



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ





پدافند کالبدی و حفاظت از زیرساخت‌ها



پدافند کالبدی





پدافند کالبدی:

مجموعه تدابیر و اقدامات فنی و مهندسی پدافند غیرعامل که بکارگیری آنها در سطوح راهبردی، عملیاتی و اجرایی در زیرساخت ها موجب تولید بازدارندگی، کاهش آسیب پذیری، تسهیل مدیریت بحران، ارتقاء تاب آوری زیرساختی، آمادگی پاسخ پدافندی به تهدید، پایداری و مصونیت بخشی، مدیریت مخاطرات و تضمین تداوم کارکرد و استمرار خدمات اساسی در برابر تهدیدات و اقدامات نظامی دشمن می شود.



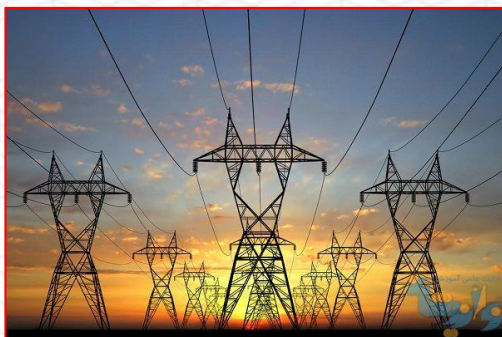


پدافند کالبدی مجموعه اقدامات مهندسی مستقیم و غیرمستقیم موثر بر **طرح های عمرانی کشور** است که منجر به **کاهش آسیب پذیری، ارتقای پایداری ملی و تداوم خدمات ضروری زیرساخت های** موجود و آتی الاحداث می گردد.





در پدافند کالبدی منظور از کالبد تمام زیرساخت ها، شریان های ارتباطی، خطوط انتقال انرژی و ارتباطی مراکز حیاتی، حساس و مهم کشور و به طور کلی پیکره کشور است.





دانشتني هاي
پدافند غير عامل

پدافند کالبدی یعنی مصون سازی، مستحکم سازی،
پایدار سازی و حفاظت از زیرساخت های کشور با اعمال
ملاحظات فنی و مهندسی در طرح ها و پروژه های کشور







حفاظت از زیرساخت‌ها





زیرساخت های هر کشور، بستر مهم حیات، رشد و پویایی آن به شمار می رود، برخی از **زیرساخت ها** نقشی حیاتی در حفظ منافع ملی دارند و بعنوان یکی از ارکان مهم پیشرفت، **اختلال** هرچند کوتاه مدت در عملکرد آنها می تواند منجر به **آسیب جدی** در اقتصاد و امنیت ملی شود؛ از آنجا که **زیرساخت ها**، جریانی به هم پیوسته از خدمات و پشتیبانی ها را برای تأمین نیازهای اساسی به جامعه ارائه می دهند و آسیب یا **اختلال** در عملکرد و کارکرد آنها می تواند قطع خدمات **زیرساختی** به مردم و جامعه را در پی داشته باشد.





زیرساخت ۱: به مجموعه‌ای از **مراکز و تأسیسات زیربنایی و شریان‌های عمده** که خدمات و نیازهای ضروری و اساسی کشور را به مردم و جامعه ارائه می‌کند، اطلاق می‌گردد؛ **زیرساخت** مشتمل بر **فرابخش ۲ (حوزه)**، **بخش ۳**، **زیربخش ۴**، **دارایی ۵** و اجزاء آن می‌باشد.



1- Infrastructure

2- Sector

3- system

4- subsystem

5- Asset & components





طبقه بندی زیرساخت ها

زیرساخت ها را می توان به روش های مختلفی همچون بر اساس **کارکرد** و **حوزه خدمات رسانی** طبقه بندی کرد. اگر طبقه بندی زیرساخت ها با توجه به کارکرد و ماهیت خروجی آنها انجام شود، به دو دسته زیر تقسیم می شوند:

۱. دسته اول، زیرساخت هایی هستند که **تولید محصول** می کنند (مانند تولید بنزین در یک پالایشگاه).



