فرهنگ واژگان موضوعی

پدافند غیر عامل

موضوعات:

فن آوری اطلاعات و تهدیدات سایبر ، تهدیدات: نرم ، سخت و نیمه سخت

(بیولوژیک و شیمیایی ، EMP) مدیریت ریسک و ...

به همراه فرهنگ انگلیسی به فارسی(بخش دوم)

تدوین و گردآوری:

حمید اسکندری

بسم الله الرحمن الرحیم

این موضوع را قبلا هم ابلاغ کرده ام و الان هم تأکید می کنم که تدابیر کارساز در باب پدافند غیر عامل را عملی کنید.

(مقام معظم رهبری)

فرهنگ واژگان موضوعی
پدافند غیرعامل

گرد آوری و تدوین :

حمید اسکندری

سرشناسه	: اسکندری ، حمید ، ۱۳۳۸
عنوان و نام پدیدآور	: فرهنگ واژگان موضوعی پدافند غیر عامل / گردآوری و تدوین حمید اسکندری.
مشحصات نشر	: تهران : بوستان حمید ، ۱۳۹۱ .
مشخصات ظاهری	: ۲۰۸ ص.: مصور.
شابک	: ۱-۱۹-٦٤١٢- ٦٠٠-۹۷۸
وضعیت فهرست نویسی	: فیپا
یادداشت	: کتابنامه.
موضوع	: دفاع از غیرنظامیان -- اصطلاح‌ها و تعبیرها
رده بندی کنگره	: ۱۳۹۱ ٤ف٥الف/U۹۲٦
رده بندی دیویی	: ۳۵۰۳/۳٦۳
شماره کتابشناسی ملی	: ۲۹۳۲٥٤٦

انتشارات

عنوان: فرهنگ واژگان موضوعی پدافند غیرعامل

تدوین و گردآوری : حمید اسکندری

ویراستار علمی: مهندس محمدصادق اسکندری

ناشر : بوستان حمید

چاپ : اول پاییز ۱۳۹۱

شمارگان : ۲۰۰۰

قیمت : ۹۰۰۰ تومان

تلفن ناشر : ۳۳۷۰۰۹۲۷ ۰۹۱۲۲۳۷۵۰۳۹ ۰۹۳۷۲۳۷۵۰۳۵

پیش گفتار

رشد فن آوری در حوزه های ماهواره، سنجش از راه دور ، فن آوری اطلاعـات ، سـامانه های عملیات روانی، عملیات رسانه ای و فن آوری سایبری باعث شده که تهدیدات و تفکرات سلطه جویانه عرصه های متفاوتی را در بر گیرد و از حوزه های صرفاً نظامی به سایر حوزه هـا مثل حوزه های سیاسی، فرهنگی، اقتصادی، نظامی و فن آورانه و ... گسترش یابد. ایـن توسـعه علمی باعث شده که تهدیدات در حوزه های متفاوتی شکل بگیرد و توانمندی رقبا و دشمنان را تحت تأثیر قرار دهد، از این رو تهدیدات حوزه های غیر نظامی هم توسعه می یابد.

امروزه شاهد مفاهیم جدیدی همچون جنگ نرم ،جنگ رسانه، جنگ اقتصادی و... هسـتیم و در واقع وارد حوزه هایی شده ایم که در آن رسانه و عملیات روانی دارای کارکرد بسیار گسترده ای است و این موضوع تا حدودی از گسترش حوزه های مربوط به کارکردهـای نظـامی کاسـته ، بـه عبارتی حوزه هایی همچون حوزه های اقتصادی، سیاسی، علمی، دانش و فنـاوری، حـوزه هـای جدید جنگی محسوب می شوند. به عنوان مثال امـروز در موضـوع هسـته ای کـه در واقـع دارای عملکرد اقتصادی است، شاهد درگیری های سـختی بـین غـرب و ایـران هسـتیم و مـا در چنـین جبهه ای با تلاش های کارشناسی برای کسب،ارتقاء و تحلیل این دانش، در حال دفاع می باشیم.

در این شرایط توجه به اهداف، اصول و ملاحظات پدافند غیرعامل امری ضروری بـوده و در این راستا دسترسی آسان بـه مفـاهیم و واژگـان موضـوعی آن از نیازمنـدی هـای مـدیران و کارشناسان می باشد.

کتاب حاضر برای آگاه‌سازی مدیران و کارشناسان دستگاه‌های اجرایی کشوری ، لشکری و

همچنین دانشجویان عزیز به عنوان تنها فرهنگ واژگان **موضوعی** پدافند غیرعامل گردآوری و تدوین گردیده و از طرفی فرهنگ انگلیسی به فارسی در انتهای کتاب در دسترس کارشناسان ، مترجمین ، دانشجویان و سایر علاقه مندان در این حوزه ، قرار داده شده است.

امیدواریم این فرهنگ نامه به عنوان بسته دانشی ، با ایجاد زمینه تحقق مدیریت دانش در این حوزه ، به توسعه و ترویج فرهنگ پدافند غیرعامل کمک نماید.

در حال حاضر با توجه به استقبال مخاطبین از نسخه اولیه فرهنگ اصطلاحات پدافند غیرعامل و همچنین نیاز سازمان ها ، دستگاه های اجرایی و دانشجویان عزیز ، نسخه جدیدتر و کامل تر آن را بصورت تخصصی و موضوعی تدوین و چاپ نموده و به واژه های موضوعات مهم مثل فن آوری اطلاعات و تهدیدات سایبر ، تهدیدات نرم ، سخت و نیمه سخت بیشتر توجه شده است. این مجموعه شامل برداشت مطالب از کتب تدوین شده و نظرات مؤلفین محترم در این حوزه بوده که در انتهای کتاب در کتابنامه لیست شده و در متن ارجاع داده شده است.

البته این اثر بدون نقص و اشکال نبوده ، انشاالله در فرصت های آینده در ویرایش های بعدی، این فرهنگ از جامعیت بیشتری برخوردار شود ، لذا از انعکاس راهنمایی و ارشاد های اساتید و سروران گرامی بهره مند خواهیم شد.

حمید اسکندری

فهرست مطالب

با دانش باید بتوان تولید ثروت و با ثروت، تولید قدرت، در حوزه‌های مختلف نظامی و غیرنظامی نمود و این موضوع به میزان زیادی تابع زیرساخت‌ها، ظرفیت‌ها و توانمندی‌های علمی،فناوری و اقتصادی کشور است.

مقام معظم رهبری

«چند سال پیش، اول بار در دانشگاه امیرکبیر، مسأله جنبش نرم افزاری را مطرح کردم و آن یعنی اینکه در زمینه علم، تولید علم و شکستن مرزهای علم، یک جنبش و یک حرکت عظیم به وجود بیاید...

مقام معظم رهبری

بخش اول

فرهنگ واژگان موضوعی

فصل اول

واژگان عمومی(اصول و مبانی)

«من برنامه های استکبار جهانی علیه ملت ایران را در سه جمله خلاصه می کنم: اول جنگ روانی، دوم جنگ اقتصادی و سوم، مقابله با پیشرفت و اقتدار علمی» (۱۳۸۶/۱/۱، مشهد)

مقام معظم رهبری

)

بخشی از دستگاه های سوخت هسته ای

آسیب پذیری Vulnerability

میزان خسارت و صدمات ناشی از عوامل و پدیده های بالقوه و یا بالفعل خسارت زا نسبت به نیروی انسانی، تجهیزات و تأسیسات با شدت صفر تا صد درصد.(منبع ۳)

آشکار سازی Detection

یک راهبرد از اقدامات متقابل که منظور از آن شناسایی تلاش های یک متخاصم برای ارتکاب یک رویداد امنیتی یا دیگر فعالیت ها می باشد بطوری که بررسی به موقع و همچنین آنالیز فعالیت ها ، شناسایی متخاصم را موجب می شود.(منبع ۲۲)

آمادگی Preparedness

مجموعه اقداماتی است که توانایی جامعه را در انجام مراحل مختلف مدیریت بحران افزایش می دهد. آمادگی شامل جمع آوری اطلاعات ، پژوهش، برنامه ریزی، ایجاد ساختارهای مدیریتی، آموزشی، تأمین منابع، تمرین و مانور است (منبع ۳)

آنالیز اقدامات متقابل Counter measures analysis

مقایسه کارایی مورد انتظار از اقدامات موجود برای یک تهدید معلوم در برابر سطح کارایی کارشناسی شده که برای تعیین نیاز اقدامات امنیتی نیاز می شود.(منبع ۲۲)

آنالیز هزینه- سود Cost-Benefit analysis

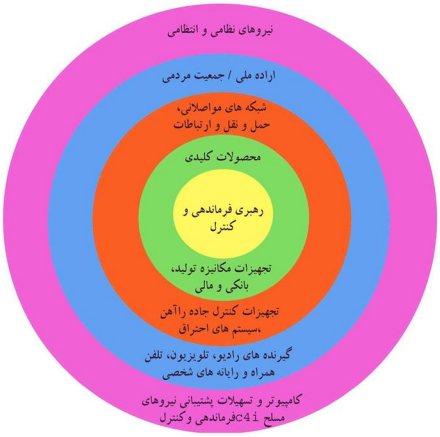
قسمتی از فرآیند تصمیم گیری که در آن هزینه ها و منافع هر انتخاب اقدام متقابل، مقایسه می شود و مناسب ترین انتخاب برگزیده می شود. هزینه ها شامل هزینه موارد محسوس و همچنین هزینه های عملیاتی مستمر مرتبط با اجرای اقدامات متقابل می باشد.(منبع ۲۲)

اتمام بسیج عمومی Demobilization

بازگشت منظم ، ایمن و کار آمد منابع به موقعیت و محل اصلی و اولیه .

