شیمیایی پرمصرف عمومی‌تقسیم نمود.

این ساختارها اهمیت ویژه ای برای هر کشور از لحاظ اقتصادی داشته و از طرفی تولید، ذخیره سازی، استفاده و حمل و نقل این مواد نقش مهمی در ادامه فعالیت دیگر زیر ساخت‌های حیاتی در کشور دارد.

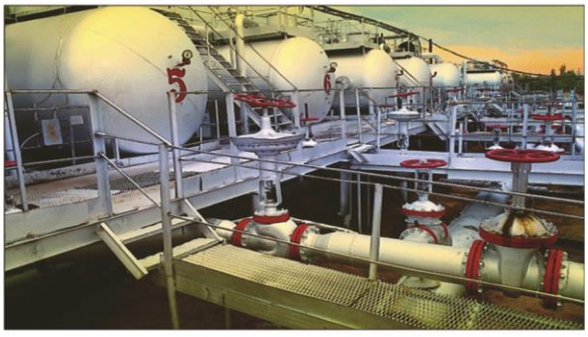
۱- مواد شیمیایی پایه (سوخت‌های فسیلی، پالایشگاهی و پتروشیمی):

این گروه شامل مواد شیمیایی تولید شده از مواد خام هیدروکربنی مانند محصولات حاصل از نفت خام و گاز طبیعی می‌باشد. مواد شیمیایی موجود در این گروه عبارتند از:

- مواد شیمیایی صنعتی و هیدروکربن ها (مانند الکل ها، اکریلیک ها و استات ها)
- مواد شیمیایی آروماتیک (مانند بنزن، تولوئن و زایلن)
- الفین ها (مانند اتیلن، پروپیلن، بوتادی ان و متانول)

۲- مواد معدنی و کودهای شیمیایی:

مواد شیمیایی این گروه شامل اسیدها (اسید سولفوریک و اسید نیتریک)، بازها (سدیم کربنات و سدیم هیدروکسید)، کلر، آمونیاک، کودهای پایه آمونیومی، مشتقات حاوی فلوئور (مانند هیدروژن فلوئورید)، فسفات‌ها، پتاس، رنگدانه‌ها (مانند تیتانیوم دی اکساید) و فلزات خاص مثل جیوه می‌باشد.



اهمیت حوزه کالبدی در حفاظت از زیرساخت های حیاتی (CIP)

مهندس محمد باقر ایزدی

تعاملات بین زیرساخت‌های حیاتی به طور فزاینده‌ای در حال نمایان تر شدن می‌باشند. تا به حال قرن بیست و یکم توسط حوادث و مخاطرات فراوان تعریف شده است که نگرش مربوط به زیرساخت‌های حیاتی و آسیب پذیر بودن، آن‌ها را با توجه به خطرات و آسیب پذیری ذاتی شان تغییر داده است. حوزه کالبدی به عنوان یک زیرساخت حیاتی مهم تلقی می‌گردد مفهوم حفاظت از زیرساخت‌های حیاتی (CIP) موضوعی چندجانبه است زیرا بسیاری از حوزه‌ها را تحت تأثیر قرار داده است. اگر بخواهیم یک تعریف کامل و جامع در حوزه حفاظت از زیرساخت‌های حیاتی (CIP) داشته باشیم که نشان دهد حوزه کالبدی به طور کامل با آن درگیر است این گونه می‌باشد که؛ به طور عمودی، این مفهوم وارد مرزهای سیاسی در سطح ملی، منطقه‌ای، ناحیه‌ای، شهری و محله‌ای می‌شود و به طور افقی تمامی اکنون نسبت به تهدیدات حساس شده اند. عدم قطعیت دستگاه‌ها یا و زارتخانه‌ها و سازمان‌های‌دولتی‌وخصوصی و شرکت‌های تابعه دولتی و خصوصی به همراه تمامی تهدیدات انسان ساخت و طبیعی را در بر می‌گیرد. از یک سو، حفاظت از زیرساخت‌های حیاتی (CIP) مسائل سیاسی مختلفی را شامل می‌شود و از سوی دیگر، مسائل علمی و مهندسی مختلفی را در بر می‌گیرد. حوزه کالبدی تمامی حوزه‌های مرتبط با دستگاه‌های اجرائی و جامعه کشور را در بر می‌گیرد. شش بخش اصلی را پوشش می‌دهد که شامل؛ بخش نفت و گاز، بخش شهری(معماری و شهرسازی)؛ بخش راه و ترابری، بخش صنعت، بخش صنعت برق، بخش آب می‌باشد. بطور مثال در بخش نفت و گاز چهار بخش اصلی این حوزه به ترتیب بخش نفت، گاز، پتروشیمی و پالایشگاه‌ها تقسیم بندی می‌شود و برای هر کدام از این بخش‌ها به ترتیب زیرساخت‌ها تفکیک و دارائی‌های هر کدام مشخص و اقدامات لازم جهت مصون‌سازی و حفاظت انجام می‌شود. وقتی از کلمه حفاظت استفاده می‌شود به بدین معناست که هر تخریب و یا خسارت فیزیکی، سایبری و یا ترکیبی بر زیر ساخت‌های حیاتی کشور می‌بایست نادر، مختصر، به لحاظ جغرافیایی محدود ، قابل مدیریت باشد

۳- گازهای صنعتی:

این گروه از مواد شیمیایی دو گروه بزرگ را در خود جای داده است.

۱. گازهایی که در مقادیر بالا جهت تسهیل تولید در فرآیندهای دیگرمورد استفاده قرار می گیرند(مانند فرآیند تولید فولاد) که شامل نیتروژن، اکسیژن، هیدروژن و کربن مونوکسید می‌شود.

۲.گازهای ویژه‌ای که در مقادیر کم، تولید می‌شوند تا در صنایع الکتریکی، غذایی و یا دیگر صنایع به کار گرفته شوند.

٤- مواد شیمیایی ویژه :

این گروه شامل مواد شیمیایی می‌شود که برای تولید مواد شیمیایی مهم دیگر مورد استفاده قرار می‌گیرند (مانند مواد شیمیایی مورد استفاده در به عمل آوردن کاغذ، تولید پلاستیک، تصفیه آب و معدن کاری)، مواد شیمیایی که به عنوان محصول نهایی مورد استفاده قرار می‌گیرند (آفت کش‌های مورد استفاده در صنعت کشاورزی)، مواد شیمیایی که در تهیه محصولات مصرفی عمومی‌و پرکاربرد استفاده می‌شوند (مانند محصولات مرتبط با بهداشت شخصی، رنگ ها، پوشش ها، چسب ها، وسایل ترمیم و عایق کاری و مواد شیمیایی مورد استفاده در صنعت عکاسی).

٥- مواد دارویی:

شامل داروهای بدون نسخه و نیازمند نسخه، مواد مورد استفاده در فرآیند تشخیص بیماری، واکسن‌ها و ویتامین های مورد استفاده برای انسان و دام ها می شود.

٦- مواد پر مصرف عمومی :

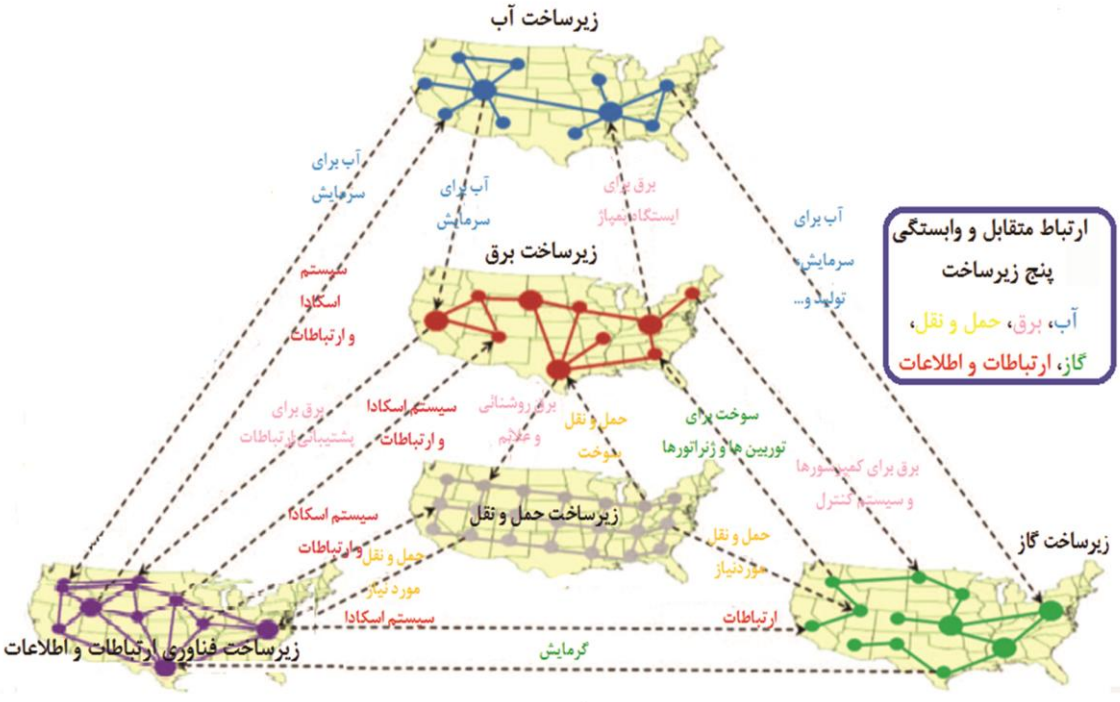
صابون‌ها، شوینده‌ها، سفیدکننده‌ها، رنگ‌ها، حلال‌ها، چسب‌ها، خمیردندان، شامپوها، لوازم آرایشی و عطرها در این گروه از مواد شیمیایی قرار می‌گیرند.

نتیجه گیری:

وقایع اتفاق افتاده در گذشته به خوبی چشم اندازی از بروز حوادث به صورت عمدی و غیرعمدی در زیر ساخت های حیاتی شیمیایی را بیان می‌نماید. بدیهی است که حوادث شیمیایی (نشت مواد سمی، انفجار و آتش سوزی) از این قبیل نگرانی ها را در مورد انتشار مواد شیمیایی و خطرات ناشی از آن بر سلامت تمامی‌موجودات زنده افزایش می‌دهد. بنابراین مجموعه‌ای از برنامه‌ها و اقدامات راهبردی، مدیریتی و عملیاتی در لایه‌های ایمنی، امنیت و دفاع درخصوص زیر ساخت‌های‌حیاتی شیمیایی بایستی توسط مسئولین، مدیران، کارشناسان تخصصی مورد توجه قرار گیرد.

و بـه خدمـات دولتـی، انسـانی و اقتصـادی و امنیـت ملـی کشـور حداقـل صدمـات را وارد نمایـد. زیرسـاخت‌هایی کـه پیـش تـر بـه عنـوان زیرسـاخت‌هایی مسـتقل و تـاب آور شـناخته می‌شـدند، مصـون سـازی و کاهـش آسـیب پذیـری فعلـی، تهدیـدات؛ اقدامـات تروریسـتی، نظامـی و حمـلات سـایبری متعـدد، موجـب بـروز بسـیاری از نقـاط ضعـف متقابـل در زیرسـاخت‌هایی شـده انـد کـه قبـلاً تصـور می‌شـد کـه بـه خوبـی محافظـت شـده و تـاب‌آور و مصـون هسـتند. قـرن بیسـت و یکـم، رویدادهـا و حـوادث بسـیاری را تجربـه کـرده اسـت کـه وقـوع آن در یـک بخـش از جهـان ممکـن اسـت پیامدهـای قابـل توجهـی بـرای جامعـه جهانـی داشـته باشـد بـه طـور مثـال فاجعـه نفـت آرامکـو عربسـتان، حادثـه قطـع بـرق ونزوئـلا ، فاجعـه هسـته‌ای فوکوشـیما، بحـران بانکـی در قبـرس، نشـت نفـت شـرکت نفـت و پتروشـیمی انگلیـس و بهـار عربـی. قبـل از ایـن حـوادث، درک و برخـورد بـا ارتباطـات متقابـل زیرسـاخت‌های حیاتـی جـزء اولویت‌هـای اصلـی نبـود. بـا ایـن حـال، در حـال حاضـر مسـائل مربـوط بـه وابسـتگی متقابـل و اندرکنش‌هـای موجـود در زیرسـاخت هـای حیاتـی بـه ویـژه تعییـن خطـرات و آسـیب پذیری‌هـای ناشـی از وابسـتگی متقابـل در زیرسـاخت‌های حیاتـی و توسـعه ابزارهایـی بـرای مدیریـت بهتـر ارتباطـات متقابـل در زیرسـاخت‌های حیاتـی امـری ضـروری می‌باشـد. در تجزیـه و تحلیـل نهایـی، چـه تهدیـدات انسـان دیدگاه‌هـای مسـتقل و وابسـتگی متقابـل، زیرسـاخت هـای حیاتـی یکسـانی در معـرض تهدیـد و خطـر هسـتند. بنابرایـن لازم اسـت ازملاحظـات مبتنـی بـر الگـوی کاهـش دهنـده علـت- معلولـی بـه الگـوی سیسـتماتیک روی بیاوریـم. الگـوی سیسـتماتیک بـا توجـه بـه روش‌هـا مختلـف آنالیـز ریسـک بومـی ارائـه می‌شـود و تمامـی شـرایط و ارتبـاط زیرسـاخت ثقـل یـا بالادسـت را از منظـر امنیـت، حساسـیت، وابسـتگی هـا، اندرکنـش هـا، پیامدهـا، هـم افزائی‌هـا و چگونگـی ارتبـاط بـا زیرسـاخت‌های پاییـن دسـت بـه صـورت سیسـتمی بررسـی و ارزیابـی می‌کنـد پـس می‌تـوان گفـت پیشـرفت‌های تکنولوژیکـی، وابسـتگی‌های متقابـل را افزایـش و در نتیجـه وابسـته نبـودن یـا خـود مختـاری زیرسـاخت‌های حیاتـی را کاهش می‌دهد.