در یک طبقه بندی جزئی تر، این زیرساخت ها را هم به دو دسته زیرساخت های **قابل انباشت** و زیرساخت های **بدون قابلیت انباشت** تقسیم می کنند. در زیرساخت های دارای **قابلیت انباشت** امکان نگهداری و ذخیره سازی مواد اولیه یا محصول زیرساخت تا حدود زمانی مشخص وجود دارد (مانند نفت و گندم) در حالی که در زیرساخت های **بدون قابلیت انباشت** این امکان اصلاً وجود ندارد (مانند شبکه تولید و توزیع برق).



به طور طبیعی حساسیت زیرساخت های نوع دو در برابر **اختلال** و **حملات خرابکارانه** نسبت به زیرساخت های نوع اول بیشتر است.





طبقه بندی زیرساخت ها

۲. دسته دوم، زیرساخت هایی هستند که خروجی آنها نه یک محصول، بلکه یک خدمت است (مانند فرودگاه، بزرگراه).

در طبقه بندی زیرساخت ها بر اساس حوزه **خدمات رسانی** می توان آنها را بر اساس محدوده های سازمانی که **خدمات** آنها ارائه می شود (مثلاً در سطح دولت، قوه مقننه یا یک شرکت ملی) یا در مناطق جغرافیایی که در آن به **ارایه خدمت** می پردازند (مانند یک شهر یا منطقه) تقسیم بندی نمود.

هر چه سطوح این طبقه بندی ها بالاتر باشد و شهروندان بیشتری از خدمات آنها بهره مند شوند از اهمیت بیشتری برای حفاظت برخوردار هستند.





زندگی در جوامع مدرن و توسعه یافته امروزی متأثر از **زیرساخت های اساسی** آن جوامع است به نحوی که **کارکرد پیوسته و بدون اختلال** این **زیرساخت ها** بر کیفیت زندگی انسانها، رفاه عمومی و امنیت اثر بسیار زیادی می گذارد.

در صورت **عدم وجود کارکرد پیوسته و یا اختلال** در **زیرساخت های اساسی** نظیر شبکه برق، گاز، آب، فاضلاب، مخابرات، حمل و نقل، بانک و ... در یک جامعه و یا **کارکرد نامطمئن** آنها، آن جامعه به سوی توسعه و پیشرفت حرکت نمی کند و با خسارات فراوان مواجه می شود.





زیر ساخت ها دارای اهمیت بسیار زیادی است و می تواند بر اداره امور مردم در شرایط عادی و **تهدید** اثر گذار باشد .

سه عنصر جدی در طراحی زیر ساخت ها وجود دارد؛

❖ نقش و کارکرد زیر ساخت ها

❖ میزان اهمیت و حساسیت آن ها

❖ ماهیت زیر ساخت ها که گاهی از ماهیت فیزیکی تبدیل به ماهیت ترکیبی می شود.

زیر ساخت ها ممکن است نقش **سلولی** داشته باشند به این معنا که کارکردهای آن محدود به خود آن زیر ساخت باشند و یا ممکن است نقش **مادر** داشته باشند و شبکه ای از ارتباط و وابستگی بین زیرساختی را تعریف کنند.





از سویی، دشمن از هدف های عمیق و راهبردی **عملیات** را آغاز می کند و **مراکز ثقل** را مورد **هدف** قرار می دهد. منظور از **مراکز ثقل**، مراکزی است که **حمله** و **انهدام** آنها (برابر نظریه جان واردن) بر روند **تغییر** **درسیاست** های **راهبردی** طرف مقابل **مؤثر** است، به گونه ای که دستیابی به **اهداف جنگ** را **شتاب** می بخشد.





در سناریوی **فلج سازی راهبردی**، اعتقاد بر این است که هر کشور **مراکزی** دارد که نسبت به بقیه **مهم تر** است و برای توانمندسازی آن کشور در راستای **استمرار فعالیت** و یا **تداوم جنگ** اهمیت زیادی خواهد داشت.