استراتژی پنج حلقه واردن Strategic of Warden

مراکز ثقل یک کشور شامل پنج حلقه مشروحه ذیل بوده و دوایر متحدالمرکزی می‌باشند که مجموعاً ساختارهای اصلی قدرت یک کشور را تشکیل می‌دهند، در تئوری مذکور مراکز ثقل یک کشور همانند اعضای یک بدن قلمداد گردیده و در صورت انهدام هر یک از حلقه‌های یاد شده پیکره و کالبد کشور مورد تهاجم فلج گردیده و قادر به ادامه فعالیت و حیات نخواهد بود: (۱) حلقه اول ، رهبری ملی (۲) حلقه دوم ، محصولات کلیدی (۳) حلقه سوم ، زیرساخت‌های حمل و نقل (٤)حلقه چهارم ، جمعیت مردمی و اراده ملی (۵) حلقه پنجم ، نیروهای عملیاتی



اصول پدافند غیرعامل Passive defence principle

اصول پدافند غیرعامل مجموعه اقدامات بنیادی و زیربنایی است که در صورت به‌کارگیری می‌توان به اهداف پدافند غیرعامل از قبیل کاهش خسارات و آسیب پذیری، کاهش قابلیت و توانایی سامانه‌های شناسایی اهداف و تحمیل هزینه بیشتر به وی، حفاظت از زیر ساخت ها و در نهایت پایداری ملی نائل گردید. اصول عمده پدافند غیرعامل عبارتند از:

۱- انتخاب عرصه‌های ایمن در جغرافیای کشور ۲- تعیین مقیاس بهینه استقرار جمعیت و فعالیت در فضا ۳- پراکندگی در توزیع عملکردها متناسب با تهدیدات و جغرافیا ٤- انتخاب مقیاس بهینه از پراکندگی و توجیه اقتصادی پروژه ۵- کوچک سازی و ارزان سازی و ابتکار در پدافند غیرعامل

٦- موازی سازی سیستم‌های پشتیبانی وابسته ۷- مقاوم سازی، استحکامات و ایمن‌سازی سازه‌های حیاتی ۸- مکان‌یابی استقرار عملکردها ۹- مدیریت بحران دفاعی در صحنه‌ها ۱۰- استتار و نامرئی سازی ۱۱- کور کردن سیستم اطلاعاتی دشمن ۱۲- اختفاء ۱۳- پوشش در همه زمینه‌ها ١٤- فریب، ابتکار عمل و تنوع در کلیه اقدامات ۱۵- حفاظت اطلاعات سیستم‌های حیاتی و مهم ١٦ - تولید سازه‌های دو منظوره.

اطلاعات Information

افزودن تحلیل و تفسیر به داده ها و مشخص نمودن ارتباطات آنها به یکدیگر باعث بوجود آمدن اطلاعات می گردد. به عبارتی اطلاعات شامل داده های خلاصه شده ای است که گروه بندی، ذخیره، پالایش، سازماندهی و تحلیل شده اند تا بیانگر موقعیت خاصی باشند. تجزیه و تحلیل اطلاعات منجر به اتخاذ تصمیم می گردد.(منبع ٢٤)

اعلام خبر Early warning

آگاهی و هشدار به نیروهای خودی مبنی بر اینکه عملیات تعرضی دشمن نزدیک می باشد ، این هشدار که برای آماده شدن بوده و ممکن است چند دقیقه ، چند ساعت، چند روز و یا زمانی طولانی تر از آغاز درگیری اعلام گردد. تجهیزات و وسائل اعلام خبر شامل رادار ، دیده بانی بصری ، آژیر ، پیامها و آگهی های هشدار دهنده می باشد.

اقدامات متقابل Counter measures

عمل یا قابلیت فیزیکی که هدف اصلی آن، کاهش یا حذف یک یا چند آسیب پذیری است. اقدام متقابل، تهدید ها (قصد و یا قابلیت) و نیز ارزش اموال را تحت تاثیر قرار می دهد. (منبع ۲۲)

امنیت ملی National Security

حفظ قدرت (نظامی، سیاسی، اقتصادی، فرهنگی) و اعمال حکومت در امور داخلی و خارجی علیه نفوذ بیگانگان و جلوگیری از عملیات غیرقانونی دشمن که به منظور تضعیف و یا سرنگونی حکومت و دولت باشد. (منبع ۱)

اهداف کلان پدافند غیرعامل Passive defence great goals

۱) ایمن سازی مراکز حیاتی و حساس کشور. ۲) نهادینه کردن رعایت اصول و ضوابط پدافند غیر عامل در طرح های توسعه منتهی به ایجاد مراکز طبقه بندی. ۳) دستیابی به علوم و فن آوری با

تأکید بر تولید دانش و گسترش مراکز علمی ، پژوهشی و آموزشی. ٤) توسعه کمی و کیفی نیروی انسانی متخصص. ٥) فرهنگ سازی و ایجاد باور عمومی در مورد تأثیر پدافند غیرعامل در کاهش آسیب پذیری. ٦) افزایش آستانه مقاومت ملی و تقویت مؤلفه های مقاومت در مقابل تهدیدات. ۷) بالا بردن قابلیت بقا و حفظ کشور در شرایط بحران. ۸) کاهش مجموعه آسیب پذیری های کشور و نمایان کردن اقتدار ملی ناشی از آن به عنوان یکی از مؤلفه های اصلی بازدارندگی.

۹) ایمن سازی مراکز اصلی نیروهای مسلح و کاهش آسیب پذیری در مقابل حوادث غیر مترقبه و بلایای طبیعی.

آیین‌نامه اجرایی بند (۱۱) ماده (۱۲۱) قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی

مواردی از **آیین‌نامه** شماره : ۱۹٤٥٤ت۳۳۲٦۰/هـ تاریخ : ۱۳۸٤/۰٤/۲۲ سازمان مدیریت راهبردی:

ماده ۷ـ وظایف و اختیارات کمیته‌های دستگاه های اجرایی عبارتند از:

۱) بررسی و پیشنهاد سطح بندی و اولویت بندی مراکز دستگاه مربوط

۲) پیگیری تهیه و اجرای طرح پدافند غیرعامل مراکز موجود براساس مصوبات کمیته دائمی و نظام فنی واجرایی کشور به نحوی که در طول برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی‌ایران ـ مصوب ۱۳۸۳ـ حداقل مراکز حیاتی و حساس کشور ایمن سازی شوند.

۳) نظارت بر اعمال ضوابط و مقررات پدافند غیرعامل در طرح های دستگاه مربوط

٤) انجام پژوهش ها و آموزش های تخصصی و عمومی در زمینه پدافند غیرعامل مرتبط با موضوعات تخصصی دستگاه مربوط

ماده ۸ ـ در مورد طرح های مصوب و در دست اجرا یا در دست مطالعه که اعتبار آنها از محل بودجه‌عمومی کشور تأمین می‌گردد، دستگاه اجرایی موظف است اعتبار مربوط به رعایت اجرای ضوابط و مقررات پدافند غیرعامل را ضمن اعتبار سالانه آن دستگاه پیش‌بینی نماید.

بارکد Bar Code

یک نوار چاپ شده بر روی کاغذ سفید که می تواند به راحتی توسط اسکنرهای نوری خوانده شود.این نوع از رمز گذاری برای کنترل ورود و خروج موارد حساس نمی تواند کاربرد داشته باشد

چون به راحتی می توان از نوع رمزگذاری کپی برداری کرد.برای ایمنی بیشتر مـی تـوان روی آن را بـا یک ماده شفاف پوشاند.برای خواندن رمز از یک اسکنر مادون قرمز(IR) استفاده می شود.(منبع ٤٤)

بازدارندگی Deterrence

یک راهبرد از اقدامات متقابل که منظور از آن جلوگیری و سست کردن وقوع تهاجم دشمن اسـت. اقدامات مهندسی و زیربنایی پدافند غیرعامل از این دسته اقدامات هستند. بازدارندگی می توانـد شـامل برنامه‌ها و اقداماتی شود که باعث دلسردکردن یا تضعیف روحیه فرد یا گروه حمله کننده بصورت بالقوه می شود، هزینه های یک حمله موفق را افزایش می دهد و احتمال عدم موفقیت در حمله، دسـتگیری و مجازات را گوشزد می‌نماید. (منبع ١٤)

برنامه پنجم توسعه کشور(مرتبط با پدافند غیرعامل) Development five program

موارد مرتبط پدافند غیرعامل از فصل هفتم **برنامه پنج ساله پنجم** توسعه کشور:

ماده ۱۹۸- به منظور کاهش آسیب پذیری زیرساخت ها، ارتقاء پایداری ملی، حفاظت از مردم و منابع ملی کشور و تضمین تداوم خدمات به آن در راستای تکمیل چرخه دفاع غیر نظامی، اقـدام های زیر انجام می شود:

الف – تدوین استانداردهای فنی مورد نیاز پدافندغیرعامل طی سال اول برنامه

ب – ایجاد سامانه پایش، هشدار و خنثی سازی در خصوص تهدیدات نـوین در مراکـز حسـاس، حیاتی و مهم.