بطـور مثـال اگرچـه ممکـن اسـت زیرسـاخت گاز مسـتقل از دیگـر زیرسـاخت‌های حیاتـی درنظرگرفتـه شـود، امـا ایـن جدایـی در واقعیـت محـدود اسـت. در شـکل زیـر رابطـهٔ زیرسـاخت گاز را بـا چهـار زیرسـاخت حیاتـی دیگـر را می‌بینیـم کـه در همـه مـوارد از جملـه زیرسـاخت بـرق، زیرسـاخت حمـل و نقـل، زیرسـاخت آب و ارائـه خدمـات بـه زیرسـاخت فنـاوری اطلاعـات و ارتباطـات وابسـتگی متقابـل وجـود دارد. افزایـش وابسـتگی متقابـل باعـث می‌شـود کـه ایـن زیرسـاخت در رابطـه بـا سـایر زیرسـاخت‌های حمایـت کننـده مـورد توجـه قـرار گیـرد و رویکـرد سیسـتمی بـه ایـن زیرسـاخت یـا سـایر زیرسـاخت‌های حیاتـی داشـته باشـیم.



مصون سازی یا امنیت باید اولویت اصلی و اول در مورد زیرساخت‌های حیاتی باشد، در عوض، باید از نظر سلسله مراتبی از امنیت و یا فرا امنیت بهره بگیریم تا نشان دهیم که ارتباطات متقابل باید بیشتر در نظر گرفته شود. امنیت مستقل از امنیت زیرساخت‌های انتقالی وابسته به سطح بالاتر وجود ندارد که در آن تطبیق پذیری را انجام دهیم. گسترش مرزهای تجزیه و تحلیل به این معنی است که فرصت‌های بیشتری برای ظهور مسائل ناشی از دیگر زیرساخت‌های حیاتی و همچنین روابط متقابل میان زیرساخت‌های حیاتی دیگر به وجود می‌آید. همچنین مهم است که جنبه‌های بالقوه زمانی بین روابط را معرفی کنیم. قطعاً احتمال تأخیر زمانی میان وقوع اتفاقات و اختلالات که در سراسر زیر ساخت‌های انتقالی مرتبط به هم پیوسته‌اند، وجود خواهد داشت.

به طور کلی می‌توانیم دیدگاهی از زیرساخت‌های حیاتی را که برای اهداف سیستمی ارائه دهیم. چشم انداز ما این است که زیرساخت‌های حیاتی سیستم‌هایی هستند که خدمات و محصولاتی را ارائه می‌دهند که برای سلامتی جامعه در سطح جامعه، منطقه‌ای، ملی و بین المللی مورد نیاز است. این سیستم‌ها عبارتند از سیستم‌های دولتی، سیستم‌های حمل‌ونقل(هوایی، دریایی، جاده ای و ریلی)، سیستم‌های انرژی، سیستم‌های آموزشی، سیستم‌های اورژانس و بیمارستان، سیستم‌های اجرای قانون (دستگاه‌های دولتی)، سیستم‌های امنیتی، سیستم‌های مخابراتی و سایر سیستم‌ها، این سیستم‌ها به سرعت در حال گسترش هستند و وابستگی پیچیده‌ای میان آن‌ها وجود دارد.

بنابراین تصمیم گیرندگان و سرمایه گذاران اعم از کارفرمایان، مجریان، مشاوران و ذی‌نفعان، زیرساخت‌ها را (بخصوص زیرساخت‌های حیاتی و حساس) باید با برنامه‌ریزی مناسب پیش ببرند، سه گام می‌تواند به منظور مدیریت بهتر سیستم، به ویژه هنگامی که وابستگی‌های متقابل شدید بین بخش‌های زیرساخت‌های حیاتی وجود دارد، مورد استفاده قرار بگیرند:

(۱) تشویق به توجه و ارزیابی مجدد وابستگی های متقابل بین زیرساخت‌های حیاتی؛

توضیح : استفاده از نظریه سیستم‌ها و تفکر سیستمی مورد تشویق قرار گیرد این تفکر به عنوان پایه ای برای ایجاد و استفاده از چشم انداز جامع برای رسیدگی به پایداری زیرساخت‌های حیاتی ناشی از ارتباط های متقابل با دیگر زیرساخت‌های حیاتی می‌باشد.

(۲) تصمیم گیری آگاهانه بر اساس درک روابط بین زیرساخت ثقل و دیگر زیرساخت های ؛ حیاتی و تصمیمات با درک بین روابط یک زیرساخت با زیرساخت وابسته به آن انجام شود.

(۳) اعمال قانون و مقررات جهت بررسی جامع (نگرش اکوسیستمی) وابستگی‌های متقابل موجود بین زیرساخت‌های حیاتی (از وابستگی‌های بالادستی تا پایین دستی).

توضیح: یک سیستم جامع زیر سیستم‌هایی دارد که می‌بایست مورد توجه قرار گیرد که باعث افزایش درک و مدیریت پایدار می‌شود که از ارتباطات با دیگر زیر ساخت‌های حیاتی به وجود آمده است پس می‌توان با اعمال قانون و مقررات مصوب این عمل را انجام داد.

به طور خلاصه، سه رویکرد و یک اقدام اساسی پیشنهاد می‌شود تا تفکر ما را نسبت به روابط رویکرد مبتنی بر ریسک و دیدگاه سیستماتیک زیرساخت‌های حیاتی با وابستگی متقابل، گسترش دهند.

اول: مخاطرات ناشی از وابستگی متقابل زیرساخت‌های حیاتی فراتر از مرزهای سنتی تجزیه شود و تحلیل برای زیر ساخت‌های حیاتی در کنار آن انجام شود تا از این طریق یک چشم انداز جامع ارائه شود که شامل طبقه بندی جدیدی از مخاطرات مرتبط بین زیر ساخت‌های‌حیاتی‌می‌باشد.

دوم: به نظر می‌رسد که مخاطرات ناشی از وابستگی متقابل زیرساخت‌های حیاتی، در حال ظهور است، و این نشان می‌دهد که این خطرات به عنوان خطرات بسیار نامعلوم شناخته می‌شوند؛ وقوع حوادث در وابستگی‌ها و اندرکنش‌ها بین زیر ساخت‌های حیاتی پیش از این قابل شناسایی نبود و احتمال وقوع این رخدادها را نمی‌توان تعیین کرد.

سوم: بهترین راه حل برای توسعه واکنش‌ها به حوادث ناگوار از طریق روشی است که سناریوهای بسیار نامعلوم را تجزیه و تحلیل می‌کنند.

اقدام اساسی: یکی از مؤثرترین و پایدارترین روش‌های مصون سازی در مقابل مخاطرات زیرساخت‌های حیاتی کشور داشتن الگوها، اصول و ضوابط، الزامات، ملاحظات، مقررات و استانداردهای فنی و مهندسی با توجه به سه رویکرد گفته شده در برابر تهدیدات و کاهش آسیب پذیری در سناریوهای مختلف می‌باشد.

آینده پژوهی زیرساخت انرژی هسته‌ای

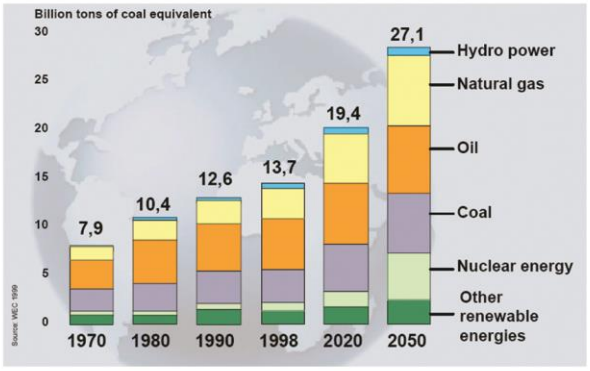
زیر کار گروه هسته‌ای سازمان پدافند غیرعامل

وقتی در مورد نیازهای آینده به انرژی صحبت می‌کنیم، فاکتورهای زیادی وجود دارد، از جمله: افزایش جمعیت، توسعه اقتصادی، ذخائر تامین انرژی و در نهایت مسائل زیست محیطی. منابع انرژی که ما داریم شامل فسیلی، شکافت هسته‌ای، خورشیدی، همجوشی هسته‌ای، آب، باد، زمین گرمایی و ... است.کارآمدترین آن‌ها برای تولید الکتریسیته فقط منابع فسیلی (ذغال سنگ، گاز و نفت) و شکافت هسته‌ای هستند و بقیه نمی‌توانند میزان انرژی مورد نیاز را تأمین نمایند.

نیروگاه‌های هسته‌ای الکتریسیته تمیز، مطمئن و مقرون به صرفه تولید می‌کنند. در آن واحد از بالاترین ضرایب ایمنی و امنیتی در مقایسه با سایر تاسیسات صنعتی برخوردارند.

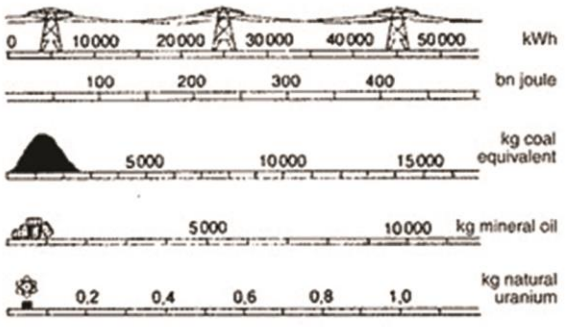
انرژی هسته‌ای به حفاظت از محیط زیست کمک می‌کند. نیروگاه‌های هسته‌ای الکتریسیته را بدون تولید تشعشعات مضر و گازهای گلخانه‌ای تولید می‌کنند. به دلیل فشردگی بالای انرژی، انرژی هسته‌ای سهم عمده‌ای در تولید الکتریسیته بدون گاز گلخانه‌ای دارد. انرژی هسته‌ای می‌تواند در مصرف سایر منابع انرژی صرفه جویی نماید. به علاوه، تکنولوژی هسته‌ای در پزشکی برای درمان سرطان‌ها، در هشدار دهنده‌های دود، در کاربردهای بی شمار صنعتی، در تعیین عمر آثار باستانی کاربرد دارد و کاربردهای تکنولوژی هسته‌ای در حال توسعه روزافزون است. در سال‌های اخیر، مزایای زیست محیطی انرژی هسته‌ای علاوه بر برق، به سایر محصولات انرژی نیز گسترش یافته است. به عنوان مثال ، انرژی هسته‌ای می‌تواند برای تولید هیدروژن برای استفاده در پالایش نفت؛ و به عنوان سوخت حمل و نقل برای کاهش وابستگی به نفت؛ و برای شیرین کردن آب در مناطقی که آب شیرین کم است، استفاده شود.

نزدیک ۱۰ درصد برق مورد نیاز جهان از طریق شکافت هسته‌ای تامین می‌شود. چشم انداز حاصل از آینده پژوهی WEC نشان می‌دهد که مقدار خالص آن تا سال ۲۰۵۰ سه برابر خواهد شد و بیشترین رشد را نسبت به سایر منابع انرژی خواهد داشت. طبق گزارش دوسالانه IAEA و NEA کشورهایی هم چون چین سرمایه گذاری وسیعی در زمینه اکتشاف منابع داخلی و خارجی و طراحی نیروگاه‌های هسته‌ای انجام می‌دهند. درحال‌حاضر حدود ۴۵۰ راکتور هسته‌ای فعال در جهان وجود دارد که بیش از ۱۰درصد انرژی الکتریکیمی‌کنند و این بالاترین سهم از منابع تولید انرژی بدون گاز گلخانه‌ای (انرژی‌های پاک) است.



مقایسه میزان سهم هر یک از منابع انرژی در تامین الکتریسیته جهان

یک قرص ۶ گرمی‌اورانیوم غنی شده می‌تواند به اندازه ۱ تن ذغال سنگ یا ۴۵۰ لیتر نفت یا ۴۸۰ متر مکعب گاز طبیعی انرژی تولید نماید؛ حال آن که در سوخت مصرف شده که از راکتور خارج می‌شود، حدود ۹۵ درصد اورانیوم موجود در آن به صورت استفاده نشده باقی می‌ماند. حال اگر با استفاده از راکتورهای نسل جدید و فرآیند بازفرآوری، این قرص ۶ گرمی می‌تواند به اندازه ۵۰ تن ذغال سنگ انرژی تولید نماید و چنین فشردگی انرژی در هیچ یک از منابع انرژی وجود ندارد. نکته حائز اهمیت این که این مقدار انرژی بدون ایجاد حتی یک گرم گاز گلخانه‌ای اتفاق می‌افتد و به طور مثال سوزاندن ذغال سنگ آلاینده‌هایی از جمله دی اکسید گوگرد، فلزات سمی، آرسنیک، کادمیوم و جیوه تولید می‌کند. مزایای بازفرآوری به این ختم نمی‌شود و با استفاده از این فناوری می‌توان کل نیاز جهان به عناصر پلاتین، پالادیوم و رنیوم را بدون حتی یک هزارم درصد اکتیویته اضافی تامین کرد.