دشمن اعتقاد دارد، چون **تخریب** این اهداف، که در حقیقت **منابع ارزشمند ملی** و **زیرساخت های حیاتی** هستند، می تواند طرف مقابل را **فلج** سازد؛ از این رو باید منابع **قدرت هوایی و موشکی** را تنها روی همان **اهداف** متمرکز کرد.





در ۲۰ سال گذشته اصلی ترین عنصر، **تهدید** زیرساخت های هستند که به واسطه آن مردم اداره می شوند در نتیجه **تهدیدات**، سعی می کنند با **حذف عملکرد زیر ساخت**، کنترل **اداره مردم** را در دست گیرند. لذا به هرمیزان که **زیر ساخت ها** در **اداره مردم** نقش بیشتری داشته باشند، از اهمیت بالاتری برخوردار هستند.





انهدام زیرساخت ها

عدم پاسخ گوی دولت به نیازها و ناتوانی در تامین نیازهای اساسی مردم

ایجاد نارضایتی در مردم

توسعه نارضایتی ها و تبدیل آن به شورش

تشویق و هدایت شورش و تخاصم و درگیری با حاکمیت

عملیات نظامی احتمالی کمکی و هدایت شورشیان (مردم تحریک شده)
به مراکز دولتی

اقدامات اولیه سقوط دولت





در مناطق شهری، **صدمات جنگی** شامل ترکیبی از **ویرانی های کالبدی** و **اختلال** در عملکرد عناصر و زیرساخت های شهری است. **انهدام** سازه ها و ساختمان ها، شبکه راه ها و دسترسی ها مثل پل ها و جاده های ارتباطی، تأسیسات اساسی مثل مخازن آب، نیروگاه ها، خطوط ارتباطی تلفن، برق، لوله کشی آب، گاز و ... از آن جمله هستند.





دشمن تلاش دارد در **حمله** به **زیرساخت ها** ضمن **تاثیر روانی و ایجاد استرس، سلب انگیزه های دفاعی مردم** به یکی از دو هدف کلی زیر نایل آید .

۱- حذف دارایی (**نابودی کامل زیرساخت**)

۲- حذف کارکرد (**توقف تولید یا استمرار خدمات و یا ایجاد اختلال**)

انتخاب هر کدام از اهداف فوق بطور مستقیم بر شیوه و نحوه و ابزار تهاجم تاثیر فراوان خواهد گذاشت، لذا دشمن در هر سناریوی خود و در ابتدای امر یکی از دو هدف فوق را برای خود انتخاب می نماید تا در برنامه تهاجمی خود رعایت هزینه، تلفات و زمان اندک را بنماید و از هدر رفت توان خود بکاهد.

از سوی دیگر تشخیص دقیق اهداف دشمن برای نیروهای مدافع نیز بسیار حائز اهمیت بوده و در انتخاب راهکارهای دفاعی موثر می باشد.





حوزه های با اهمیت بالا:

۱- انرژی،

۲- آب،

۳- غذا و کشاورزی،

۴- حمل و نقل،

۵- بهداشت و سلامت،

۶- دفاعی و امنیتی،

۷- صنعت،



۸- رسانه،

۹- هسته ای،

۱۰- فضا،

۱۱- جمعیت،

۱۲- حاکمیتی،

۱۳- خدمات ضروری و فوریتی،

۱۴- پولی و مالی،

۱۵- ارتباطات و فناوری اطلاعات،





حوزه های **با اهمیت** با توجه به شاخص های زیر، بعنوان **حوزه های کلیدی** از منظر **پدافند غیرعامل** دسته بندی می شوند:

حوزه های کلیدی از منظر پدافند غیرعامل



۱- انرژی،



۲- آب،



۳- ارتباطات و فناوری اطلاعات،

۴- حمل و نقل،



۵- بهداشت و سلامت،

۶- غذا و کشاورزی،



۷- دفاعی و امنیتی

۸- حاکمیتی

❖ اهمیت کارکرد هر حوزه در **تأمین نیازهای حیاتی** مردم در **شرایط اضطراری**

❖ **شدت اثرگذاری** بر اقتصاد، امنیت ملی و سلامت مردم

❖ **وابستگی زیرساخت های** سایر حوزه ها به عملکرد آنها

❖ **شدت پیامد** وقوع **تهدید** مبتنی بر جغرافیا و جمعیت





حفاظت از زیرساخت ۷:

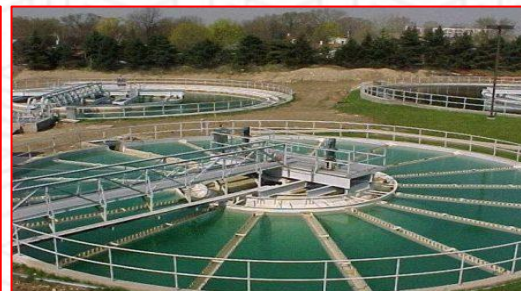
مجموعه تدابیر و اقدامات پدافند غیرعاملی که توانایی و آمادگی عملیاتی زیرساخت و تداوم کارکردهای آن و دستگاههای اجرایی مسئول برای پاسخ مؤثر به حوادث و سوانح ناشی از تهدیدات نظامی، تهدیدات امنیتی و تروریستی، تهدیدات سایبری زیرساختی و تهدیدات از درون دشمن پایه را افزایش می دهد بطوری که فعالیت آن حفظ گردیده و خسارات انسانی و مادی ناشی از آن را به حداقل می رساند.





مراکز ضروری:

مراکز و تاسیساتی که فقدان یا اختلال در عملکرد آنها زندگی مردم را با چالش مواجه می سازد.





شریان های اصلی و حیاتی:

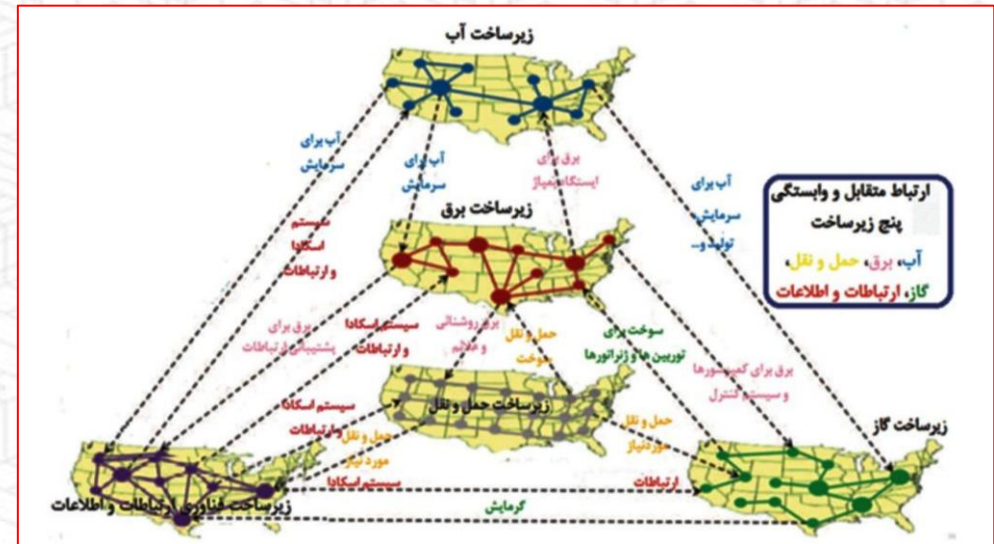
به شبکه های زیرساختی و ارتباطی که نقش اصلی و حیاتی در تامین نیازهای اساسی اداره کشور و امور مردم را دارند اطلاق می شود؛ مانند شبکه های ارتباطات، آب و گاز و سایر.





وابستگی متقابل:

عبارت است از ارتباط عملکردی اجزا و فرآیندها به یکدیگر که در صورت **اختلال** در یک سیستم احتمال ایجاد **اختلال** در مراکز و تاسیسات وابسته وجود دارد و به انواع فیزیکی، جغرافیایی، سایبری و منطقی تقسیم می شود.