ج – ایمن سازی و حفاظت از مراکز حیاتی، حساس و مهم کشور و تداوم فعالیـت امـن و پایـدار آنان .

ماده ۱۹۹ – پروژه های موضوع پدافند غیرعامل با پیشنهاد دبیر کمیتـه دائمـی و تصـویب رئـیس کمیته دائمی به اجرا در خواهد آمد.موافقتنامه این گونه پروژه ها بین رئیس کمیته دائمی پدافند غیرعامل و معاونت مبادله خواهد شد.

ماده ۲۰۱- دولت موظف است به منظور تقویـت بنیـه دفـاعی کشـور و ارتقـاء تـوان بازدارنـدگی نیرو های مسلح و حفاظت از تمامیت ارضی و امنیت کشور و آمادگی در برابر تهدیـدات و حفاظـت از منافع ملی ، انقلاب اسلامی ایران و منابع حیاتی کشور و هوشمندسازی سیستم های دفاعی اقـدام هـای زیر را در صورت تصویب فرماندهی کل نیرو های مسلح به عمل آورد:

الف: تقویت مؤلفه های بنیه دفاعی با تأکید بر مدرن سازی و هوشمندسازی تجهیزات، ارتقاء منابع انسانی و سامانه های فرماندهی و کنترل

ب: .....

ک : **رعایت اصول پدافند غیرعامل در طراحی و اجرای طرح های حساس و مهم و یا در دست مطالعه و نیز تأسیسات زیر بنایی و ساختمان های حساس ، شریان های اصلی و حیاتی کشور و آموزش عمومی مردم توسط دستگاه های اجرایی موضوع ماده (۱۷۹) این قانون ، به منظور پیشگیری وکاهش مخاطرات ناشی از سوانح غیر طبیعی.**

ماده۲۱۵ پیشنهاد طرح های تملک دارائی

قانون و ماده ۳۲ برنامه نظام عمرانی کشور که در برنامه ۵ ساله پنجم تبدیل به ماده ۲۱۵ شده است:

ماده۲۱۵ـ پیشنهاد طرح های تملک دارائی های سرمایه‌ای جدید در لوایح بودجه سنواتی با رعایت موارد زیر امکان‌پذیر است:

الف ـ عناوین، اهداف کمی و اعتبارات طرح های تملک دارائیهای سرمایه‌ای جدید با رعایت مواد (۲۲) و (۲۳) قانون برنامه و بودجه براساس گزارش توجیهی فنی (حجم کار، زمانبندی اجرا) اقتصادی، مالی و زیست‌محیطی و **رعایت پدافند غیرعامل** از سوی مشاور و دستگاه اجرائی پس از تأیید معاونت برای یک بار و به قیمت ثابت سالی که طرح های مورد نظر برای اولین بار در لایحه بودجه سالانه منظور می‌گردد به تفکیک سال های برنامه و سال های بعد به تصویب مجلس شورای اسلامی می‌رسد.

پدافند غیرعامل Passive Defense

عبارت است از مجموعه اقدامات غیر مسلحانه که موجب افزایش بازدارندگی، کاهش آسیب پذیری، تداوم فعالیت های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می گردد. (مصوب مجمع تشخیص مصلحت نظام)

پدافند غیرعامل در روسیه passive Defence in Russian

در شوروی سابق سازمان دفاع غیرعامل در اواسط سال ۱۹۶۰ میلادی تأسیس گردیده و به سرعت توسعه یافت و از سال ۱۹٦٦ با تحولی بزرگ، تجدید سازمان گردید و سپهبد آلتونین از سوی لئونید برژنف به عنوان رئیس سازمان دفاع غیرعامل منصوب گردید . ساخت پناهگاه‌های ضد هسته‌ای و

دو منظوره کردن بسیاری از تأسیسات مانند ایستگاه‌ها و معابر مترو و پارکینگ‌های زیرزمینی از همان زمان در دستورکار قرار گرفت و با ساخت استحکامات ایمن و زره‌های مقاوم در مقابل انواع بمب و موشک توسعه یافت.لیکن انتشار اندک اطلاعات موثق در این خصوص ، تحلیل وضعیت شوروی سابق در حوزه پدافند غیر عامل را دشوار ساخته است.

پدافند غیرعامل در کره

در کشور کره شمالی هم که با تهدید آمریکا روبرو است پدافند غیرعامل به صورت گسترده‌ای مورد استفاده قرار می‌گیرد. معابر مترو و ایستگاه‌های زیرزمینی شهر پیونگ‌یانگ در عمق بین ۹۰ تا ۱۰۵ متری زمین احداث شده‌اند، بسیاری از کارخانجات صنایع نظامی در تونل‌های بزرگ استقرار یافته‌اند و هواپیماهای نظامی پس از فرود می‌توانند در تونل‌های حفر شده مخفی شوند.

پدافند غیرعامل و ائمه

حضرت امیرالمؤمنین علی(ع) در نامه ۱۲ نهج‌البلاغه می‌فرمایند:

«آن‌گاه که در میدان جنگ در مقابل دشمن قرار گرفتید می‌باید قرارگاه شما در دامنه کوه‌ها و تپه‌ها و یا در کنار رودها باشد تا پوشش و حفاظ شما گردد و شما را از دشمن نگهبانی کند.»

پدافند غیرعامل و قران

آیه ۸۰ از سوره مبارکه انبیاء می‌فرماید:

«وَ عَلَّمناهُ صَنعَهَ لَبوُسٍ لَکُمْ لِتُحصِنکُمْ مِنْ بَأسکُم فَهَلْ اَنتُم شاکِرونَ»

و ما به او (حضرت داود علیه‌السلام) ساخت زره را تعلیم نمودیم تا شما را از آسیب جنگ در امان بدارد، پس آیا از شکرگزارانید؟

پول شویی Money laundering

پول شویی به فرایندی اطلاق می گردد که از طریق آن، عایدات مالی بدست آمده از راه های خلاف و مجرمانه به سرمایه ها و دارایی هایی تبدیل می شود که ظاهراً از منابع قانونی بدست آمده اند. این فرایند معمولاً در سه مرحله انجام می پذیرد: تبدیل، لایه بندی، تکمیل. (منبع ۱۳)

به عبارت ساده‌تر قانونی کردن درآمدهای غیر قانونی، مشروع کردن پول‌های نامشروع و تطهیر پول‌های حرام و یا تبدیل پول‌های کثیف ناشی از اعمال خلاف به پول‌های تمیز و پاک، پولشویی می‌باشد.

پیامد Consequence

نتیجه حملات تروریستی یا دیگر مخاطرات که سطح، استمرار و طبیعت تلفات حاصل از حادثه را منعکس می کند. برای اهداف حفاظت زیرساخت ها ، پیامدها به چهار دسته اصلی تقسیم می شوند: اثرات دولتی، روانی، اقتصادی، ایمنی و سلامت عمومی. (منبع ۲۲)

تهدید Threat

تهدید، یک خطر بالقوه است که هنوز محقق نشده و صرفاً در حد یک ایده می باشد به عبارت دیگر تهدید، مفهومی به کلی انتزاعی است به طوری که تعیین زمان و چگونگی مورد تهدید واقع شدن بسادگی امکان پذیر نمی باشد. برآیند وضعیتی است که عوامل مختلف بر خلاف خواسته ما و خارج از کنترل عمل می‌کنند و از این حیث روند امور، مطلوب ما نیست و احتمال آشفتگی، خطر یا خسارات جبران ناپذیر را برای ما به وجود آورده و باعث ایجاد اختلال در امنیت عمومی و ملی می گردد(منبع ١٤)

تهدید هوایی Air Threat

هر نوع عملیات هوایی دشمن که وضعیت پدافندی کشور مورد تهاجم را به مخاطره اندازد.

جنگ اقتصادی Economic warfare

اقدام برنامه ریزی شده یک یا چند دولت از طریق محدود کردن مناسبات اقتصادی برای اعمال فشار بر کشور هدف با مقاصد مختلف سیاسی است.

تحریم اقتصادی Trade Embargo

در واقع یک ابزار سیاست خارجی است و اغلب به عنوان جایگزین جنگ و اعمال قوه قهریه تلقی می شود. مقصود از مناسبات اقتصادی نیز همه انواع روابط اقتصادی اعم از تجاری و مالی است. کشورهای مختلف از تحریم های محدود اقتصادی برای مقاصد سیاسی خود علیه کشورهای هدف استفاده می کنند. بطور معمول تحریم اقتصادی را در دو زمینه اعمال می کنند: اول، تحریم تجاری که در آن صادرات و واردات به کشور هدف، محدود یا قطع می شود. دوم، اعمال محدودیت ها، پایمال شدن یا قطع مناسبات مالی. از سوی دیگر بسته به منشأ تحریم آن را به سه نوع تقسیم می کنند:

۱) تحریم های یک جانبه ۲)تحریم از سوی چند کشور ۳) تحریم توسط شورای امنیت سازمان ملل متحد

تحریم‌های اقتصادی از جهت هدف، دو نوع هستند: اول، تحریم اقتصادی به منظور بی‌ثبات کردن رژیم سیاسی کشور هدف است که در واقع برگرفته از تضاد در منافع استراتژیک کشور تحریم کننده و کشور هدف می‌باشد. این نوع تحریم برای تغییر رژیم کشور هدف است.