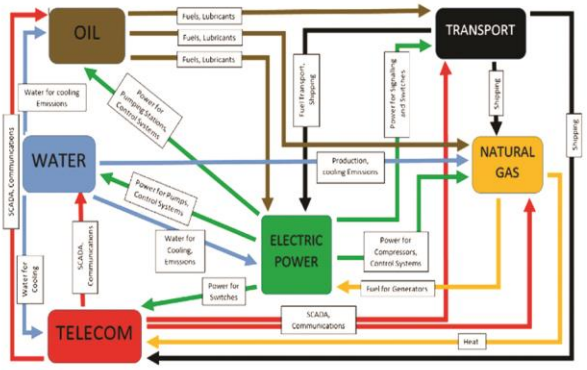


مقایسه میزان انرژی اورانیوم طبیعی با سایر منابع انرژی

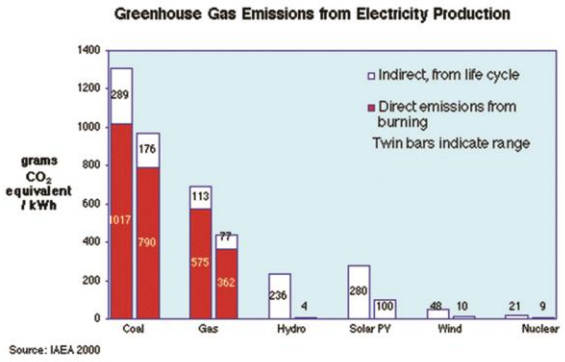
حفاظت از زیرساخت‌های حیاتی صنعت برق

مهندس مصطفی غضنفری

صنعت برق به عنوان مولد انرژی الکتریکی، پیش‌نیاز مهمی در پیشرفت حوزه‌های اقتصادی، اجتماعی و رفاهی در کلیه جوامع و کشورها محسوب می‌شود. به‌ویژه در کشورهای درحال توسعه یا کمتر توسعه‌یافته، در دسترس بودن برق با قابلیت اطمینان بالا، همراه نقش بسزایی در رشد و توسعه اقتصادی و اجتماعی دارد و این صنعت فقط در خدمت رسانی مستقیم به مردم و اهمیت برق، فقط به عنوان یک کالای خدماتی خلاصه نمی شود. صنعت برق ضمن اینکه الزام و نیاز ضروری توسعه صنایع دیگر است، دارای اهمیت زیادی در ابعاد امنیتی و سیاسی برای کشور است. بدون وجود شبکه سراسری برق، سیستم های برق اضطراری مراکز کلیدی، مدت زیادی دوام نخواهد آورد. پمپ های آب سیستم های آب‌رسانی شهری، سیستم های امنیتی بانک ها و مراکز دولتی، چراغ های راهنمایی و رانندگی و حتی سیستم های پمپاژ چاه های نفت از فعالیت باز خواهد ایستاد و ممکن است پیامدهای ناگوار و بعضاً غیر قابل جبرانی را به دنبال داشته باشد. از این رو است که این صنعت و عناصر تشکیل دهنده آن، در تمامی‌دنیا به عنوان یکی از زیرساخت های حیاتی مورد توجه قرار گرفته و راهبردها و برنامه های عملیاتی و اجرایی هدفمندی را، برای حفاظت از آن در دستور کار قرار می‌دهند.



زیرساخت حیاتی برق در ادبیات غالب کشورها، ذیل زیرساخت‌های حیاتی حوزه انرژی دسته بندی می شود و نفت، گاز و برق، سه جزء



میزان تولید گازهای گلخانه‌ای از منابع انرژی برای تولید الکتریسیته

در جدول زیر قیمت تمام شده برق تولیدی شامل بهره برداری، تعمیرات و سوخت از منابع مختلف از سال ۲۰۰۸ تا ۲۰۱۸ در آمریکا به واحد cent/KWh آمده است. وشکل بعد سهم هریک از منابع انرژی در تامین الکتریسیته آمریکا ذکر شده است.

0.01$/KWh	هسته‌ای	بخار تولیدی از سوخت فسیلی	برق آبی	توربین گازی و مقیاس کوچک
۲۰۱۰	۲,۴۰	۳,۵۸	۰,۹۲	۴,۸۷
۲۰۱۴	۲,۶۸	۳,۹۰	۱,۱۹	۴,۲۶
۲۰۱۸	۲,۳۹	۳,۵۹	۱,۰۷	۳,۲۴

چهار مرحله برای آمادگی حفاظت از زیرساخت‌های حیاتی:

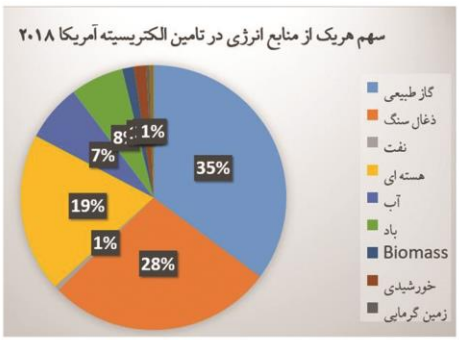
۱- شناسایی زیرساخت‌های حیاتی متعلق و در حال کار

۲- درک کردن وابستگی‌های متقابل زیرساخت‌های حیاتی

۳- احصا کردن مزایای منابع کشوری، استانی و منطقه‌ای

۴- دانستن این که در شرایط اضطرار چه کسانی حمایت می‌کنند.

در این مجال به مرحله اول آمادگی برای حفاظت از زیر ساخت‌های هسته‌ای پرداخته شد و این موضوع ادامه خواهد داشت.

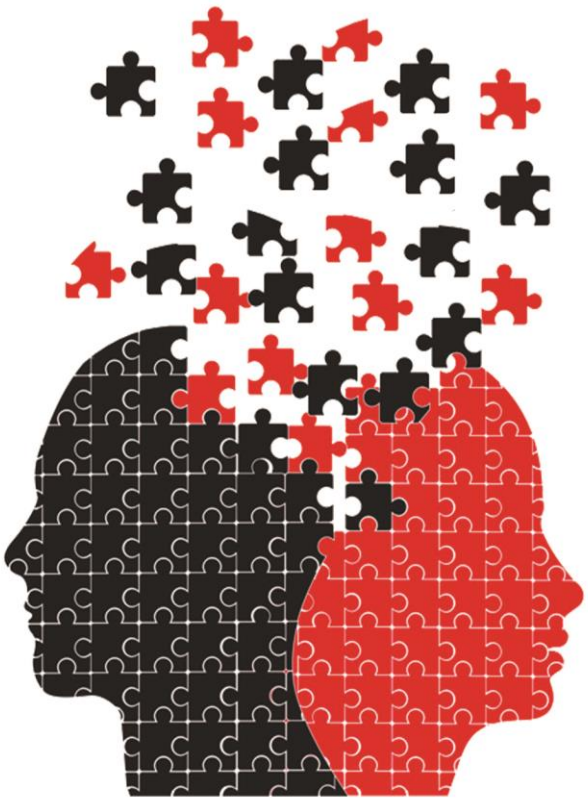


سهم هریک از منابع انرژی در تامین الکتریسیته آمریکا ۲۰۱۸

تشکیل‌دهنده زیرساخت های حیاتی انرژی در آن کشورها به شمار می رود. در جمهوری اسلامی‌ایران، باتوجه به تفکیک مدیریتی و نظام تصمیم گیری دو حوزه نفت و گاز از حوزه برق، زیرساخت برق در سه بخش کلان تولید، انتقال و توزیع به صورت مجزا مورد تحلیل قرار می‌گیرد. البته این مجزا بودن، به معنای عدم درنظر گرفتن وابستگی متقابل فی مابین زیرساخت برق با سایر زیرساخت‌های کشور از جمله نفت و گاز در تحلیل‌های حفاظتی نیست. شناخت وابستگی متقابل زیرساخت‌های مختلف یک مؤلفه ضروری جهت طراحی سیستم‌های تاب آور مورد نیاز زندگی است. این شناخت، به ویژه، شامل تبیین زنجیره تأمین و جایی که عملکرد یک سیستم برای عملکرد دیگری ضروری است، می شود. به صورت تخصصی، تحلیل وابستگی‌ها در حوزه برق، در سه گروه کلی مورد توجه است: تأمین سوخت مورد نیاز تأسیسات و تجهیزات تولید برق، تأمین منابع (وابستگی‌های فرادستی) مورد نیاز برای بهره‌برداری از تأسیسات (مانند آب مورد استفاده برای خنک کننده)، و عرضه برق به زیرساخت های مهم دیگری که برای بهره‌برداری، به زیرساخت برق تکیه می‌کنند (از قبیل زیرساخت‌های توزیع حوزه آب، زیرساخت‌های خدماتی نظیر بیمارستان‌ها، مراکز تصمیم گیری و...).

همانند سایر زیرساخت‌های حیاتی، حفاظت از زیرساخت‌های صنعت برق مستلزم شناسایی دقیق تهدیدات پیش روی این صنعت و در گام‌های بعدی، سنجش پیامدها (با تأکید بر پیامدهای آبشاری در حوزه صنعت برق) و ارزیابی آسیب‌پذیری و ریسک می‌باشد، تا اقدامات انجام شده در جهت حفاظت، کارا، مؤثر و بهینه باشد. تهدیدات متوجه بخش‌های مختلف صنعت برق را می‌توان در قالب تهدیدات سایبری، تهدیدات سخت و فیزیکی، مخاطرات طبیعی، رخدادهای جوی و حملات تروریستی دسته‌بندی نمود. با تبیین دقیق هر یک از تهدیدات در خصوص هر یک از عناصر تشکیل‌دهنده زیرساخت برق، می‌توان پیامدها و آسیب‌پذیری‌ها و در ادامه، اقدامات حفاظتی و کاهش ریسک را منطبق با اصل هزینه – فایده، تعیین نمود. قابل توجه است، در اسناد راهبردی حفاظت از زیرساخت‌های حیاتی اتحادیه اروپا در حوزه‌انرژی، همواره یک گزینه ریسک تحت عنوان "ریسک‌های شناخته نشده جدید و ناشی از ترکیب حملات فیزیکی و سایبری" برای تمامی‌زیرساخت‌های انرژی در نظر گرفته می‌شود تا بسته به موقعیت مکانی و زمانی، تحلیل‌های خاص برای زیرساخت مورد بررسی، مغفول واقع نگردد. شایان ذکر است، موارد مرتبط با بهره برداری از زیرساخت های صنعت برق از جمله تهدیدات ناشی از فرسودگی تجهیزات شبکه و نیروی کار سالخورده نیز در ادبیات حفاظت از زیرساخت های حیاتی برخی کشورها به چشم می خورد، به گونه‌ای که اثرات آن ها را بر ناپایداری تولید در شرایط عادی، زمینه ساز بحران ها و اقدامات امنیتی بعدی معرفی می نماید.

در مجموع، سیستم تأمین برق شامل تولید، توزیع و انتقال به عنوان یک زیرساخت حیاتی به شمار رفته و در صورتی که هر کدام از اجزای سیستم مختل شود، خاموشی برق رخ خواهد داد و «عدم تأمین برق» نیز یک بحران تلقی می‌شود. ازاین‌رو است که در ادبیات کشورهای مختلف، از زیرساخت های حیاتی انرژی (با تأکید بر حوزه برق) به عنوان زیرساخت پایه و زیرساختی که سایر زیرساخت‌ها برای تداوم عملکرد به آن نیازمند هستند، یاد می‌شود. در داخل کشور نیز این نگاه وجود داشته و پایداری تولید و شبکه از نگاه بهره‌برداری در سطح قابل قبولی قرار دارد. اما این موضوع نباید مانع از نگاه مصون سازی این زیرساخت حیاتی در برابر تهدیدات و مخاطرات انسان ساخت و طبیعی شود. این مصون‌سازی به خصوص در برابر تهدیدات سایبری و تهدیدات امنیتی از جنس تروریستی متوجه صنعت برق، در سال‌های اخیر همواره مورد توجه تمامی‌کشورها و از جمله جمهوری اسلامی‌قرار گرفته است و ضروری است این توجه و اقدامات مؤثر اجرایی در جهت مقابله با آن ها، با تجمیع دانش تخصصی و همت اجرایی ادامه یابد.



حفاظت از زیرساخت‌های حیاتی سایبری و وابسته به سایبر

مهندس هادی کریمی‌نیسیانی

۱. مقدمه:

در حال حاضر، بخش عمده ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور، در کلیه سطوح، اعم از افراد، موسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبر انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود، بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور نیز، به این فضا منتقل و یا اساساً در این فضا، شکل گرفته است.

عمده فعالیت‌های رسانه ای به این فضا منتقل شده، بیشتر مبادلات مالی از طریق این فضا انجام می گیرد و نسبت قابل توجهی از وقت و فعالیت‌های شهروندان، صرف تعامل در این حوزه می‌گردد. سهم درآمد حاصل از کسب وکارهای فضای سایبر در تولید ناخالص ملی افزایش چشم‌گیر یافته و از میان شاخص‌های تعیین شده برای سنجش میزان توسعه یافتگی کشور، شاخص‌های حوزه سایبر، سهم عمده‌ای را به خود اختصاص داده‌اند. بخش قابل توجهی از سرمایه‌های مادی و معنوی کشور، صرف این حوزه شده و بخش قابل توجهی از درآمدهای مادی و اکتسابات معنوی شهروندان نیز از این حوزه کسب شده و یا تاثیر عمده‌می پذیرد به‌عبارت‌دیگر، وجوه مختلف زندگی شهروندان، به معنای واقعی، با این فضا در آمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، مستقیماً وجوه مختلف زندگی شهروندان را به مخاطره خواهد انداخت. از طرفی زیرساخت‌ها، بسترهای مهم حیات، رشد و پویایی جوامع به شمار می‌روند. در این میان، برخی از زیرساخت‌ها نقشی حیاتی و حساس در منافع ملی دارند و اختلال هر چند کوتاه‌مدت در عملکرد آنها می‌تواند منجر به آسیب جدی در اقتصاد، امنیت یا ایمنی جامعه شود. یکی از ملاحظات مهم پیرامون زیرساخت‌های اساسی هر کشور، حفاظت از آنها در برابر تهدیدهای درونی و بیرونی است. مرور تجربه‌های گذشته کشور ما نشان می‌دهد که تهدیدها و اقدام‌های دشمنانه برخی دولت‌های خارجی در قبال ایران، محدود به حملات نظامی‌نبوده و در مقاطع زمانی مختلف، حوزه‌های گوناگونی از جمله انرژی صلح آمیز هسته‌ای، حمل و نقل هوایی، دریانوردی، بانکداری، فناوری اطلاعات و صنایع نفتی، عرصه‌های تجاوز به زیرساخت‌های مهم کشورمان بوده اند. انجام حملات سایبری مخرب، از جمله حمله به سایت هسته‌ای نطنز به استفاده از بدافزار استاکس‌نت و حمله سایبری به وزارت نفت توسط بدافزار فلیم ، نمونه‌های مشهوری از این اقدام‌های دشمنانه هستند. با بررسی دقیق تر طیف تهدیدات و جنگ های متصور، موضوعاتی مانند جنگ‌های هیبریدی (تلفیق جنگ‌های سایبری، اقتصادی، اطلاعاتی، نظامی‌و ...)، جنگ‌های شناختی (عملیات روانی و شبکه سازی در حوزه مردم) و جنگ‌های رسانه‌های اجتماعی در قالب جنگ نوین به عنوان مسائلی مهم مطرح هستند. تجربه حملات نظامی به کشورهای دیگر نشان دهنده این واقعیت است که فضای سایبری به نوعی به عنوان شروع کننده یا مکمل جنگ نظامی‌مطرح است. کشور حمله کننده در ابتدا زیرساخت‌های کشور هدف را از طریق حملات سایبری مورد آماج قرار داده و پس از فلج سازی دولت در ادامه خدمات ضروری و به حداقل رساندن آستانه تحمل مردم، اقدام نظامی‌را شروع می‌نمایند.