وابستگی سیستمی در شریان ها و زیرساخت های حیاتی

حفظ عملکرد یک جامعه در پیش و پس از **بحران ها**، به عملکرد **شریان ها و زیرساخت های حیاتی** وابسته است و با توجه به برهم کنش و وابستگی شدید این **شریان ها** به یکدیگر، بررسی رفتار این **شریان ها** و **برهم کنش** آنها در زمان وقوع **بحران** ضروری است.

مسئله اصلی این است که وابستگی **شریان ها** تنها از نوع وابستگی فیزیکی دو **شریان حیاتی** به هم نبوده و آن ها از نظر اطلاعاتی و همین طور وابستگی های خارجی همچون اثرات زیست محیطی، سیاسی، اجتماعی و امنیتی نیز به یکدیگر وابسته اند. بررسی هر یک از این ها، نیاز به بررسی سیستم ها و تجهیزات زیرمجموعه های آن **زیرساخت** دارد.





از آنجا که **زیرساخت ها**، یک شبکه یکپارچه و به هم وابسته را تشکیل می دهند، وقوع اختلال در یک زیرساخت (یک زیرسیستم) می تواند در تمامی سیستم ها نیز منتشر شده و حتی به تدریج در سایر زیرساخت ها هم تشدید شود.

تهدیدها و حملات مختلف، چه به صورت داخلی و چه خارجی به **زیرساخت ها** می توانند آغازگر جریانی از اختلال های **مخرب** در **شبکه زیرساختی** بوده و فعالیت های مدیریت بحران و حتی برخی فعالیت های طبیعی را با مشکل مواجه سازند.

اختلال های آبشاری در **زیرساخت ها** بر اثر **حملات شدید** می توانند **زیرساخت ها** را با مشکلات جدی در امر **خدمات رسانی** روبرو کنند.

بر این اساس، اتخاذ روش هایی برای کاهش آسیب پذیری و محدود کردن دامنه انتشار عوارض ناشی از **حملات** در **زیرساخت ها** ضروری است.





خرابی آبشاری

یک **خرابی آبشاری** زمانی روی می دهد که **خرابی** در یکی از **زیرساخت ها** منجر به **خرابی** یکی از **اجزای زیرساخت** دیگر شود؛ امری که خرابی **زیرساخت** دوم را هم در پی خواهد داشت. به عنوان مثال، یک **خرابی** در شبکه **توزیع گاز طبیعی** (به عنوان یکی از زیرساخت ها) به علت اتفاق، حادثه طبیعی (مانند زلزله، طوفان، سیل و غیره) یا خرابکاری تعمیدی می تواند منجر به **خرابی** یک واحد تولیدی **نیروگاه برق** شود که در مسیر خدماتی این سیستم گازی قرار دارد. این واقعه به نوبه خود می تواند به کسری تولید برق در آن منطقه بیانجامد؛ امری که می تواند موجب **قطع برق** شود.

به این نوع **خرابی ها**، **خرابی آبشاری** از زیرساخت گاز طبیعی به **زیرساخت** برقی می گویند. ادامه این حادثه قطعی برق می تواند به نوبه خود، به خرابی و قطعی در سایر امور **زیرساختی** منجر شود.





زیرساخت های ویژه

زیرساخت های ویژه زیر ساخت هایی هستند که چند زیر ساخت دیگر را کنترل می کنند و زمانی که آسیب می بینند، زیر ساخت های وابسته به آن نیز دچار آسیب می شوند و همچنین با منافع بقا نظام و حاکمیت در ارتباط هستند.

همچنین برخی از زیر ساخت ها **فرا تر از حوزه های نفوذ جغرافیایی و محدودیت های مکانی** خاص سرویس دهی می کنند.





هوشمند سازی زیر ساخت ها

ما امروزه شاهد ورود فناوری سایبری در صنعت زیر ساخت هستیم و با پدیده ای تحت عنوان هوشمند سازی زیر ساخت ها روبرو هستیم. با رشد روز افزون هوشمند سازی تاسیسات و زیر ساخت ها، مفهوم زیرساخت فناوری اطلاعات و سایر پدید آمده است این پیشرفت تا جایی رخ می دهد که زیر ساخت فناوری اطلاعات در حال تبدیل شدن به زیر ساخت مادر یعنی زیرساخت تمام زیر ساخت ها است.