دوم، تحریم اقتصادی برای تغییر رفتار سیاسی یا اقتصادی کشور هدف صورت می‌گیرد. این نوع تحریم به مراتب ملایم‌تر از نوع اول است.(منبع ٤٩)

حافظت از زیرساخت‌های حیاتی Protection of Critical Infrastructures

مطالعه، طراحی و اجرای اقدامات احتیاطی که هدف از آنها کاهش ریسک ایجاد نقص در زیرساخت‌های حیاتی در نتیجه جنگ، فجایع، بلایا و حوادث، ناآرامی های اجتماعی، خرابکاری ها و حوادث تروریستی می باشد. حافظت از زیرساخت‌های حیاتی می تواند به عنوان برنامه هایی تعریف شود که آسیب پذیری را ارزیابی می کنند .خطر را به حداقل رساننده و اقدامات حافظتی را برای کاهش آسیب پذیری های آن ها بکار می گیرند. (منبع ١٤)

حافظت از زیرساخت‌های فن آوری اطلاعات Protection of ICT Infrastructures

ما در جهانی زندگی می‌کنیم که بطور روز افزون وابستگی آن به اطلاعات و فناوری که امکان ارتباط و انجام تجارت با سرعت نور را فراهم می‌آورد، بیشتر می‌شود. از آنجا که صنایع زیرساخت حساس دولت به شدت به خدمات حیاتی زیرساخت عمومی ارتباطات وابسته می‌باشند حفاظت از آن از اهمیت ویژه‌ای برخوردار می‌باشد. ماهیت ساختاری حساس بخش ارتباطات آن را در تمام جبهه‌ها آسیب‌پذیر می‌نماید. آسیب به یک نقطه خاص ممکن است باعث انعکاس عمده در کل این بخش گردد. در طی حملات ۱۱ سپتامبر سال ۲۰۰۱، آسیب های مشخصی به تجهیزات، خطوط، و تأسیسات ارتباطی وارد گردید و قطع سرویس ارتباطات و نیز آسیب به زیرساخت های برق ، حمل و نقل و ...، باعث تأخیر در بازگشایی بازارهای مالی شد.

حفاظت از دارایی Asset Protection

برنامه های امنیتی که برای حفاظت از کارکنان، امکانات و تجهیزات در تمام قسمت ها مورد

استفاده قرار می گیرد.این برنامه ها برای جلوگیری از حملات تروریست ها و غیره کاربرد دارد.(منبع ٤٤)

خِرد Wisdom

کاربرد دانش یا به عبارتی دیگر بکارگیری دانش به منظور رسیدن به اهداف سازمانی را خرد گویند.

دارایی Asset

یک منبع مورد نیاز و مفید که می بایست از آن حفاظت کرد، که می تواند شامل قراردادها،امکانات و غیره می‌باشد. این دارایی ها می توانند قابل لمس باشند(مانند:ساختمان ها ،امکانات ،تجهیزات) یا غیر قابل لمس باشند(مانند اطلاعات یا اعتبار یک شرکت).(منبع ٤٤)

دانش knowledge

عبارت است از: قدرتی برای عمل و تصمیم گیری – افزودن درک و حافظه به اطلاعات و خلاصه سازی هر چه بیشتر اطلاعات اولیه (بقایی نیا،١٣٨٦)

در واقع دانش به منزله بینش حاصل از اطلاعات و داده ها می باشد. دانش کمک می کند تا اطلاعات مفید جمع آوری و اطلاعات ناخواسته حذف گردند.(منبع ٢٥)

دانش صریح یا آشکار Explicit Knowledge

دانش صریح یا آشکار دانشی است که به آسانی قابل انتقال می باشد و می توان آن را به کمک یک سری از نشانه ها (حروف، اعداد و...) در قالب نوشته، صدا، تصویر، عکس، نرم افزار، پایگاه داده مدون و کدگذاری کرد. به همین دلیل به اشتراک گذاری دانش صریح به راحتی امکان پذیر است.(منبع ٢٦)

دانش ضمنی یا پنهان Implicit Knowledge

دانش ضمنی یا پنهان دانشی است ذهنی و شخصی که به آسانی قابل بیان، انتقال، اشتراک و فرموله کردن نیست. بینش، بصیرت، شعور و درک هر شخص، ترفندها و فوت و فن های به کاررفته توسط هر فرد در حوزه دانش ضمنی او قرار دارد.(منبع ٢٦)

دفاع defence

دفاع به مجموعه اقداماتی گفته می شود که با به‌کارگیری کلیه وسایل ، امکانات و روش‌های تاکتیکی جهت جلوگیری از ورود دشمن به منطقه پدافندی و انهدام او صورت می‌گیرد. به عبارت دیگر

تدابیری که برای مقاومت در مقابل حملات سیاسی، نظامی، اقتصادی، اجتماعی، روانی و یا فناوری توسط یک یا چند کشور مؤتلف اتخاذ می‌شود. توانایی‌های دفاعی، بازدارندگی را تقویت می‌کنند و بازدارندگی نیز به این توانایی‌ها نیرو می‌بخشد (منبع ۳)

دفاع شهروندی (غیرنظامی) Civile defence

دفاع شهروندی برای جلوگیری از ریسک‌های مختلف، آگاه سازی و هشدار به جمعیت‌ها ، محافظت از افراد، دارایی ها و محیط در مقابل حوادث و وقایع ناگوار طبیعی و غیرطبیعی می باشد که با طرح ریزی اقدامات و بکارگیری منابع مناسب توسط دولت، جوامع مستقل یا نهادهای دولتی و خصوصی انجام می شود. (منبع ١٤)

دفاع عامل Active Defense

عبارت است از به‌کارگیری مستقیم جنگ‌افزار، به منظور خنثی نمودن و یا کاهش اثرات عملیات خصمانه هوایی، زمینی، دریایی، نفوذی و خرابکارانه بر روی اهداف مورد نظر.

بعبارت دیگر مجموعه ابزار ، فن‌آوری وتاکتیک هایی که بتوان به‌وسیله آن انواع تهاجم نظامی دشمن را دفع نمود، دفاع عامل می باشد. دفاع عامل شامل بکارگیری تجهیزات ضدهوایی، ابزار اختلال در دید و ابزارهای هشداردهنده برعلیه دشمن نیز می‌باشد.

دفاع غیرعامل Passive Defense

به مجموعه اقداماتی اطلاق می‌گردد که مستلزم به‌کارگیری جنگ‌افزار نبوده و با اجرای آن می‌توان از وارد شدن خسارات مالی به تجهیزات ، تأسیسات حیاتی ، حساس نظامی و غیرنظامی و تلفات انسانی جلوگیری نموده و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد.

رسالت پدافند غیرعامل pasive defence prophecy

رسالت پدافند غیر عامل کشور عبارت است از:

"حفظ و پایدارسازی و کاهش آسیب‌پذیری زیرساخت‌های کشور، حفاظت از مردم، استمرار خدمات ضروری دستگاه‌ها در برابر تهدیدات خارجی."

رهبری ملی National Leadership

هداف و عناصر مربوط به رهبری ملی عبارتند از : رهبری سیاسی، مراکز اصلی تصمیم‌گیری‌های

کلان سیاسی و نظامی (وزارتخانه‌ها، تأسیسات و مراکز عمده ستادی و دولتی، قرارگاه های عمـده فرماندهی، مخابرات راه دور، مراکز و قرارگاه های عمده پلیس)، سازمان مرکزی صدا و سیما.

زیرساخت Infrastructure

فرهنگ واژه‌های میراث آمریکا زیرساخت را چنین معنی می کند: تأسیسات، خدمات و سامانه‌ها و دارایی هایی که برای کارکرد یک جامعه ضروری هستند. می توان گفت منظور از زیرساخت، دارایی ها و تأسیساتی که دارای: هزینه ثابت بالا – حیات اقتصادی طولانی – ارتباط قوی با توسعه اقتصادی– یـا سلامت و بهداشت عمومی – و همچنین دارایی های فیزیکی که قادر به ارائه خـدمات یـا دیگـر منـافع برای سال‌های طولانی باشند، است. (منبع ١٤)

زیرساخت حیاتی Critical Infrastructure

این واژه برای توصیف حداقل دارایی ها و تأسیساتی بکار می رود که وجود و کـارکرد صـحیح آن برای ادامه کارکرد اجتماع و اقتصـاد ضـروری اسـت. واژه زیرسـاخت حیـاتی بـه معنـی سـامانه‌هـا و دارایی‌های فیزیکی (سخت افزاری) و مجازی (نرم افزاری) است که بـه قـدری بـرای کشـور ضـروری هستند که ناتوانی یا عدم کارکرد و یا اختلال در آنها دارای تـأثیر تضـعیف کننـده و آسـیب‌رسـان روی امنیت عمومی ملی، امنیت اقتصاد ملی، سلامت یا ایمنی عمومی ملی یا هـر ترکیبـی از مـوارد یادشـده، می باشد (منبع ١٤)

سطح اجرائی و تاکتیکی پدافند غیرعامل Passive defense tactical level

این سطح از اقدامات شامل اقدامات اجرایی مدیریت بحران ، آمادگی مقابله و اجرای برنامه های مقابله با حوادث و بلایا می باشد.