۲. تهدیدات نوین سایبری علیه زیرساخت‌های حیاتی و حساس:

با رشد و گسترش استفاده از ارتباطات و فناوری اطلاعات در زیرساخت‌های حیاتی و همچنین همه گیر شدن بهره برداری از زیرساختهای نرم افزاری و نرم افزارهای کاربردی در ایجاد، مدیریت، تعمیر و نگاهداری زیرساختهای حیاتی و به تبع آن لزوم شبکه ای شدن این زیرساخت‌ها برای کارایی بیشتر و کاهش هزینه‌ها تهدیدات، آسیب پذیری‌ها و مخاطرات این زیرساخت‌ها بطور فزاینده‌ای افزایش یافته است. به طور کلی تهدیدات علیه زیرساختهای حیاتی، با تهدیدات دیگر زیر ساخت‌ها تفاوت‌های بنیادی دارد. تهدیدات زیرساخت‌های دیگر ساده، فرصت طلب و عمومی‌می‌باشند. به عبارت دیگر این گونه از تهدیدات برای تمام افراد، زیرساخت‌ها و مراکز به یک ترتیب است و مکانیزم شناسایی و حفاظت از آنها نسبتاً آسان می‌باشد. در طرف دیگر تهدیدات علیه زیرساخت‌های حیاتی، بسیار پیچیده، هدف مند، ماندگار و منعطف APT مبتنی بر هوش مصنوعی و استفاده از Zero Dayها و بهره گیری از روش‌های دور زدن مولفه‌های امنیتی است. به عبارت دیگر دشمنان برای ضربه به زیرساخت حیاتی و بطور اخص زیرساخت‌های دارای وابستگی متقابل بالا، از مدت‌ها پیش اقدامات اطلاعاتی و فنی انجام میدهند تا بدافزاریا بطور دقیق تر سلاح سایبری را تولید نمایند که مکانیزم تشخیص آن بسیار پیچیده باشد و فقط بر روی اهدافی خاص آن هم تشخیص آن بسیار پیچیده باشد و فقط بر روی اهدافی خاص آنهم به صورت ماندگار و منعطف عمل نماید و در دیگر

شبکه‌ها اقدامی‌نداشته باشد. استاکس نت نمونه‌ای از این نوع سلاح‌های سایبری است که بسیار پیچیده و خاص منظوره تولید شده بود.

۳. کمیته حفاظت از زیرساخت‌های حیاتی سایبری و وابسته به سایبر:

سازمان پدافند غیر عامل کشور، به عنوان سازمان متولی سیاست گذاری و راهبری حفاظت و صیانت از زیر ساخت‌ها، تاسیسات زیر بنایی و شریان‌های حیاتی، حساس و مهم سایبری کشور در برابر انواع تهدیدات متصور، در نظر دارد که با رویکرد علمی، دقیق و همه جانبه از زیر ساخت‌های حیاتی سایبری و وابسته به سایبر حفاظت نموده و با بکار گیری توان علمی، تخصصی، اجرایی، تجربی و مدیریتی کشور گامی مهم در حفاظت و مصون سازی زیر ساخت‌های حیاتی کشور بردارد. لذا ضرورت و اهمیت حفاظت از فضای سایبری و سرمایه‌های ملی سایبری و وابسته به سایبر کشور، در مقابل انواع تهدیدات و تهاجمات سایبری و بویژه جنگ سایبری و هیبریدی، موجب گردید با هدف تمرکز بر دفاع از زیر ساخت‌های حیاتی، حساس و مهم کشور در مقابل انواع تهدیدات و تهاجمات سایبری، کارگروه حفاظت از زیرساخت های سایبری و وابسته به سایبر در سازمان پدافندغیرعامل کشور ایجاد شود.

٤. هدف اصلی :

حفاظت از زیرساخت‌های حیاتی سایبری و وابسته به سایبر (CCIP) در سه سطح زیرساختی، حوزه‌ای و ملی در مقابل طیف متنوع تهدیدات سایبری

۵. اهداف فرعی:

- تولید ادبیات و مبانی نظری در حوزه حفاظت از زیر ساخت‌های حیاتی سایبری و وابسته به سایبر
- تدوین سند راهبردی حفاظت از زیرساخت‌های حیاتی سایبری و وابسته به سایبر
- تعامل با بخش دانشگاهی و حوزه صنعت برای تولید محصولات بومی‌و امن جهت حفاظت از زیرساخت‌های حیاتی سایبری و وابسته به سایبر
- اشتراک اطلاعات عملی و مرتبط در بین مجموعه زیر ساخت‌های حیاتی به منظور ایجاد آگاهی در مقابل تهدیدات
- ایجاد سازوکاری جهت تشکیل مرکز رگولاتوری تخصصی حوزه‌های مشترک فیزیکی سایبری

- تدوین مجموعه مقررات، الزامات و ملاحظات جهت حفاظت از زیرساخت‌های حیاتی سایبری و وابسته به سایبر
- تدوین متدولوژی علمی‌و کارا برای حفاظت از زیرساخت‌های سایبری و وابسته به سایبر با درنظر گرفتن وابستگی‌های متقابل
- طراحی آموزش‌های طولی (کارشناسی ارشد، دکتری) و عرضی (مدیران و کارشناسان)
- برگزاری جلسات و همایش‌های تخصصی جهت هم اندیشی و هم افزایی دانش در حوزه حفاظت از زیرساخت‌های حیاتی سایبری و وابسته به سایبر

حفاظت از زیرساخت‌های حیاتی حوزه صنعت

دکتر سیدفضل الدین جمالیان - دکتر مهناز میرزا ابراهیم طهرانی

مقدمه:

اگر تمام فعالیت‌های اقتصادی که با تولید کالا و خدمات با استفاده از ماشین‌آلات و تجهیزات ساخته دست بشر سروکار دارند را به عنوان یک کل تصور کنیم، هرصنعت، زیرمجموعه ای از این کل است که عده فراوانی از فعالیت‌های مشابه را شامل می‌شود.تعریف مهم برای صنعت: به مجموعه تمام یگان‌هایی که در تولید، توزیع یا مصرف یک فراورده یا یک دسته از فراورده‌های مشابه فعالیت می‌کنند، «صنعت» گفته می‌شود.

کشورها دارایی ها و سرمایه‌های مختلفی دارند که در اداره امور کشور مورد استفاده قرار می‌گیرد.به طور طبیعی آسیب دیدن برخی از این زیرساخت‌ها لطمات جبران ناپذیری به کشور مربوطه وارد می‌کند.زیرساخت‌های حوزه صنعت برای هر کشوری از اهمیت خاصی برخوردار بوده و نقش مهمی در اقتصاد و اشتغال ایفا می کند.اکثریت زیرساخت‌های حیاتی کشور،وابستگی متقابل با زیرساخت‌های حوزه صنعت و تولید دارند.با توجه به جذابیت بالای زیرساخت‌های حوزه صنعت همانند مجتمع‌های فولاد و مس ، مناطق ویژه اقتصادی،شهرک‌های صنعتی و ... همواره مورد تهدیدات دشمن می باشد. از جمله متصور در حوزه صنعت ،تهدیدات اقتصادی ،تهدیدات تروریستی ،خرابکاری فنی و صنعتی ،تهدیدات شیمیایی و به تبع آن پیامدهای شیمیایی و تهدیدات سایبری را شامل می شوند.

زیرساخت حیاتی حوزه صنعت:

زیرساختی حیاتی است که در صورت اختلال یا تخریب، مؤلفه‌های امنیت ملی را تحت تأثیر قرار داده و امنیت ملی را به خطر می اندازد.با این تعریف زیرساخت‌های حوزه صنعت را می‌توان به بخش‌هایی همچون برق،گاز،آب،مواد اولیه (مواد خام)،زیرساخت‌های انتقال و توزیع انرژی ،سیستم‌های حمل نقل (زمینی،هوایی،ریلی،دریایی)،سیستم جمع آوری فاضلاب ،سیستم تصفیه‌خانه فاضلاب،مدیریت مواد زائد جامد،سیستم واکنش در شرایط اضطراری (سیستم‌های آتش نشانی و ...)،سیستم ایمنی،بهداشت و کیفیت (آزمایشگاه و...)،ماشین آلات و تجهیزات و تکنولوژی تولید،سرمایه تولید،تسهیلات مالی (وام و ...)بازار فروش محصولات (میزان تقاضا)،شبکه‌های کامپیوتری،سیستم وایرلس،نرم افزارهای طراحی و تولید،سیستم تضمین کیفیت تولید،دستورالعمل‌ها و روش‌های تولید صنعتی و نیروی انسانی باصلاحیت را نام برد.هرچند لازم است این تقسیم بندی ها برمبنای تولید خطر ،پیچیدگی‌های زیرساختی ،سلولی بودن یا سیستمی بودن نیز مورد توجه قرار گیرد.در ادامه به برخی از این تقسیم بندی‌ها می پردازیم:

الف-تقسیم بندی اولیه صنایع بر اساس سطوح مختلف فناوری

در این تقسیم بندی صنایع به دسته های زیر تقسیم می‌شوند:

- صنایع با فناوری برتر
- صنایع با فناوری بالاتر از متوسط
- صنایع با فناوری پائین تر از متوسط
- صنایع با فناوری پائین

ب-طبقه بندی صنایع تعریف شده در بورس اوراق بهادار تهران

در این تقسیم بندی صنایع به ۳۳ دسته تقسیم می شوند

ج-طبقه صنایع با توجه به فرآیند تولید توسط وزارت صنعت معدن با نگرش محیط زیستی

در این رویکر صنایع به ۱۱ دسته تقسیم می‌شود.

انقلاب صنعتی چهارم در صنعت:

به منظور توانمندسازی صنایع برای پیاده‌سازی مفاهیم Industry ۴,۰ موارد زیر حائز اهمیت هستند:

- ارائه پهنای باند بالا، اتصالات شبکه باسیم و بی‌سیم امن و ایمن
- دیجیتال‌سازی تجهیزات تولید مانند ماشین‌آلات، سیستم های حمل و نقل، دستگاه‌های ذخیره‌سازی، سنسورها، ابزارهای اندازه‌گیری، پایانه‌ها، چاپگرها، و غیره
- دیجیتال‌سازی کل زنجیره تولید به منظور اتصال به یک شبکه شرکتی (دیجیتالی‌کردن زنجیره عمودی)دیجیتال‌سازی تمام شرکت، تامین‌کننده‌ها و زنجیره مشتریان (ادغام افقی)دیجیتال‌سازی محصولات و خدماتتوانمندسازی شرکت‌ها برای توسعه مدل‌های کسب و کار دیجیتال جدید و پیشرفتهتوانمندسازی شرکت‌ها برای ایجاد یا استفاده از خدمات ابری در دسترس با پهنای باند بالاتجهیز کردن اپراتورها به رایانه، تبلت، تلفن هوشمند و غیره که باید دائم آنلاین بوده و به شبکه متصل باشند.

جمع بندی:

برای حفاظت از زیرساخت‌های با اهمیت حوزه صنعت و تولید ،تهیه و تدوین یک برنامه جامع ملی حفاظت از زیر ساخت‌های حیاتی ضروری است.تهیه و تدوین الزامات و ملاحظات،دستورالعمل و پروژه‌هایی مانند تداوم تولید(PCP) واکنش در شرایط اضطراری (ERP)،تداوم کسب و کار(BCP) حوزه صنعت دسته بندی صنایع و سطح بندی زیرساخت‌ها شناسایی و دسته بندی آسیب پذیری‌ها ،شناسایی تهدیدات و تدوین الگوی بومی آنالیز ریسک زیرساخت‌های حوزه صنعت ،کتاب شناسی و کسب تجربیات و اطلاعات موفق دیگران و ...مقدمه تدوین برنامه جامع حفاظت از زیرساخت‌های حیاتی حوزه صنعت می‌باشد.

در بخش زیرساخت‌های حیاتی، مطالعات علمی‌فراوانی صورت گرفته که قالب این مطالعات هم، بررسی این سامانه از دیدگاه‌های فنی، پدافند غیرعاملی و همچنین مدیریت بحران بوده است. نوراللهی و همکاران یکی از این مطالعات را انجام داده اند. این اثر در مهرماه ۱۳۹۴ پذیرفته شده و در دوفصلنامه علمی- پژوهشی مدیریت بحران چاپ بهار و تابستان به شماره هفتم به چاپ رسیده است.

در این مطالعه و تحقیق، آن ها زیرساخت‌های متعددی را مورد ارزیابی قرار داده‌اند. فرآیند و الگوی پیشنهادی این مطالعه به دنبال تلفیق مفاهیم خطرپذیری در زیرساخت‌های حیاتی با اهداف برنامه ریزانه در نگاه آمایشی به شهر است. در ادامه چکیده این مطالعه بصورت کامل بیان شده است.