روابط سیستمی زیرساختی:

روابط حاکم بر زیرساخت ها مبتنی بر رویکرد سیستم از سیستم^۱ و تعامل بین اجزای سیستم زیرساختی که منجر به ایجاد روابط سیستمی از قبیل هم افزایی، تضاد، وابستگی و وابستگی متقابل می شود.



1-System of system





آسیب پذیری ۲:

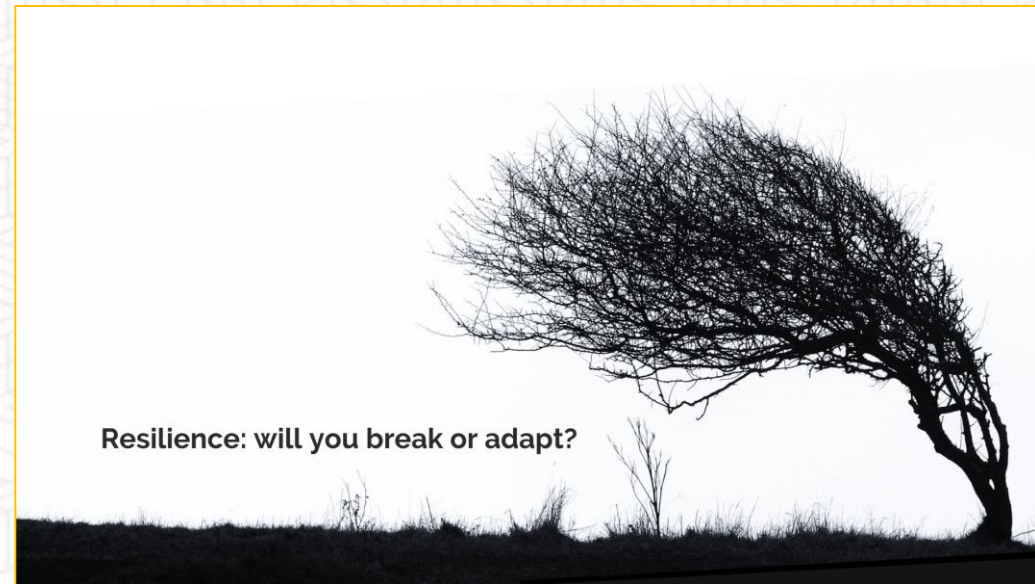
میزان خسارات و صدماتی است که از عوامل و پدیده های بالقوه (تهدیدات) یا بالفعل خسارت را به نیروی انسانی، تجهیزات و تأسیسات با شدت صفر تا صد درصد ناشی می گردد.





تاب آوری^۳:

به توانایی یک **نظام، جامعه، دستگاه اجرایی و یا زیرساخت** برای **ایستادگی، تحمل، انعطاف پذیری و حفظ کارکرد، تطبیق و برگشت پذیری در برابر مخاطره امنیتی – نظامی** گفته می شود.



3- Resiliency



اهداف و مأموریت‌های عمده





اهداف و مأموریت های عمده در **حفاظت از زیرساخت های کشور** عبارت است از:

- (۱) **سطح بندی روزآمد زیرساخت ها** و دارایی های حوزه های با اهمیت بالا،
- (۲) **رصد و پایش، تشخیص، هشدار و مدیریت تهدیدات زیرساختی،**
- (۳) **مصون سازی، امن سازی، تاب آور نمودن زیرساخت ها** متناسب با سطح اهمیت آنها،
- (۴) **تضمین و تسهیل تداوم کارکرد و استمرار خدمات ضروری زیرساخت های حیاتی** در کشور،
- (۵) **بهینه سازی سطح وابستگی و کاهش مستمر آسیب پذیری در زیرساخت ها** متناسب با سطح اهمیت آنها،
- (۶) **نهادینه سازی اصول و الزامات پدافند غیرعامل در ذات طرح های توسعه زیرساختی** کشور،