مسئولیت اجرایی در این سطح از اقدامات پدافند غیرعامل به عهده مسئولین اجرائی دسـتگاه هـای اجرائی می باشد و این اقدامات شامل:

- ✓ اجرای با کیفیت برنامه ها
- ✓ ایجاد آمادگی مقابله در دستگاه ها
- ✓ اجرای اموزش و تمرین منظم
- ✓ اجرای مانور های منظم سالیانه و فصلی

- ✓ برطرف کردن آسیب پذیری های اجرائی دستگاه ها

سطح عالی و راهبردی پدافند غیرعامل. Passive defense sterategic level

مفاهیم و اقدامات پدافند غیرعامل در این سطح، شامل اقدامات راهبردی در عالی ترین سطح کشور بوده این اقدامات شامل پیش بینی در موارد زیر می باشد. :

- ✓ در سطح تدابیر رهبری معظم انقلاب اسلامی
- ✓ در قانون اساسی کشور
- ✓ در قوانین موضوعی کشور
- ✓ در سطح چشم انداز ۲۰ ساله کشور
- ✓ در قوانین برنامه بلند مدت کشور
- ✓ درسطح سیاست های کلی نظام

سطح عملیاتی اقدامات پدافند غیرعامل Passive defense sterategic level

این سطح اقدامات می توانند کیفیت و چگونگی اجرای پدافند غیرعامل را تضمین نمایند لذا از اهمیت بالایی برخوردار می باشد این موارد شامل :

- ➢ آئین نامه اجرائی قوانین مصوب مجلس
- ➢ آئین نامه نظام مهندسی اجرائی کشور
- ➢ آئین نامه های فنی

- استانداردهای فنی در حوزه های مختلف فنی
- دستورالعمل های مدیریتی و اجرائی و.....

سیاست‌های کلی نظام در پدافند غیرعامل General policies of passive defense

این سیاست‌ها در ۱۳ بند که قبلا در مجمع تشخیص مصلحت نظام تصویب گردیده و اخیرا مقام معظم رهبری ابلاغ فرموده اند، به شرح زیر می باشد:

(۱) تأکید بر پدافند غیرعامل که عبارت است از مجموعه اقدامات غیرمسلحانه که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می‌گردد.

(۲) رعایت اصول و ضوابط پدافند غیرعامل از قبیل انتخاب عرصه ایمن، پراکنده‌سازی یا تجمیع حسب مورد، حساسیت‌زدایی، اختفاء، استتار، فریب دشمن و ایمن‌سازی نسبت به مراکز جمعیتی و حائز اهمیت به ویژه در طرح های آمایش سرزمینی و طرح‌های توسعه آینده کشور.

(۳) طبقه‌بندی مراکز، اماکن و تأسیسات حائز اهمیت به حیاتی، حساس و مهم و روزآمد کردن آن ها در صورت لزوم.

(٤) تهیه و اجرای طرح های پدافند غیرعامل (با رعایت اصل هزینه – فایده) در مورد مراکز، اماکن و تأسیسات حائز اهمیت نظامی و غیر نظامی موجود و در دست اجرا بر اساس اولویت‌بندی و امکانات حداکثر تا پایان برنامه ششم و تأمین اعتبار مورد نیاز.

(٥) تهیه طرح جامع پدافند غیرعامل در برابر سلاح های غیرمتعارف نظیر هسته‌ای میکروبی و شیمیایی.

(٦) دو یا چند منظوره کردن مستحدثات، تأسیسات و شبکه‌های ارتباطی و مواصلاتی در جهت بهره‌گیری پدافندی از طرح های عمرانی به ویژه در مناطق مرزی و حساس کشور.

(۷) فرهنگ‌سازی و آموزش عمومی در زمینه به کارگیری اصول و ضوابط پدافند غیرعامل در بخش دولتی و غیردولتی، پیش‌بینی مواد درسی در سطوح مختلف آموزشی و توسعه تحقیقات در زمینه پدافند غیرعامل.

(۸) رعایت طبقه‌بندی اطلاعات طرح های پدافند غیرعامل.

(۹) ممانعت از ایجاد تأسیسات پرخطر در مراکز جمعیتی و بیرون بردن این گونه تأسیسات از شهرها و پیش‌بینی تمهیدات ایمنی برای آن دسته از تأسیساتی که وجود آنها الزامی است و ممانعت از ایجاد مراکز جمعیتی در کنار تأسیسات پر خطر با تعیین حریم آنها.

(۱۰) حمایت لازم از توسعه فناوری و صنایع مرتبط مورد نیاز کشور در پدافند غیرعامل با تأکید بر طراحی و تولید داخلی.

(۱۱) به کارگیری اصول و ضوابط پدافند غیر عامل در مقابله با تهدیدات نرم‌افزاری و الکترونیکی و سایر تهدیدات جدید دشمن به منظور حفظ و صیانت شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای.

(۱۲) پیش‌بینی ساز و کار لازم برای تهیه طرح‌های مشترک ایمن‌سازی و ایجاد هماهنگی در سایر طرح ها و برنامه‌ها و مدیریت نهادهای مسئول در دو حوزه پدافند غیرعامل و حوادث غیر مترقبه در جهت هم‌افزایی و کاهش هزینه‌ها.

(۱۳) ایجاد مرکزی برای تدوین طراحی، برنامه‌ریزی و تصویب اصول و ضوابط، استانداردها، معیارها، مقررات و آیین‌نامه‌های فنی پدافند غیرعامل و پیگیری و نظارت بر اعمال آن ها.

لایه های امنیتی حفاظت protective Security layers

مفهومی از تأمین چندین لایه مستقل و همپوشان از حفاظت کامل را بیان می کند. برای اهداف

امنیتی، شامل لایه های گوناگون حفاظتی نظیر ضد مراقبت، ضد جاسوسی، امنیت فیزیکی و امنیت سایبری می باشد.(منبع ۲۲)

مدیر ارشد دانش Chief Knowledge Officer

مدیر ارشد دانش می کوشد تا بر میزان دارایی های دانش سازمان بیافزاید و به طراحی و پیاده سازی استراتژی های مدیریت دانش بپردازد.فعالیت های یک مدیر ارشد دانش عبارتند از:

تنظیم اولویت های استراتژیک برای مدیریت دانش – ایجاد یک مخزن دانش از بهترین تجارب – متعهد کردن مدیران ارشد سازمان برای حمایت از محیط یادگیرنده و سازمان – ایجاد یک فرآیند مناسب برای مدیریت سرمایه های فکری . (منبع ۲٦)

مدیریت دانش Knowledge Management

مدیریت دانش یعنی استفاده خلاق، مؤثر و کارآمد از کلیه دانش ها و اطلاعات در دسترس سازمان به نفع مشتری و در نتیجه به سود سازمان. (منبع ۲۵)

مدیریت دانش استفاده از تجربه و دانش فردی و جمعی از طریق فرآیند تولید دانش، تسهیم دانش و بکارگیری آن به کمک فناوری به منظور دستیابی به اهداف سازمان . (منبع ۲٤)

مراکز حساس Critical Centers

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و یا دفاعی با سطح تأثیرگذاری منطقه‌ای در کشور گردد.(منبع ۱)

مراکز حیاتی Vital Centers

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات جدی و مخاطره‌آمیز در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و یا دفاعی با سطح تأثیرگذاری سراسری در کشور گردد. (منبع ۲)

مراکز مهم Important Centers

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز آسیب و صدمات محدود در نظام سیاسی، هدایت، کنترل و فرماندهی، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و یا دفاعی با سطح تأثیرگذاری محلی در کشور گردد.

فصل دوم

واژگان

فناوری اطلاعات و ارتباطات، تهدیدات سایبر و ...