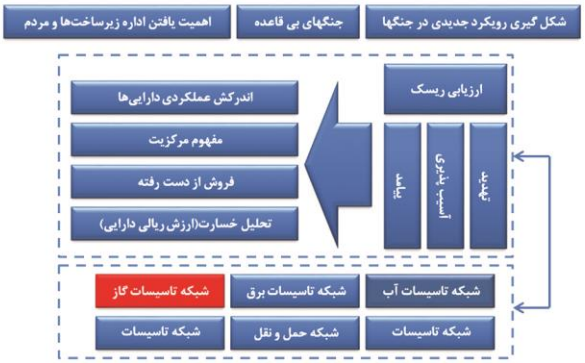
خطرپذیری = تهدید * آسیب پذیری * پیامد

چکیده:

رویکردهای متفاوتی در ارزیابی خطرپذیری شهری وجود دارد که ابعاد مختلف زندگی شهری را در برمی‌گیرد. فرآیند و الگوی پیشنهادی این مطالعه به دنبال تلفیق مفاهیم خطرپذیری در زیرساخت‌های حیاتی با اهداف برنامه ریزانه در نگاه آمایشی به شهر است. به این منظور ابتدا با استفاده از مفاهیم اندرکنش درون زیرساختی و بین زیرساختی، روابط در شبکه زیرساخت‌های حیاتی تبیین شده و سپس آسیب پذیری و پیامدهای اجزای این زیرساخت‌ها با توجه به توزیع جمعیت و فعالیت در پهنه فضا مورد ارزیابی قرار گرفته است. برای دستیابی به این مهم، در الگوی پیشنهادی از مفهوم "فروش از دست رفته" در ارتباط با عملکرد دارایی ها استفاده شده است. استفاده از این مفهوم علاوه بر افزودن ملاحظات آمایشی به مطالعه زیرساخت‌های حیاتی، امکان مقایسه بین دارایی های مختلف را نیز فراهم کرده است. برای عینی شدن این تحلیل، فرایند مذکور در یک منطقه شهری فرضی پیاده سازی شده است.

مقدمه:

در این تحقیق، به منظور تحلیل آسیب پذیری از شاخص مرکزیت و ماتریس‌های مجاورت استفاده شده است. در این راستا ماتریسی که در آن تمامی‌دارایی‌ها و وابستگی داخل شبکه‌های و خارج شبکه‌های آنها مورد بررسی قرارگرفت، تشکیل و برای حل دستگاه فوق از نرم افزار متلب استفاده شده‌است.



شکل الگوی ارزیابی ریسک پیشنهادی از طرف نویسندگان

تحلیل تهدید در مطالعه موردی:

در این تحقیق، بررسی پیامدها در بدترین حالت ممکن ناشی از رخداد تهدید مدنظر قرار گرفته است؛ از آنجا که روابط داخلی و خارجی، هزینه و زمان بازسازی زیرساخت‌ها و جمعیت و مساحت تحت تأثیر و از دست رفتن کارکرد آن ها همگی از معیارهای سنجش آسیب پذیری و پیامد در این مطالعه هستند، علاوه بر تهدید نظامی، تهدیدات سایبری و اقتصادی نیز به نوعی مورد توجه قرار گرفته شده است.

شکل ساختار تشکیلاتی تهدیدات

آن‌ها همچنین هزینه و زمان مورد نیاز برای احیای اجزای زیرساخت‌های مورد مطالعه که از جمله آن زیرساخت شبکه گازرسانی بوده است، را بررسی و محاسبه کرده اند.

هزینه و زمان مورد نیاز برای احیای اجزای زیرساختهای مورد مطالعه

زیرساخت	دارایی‌ها	هزینه مورد نیاز(ریال)	زمان مورد نیاز(ماه)
گاز	پالایشگاه	۴۲,۰۰۰,۰۰۰,۰۰۰,۰۰۰	۶۲
	CGS	۱۶,۱۶۳,۲۵۰,۰۰۰	۱۱
	(خط انتقال گاز)هر کیلومتر	۶,۸۰۰,۰۰۰,۰۰۰	۲

نتیجه گیری:

خطر پذیری برآمدی است از عامل‌های تهدید، آسیب پذیری و پیامد. در این مطالعه با تلفیق رویکرد آمایشی و عملکردی و با استفاده از یک مفهوم میانی)فروش از دست رفته(میزان خطر پذیری حاصل از تخریب و از بین رفتن زیرساخت‌های حیاتی به صورت کمی‌تعیین و محاسبه شد. در این مفهوم با تبدیل تمامی‌عامل‌ها به هزینه ریالی، علاوه بر ایجاد تصویری از میزان خطرپذیری در کل شبکه، امکان مقایسه بین زیرساخت‌ها و اجزای آنها نیز فراهم آمد. هما نطور که انتظار می‌رفت نتایج نمونه موردی نیز مبیّن این مهم است که هر یک از اجزای زیرساخت‌ها که مرکزیت، جمعیت، وسعت، هزینه و زمان احیای بیشتری دارد، میزان فروش از دست رفته و خطرپذیری آن در کل شبکه بالاتر است. با دانستن این مطلب که کدام یک از زیرساختهای حیاتی یک شهر می‌تواند تأثیرات مخرب بیشتری بر عملکرد شهر)از نظر هزینه وارده بر سیستم(داشته باشد، برنامه ریزان شهری می‌توانند تصمیمات و پیش بینی‌های مطلو بتر و واقعی تری برای ارتقای امنیت و بازدارندگی ارائه دهند. این تصمیمات می‌توانند گستره وسیعی از راهبردها را شامل شود. نمونه کوچکی از عناوین کلی این راهبردها می‌تواند شامل موارد زیر باشد:

-ایجاد تغییرات در شبکه و کاهش بار عملکردی اجزا؛

-ایجاد سامانه‌های پشتیبانی؛

-تأمین امکان خدما ترسانی به نقاط جمعیتی از راههای گوناگون؛

-استفاده از اجزای جایگزین در شبکه‌ها،

-توزیع متناسب اجزای شبکه با توجه به نقاط جمعیتی.

-همچنین با توجه به وضعیت شبکه ی مورد بررسی و امکانات و توان اقدام در هر محدوده مورد مطالعه، می‌توان راهکارهای گوناگونی برای کاهش میزان خطرپذیری ارائه داد.

تجزیه و تحلیل فاکتور های ریسک بحرانی مربوط به پروژه‌های خط لوله گاز و نفت در عراق (۲۰۱۹)

Analyzing the Critical Risk Factors Associated with Oil and Gas Pipeline Projects in Iraq

Layth Kraidi, Raj Shah, Wilfred Matipa, Fiona Borthwick

International Journal of Critical Infrastructure Protection
Pages ,2019 March ,24 Volume
14-22

چکیده:

اگر چه خط لوله‌های گاز و نفت به عنوان زیرساخت های حیاتی هر کشوری، حالت و شرایطی اقتصادی و امن برای انتقال محصولات نفتی در سرتاسر جهان هستند، اما این زیرساخت ها با چالش‌هایی ناشی از فاکتورهای ریسک مواجه می‌شوند. این ریسک‌ها شامل ریسک‌های ایمنی، امنیت، طراحی، ساخت و عملیاتی با توجه به اقدامات تروریستی، به ویژه در کشورهای در حال توسعه و ناامن و ناپایدار همانند عراق، می‌باشد. عدم دانش درباره مدیریت این چنین ریسک‌هایی و کمبود داده‌های گذشته درباره خرابی‌های خط لوله، مانع سیستم‌های مدیریت ریسک خط لوله‌های گاز و نفت (OGPs)می‌شود.

از این رو این مقاله بر روی شناسایی و تحلیل ریسک‌هایی ناشی از اختلال شخص ثالث (Third Party Disruption) به منظور توسعه مدل مدیریت ریسک جامع تمرکز دارد. یک پرسش‌نامه با استفاده از ۳۰ فاکتور ریسک شناخته شده از طریق مروری بر مطالعات جامع، طراحی شده است و در میان سهامداران خط لوله‌های گاز و نفت در عراق از طریق ابزار نظر سنجی آنلاین، جهت جمع آوری داده‌های پژوهش، توزیع شده است. از SPSS نیز برای تجزیه و تحلیل داده‌ها و ارزیابی فاکتورهای ریسک، مورد استفاده قرار گرفته شده است. یک چارچوب مفهومی‌برای مدل مدیریت ریسک (RMM)، بر مبنای مرور مطالعات و یافته‌های نظر سنجی، ارائه شده است. نتایج آشکار می‌کند که تروریسم، خرابکاری و فساد رسمی‌و بی قانونی موثرترین فاکتورها برای ریسک می‌باشد. همچنین محل خط لوله "Hot-Zones" تاثیری جدی بر روی خرابی خط لوله‌ها دارد.

مقدمه:

در این مقاله، اختلال شخص ثالث (TPD) اشاره به همه اقدامات فردی و گروهی که منجر به آسیب احتمالی یا غیر منتظره در خطوط لوله در هر مرحله از پروژه خط لوله می‌شود.

در حال حاضر، شرایط ناامن در سطح جهانی دلایل بیشتری را برای نگرانی و پیامدهای بالقوه جدی برای پروژه‌های OGP اضافه کرده است. این مورد به ویژه در کشورهایی با سطح پایین امنیتی که در آن‌ها خطوط لوله گاز و نفت (OGPs) اغلب از حملات تروریستی زیان آور رنج می‌برند، صادق است. چنین محیط‌های خطرناک باعث می‌شود مدیریت ریسک خطوط لوله نفت و گاز (OGP) چالش برانگیز و پیچیده شود. پروژه‌های OGP پیچیده و پر مخاطره هستند اما بسیار حیاتی هستند. در نتیجه، چالش‌های مدیریت ریسک و مشکلاتی که OGPها با آن‌ها مواجه هستند، روز به روز با توجه به طیف گسترده ای از مشکلات که پروژه‌های خط لوله روبرو هستند به دلیل محیط جهانی بی ثبات رو به افزایش است. توجه مناسب به فاکتورهای ریسک خطوط لوله گاز و نفت نیاز است زیرا بی توجهی به آنها باعث تلفات درمورد اختلال در فعالیت‌های تجاری و زیان‌های اقتصادی می‌شود.

در حوزه مدیریت ریسک OGP، مشکلاتی مربوط به درک درست، دسترسی به داده‌ها و تسهیلات ارزیابی ریسک، به ویژه در کشورهای در حال توسعه و ناپایدار مانند عراق دیده شده است. این بدان معنی است که مطالعات مدیریت ریسک می‌بایست به فرمت‌هایی تبدیل شود و هدایت شود که بتواند به منظور حفظ ساخت و سازهای ایمن و محیطی عملیاتی مورد بررسی، درک و تحلیل قرار گیرند.

برای دستیابی به نتایج معنی دار از رویکرد کیفی و کمی‌که در این تحقیق استفاده می‌شود، یک الگو عملگرا اتخاذ شده است. روش شناسی که در این تحقیق مورد بررسی قرار گرفته است بر اساس یک چارچوب جامع از یک مدل مدیریت ریسک (RMM) است که دارای سه مرحله است که در شکل ۱ نشان داده شده است. فاز اول در مورد شناسایی عوامل خطر OGP از طریق یک پایگاه داده در دسترس یا از طریق مرور ادبیات قبلی، در صورتی که پایگاه داده‌ای موجود نباشد، است. این مرحله می‌تواند به محققان در راستای قلب بر مشکلات ناشی از کمبود داده‌های موجود کمک کند. یافته‌های فاز اول در جدول ۱ ارائه شده است.

مرحله دوم در مورد تحلیل ریسک و جمع آوری داده‌ها است. در این مرحله، پرسش نامه‌ای طراحی شده و در میان ذی نفعان و سهامداران OGPs در عراق برای جمع آوری ادراکات خود پیرامون احتمال و شدت سطح عوامل خطر OGPs توزیع می‌شود. برای تعیین مقادیر عددی احتمال ریسک (RL) و شدت خطر (RS)، تجزیه و تحلیلی آماری و توصیفی بر نظر سنجی انجام شده است.

در نهایت، مرحله سوم در مورد شبیه سازی عوامل خطر با استفاده از الگوریتم ریاضی و مدلی مبتنی بر کامپیوتر بر اساس یافته‌های مراحل I و II می‌باشد. این مدل مدیریت ریسک (RMM) توسعه یافته رویکردی جامع و منظم (سیستماتیک)برای شناسایی و ارزیابی خطر خطوط لوله گاز و نفت (OGP)، به ویژه برای دولت‌ها و سازمان‌ها که در ابتدای تلاش‌های مدیریتی خود در زمینه شناسایی عوامل خطر، ثبت داده‌ها و مدیریت ریسک سیستماتیک هستند، ارائه می‌دهد. علاوه بر این در این تحقیق، یک پایگاه داده جدید برای ذخیره یافته‌ها و توصیه‌های این تحقیق برای استفاده در تحقیقات آینده ایجاد خواهد کرد.

جدول فاکتورهای ریسک

ردیف	عوامل خطر(فاکتور ریسک)
۱	عوامل اجتماعی-سیاسی مانند سطح تحصیلات و فقر
۲	سطوح پایین آگاهی قانونی و اخلاقی عموم مردم
۳	دزدان
۴	تروریسم و خرابکاری
۵	تهدید به کارکنان (آدم ربایی و / یا قتل)
۶	نشت اطلاعات حساس
۷	موقعیت جغرافیایی مانند "Hot-Zones"
۸	مناقشه بر سر مالکیت زمین
۹	قابلیت دسترسی خطوط لوله
۱۰	خطرات زمین شناسی مانند حرکت خاک و لغزش‌های زمینی
۱۱	تصادفات خودرو
۱۲	تصادفات حیوانی
۱۳	عدم انطباق با مقررات ایمنی
۱۴	عدم دسترسی به نشانه‌های هشدار دهنده
۱۵	عدم نگهداری مناسب و بازبینی منظم
۱۶	فرصت خرابکاری درخطوط لوله در معرض
۱۷	روش‌های مدیریت ریسک نامناسب
۱۸	بلایای طبیعی و شرایط آب و هوایی
۱۹	توانایی ضعیف برای شناسایی و نظارت بر عوامل خطر
۲۰	کمبود خدمات IT با کیفیت بالا و مدرن
۲۱	خوردگی و عدم اقدام ضد خوردگی
۲۲	نقص طراحی، ساخت و ساز، مواد و تولید
۲۳	خطاهای عملیاتی به عنوان مثال خطای انسانی و خرابی تجهیزات
۲۴	حملات هکرها در سیستم عامل‌های و یا کنترلی
۲۵	قانون که به خرابکارها اعمال نمی‌شود (بی قانونی)
۲۶	سهامداران توجه جدی نمی‌کنند
۲۷	تعداد کمی از محققان با این مشکل برخورد می‌کنند
۲۸	کمبود سوابق تاریخی در مورد حوادث و ثبت ریسک
۲۹	کمبود برنامه‌های آموزشی مناسب
۳۰	فساد