۷) کاهش و خنثی سازی درونی و ذاتی **مخاطرات زیرساخت های** دارای **پتانسیل خطر** در زمان طراحی و ساخت،

۸) **مصونیت زیرساخت های** سایبری و وابسته به سایبر و هوشمند،

۹) پاسخ به **حوادث و تهدیدات** و ایجاد **آمادگی** در برابر آنها در **زیرساخت های** حوزه های با اهمیت بالا،

۱۰) مدیریت و کاهش **تهدیدات درونزا** در **زیرساخت های** حوزه های با اهمیت بالا،

۱۱) توانمندسازی و آموزش مدیران و کارکنان دستگاه های متولی راهبری **زیرساخت های** حوزه های با اهمیت بالا،

۱۲) هماهنگی حداکثری و هم افزایی دستگاهی برای ارتقاء آمادگی های عملیاتی و تداوم کارکردهای ضروری،



راهبردها





۱- سطح بندی زیرساخت ها مبتنی بر مؤلفه های ماهیت، اهمیت، هوشمندی، کارکرد، سیستمی یا غیرسیستمی بودن و خطرزایی با نظام روزآمد سطح بندی زیرساخت ها و دارایی ها،

۲- توسعه و پیاده سازی سامانه رصد، پایش، ارزیابی، تشخیص و هشداردهی روزآمد تهدیدات و آسیب پذیری ها در زیرساخت ها و جریان های حیاتی و شبکه سازی آن در قالب سامانه یکپارچه ملی،





۳- نهادهای سازی اصول، الزامات و ملاحظات **حفاظت** از **زیرساخت** در **ذات طرح های توسعه زیرساخت** در برابر انواع **تهدیدات** (مهاجرت پدافند از پیوست به ذات طرح) از طریق:

- **مصون سازی** در لایه طرح های پایه با چارچوب های فنی و مهندسی با رعایت اندرکنش سیستمی **زیرساخت ها**

- **مصون سازی** با تاکید بر انتخاب فناوری موردنیاز طرح و پیش بینی الزامات پدافندی در **ذات فناوری و طرح**





۴- ارتقاء امنیت و پایداری زیرساخت ها و شریان های حیاتی کشور با تهیه طرح های جامع عملیاتی پدافندی در جهت مصون سازی، افزایش آمادگی، ارتقاء تاب آوری و امن سازی اضطراری - EOP1 - با رویکرد زیست بوم، متمرکز بر اقدامات اساسی زیر:

تهیه و پیاده سازی طرح پاسخ اضطراری به حوادث و تهدیدات زیرساختی - ERP2

تهیه و پیاده سازی طرح تضمین و تسهیل تداوم کارکردهای اساسی - BCP3

تهیه و پیاده سازی طرح بازیابی و برگشت پذیری زیرساختی و سیستمی - DRP4

تهیه و پیاده سازی طرح امن سازی و مصون سازی و تاب آوری - ISP5

تهیه و پیاده سازی طرح کاهش آسیب پذیری - VRP6

تهیه و پیاده سازی طرح بهینه سازی وابستگی و وابستگی های متقابل - OIP7

تهیه و پیاده سازی طرح های ارزیابی و ارتقاء آمادگی های زیرساختی - PPP8

1- Emergency operations Plan 2- Emergency Response Plan 3- Business Countinuty Plan 4- Disaster Recovery Plan 5- Immunius & Security Plan
6- Vulnerability Reduction Plan 7-Optimizing Interdependency Plan 8- Preparedness Promotly Plan





۵- حفظ و تداوم کارکردهای ضروری و تأمین نیازهای اساسی کشور از طریق طراحی، پیاده سازی و روزآمدسازی نظام عملیاتی حفظ و تداوم کارکرد زیرساخت ها،