۱- واژگان فناوری اطلاعات و ارتباطات،تهدیدات سایبر

۲- واژگان جنگ الکترونیک

1- واژگان فن آوری اطلاعات و ارتباطات و فضای سایبر

آنالیز ترافیک Traffic Analyse

در این نوع حمله، نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده ها می پردازد. به عبارت دیگر بسته یا بسته های اطلاعاتی به همراه یکدیگر، اطلاعات معناداری را ایجاد می کنند.(منبع 43)

احراز اصالت Authenticity

عمل تصدیق هویت ادعا شده از سوی یک موجودیت. به بیان ساده تر یعنی گیرنده از هویت فرستنده آگاه شود.(منبع 43)

اختلال Jamming

بطور کلی یک اختلال کننده قادر است که در یک محدوده از باند فرکانسی، اطلاعات را مبهم نموده و یا در نهایت از بین ببرد. این کار از طریق ارسال یک سیگنال تداخل در باند فرکانسی مزبور انجام می‌شود. این سیگنال می‌تواند نویز سفید و یا سایر نویزها نظیر صدای جرقه، مرس تلگراف و ... باشد. البته چون اختلال‌کننده ممکن است برضد رادارها و گیرنده‌های ارتباطی و یا فیوزها عمل کند ماهیت سیگنال اختلال بسته به اینکه برضد کدامیک عمل کند، متفاوت است (منبع 29)

اختلال در سیستم های مخابراتی Jamming in Communication system

اختلال در درسیستم های مخابراتی دشمن، مستلزم رساندن قدرت اختلال کافی به ورودی گیرنده دشمن می‌باشد. این مقدار بایستی بر قدرت سیگنال اصلی گیرنده غلبه داشته باشد. به تعبیری در جنگ قدرت بین سیگنال دلخواه گیرنده و سیگنال ناخواسته اختلال، بایستی سیگنال اختلال برتری پیدا کند. (منبع 29)

اختلال کننده جاروبی نقطه ای Sweep Lock- on jammer

این اختلال کننده نیز یک سیگنال با پهنای باند باریک را در باند وسیعی از فرکانس، جاروب نموده، مضافا براینکه می‌تواند روی یک فرکانس خاص قفل نماید. یعنی یک اختلال کننده جاروب کننده با قابلیت تمرکز روی یک فرکانس ثابت می‌باشد. (منبع 29)

اختلال کننده جاروبی Sweep jammer

این نوع اختلال کننده دارای سیگنالی با پهنای باند باریک می‌باشد که توسط فرستنده آن در طول باند مشخص و عریضی جاروب می‌شود. به این ترتیب هم از قدرت بالای اختلال کننده نقطه‌ای برخوردار است و هم عرض باند وسیعی را می‌پوشاند و به همین دلیل بطور مؤثر قادر است روی رادار و سیستم های ارتباطی اختلال نماید. (منبع 29)

اختلال کننده سدی Barrage jammer

این اختلال کننده دارای پهنای باند عریض بوده و برعلیه گیرنده‌های راداری و ارتباطی قابل بکارگیری است. بدلیل داشتن پهنای باند عریض قادر است چند کانال مختلف را همزمان مختل کند و یا در رادار فرکانس متغیر بدون هیچگونه تنظیم خاصی ایجاد اختلال نماید. (منبع 29)

اختلال کننده نقطه‌ای Spot jammer

این اختلال کننده دارای پهنای باند باریک بوده و برای اختلال در محدوده باریک و مشخصی از باند بکار گرفته می‌شود و قادر است اطلاعات مربوط به زاویه و مسافت را در رادارها از بین برده و مکالمات و سایر سیگنال های مدوله شده را در گیرنده‌های ارتباطی نامفهوم سازد.(منبع 29)

اسب تروجان Trojan Hourse

اسب تروجان (تراوا) برنامه‌ای است که در ظاهر مفید است اما در واقع حاوی کدی مخفی است که هنگام فراخوانی برخی وظایف زیان بخش یا ناخواسته را انجام می‌دهد.کاربران غیرمجاز از برنامه‌های اسب تراوا برای انجام دادن وظایفی که نمی‌توانند آنها را بطور مستقیم انجام دهند، استفاده می‌کنند. به عنوان مثال، به منظور دسترسی به فایل‌های سایر کاربران بر روی یک سیستم چند کاربره، یک کاربر

می‌تواند یک برنامه ی اسب تروا ایجاد کند که هنگام اجراء، رمز عبور فایل‌های کـاربران را بـه گونـه‌ای تغییر دهد که آن فایل‌ها توسط سایرین قابل خواندن باشد (منبع 11)

اسب تروجان برنامه‌ای مستقل است که در زمان فراخوانی توسط کاربر کارآیی مثبت خواهد داشت ولی ممکن است کارکرد ناخواسته نیز داشته باشد و بر کاربر برتری یابد.(منبع 14)

استاندارد 27001 ISMS

این استاندارد که نسخه ی ISO شدهء استاندارد BS 7799-2:2005 است سعی بر آن دارد تا پـس از شناسایی و دسته بندی دارایی های ناملموس سازمان (از جمله اطلاعات با ارزش سازمان)، مخاطراتی که آنها را تهدید می کند را شناسایی کرده و با ایجاد یک مدیریت صحیح از منظر امنیت اطلاعات و بـا اتخاذ تدابیر مناسب برآمده از « مدیریت ریسک » هر گونه تهدید برای این دارایی ها را از بین بـرده یـا تا حد امکان کاهش دهد. این استاندارد دارای 11 بخش اصلی است که بعضی از آنها قرابت زیـادی بـا مفاهیم مدیریت کیفیت دارند و بدلیل وجود منطق مستحکم در آن ها (همچـون اقـدامات اصـلاحی و پیشگیرانه) در مدیریت امنیت اطلاعات نیز بکار گرفته شده اند.(منبع 43)

استانداردهای ISMS

این استاندارد ها عبارتند از:

استاندارد مدیریتی BS7799 مؤسسه استاندارد انگلیس - استاندارد مدیریتی ISO/IEC 17799 مؤسسه بین‌المللی استاندارد - استانداردهای مدیریتی سری 27000 مؤسسه بین المللی استاندارد- گزارش فنـی ISO/IEC TR 13335 مؤسسه بین‌المللی استاندارد- استاندارد ITBPM ، اسـتاندارد امنیتـی ACSI33 و ... (منبع 43)

اصالت داده Authenticity of data

فرآیندی که برای تصدیق تمامیت داده به کار می رود. اصالت: یعنی هویت واقعی یک موجودیـت با هویت مورد ادعا یکسان باشد. (منبع 43)

افشا (داده) Overtures

نقض امنیت رایانه ای به قسمی که داده در دسترس کاربر غیرمجاز قرار گیرد.(منبع 43)

الگوریتم کلید رمز متقارن Concurrent code key algorithm

در این الگوریتم ها برای رمزگذاری و رمزگشایی پیام از یک کلید رمز استفاده می شود. الگوریتم های کلید رمز متقارن گاهی الگوریتم های کلید رمز سری و گاهی هم الگوریتم های کلید رمز خصوصی نامیده می شوند.(منبع 43)

الگوریتم کلید رمز نامتقارن Nonconcurrent code key algorithm

در این الگوریتم ها یک کلید برای رمزگذاری پیام بکار می رود و کلید دیگر برای رمزگشایی آن.(منبع 43)

الگوگذاری دیجیتال سند Watermark Pattern

مانند یک الگوگذاری روی سربرگ (عنوان چاپی بالای کاغذ)، یک الگوگذاری دیجیتال جهت کمک به شناسایی مالکیت یک سند یا فایل دیگر به کار می رود. شامل رشته های منحصربفرد جاسازی شده داده ها است که درک حسی فایل عکس، فایل موسیقی یا فایل داده های دیگر را تغییر نمی دهند. (منبع 23)

امضای دیجیتالی Digital signature

امضای دیجیتالی، فن آوری دیگری است که توسط رمزنگاری کلید عمومی فعال گردید و این امکان را به مردم می دهد که اسناد و معاملات را طوری امضاء کنند که گیرنده بتواند هویت فرستنده را تأیید کند.امضاء دیجیتالی شامل یک اثر انگشت ریاضی منحصر به فرد از پیام فعلی است که به آن One-Way-Hash نیز گفته می شود.

امنیت اطلاعات رایانه ای Computer information security

امنیت اطلاعات حفاظت از محرمانگی، تمامیت و دسترس پذیری اطلاعات است. علاوه بر این ها سایر ویژگی ها از قبیل اصالت ، قابلیت جوابگویی، اعتبار ، انکار ناپذیری و قابلیت اطمینان اطلاعات نیز می توانند مشمول این حفاظت باشند. (منبع 43)

انباشتگی بیش از حد

این اصطلاح به یک حمله مهندسی اجتماعی مربوط می شود که در آن فرد مهاجم، مقادیر زیادی اطلاعات را در عرض مدت کوتاهی در اختیار قربانی می گذارد تا وی را به یک حالت روانی انفعالی منتقل کند.

انگشت نگاری Finger- Scan

استفاده از اثرانگشت بعلت اجبار قانونی در مقاصد شناسایی، از دیرباز مورد پذیرش عموم بوده است. تا جائیکه این فناوری از حالت اجبار قانونی به یک ابزار مدنی و نیز دارای قالب تجاری و سهم بازار بالا، تبدیل شده است و در محدوده وسیعی از کاربردها استفاده می‌شود.