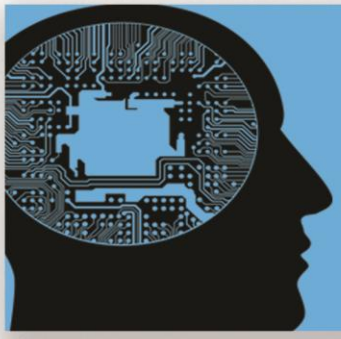
بحث و مباحثه:

عراق دارای یک شبکه گسترده خط لوله برای حمل و نقل محصولات نفتی برای مصرف محلی و صادرات از طریق بنادر و کشورهای همسایه است. برای کنترل و در دست گرفتن افزایش تولید نفت و صادرات، تعداد قابل توجهی از خطوط لوله جدید باید در داخل و خارج از عراق ساخته شوند. همچنین، بسیاری از خطوط لوله موجود نیازمند به تعمیر و توسعه می‌باشند. ضمنا، ضرورتی فوری برای کشور در راستای

غلبه بر چالش‌های دشوار و عوامل خطر که مانع عملکرد خط لوله و توسعه پروژه‌های جدید می‌شود، وجود دارد. شاخص ریسک که عوامل خطر را شناسایی می‌کند و احتمال و شدت هر ریسک را ارزیابی می‌کند، برای مدیریت ریسک اساسی است. درک و ارزیابی عوامل خطر OGP به ذی نفعان (سهامداران)، تصمیم گیرندگان، سیاستگذاران و محققان برای پیاده سازی یک استراتژی مدیریت ریسک پایدار در مراحل مختلف پروژه‌های خط لوله کمک خواهد کرد. چارچوب کلی مدل مدیریت ریسک (RMM) که در اینجا توسعه شده است، هدف از پشتیبانی از شناسایی، تجزیه و تحلیل و رتبه بندی عوامل خطر OGP به صورت جامع تر و سیستماتیک تر دارد. به همین ترتیب، این مقاله بر مبنای مرور ادبیات گسترده‌ای است که پایه و اساس آن ارائه یک نظریه جامع در مورد عوامل خطر OGP به ویژه در محیط‌های ناامن تشکیل می‌دهد. عوامل خطر OGPs بر اساس مشاهدات واقعی سهامداران مورد تجزیه و تحلیل قرار گرفته و رتبه بندی شده اند. RMM توسعه یافته در اینجا یک رویکرد جامع و سیستماتیک برای مدیریت ریسک را فراهم می‌کند. همچنین یک پایگاه داده جدید که اطلاعات ضروری برای فرایندهای مدیریت ریسک را عرضه می‌کند، مانند لیست احتمالی از عوامل خطر و احتمال و شدت این عوامل، را فراهم می‌کند. یافته‌های این مقاله و توصیه‌های موجود درآن مناسب و قابل استفاده برای OGPs در عراق و بسیاری از کشورهای دیگر در شرایط مشابه است.

ذی نفعان و سهامداران OGP می‌توانند از یافته‌های این مقاله، برای بهبود مدیریت ریسک در طول مراحل پروژه‌های خط لوله استفاده کنند.

نتایج به دست آمده از پرسشنامه قابل اعتماد بودند زیرا تمام مقادیر a بیش از ۰,۷ است. اطلاعات دموگرافیک در مورد ۱۹۴ پاسخ دهنده تنوع نمونه را بازتاب می‌دهد این سطح از تنوع به این معنی است که این پرسشنامه به جمعیت مورد نظر رسیده است به گونه‌ای که همه گروه‌های ذینفعان و سهامدارن را شامل می‌شود. نتایج نشان می دهد که تروریسم و اقدامات سرقت اولین و پنجمین فاکتور مهم هستند. فساد دومین فاکتور ریسک بالا است و پس از آن موقعیت جغرافیایی به عنوان مثال "Hot-Zones" و قانون هنگامی که قابل الزام به خرابکارها و دزدان نیست، که همه آنها مانع پروژه‌های خط لوله می‌شوند. نتایج همچنین نشان می‌دهد که ذی نفعان و سهامداران OGP عراق بیشتر در معرض عوامل خطر امنیتی و اجتماعی، موقعیت جغرافیایی خطوط لوله و عوامل HSE قرار دارند. برای ایجاد یک رویکرد مدیریت ریسک موثر در OGP در عراق، درک ذی نفعان و سهامداران برای کمک به شناسایی و تجزیه و تحلیل مشکلات OGP ضروری است، زیرا این ادراک مبتنی بر تجربه واقعی پروژه‌های خط لوله و مشکلات موجود در این زمینه هستند. به همین علت، یافته‌های مقالات و نتایج نظر سنجی، درک روشنی از عوامل خطر OGP را فراهم می‌کند.



زیرساخت‌های حیاتی و آسیب‌پذیری در آن‌ها

آسیب پذیری در زیرساخت‌های حیاتی در جنگ‌های گذشته:

کارکرد پیوسته و مطمئن زیرساخت‌های حیاتی نقش کلیدی در تأمین رفاه اجتماعی، بهره اقتصادی و امنیت ملی برای کشورها دارد. یکی از تهدیداتی که بسیاری از کشورهای جهان را موردتهدید قرار می دهد، تهدیدات تروریستی و بعضا حملات نظامی‌می باشد. امروزه و در تازه ترین این موارد را می توان به اقدامات گروهک های تروریستی داعش در عراق و سوریه و همچنین جنگ نظامی‌بین عربستان و یمن اشاره نمود. یکی از مهمترین پیامدهای حملات نظامی و یا حتی اقدامات تروریستی، تخریب و آسیب به زیرساخت های حیاتی بوده که بشر در طول تاریخ تاکنون، شاهد این اقدامات خصمانه بوده است.

زیرساخت های حیاتی به عنوان بنیان های اصلی و چارچوب های پایه ای هر جامعه به شمار می آیند و در برگیرنده تمامی‌تاسیسات، خدمات و تسهیلات مورد نیاز آن جامعه است. در زندگی مدرن، با افزایش وابستگی سریع به این امکانات، این نیاز روزافزون شده است. بطور کلی زیرساخت های حیاتی به نوعی مراکز ثقل یک کشور محسوب می شوند که در صورت انهدام هر یک، پیکره و کالبد کشور مورد تهاجم فلج می گردد و کشور قادر به ادامه فعالیت طبیعی مانند گذشته نخواهد بود. از طرف دیگر، براساس طرح جنگ بی قاعده از بین رفتن خدمت رسانی شریان ها منجر به کاهش رفاه اجتماعی و در انتها موجب سلب مشروعیت دولت مرکزی خواهد شد. اما به نظر می رسد تخریب زیرساخت های برخی کشورهای جهان اسلام که از سوی بعضی بازیگران منطقه ای و بین المللی صورت می گیرد، فراتر از نگاه‌های کوتاه مدت بوده و صرفاً در چارچوب پیروزی در جنگ قابل تحمل نیست. به عنوان مثال در سوریه و عراق، آمریکا که ائتلاف بین المللی علیه داعش را رهبری می‌کند، به بهانه تضعیف اقتصادی داعش، بسیاری از زیرساخت‌های حیاتی سوریه را مورد هداف قرار می‌دهد. در گذشته و در لیبی نیز این حملات با تفاوت‌هایی توسط ناتو صورت گرفت.

جنگ با یمن البته متفاوت است و این بار یک کشور عربی اسلامی یعنی عربستان سعودی تخریب گسترده زیر ساخت‌های حیاتی کشور یمن را برعهده گرفته و اهداف خاصی را در دستور کار دارد. هرچند کشور یمن نیز به منظور پایان دادن به جنگ و تحت فشار قرار دادن کشور سعودی، نیز به این موضوع مورد توجه ویژه قرار داده است. از جمله آن میتوان به حمله یمن به تاسیسات نفتی عربستان و از کارانداختن بخش زیادی از این زیرساخت حیاتی در کشور عربستان اشاره نمود. در دنیا حوادث و تهدیدات مشابه زیادی وجود داشته که در ادامه به آنها اشاره شده است.

سوابق وقوع تهدیدات مختلف در زیرساخت های حیاتی:

روز دوّم مهر سال ۵۹ تصمیم گرفته شد تا یکی از مهم‌ترین مراکز عراق موردحمله تیزپروازان نیروی هوایی قرار بگیرد. در این زمان سوخت برای هر دو کشور عامل حیاتی بود و با

توجّـه بـه شـرایط بحرانـی امـکان تهیـه سـوخت بـرای جنـگ افزارهـا به‌سـختی انجـام می‌شـد. لـذا فرمانـده عملیـات پایـگاه و دیگـران همـکاران دسـت بـکار شـدند و طرحـی را آمـاده نمودنـد تـا مخـازن نگهـداری سـوخت عـراق را مـورد آمـاج حمـلات خـود قـرار دهنـد کـه طـی ایـن طـرح انهـدام بزرگ‌تریـن مخـزن سـوخت عـراق در الهوریـه و تجمّـع مخـازن اربیـل در دسـتور کار قـرار گرفـت. مقـرر شـد ابتـدا مخـازن سـوخت شـهر اربیـل و سـپس مخـازن الهوریـه منهـدم شـود. در ایـن عملیـات خلبانـان غیـور میهنمـان توانسـتند بـه هـر دو ایـن اهـداف توسـط ۴ فرونـد فانتـوم خسـارات بسـیار جـدی وارد سـازند و مخـازن را منهدم نمایند.

پـس از حـدود ۲۰ روز از آغـاز جنـگ تحمیلـی طرّاحان نیـروی هوایی بـه دنبـال اهدافـی می‌گشـتند کـه کمتـر در ایـن مـدّت موردحملـه قرارگرفتـه باشـد، پایـگاه حبّانیـه و پالایشـگاه البکـر جـزء ایـن اهـداف بودنـد کـه در ایـن مـدّت بـه دلیـل بعـد مسـافت، کمتـر مـورد توجّـه قرارگرفتـه بودنـد. دو فرونـد جنگنـده فانتـوم جهـت عملیـات، دو فرونـد ره‌گیـر F۱۴ و یـک هواپیمـای سوخت‌رسـان انتخـاب شـدند. در ایـن عملیـات پالایشـگاه البکـر بـه سختی بمباران می‌شود.

پـس از حـدود ۴ سـال از آغـاز جنـگ تحمیلـی طـرح حملـه بـه پالایشـگاه کرکـوک و قطـع صـدور نفـت ریختـه شـده و بـه اجـرا درآمـد. ابتـدا هواپیمـای فانتـوم شناسـایی از منطقـه موردنظـر اطلاعـات جمـع‌آوری کـرده و پـس از تجزیه‌وتحلیـل اطلاعـات و نقشـه‌ریزی طـی یـک مأموریـت بسـیار سـخت و سـنگین بـه پالایشـگاه کرکـوک حملـه شـد. بـا انجـام ایـن عملیـات تـا مـدّت هـا صـدور نفـت از پالایشـگاه کرکـوک متوقّـع شـده بـود و عـراق یکی از منابع اصلی تأمین تجهیزات خود را ازدست‌داده بود.

پالایشـگاه اصفهـان بـه علّـت اهمیتـی کـه در تهیـه سـوخت موردنیـاز هواپیماهـا و خودروهـا در جنـگ داشـت و تأمین‌کننـده بخـش مهمـی‌از نیازهـای کشـور بـود، یکـی از اهدافـی محسـوب می‌شـد کـه دشـمن بـرای ضربـه زدن بـه آن از خـود چنـگ و دنـدان نشـان مـی‌داد و ضـرورت تقویـت سیسـتم دفاعـی مراکـز صنعتـی پالایشـگاه و نیـروگاه اصفهـان کـه نزدیـک هـم تأسـیس شـده بودنـد، همـواره از سـوی مسـئولین مـورد تأکیـد قـرار مـی گرفـت. تقریبـاً شـش مـاه قبـل از درگیـری موفقیت‌آمیـز ۱۳۶۷/۱/۱۴ اقدامـات مؤثـری در تکمیـل سیسـتم دفاعـی ایـن منطقـه انجام گرفت. در تاریـخ ۱۳۶۷/۱/۱۴ دو فروند هواپیمای عراقی بـه سـمت پالایشـگاه اصفهـان حملـه‌ور شـدند کـه در ایـن حملـه یـک هواپیمـا سـرنگون و دیگـری نیـز بـدون دسـت یافتـن بـه اهدافش فرار کرد.

در تیرماه ۱۳۸۵ حزب‌الله لبنان ایستگاه راه‌آهن، مخازن گاز و پالایشگاه و پتروشیمی حیفا را هدف موشک‌های خود قراردادند. وزیر جنگ رژیم صهیونیستی نیز میزان خسارت وارده براثر تهاجم موشکی حزب‌الله را بسیار سنگین خواند.

یک مقام امنیتی کویت در مردادماه ۱۳۸۸ اعلام کرد یک گروه شش نفرِ القاعده قصد داشت به پالایشگاه نفت شعیبِ و پایگاه ارتش آمریکا در این کشور حمله کند که کویت توانسته است این طرح حمله به پالایشگاه نفت را خنثی کند.
در خردادماه ۱۳۸۷ شاخه «جندالیمن» القاعده ۳ راکت را به‌سوی پالایشگاه نفت عدن شلیک کرد. در اسفندماه ۱۳۸۴مقام‌های عربستان اعلام کردند که یک عملیات تروریستی را در تأسیسات نفتی ابقیق در شرق این کشور خنثی کرده‌اند، در این عملیات دونیروی امنیتی و دو تن از اعضای القاعده کشته شدند. همین طور یک مظنون، بمبی را دریکی از تأسیسات نفتی در منطقه ابقیق واقع در شرق عربستان منفجر کرد. در آذرماه ۱۳۸۶ نیز براثر حمله‌ی موشکی به پالایشگاه نفتی «الدّوره» واقع در جنوب بغداد، آتش‌سوزی مهیبی در این پالایشگاه رخ داد.