۶- پایدارسازی و تاب آور نمودن زیرساخت های حیاتی با قابلیت برگشت پذیری سریع، انعطاف پذیر بودن در برابر تهدیدات، مقاوم بودن در برابر حوادث، حفظ تداوم عملکرد، ارتقاء ضریب افزونگی با تمرکز بر حفظ کارکرد اصلی در سطح پاسخگویی به نیاز،

۷- بهینه سازی وابستگی متقابل در زیرساخت های حیاتی کشور از طریق ذخیره سازی، امن سازی، جایگزینی خدمات، تطبیق پذیری با تمرکز بر برطرف نمودن یا موازی نمودن گره های زنجیره تولیدات و خدمات،





۸- استفاده حداکثری از ظرفیت های دستگاهی با تاکید بر تداوم کارکرد زنجیره فعالیت / خدمت از طریق نقش پذیری مناسب دستگاه های ذی نقش با هماهنگی و هم افزایی دستگاهی و مدیریت و فرماندهی یکپارچه،

۹- طراحی، پیاده سازی نظام، ساختار و الزامات تحقق برنامه کاهش مستمر تهدیدات درونزا با رصد و مراقبت نوبه ای،

۱۰- ارتقاء آمادگی حداکثری و توانمندسازی مدیران و کارشناسان دستگاه های متولی راهبری حوزه های با اهمیت بالا با تاکید بر تجهیز، تمرین، رزمایش، ارتقاء آمادگی و بازخورد و اصلاح طرح های عملیاتی پدافندی و رزمایش های تخصصی،





۱۱) مصون سازی سایبری همه جانبه، چندلایه و تطبیق پذیر زیرساخت های حائز اهمیت سایبری و وابسته به سایر کشور در مقابل تهدیدات سایبری دشمن از طریق:

- ۱- شناسایی و ارزیابی **دارایی های** سایبری و تعیین سطح اهمیت آنها،
- ۲- رصد، پایش، برآورد **تهدیدات** و اشتراک گذاری **اطلاعات**،
- ۳- رفع یا کاهش آسیب پذیری های سایبری **دارایی های** سایبری و وابسته به سایبر،
- ۴- برآورد، تحلیل و مدیریت **مخاطرات** سایبری **زیرساخت** و **پیامدهای آبخاری** آن،
- ۵- **نظام مند** کردن ساختار **امنیت** و **پدافند** سایبری و فرآیندها و نیروی انسانی،
- ۶- **روزآمدسازی** و **بومی سازی** هوشمندی در **زیرساخت های حیاتی کشور** وابسته به فضای سایبر،
- ۷- **حفاظت** سایبری از **زیرساخت های** وابسته به فضای سایبر با **تهیه** و **پیاده سازی طرح های عملیاتی** پدافند سایبری -
CERP1,CVRP2,CBCP3,CDRP4,CCIP5,CPPP6

1-Cyber Emergency Response Plan
Recovery Plan

2- Cyber Vulnerability Reduction Plan
5- Cyber Critical Infrastructure Protection Plan

3- Cyber Business Countinuty Plan
6- Cyber Preparedness Promotly Plan

4- Cyber Disaster





۱۱- کاهش و مدیریت مخاطرات زیرساخت های با قابلیت تولید خطر بالا (پرخطر) از طریق:

سطح بندی زیرساخت ها از منظر خطرپذیری،

آمادگی و پاسخ دائمی به حوادث و رخدادها و مخاطرات،

بهره گیری از رویکرد طراحی و مصون سازی تخصصی در ذات طرح مبتنی بر طراحی ذاتاً ایمن، ذاتاً آمن و طراحی براساس **تهدید**، پیش بینی و تأمین تجهیزات، ملزومات و فناوری های مقابله با **مخاطرات** مانند؛ شبکه پایشگر مخاطرات، شبکه اطفاء حریق و **رفع آلودگی** و سایر،

مدیریت و کاهش و خنثی سازی **مخاطرات** مفروض **زیرساخت** با طراحی و پیاده سازی عناصر، مولفه ها و اجزاء طرح،





بیانات رهبر معظم انقلاب
در اولین نشست اندیشه‌های راهبردی

... این آغاز یک راه است!
این کار باید ادامه پیدا کند.