انکار خدمات DoS Denial of Service

به حمله ای اشاره دارد که منبعی در فضای سایبر ر ا با درخواست هایی درگیر می سازد تا استفاده اشخاص معتبر از منبع را ، جلوگیری نماید. (منبع 23)

بازرسی در سطح شیء Auditing in object

در پایگاه های داده معمولاً بخشی از اطلاعات به لحاظ امنیتی از سایر بخش ها مهمتر می باشند و به همین جهت بیشتر از سایر اطلاعات ذخیره شده در سیستم، مورد تجاوز و حمله قرار می گیرند. در سیستم های مدیریت پایگاه های داده امکاناتی وجود دارد که می توان کلیه مراجعات به بخش یا تمام اطلاعات پایگاه های داده را ثبت نموده و بررسی کرد. به این عمل در پایگاه های داده بازرسی در سطح شیء گفته می شود. (منبع 30)

بررسی یکپارچگی و صحت فایل Authenticity of file

بررسی یکپارچگی و صحت فایل ها در یک سیستم می تواند دلایل بیشماری داشته باشد، یکی از اصلی ترین دلایل آن تشخیص تغییرات بوجود آمده بعد از یک حملهٔ نفوذ یا دستکاری است.(منبع 43)

بروت فورس (نیروی بی خرد) Brute force

یک روش هک که برای پیداکردن رمزهای عبور یا کلیدهای محرمانه، تمام ترکیبات ممکن کاراکترها را مورد آزمون قرار می دهد. اول نام ها و کلمات معمول آزمایش می شوند و سپس از تلفیق حروف مختلف استفاده می شود.

برون سپاری بین المللی International hosting

یک فرآیند تولید که کارهای مختلف به افراد خارجی سپرده می شود که آنها مسئول تکمیل این کارها هستند. بسیاری از شرکت ها کارهای تولیدی خود را به خارج برون سپاری می کنند، امروزه نوع کار برون سپاری شده شامل محدوده وسیعی از کارها می شود مثل : مدیریت فناوری اطلاعات، برنامه نویسی بازی ها و نرم افزارها، حسابداری و نسخه برداری پزشکی. (منبع 23)

بمب پست الکترونیکی E-mail Bomb

برنامه ای که اگر به اجرا در آید، پیام های فراوانی به آدرس داده شده می فرستد تا دیسک را پر کند و یا سرویس دهندهٔ پست الکترونیکی یا وب را از کار بیاندازد.

پروتکل معادل بی سیم WEP

این پروتکل برای پیاده سازی در شبکه های WLAN طراحی شده تا خصوصیا ت امنیتی شبکه های سیمی را بوجود آورد(ویژگی ها مثل: محرمانگی،کنترل دسترسی، و یکپارچگی داده ها)، ولی به دلیل آشکار شدن یک نقص امنیتی در آن، کاربرد آن معمولا با تدابیر ویژهٔ دیگری همراه می شود.

پروتکل انتقال بسته پستی Simple Mail Transport Protocol (SMTP)

یک استاندارد غیر رسمی برای انتقال ایمیل از طریق اینترنت است. SMTP یک پروتکل مبتنی بر متن ساده با استفاده از Port 25 TCP است..

پشتیبان گیری Backup

یک کپی از فایل ها و برنامه ها که در هنگام نیاز دسترسی به آنها آسان باشد.(منبع 44)

تأیید اعتبار دسترسی Access Authorization

مجوز فرآیندی که طی آن کاربران، برنامه ها و ایستگاه های کاری برای دسترسی مورد بررسی و تأیید قرار می گیرد.

تالار چت(گفتگو) Chat room

یک مسیر ارتباطی است اما عبارت اتاق برای توسعه کنایه های چت برای یک مکان آنلاین که گروهی از افراد می توانند درباره موضوع خاص یا تنها چت (گفتگو) ارتباط برقرار کنند، استفاده می شود (منبع 23)

تروریسم سایبر Cyber terrorism

تروریسم سایبر، حمله یا تهدید به حمله ، به شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آن ها به قصد ایجاد رعب و وحشت یا وادارکردن دشمن (اهداف) به انجام یک کار است. سه نوع از این تروریسم نرم افزاری عبارتند از :

1) حمله به نتایج حاصل از اکتشافات نظامی، ارتباطات ، فرماندهی و کنترل و جنبه‌های مختلف اطلاعات محرمانه 2) حمله به حلقه‌های مهم برقراری ارتباط در جامعه (از جمله صدا و تصویر، نقل و انتقال داده‌ها یا سامانه‌های تلفنی) 3) بکارگیری تلویزیون، رادیو و سایر ابزارهای مشابه برای حمله یا تحت تأثیر قرار دادن دیدگاه‌های افراد نظامی یا جامعه، سیاستمداران و رهبران اقتصادی (منبع 14)

تسخیر داده Data Capture

نقض امنیت رایانه ای به قسمی که برنامه ها یا داده ها توسط موجودیت های غیرمجاز تغییر کرده، تخریب شده، یا در دسترس آن ها قرار گیرد.(منبع 43)

تهدیدات شبکه های اجتماعی Social network threats

دسترسی کارکنان درون سازمانی به شبکه های اجتماعی نیز اکنون به یکی از مهمترین راه های نفوذ کدهای مخرب، اجرای حملات هک و افزایش دسترسی های غیرمجاز به محیط های سازمانی، تبدیل شده است.بنابراین، به مدیران شبکه های محلی و سازمانی توصیه شده که در تدوین سیاست های امنیتی سازمان متبوع خود، کنترل دسترسی و امنیت کاربرد شبکه های اجتماعی را به عنوان یک تهدید عمده، مدنظر قرار دهند و معیارهای مؤثری را برای رفع مشکلات موجود در حوزه حریم تجاری و حیثیت سازمانی در اینترنت تعریف کنند.(منبع 43)

جاسوس افزار Spyware

یک نوع مهم اسب های تروجان، جاسوسی خودکار در فضای سایبر، است. این برنامه به طور پنهانی اطلاعات مفیدی را درباره فعالیت های کامپیوتری به یک مهاجم منتقل می کنند و بنابراین از نوع فریب تجربه گر هستند. جاسوس افزار اخیراً مسری شده است، هرچند شیوع آن نسبت به نرم افزار آنتی ویروس ،رو به کاهش می باشد. جاسوس افزارهای تجاری، وب سایت هایی که یک کاربر بررسی می کند، را گزارش می کنند، اما این تکنیک ها می توانند برای جاسوسی هر آنچه کاربر روی یک صفحه کلید تایپ می کند، یعنی توانایی دزدی کلمات رمز و کلیدهای رمز(نگاری)، به کار گرفته شوند. (منبع 23)

جرم سایبری Cyber Crime

تخلف و تجاوز به حقوق دیگران در فضای سایبری رایج است.مواردی از این جرایم عبارتند از : جرائم علیه محرمانگی داده، جاسوسی رایانه ای، جعل رایانه ای و ... (منبع 11)

جنگ سایبری Cyber warfare

جنگ سایبری در لغت به معنای تهاجم بر عناصر سایبری است و اصطلاحا به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستم های اطلاعاتی با هدف به مخاطره انداختن عناصر اطلاعاتی (اطلاعات ، فرایند های مبتنی بر اطلاعات ، سیستم های اطلاعاتی ، شبکه های رایانه ای) دشمن در یک فضای سایبری است.(منبع 11)

چهره نگاری Facial-Scan

اساس این فناوری استفاده از ویژگی های متمایزکننده چهره است. امروزه چهره نگاری در شناسایی های N: 1 کاربرد رو به گسترش یافته است. این سیستم ها دارای دو گونه اصلی تصویر برداری ویدیویی و حرارتی هستند که نوع اول رایج تر و کاربردی تر است.

حسگر مادون قرمز Infra-red Sensor

سنسوری که قابلیت عملکرد در دو نوع فعال و غیر فعال را دارد.یک سنسور فعال در محدوده های نزدیک تابش مادون قرمز فعالیت می کند و اعلام خطر را در این نواحی انجام می دهد.یک سنسور غیر فعال تشعشعات مادون قرمزی که از گرم شدن اجسام ساتع می شوند، تشخیص می دهد.

حق تقدم هشدار ها Alarm Priority

مرتبه بندی هشدارها بر اساس اهمیتشان می باشد. این موضوع اغلب در سیستم های بزرگ که میزان داده ها در آن ها زیاد هستند، مورد استفاده قرار می گیرد.(منبع 44)

حملات سایبری Cyber Attack

این گونه حملات شامل موارد ذیل است : 1- بهره برداری از اطلاعات 2- جلوگیری از ارائه سرویس 3- دستکاری 4- تخریب 5- حذف داده‌ها 6- نفوذ

حملات غیرفعال passive attack

در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می یابد ولی اقدام به تغییر محتوای اطلاعات منبع نمی کند. این نوع حمله می تواند یکی از اشکال شنود ساده یا آنالیز ترافیک باشد.(منبع 43)

حملات فعال Active Attack

در این نوع حملات، برخلاف حملات غیرفعال، نفوذگر اطلاعات مورد نظر را، که از منابع به دست می آید، تغییر می دهد، که تبعاً انجام این تغییرات مجاز نیست. از آن جایی که در این نوع حملات اطلاعات تغییر می کنند، شناسایی رخداد حملات فرایندی امکان پذیر است. در این حملات به چهار دسته ی مرسوم زیر تقسیم بندی می گردند : تغییر هویت - پاسخ های جعلی - تغییر پیام - حمله انکار خدمات(منبع 43)

حمله از طریق استراق سمع Attack with logon Abuse

عبارت است از نفوذ غیرمجاز به ارتباطات شبکه و افشا کردن داده های مبادله شده.(منبع 43)