اما در تازه‌ترین اخبار، حمله تروریستی در سال ۱۳۹۷ و در پی آن انفجار در خط لوله نفت کرکوک بوده که افراد مسلح مظنون به وابستگی به گروه تروریستی داعش یک خط لوله نفت در استان کرکوک عراق را منفجر کردند.
در سال ۱۳۹۸ نیز جریان انصارالله یمن در عملیاتی که بزرگترین عملیات از زمان آغاز جنگ رژیم آل سعود ضد این کشور به شمار می‌رود، موفق شد با ۷ هواپیمای بدون سرنشین دو تأسیسات نفتی وابسته به شرکت عربستان سعودی را هدف قرار دهد. حمله مذکور خط لوله‌ای به طول ۱۲۰۰ کیلومتر را هدف قرار داده که روزانه دست کم ۵ میلیون بشکه نفت را از چاه‌های منطقه الشرقیه عربستان به بندر ینبع در سواحل غربی این کشور منتقل می‌کند.

خبر دیگر مربوط به حمله پهبادی یمن به زیرساخت¬های حیاتی عربستان در شهریورماه ۹۸ (۱۴ سپتامبر ۲۰۱۹) بوده که در طی آن تاسیسات نفتی عربستان به شدت آسیب دیده است. انصارالله یمن اعلام کرده که با هفت پهباد حامل ۴ کلاهک، با طی مسافت ۱,۷ هزار کیلومتری از سه موقعیت مختلف به پرواز درآمده و به تاسیسات نفتی آرامکو آسیب جدی رسانده است. این حادثه در عربستان سعودی در حال حاضر جدی¬ترین وقفه در تامین نفت در تاریخ منجر شده است و حتی خسارت حمله به آرامکو، بیش از خسارت ناشی از انقلاب اسلامی‌در ایران در سالهای ۱۹۷۸-۱۹۷۹ و تحریم نفت پس از جنگ اعراب و اسرائیل در سالهای ۱۹۷۴-۱۹۷۳ است.

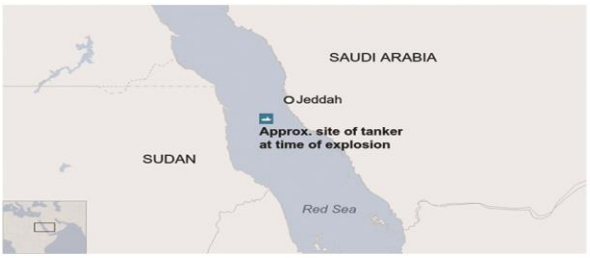
ایالت هاوایی در ۸ آبان ۱۳۹۸ در آمریکا تصمیم به آزمایش شبکه انرژی خود در برابر تهدیدات سایبری گرفت. در این آزمایش یک تمرین از راه دور که توسط یک شرکت الکتریکی انجام شده است، این سناریو را در شبکه الکتریکی هاوایی شبیه سازی و آزمایش میکند که نقاط قوت و ضعف دولت در پاسخ و بازیابی در چه مواردی قرار دارد. در همین رابطه رئیس بخش انرژی هاوایی گفت:

"ما مشتاقانه منتظر هستیم تا تجربه منحصر به فرد هاوایی را با شبکه های الکتریکی جدا شده آن به اشتراک بگذاریم و در مورد بهترین شیوه هایی که سایر کشورها هنگام برخورد با مسائل مربوط به امنیت شبکه استفاده می کنند، آگاهی یابیم. ".

در حین تمرین، کارشناسان هاوایی، کلرادو، آیداهو و مریلند به حملات شبیه سازی شده پاسخ خواهند داد تا چگونگی واکنش سازمان های ایالتی و مقامات دولتی در یک وضعیت واقعی را ارزیابی کنند. بازخورد از این شبیه سازی به ایالات متحده کمک می کند تا ارتباطات اضطراری را بهبود بخشیده و نیازهای تاب آوری زیرساخت ها را شناسایی کنند. به دنبال این رزمایش، ایالت‌ها در یک کارگاه دو روزه با کارشناسان شرکت خواهند کرد تا برنامه‌های عملیاتی را برای بهبود امنیت انرژی تهیه کنند. تحلیلگر انرژی دفتر انرژی ایالتی گفت "این تمرین فرصتی به ما می‌دهد تا روابط ارتباطات بحرانی را تقویت کرده و وابستگی متقابل بین بخش انرژی و سایر بخش‌های مهم زیرساخت‌های حیاتی مربوط به پاسخ و بازیابی از قطع برق طولانی مدت با عناصر فیزیکی و سایبری را شناسایی و ارزیابی کنیم".

سوم آبان ۹۸ هکرها بار دیگر شبکه های برق ژوهانسبورگ را خاموش کردند. ژوهانسبورگ در آفریقای جنوبی یک شهر آلفا در یک قاره پررونق است یک نیروگاه اقتصادی و یکی از مهمترین شهرهای جهان. این شهر همچنین یکی از قربانیان مکرر هکرهایی است که حداقل دو بار در سه ماه خدمات و شبکه های مهم شهری را تعطیل کرده اند. این بار پنجشنبه شب، شهر ژوهانسبورگ به دلیل نقض شبکه که منجر به دسترسی غیرمجاز به سیستم های اطلاعاتی شد، وب سایت، خدمات الکترونیکی و صورتحساب خود را تعطیل کرد. رسانه های محلی گزارش دادند که هکرها خواستار باج گیری از دولت بودند.

۱۹ مهر ۹۸ یک نفتکش متعلق به جمهوری اسلامی ایران در دریای سرخ در ساحل عربستان مورد حمله قرار گرفت. نفتکش متعلق به شرکت ملی نفتکش ایران، ساعت ۵:۲۰ دقیقه بامداد روز جمعه در ۶۰ مایلی (۹۵ کیلومتری) بندر جده عربستان سعودی دچار دو انفجار شد و دو مخزن اصلی آن آسیب دید. این نفتکش در حال حرکت در دریای سرخ بود.



عباس موسوی، سخنگوی وزارت امور خارجه ایران ظهر جمعه گفت: «بررسی‌های شرکت ملی نفتکش ایران نشان می‌دهد که کشتی ایرانی از مکانی نزدیک به کریدور عبوری این نفتکش از شرق دریای سرخ، دو بار و به فاصله حدود نیم ساعت مورد هدف قرار گرفته و آسیب دیده است».

گردآورندگان : – دکتر حمید هوشنگی – مهندس محمد جنیدی

معرفی کتب خارجی

مرکز مطالعات فنی و مهندسی در راستای اغناء منابع و مراجع رشته حفاظت از زیرساخت‌های حیاتی CIP اقدام به تالیف و ترجمه کتب علمی ارزشمند در این زمینه نموده است در ادامه مروری کوتاه بر سرفصل ها و محتوای چند عنوان از این کتب شده است:

۱- کتاب "فهم، ارزیابی، و پاسخ به تروریسم ، حفاظت از زیرساخت ها و پرسنل"

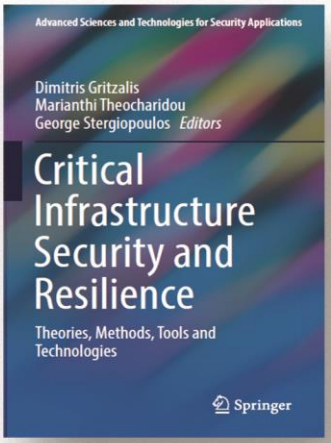
در این کتاب ۵۰۰ صفحه ای که در سال ۲۰۱۸ به چاپ رسیده است، به تروریسم و سلاح کشتار جمعی و انواع ریسک و ارزیابی ریسک پرداخته شده و از قوانین و مقررات امریکا در این حوزه مطالبی ارائه شده است.

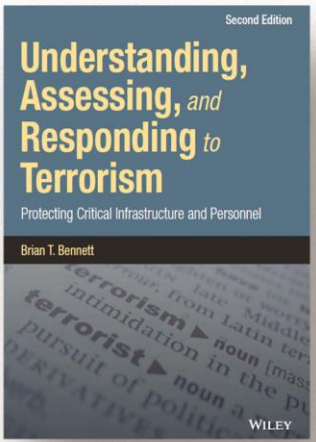
یکی از مهمترین موضوعات این کتاب، موضوع عملیات تروریستی و حملات علیه زیرساخت های حیاتی بوده که محور اصلی این کتاب را تشکیل می دهد. در بخش های مختلف به بررسی انواع حملات تروریستی و سناریوهای مختلف حملات تروریستی پرداخته که دید کافی و لازم از این حملات به زیرساخت ها را به منظور حفاظت بهتر، ارائه داده است. در این کتاب همچنین روش های گوناگون ارزیابی ریسک، ارزیابی تهدید و همچنین انواع سلاح های کشتار جمعی ذکر شده است.

۲- کتاب "امنیت و تاب آوری زیرساخت های حیاتی، فرضیات، اسلوب، اسباب و فنون"

در این کتاب که در سال ۲۰۱۹ به چاپ رسیده است، در قالب ۴ فصل و تحت موضوعاتی نظیر حکومت ها و مدیریت ریسک، وابستگی ها و تحلیل شبکه، سیستم های کنترل اتوماسیون و صنعتی و بالاخره امنیت سایبری به موضوع حفاظت از زیرساخت ها پرداخته است. از مهمترین خصوصیات این کتاب عبارتند از:

- راهبردهای حوزه مختلف انرژی، سایبر، شهری و غیره در این کتاب دیده شده است.
- از طرح موضوعات متفاوت و دیدگاه های منحصر به فرد نویسنده گان مختلف و در قالب سرفصل های متفاوت به موضوع پرداخته شده است.
- با رویکردی کاملا نوآورانه و متفاوت به موضوع پرداخته شده است.
- از ویژگی های منحصر به فرد و مزیت این کتاب جامعیت، بداعت و به روز بودن و پرداختن به حوزه های مختلف می باشد.





۳- کتاب "تاب آوری و ریسک؛ اسلوب و کاربرد در زمینه‌های محیط زیستی، سایبری، و اجتماعی"

در این کتاب که در سال ۲۰۱۷ به چاپ رسیده است، در قالب شش فصل به موضوعات جامعی در خصوص تاب‌آوری و زیرساخت‌های حیاتی فیزیکی و مجازی پرداخته و قابل استفاده برای کارشناسان و گروه‌های مختلف علمی را دارا می‌باشد.

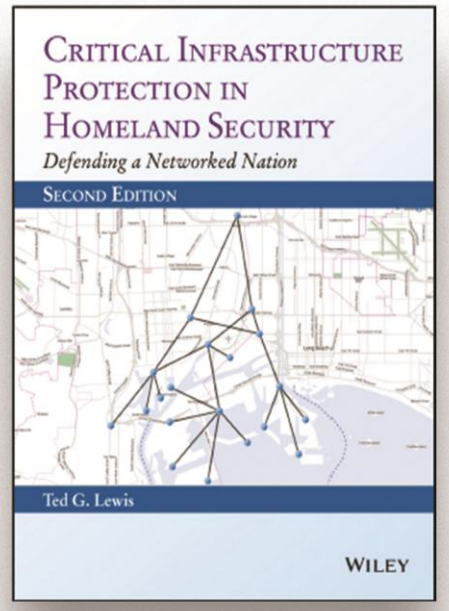
چون موضوعات در قالب مقالاتی که توسط کارشناسان مختلف تدوین و ارائه شده، لذا دیدگاه‌ها و نقطه نظرات متنوع و جامعی بصورت همه جانبه نگرانه مورد بررسی قرار گرفته است.

این کتاب از نسخه‌های جدید مربوط به زیرساخت‌های حیاتی به‌شمار می رود و مطالب آن نه تنها جهت تدوین دستورالعمل کارایی و قابلیت و کاربرد خوبی دارد بلکه مخاطبان شاغل در ستاد های اجرایی و سازمان های ذی‌ربط و نیز دانشگاه‌ها قابلیت کاربردی و استفاده را دارد.

٤-کتاب "حفاظت زیرساخت‌های حیاتی در امنیت ملی و سرزمینی"

این کتاب در پانزده فصل تهیه و تدوین شده که در آن به مبانی حفاظت از زیرساخت‌های حیاتی، معرفی کلیه زیر ساخت‌های حیاتی، معرفی انواع روش‌های ارزیابی ریسک کاربردی در زیرساخت‌های حیاتی، مفاهیم تاب آوری زیر ساخت‌ها و معرفی روش های ارتباطی در هر زیرساخت پرداخته شده است.

در این کتاب زیرساخت‌های حیاتی بر اساس دسته بندی کشور آمریکا به زیرساخت‌های ارتباطات از راه دور، سیستم‌های برق، ذخایر گاز و نفت و حمل و نقل، بانکداری و مسائل مالی، حمل و نقل، سیستم‌های تأمین آب، خدمات اضطراری (مانند درمان، پلیس، آتش و نجات) دسته بندی شده اند.



گردآورندگان : – دکتر حمید هوشنگی – مهندس محمد جنیدی

هفته پدافند غیر عامل در سال ۹۸

امسال هفته پدافند غیرعامل با شعار «مقاومت و بازدارندگی با رونق تولید» با شکوهی هر چه تمام تر و با استقبال بی‌نظیر مدیران دستگاه‌های اجرایی، اساتید و دانشجویان دانشگاه‌ها، پژوهشگران، مردم عزیز ایران اسلامی و ... برگزار گردید. در این هفته سازمان پدافند غیرعامل ۲۰ برنامه متنوع و پربار شامل برگزاری همایش‌ها در وزارتخانه‌های ارتباطات، راه و ترابری، بهداشت و درمان، جهاد کشاورزی و فرهنگ و ارشاد اسلامی و نیز انجام رزمایش های دانش‌آموزی، قطع برق، سیگنال رسانی، پدافند شیمیایی و پرتوی تهران را برگزار نمود. بخشی از برنامه ریزی انجام شده در هفته پدافند غیرعامل مربوط به زیرساخت های حیاتی و نحوه حفاظت از آن بوده که نشان دهنده اهمیت موضوع CIP در کشور و از نگاه پدافند غیرعامل می باشد.

در پایان این مراسم، ریاست محترم سازمان پدافند غیر عامل، سردار دکتر غلامرضا جلالی، پیامی به شرح زیر ارائه نمودند:

هفته پدافند غیرعامل سال ۹۸ نیز به پایان رسید. در این هفته برنامه‌ها، رزمایش‌ها و همایش‌های متعددی در سراسر کشور برگزار شد. هرچند کثرت برگزاری برنامه‌ها طی این هفته نسبت به سال قبل بسیار بیشتر بود اما مهم‌ترین ویژگی این هفته برای من دستیابی به یک زبان و فهم مشترک در حوزه پدافند غیرعامل در سراسر کشور به ویژه با بدنه دستگاه‌های اجرایی بود.

بنظر می‌رسد اکنون عموم جامعه اجرایی و علمی کشور نسبت به بنیان‌های پدافند غیرعامل و ضرورت های آن آشنایی پیدا کرده و با آن غریبه نیستند. به نظر من شاید این بزرگترین دستاورد پدافند غیرعامل در دهه دوم از فعالیت خود است. رشد جوانه‌های فهم مشترک و هم‌زبانی و نزدیک شدن دیدگاه‌ها افق روشنی را در پیش روی اجرایی سازی مفاهیم پدافند غیرعامل در عمیق‌ترین لایه‌های زیرساختی و اجرایی کشور نوید می‌دهد. به عنوان سرباز مقام معظم رهبری امام خامنه‌ای (مدظله العالی) در سازمان پدافند غیرعامل کشور از تمامی دست‌اندرکاران، مدیران، اساتید، پژوهشگران و به ویژه اصحاب رسانه که در برگزاری برنامه‌های هفته پدافند غیرعامل ما را یاری رساندند تقدیر و تشکر داشته و از خدای متعال برای آن‌ها طلب خیر می‌کنم.

دکتر غلامرضا جلالی

گردآورنده : دکتر حمید هوشنگی

همکاری با دانشگاه ها و پژوهشگاه ها

درخصوص نقشه‌ی جامع علمی نیز لازم است اساتید، مدیران و دانشجویان دانشگاه‌های کشور ازجزئیات این نقشه آگاه شوندونقشه‌ی جامع علمی به‌صورت یک «گفتمان پذیرفته‌شده»، درآید.

مقام معظم رهبری (مدظله العالی)

سازمان پدافند غیرعامل به منظور رشد و توسعه دانش مهندسی پدافند غیرعامل، همکاری گسترده ای را با دانشگاه‌های کشور آغاز نموده است. مرکز مطالعات و تدوین آیین نامه‌های فنی و مهندسی به عنوان بازوی علمی سازمان پدافند غیرعامل در سالهای اخیر، وظیفه این ارتباط و همکاری با مراکز علمی کشور را برعهده گرفته است. داتشگاه آزاد اسلامی واحد تهران شمال از جمله دانشگاه‌های پیشرو در زمینه همکاری با سازمان پدافند غیرعامل بوده که در سالهای اخیر نیز اقدام به برگزاری نشست های تخصصی با موضوعات مختلف و با همکاری مرکز مطالعات فنی و مهندسی نموده است.

یکی از راهبردهای دانشگاه آزاد اسلامی با ریاست جناب آقای دکتر طهرانچی به منظور کنشگری فعالانه‌تر در مواجهه با مسائل ملی پیچیده، توسعه رویکرد حل مسئله و تبدیل این دانشگاه به یک سازمان حل مسئله و پاسخگو به نیازهای واقعی جامعه است. در این راستا، برنامه پایش آزاد(پژوهش اثر بخش یکپارچه شبکه ای)، با هدف همسویی و هم افزایی پژوهش‌های تحصیلات تکمیلی دانشگاه اقدام شده است. در برنامه پایش آزاد، باز مهندسی ساختارها و کارکردهای نظام پژوهش تحصیلات تکمیلی دانشگاه و سازماندهی و برنامه‌ریزی هدفمند آن صورت می‌گیرد.

هم‌چنین، شناسایی استعدادهای حل مسئله در دانشگاه و توانمندسازی آن‌ها نسبت به تبدیل مسائل ملی کشور به مسائل دانشگاهی و قرار دادن آن‌ها به عنوان موضوعات پایان نامه‌های کارشناسی ارشد و دکتری اقدام می‌شود. رویکرد پژوهشی واحد تهران شمال همسو با سیاست‌های کلان دانشگاه به عنوان دانشگاه مسئله محور در حوزه پدافند غیر عامل و علوم و فنون همگراست.

• فهرست اجمالی اقدامات صورت گرفته ذیل برنامه علمی پدافند غیرعامل:

– برگزاری نشست‌های تخصصی، علمی و کاربردی با حضور مدیران سازمان پدافند غیر عامل کشور و سازمان‌ها و دستگاه‌هایی در حوزه پدافند غیر عامل با اعضای هیئت علمی و پژوهشگران واحد دانشگاه آزاد اسلامی تهران شمال

– پدافند غیر عامل در حوزه های دانشی مختلف طرح و تبدیل به زمینه‌های پژوهشی برای دانشجویان مقاطع تحصیلات تکمیلی گردید.

– راه اندازی مدرسه عالی مهارتی پدافند غیرعامل

– مشارکت در آموزش و فرهنگ سازی پدافند غیر عامل با تولید محصولات فرهنگی و تلاش در جهت اجتماعی سازی پژوهش

– برگزاری پنل های تخصصی موضوعی و مسئله محور مانند: مدیریت و ارزیابی ریسک، تاب آوری و حفاظت از زیر ساخت‌های اساسی

مرکز مطالعات و تدوین آیین نامه های فنی و مهندسی طی همکاری با دانشگاه آزاد اسلامی، در تیرماه سال ۹۸ اقدام به برگزاری نشست تخصصی با عنوان "تاب آوری و حفاظت از زیر ساخت های شهری" را با حضور اساتید و اعضای محترم هیئت علمی برگزار نموده است. در این نشست که کاملا تخصصی و مرتبط با کلیه زیرساخت های حیاتی بوده به بحث و بررسی زیرساخت هایی چون سیستم‌های توزیع برق شهری، شبکه ترابری کلان شهرها و شبکه توزیع گاز شهری پرداخته شده است. این همکاری در آینده نیز ادامه داشته و برنامه ریزی های بلند مدت به منظور ارتباط مجموعه سازمان پدافند غیرعامل(مرکز مطالعات فنی و مهندسی) با دانشگاه آزاد و حتی سایر مراکز دانشگاهی، صورت گرفته است.

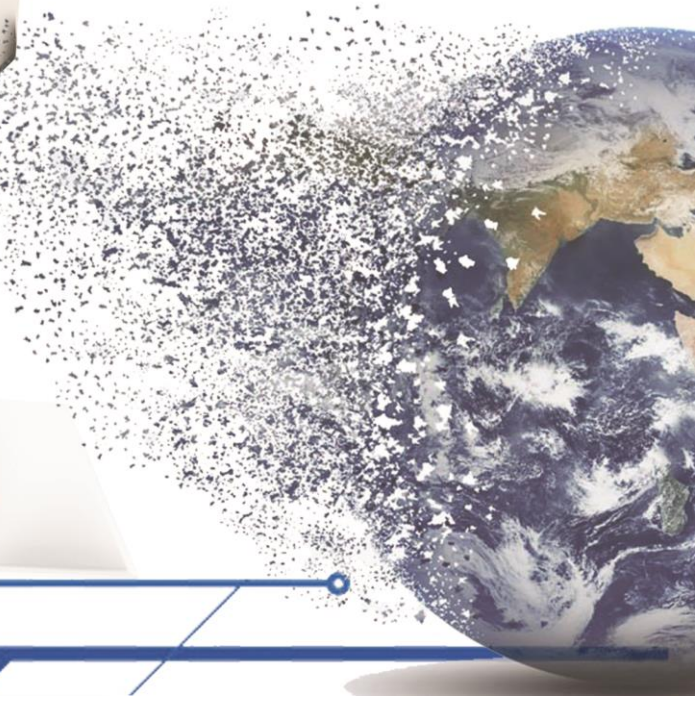
گردآورنده : دکترلاله فرهنگ متین

برنامه‌های مرکز مطالعات فنی و مهندسی در حفاظت از زیر ساخت‌های حیاتی

با توجه به اهمیت تهیه و تدوین آئین نامه‌ها، دستورالعمل‌ها، الزامات، ملاحظات، مقررات و استانداردهای فنی و مهندسی جهت حفاظت از زیر ساخت های کشور، مرکز مطالعات فنی و مهندسی بعنوان مرکز علمی-پژوهشی در راستای سیاست‌های سازمان پدافند غیرعامل، پروژه‌های مطالعاتی ارزشمندی را انجام و در دستور کار خود قرار داده است.

از دیگر اقدامات مهم مرکز مطالعات، تدوین و ترجمه کتب تخصصی است. از زمان شروع فعالیت مرکز مطالعات، کتب تخصصی زیادی ترجمه شده و با توجه به اهمیت حوزه CIP در چند سال اخیر، در این زمینه نیز کتب مختلفی در دست ترجمه و تالیف است.

تولید و توسعه علم و دانش فنی و مهندسی با تشکیل کارگروه های علمی و پژوهشی و تدوین کتب و مقالات از



جمله اقدامات مهم دیگر مرکز، برگزاری همایش‌ها و نشست‌های علمی و تخصصی بوده که در برنامه ریزی‌های انجام شده، با همکاری سازمان پدافند غیرعامل، در پی برگزاری همایش‌هایی با موضوع حفاظت از زیرساخت‌های حیاتی نیز می‌باشد.

سایر اقدامات مرکز مطالعات فنی و مهندسی عبارتند از:

۱- تشکیل کارگروه های علمی و پژوهشی
۲- تولید و توسعه دانش و ادبیات فنی (مدیریت دانش)
۳- اجرای برنامه های مطالعات علمی، پژوهشی و تحقیقاتی
۴- برگزاری دوره‌های (آموزشی) تخصصی
۵- نظارت بر بکارگیری و سازماندهی و ارتقاء علمی استادان، نخبگان، و دانشجویان حوزه فنی و مهندسی
۶- راه اندازی و سازماندهی اتاق های فکر و نشست های تخصصی
۷- ارائه خدمات علمی، پژوهشی و آموزشی از برنامه های فنی و مهندسی سازمان و دستگاه های اجرایی
۸- تکمیل بانک اطلاعاتی کتب، مقالات، پایان نامه ها و پروژه های تحقیقاتی و پژوهشی فنی و مهندسی
۹- حمایت از پژوهش های کاربردی، محصولات فناورانه، مصالح مقاوم و تجهیزات نوین بومی مورد استفاده در طرح های مطالعاتی و پدافندی
۱۰- ایجاد هماهنگی با بخش خصوصی در راستای تأمین نیازمندی های پژوهشی و فناوری های نوین حوزه فنی و مهندسی
۱۱- تعامل و هماهنگی با دستگاه‌های اجرائی کشور در جهت هماهنگ سازی طرحهای پژوهشی و فناورانه حوزه مهندسی
۱۲- تعامل و هماهنگی با مراکز علمی، دانشگاه ها، مراکز تحقیقاتی و پژوهشی و.... کشور جهت ایجاد وحدت رویه در انجام پژوهش ها و تحقیقات مهندسی و صنعتی

ارتباط با مرکز مطالعات فنی و مهندسی سازمان پدافند غیرعامل

مرکز مطالعات فنی و مهندسی به منظور **تهیه الزامات و ملاحظات پدافند غیرعامل درحفاظت از زیرساخت‌های حیاتی**، آماده همکاری با شرکت‌های‌های مهندسین مشاور و متخصصان توانمند در مراکز علمی-پژوهشی و دستگاه‌های اجرایی می‌باشد

لذا از تمامی مجریان و مشاوران دعوت بعمل می‌آید تا نسبت به ارسال مدارک مورد نظر به منظور شرکت در مناقصات مرتبط با پروژه‌های مذکور، اقدام نمایند

همچنین این مرکز **جهت تولید و توسعه دانش و ادبیات فنی و مهندسی(مدیریت دانش) و تکمیل بانک اطلاعاتی کتب، مقالات، پایان نامه ها و پروژه های تحقیقاتی و پژوهشی**، آماده همکاری با نخبگان سراسر کشور می‌باشد. در این راستا، این مرکز مطالعات مورد نیاز سازمان پدافند غیر عامل کشور را بررسی و در قالب پروژه‌های کسری و یا جایگزین خدمت تعریف و در اختیار نخبگان قرار می‌دهد

www.mafpa.ir

Email: info@mafpa.ir

Research Center of Engineering and Technical Science

تهران خیابان ولیعصر بالاتر از ایستگاه جامی کوچه اردشیر ناظم پلاک ۷ طبقه ۳ مرکز مطالعات فنی و مهندسی
۰۲۱-۶۶۹۷۸۲۲۶
۰۲۱-۶۶۹۷۱۳۰۴

یادداشت پایانی

در هر کشوری زیرساخت‌های حیاتی، اساس و بنیان آن کشور بوده و آسیب به آن‌ها می‌تواند پیامدهای جبران ناپذیری ایجاد نماید. بطوریکه آسیب به هر یک از زیرساخت ها، موجب مختل شدن کارکرد دیگر زیرساخت‌ها و در نهایت منجر به وقوع بحران در مدیریت یک کشور خواهد شد. از مطالبی که در این نشریه ارائه گردید، نتیجه می‌شود که برای مقابله با آسیب های مطرح شده در زیرساخت‌های حیاتی، بایستی با برنامه ریزی های علمی دقیق‌تری گام برداشت. این موضوع در عصری که تکنولوژی‌های نوین در خدمت تهدیدات و حملات متعدد دشمنان نظام مقدس جمهوری اسلامی ایران در آمده است، اهمیت دوچندان پیدا می‌کند.

در واقع منظور از برنامه ریزی علمی، توسعه یک برنامه کارا و پایا برای حفاظت از زیرساخت های حیاتی، جلوگیری از انجام حملات، کاهش میزان آسیب پذیری و در نهایت جلوگیری از قطع استمرار خدمات ضروری بخش های خصوصی و دولتی و ارائه دهندگان خدمات در این حوزه ها و ارتباط اطلاعاتی این بخش ها، امکانپذیر خواهد بود.

"به امید آنکه نشریه حاضر، بتواند گامی در جهت حفاظت از زیرساخت‌های حیاتی کشور برداشته و موجب افزایش سطح دانش خوانندگان خود گردد"

December,2019

Issue,1

Critical Infrastructure Protection

سازمان پدافند غیرعامل کشور

Research Center of Engineering and Techincal Sience Magazine