حمله سارقانه Hijacking Attack

عبارت است از دسترسی غیرمجاز به منابع سیستم در پوشش ارتباطات درست و قانونی و یا سوء استفاده از آن .(به طور نمونه می توان مکانیزم اسب تروجان را مثال زد)(منبع 43)

حمله فریب کارانه Spoofing Attack

عبارت است از استفاده از موجودیتی غیر مجاز مانند استفاده از یک IP جعلی برای نفوذ به سیستم.(منبع 43)

حمله فیشینگ phishing

حمله فیشینگ شکل خاصی از جرم سایبری است. مجرم یک کپی تقریباً 100درصد شبیه یک وب سایت بنگاه تجاری ،ایجاد می نماید. سپس تلاش می کند تا کاربران را جهت افشای اطلاعات شخصی : نام کاربری، کلمه عبور، PIN و غیره ، از طریق یک فرم در سایتی جعلی فریب دهد که این اجازه را به مجرم داده می شود با استفاده از این اطلاعات پول به دست آورد.فیشرها یا مجرمان فیشینگ از تکنیک های متعددی برای فریب دادن کاربران جهت دسترسی به سایت جعلی استفاده می کنند، از قبیل ارسال ایمیل هایی که به نظر می آید از یک بانک باشد.این ایمیل ها اغلب از لوگوهای قانونی و یک سبک تجاری خوب استفاده می کنند و سربرگ نامه را طوری طراحی می کنند که شبیه این به نظر برسد که از یک بانک قانونی می باشد.(منبع 43)

حمله نفوذی

عبارت است از دسترسی کاربران غیرمجاز به یک سیستم از طریق شبکه با استفاده از نقص های ایمنی آن.(منبع 43)

خدمات پیام رسانی کوتاه massaging services

خدمات پیام متنی پیشنهادی توسط سیستم تلفن سلولی دیجیتالی GSM است.

پیام های متنی کوتاه از تلفن همراه، دستگاه فکس یا آدرس IP انتقال داده می شوند. پیام باید بیشتر از حداکثر 160 کاراکتر الفبا عددی و فاقد عکس و گرافیک باشند. (منبع 23)

درب مخفی Trap Door

درب مخفی در واقع مکانیزمی نرم افزاری است که توسط طراحان و هکرها طراحی شده بطوریکه امکان ورود پنهانی به سیستم یا شبکه ی مورد نظر را فراهم می نماید . عملکرد درب های مخفی هم همانند بمب های منطقی است در مواردی برنامه نویسان یا طراحان سیستم ها ، راه هایی را درون سیستم امنیتی ، برای ورود خود لحاظ می کنند که باعث کاهش امنیت سیستم می شود . برای مثال آن ها می توانند با وارد کردن یک رمز عبور سری وارد رایانه شده ، علاوه بر دسترسی به اطلاعات ، داده ها را به طور دلخواه تغییر دهند (منبع 11)

درب پشتی Backdoor

در امنیت یک سیستم، این یک حفره است که طراحان بطور عمدی آن را بر جای می گذارند. ولی امروزه این واژه برای نرم افزارهایی بکار برده می شود که از راه دور توسط افراد خرابکار برای ورود به سیستم(از طریق یک درب پشتی) بارگذاری می شود.

دستگاه خواندن نشان بیومتریک Biometric Reader

وسیله ای برای جمع آوری و آنالیز داده های زیستی می باشد.(منبع 44)

دیواره آتش Firewall

دیواره های آتش ابزارها و نرم افزارهایی هستند که می توان با کمک قواعدی ، صحیح یا غیرصحیح بودن ارتباطات داخلی (داخلی – خارجی ، خارجی – داخلی) را کنترل کرد و در صورت وقوع یک امری خلاف اصول و قواعد تعریف شده باز به همان شکلی که برای آن تعریف گردیده از قبیل قطع ارتباط یا انحراف آن عمل نماید و حکم حصار و قلعه ای را دارد که به دور بخشی که امنیت آن باید تأمین شود، کشیده می شود. (منبع 11)

دیواره آتش شخصی Personal Firewall

این نوع دیواره ی آتش تنها در یک کامپیوتر نصب می گردد و هـدف آن تنهـا تـأمین یـک node است و حصار به دور سیستم شخصی شما می کشد تا از حملات مستقیم و دزدی اطلاعات و ویروسها مصون بمانید.

رادار پالس داپلر Duppler Pulse radar

این رادارها جهت فیلترکردن سرعت هدف های متحرک بکار می رود . استفاده از فرکـانس تکـرار پالس بالا و منبع فرکانس رادیویی ثابت از مشخصه های این نوع رادارها می باشد.(منبع 47)

رادار پالس فشرده Pulse radar

این رادارها با پیدایش فناوری پردازش دیجیتالی ظاهر گردید . انواع این رادارهـا شـامل رادارهـای تصویر بردار روزنه مصنوعی یا سار و رادارهای نشاندهنده اهداف ثابت از متحرک می گردد.(منبع 47)

رادار پالسی معمولی General pulse radar

ویژگـی هـای ایـن رادارهـا فرکـانس یـا فرکـانس تکـرار پـالس ثابـت و منبـع تـوان مگنترونـی می باشد.(منبع 47)

رادار مقاوم در رهگیری Low Probability in tracking

رادارهای مقاوم در مقابل رهگیری ، نسل جدید رادارها هستند. این رادارها از انواع مختلف فناوری طیف گسترده ، آنتن های با سطح گلبرگ پایین و مدیریت توان بالا استفاده می کنند .(منبع 47)

رادارهای فراسوی افق Ultra- horizon radar

رادارهای فراسوی افق که در بخشی از طیف الکترومغنـاطیسHF قـرار دارنـد، از جملـه رادارهـای دوربرد می باشند که از تغییرات لایه یونیسفر و انعکاس امواج از این لایـه بـرای کشـف اهـداف بهـره می گیرند. فرستنده و گیرنده این نوع رادارها جدا از هم و در فاصله 80 تا 160کیلـومتری از یکـدیگر قرار دارند. هدف اولیه از بکارگیری اینگونه رادارها کشف موشک های بالستیکی میـان بـرد و دور بـرد قاره پیما و همچنین موشک های کوتاه برد بالستیکی می باشد، با اینحال رادارهای فراسوی افق، قادر به تأمین اطلاعاتی پیرامون انفجارات هسته ای نیز بوده که این اطلاعات شامل موقعیت یـابی و شـدت یـا قدرت انفجار می گردد.(منبع 47)

رمز ترکیبی Combined Encryption

یک نمونه از سیستم های رمز، سیستم رمز ترکیبی می باشد بدین ترتیب که در مقابل هـر کـدام از مطالب کشف آن امکان دارد یک حرف یا ترکیبی از حرف و عدد و یا کلمه و یا جمله قرار گیرد.

رمز ویژنر Vigenere Code

یکی از رمزهای معروف چند الفبایی دستی رمز ویژنر است که از جـدولی بـه نـام جـدول ویژنـر استفاده می کند.حرفهایی که در ستون کناری سمت چپ قرار دارند سطرهای جـدول را مشـخص مـی کنند درحالیکه هر سطر بیانگر یک رمز جمعی است. بنابراین هر حرف ستون کناری رمز جمعی خاصی را مشخص می کند.در این سیستم با انتخاب یک کلید و نوشتن آن در زیر پیام،متن رمز شده با اسـتفاده از جدول بدست می آید.در صورتیکه طول متن بزرگتر از طول کلید باشد کلید تکرار می شود.(منبع30)

رمزدارکردن Encryption

یک روش سیستماتیک و برگشت پذیر برای ساخت یک پیام پیچیده با اسـتفاده از کلیـدهای رمـز، است. (منبع 23)

رمزشکن رمز عبور Password Cracker

یک برنامهٔ نرم افزاری شامل فرهنگ های لغات کامل که سعی در یافتن رمزهای عبور کاربران دارد.

رمزگذاری داده Data Encryption

رمز نگاری و استفاده از الگوریتم های رمز یکی از متداول ترین روش های امنیتی در سیستم هـای رایانه ای بوده و هست. بدیهی است که استفاده از رمز در ذخیره و بازیابی اطلاعـات تـاثیر مناسـبی بـر جلوگیری از دسترسی های غیرمجاز به اطلاعات ذخیره شده دارد.امروزه در اکثر سیستم های مـدیریت پایگاه داده امکاناتی جهت رمز گذاری اطلاعات ذخیره شده در پایگاه داده وجود دار د . (منبع 30)

رمزنگاری کلید رمز همگانی Public Key Encryption

یک دستهٔ مهم الگوریتم های کلید رمز نامتقارن است . در این الگوریتم ها معمولا کلید رمزگـذاری را « کلید رمز همگانی» می نامند، چون می تواند بدون اینکه خدشه ای بـه سـری بـودن پیـام یـا کلیـد رمزگشایی وارد شود در دسترس همگان قرار داشته باشد . الگوریتم های کلید رمز همگـانی بـا مجـزا کردن کلیدهای رمزگذاری و رمزگشایی، مشکلات الگوریتم های کلید رمز متقارن را تـا حـدود زیـادی حل می کنند. از دید مبتنی بر تئوری، فناوری کلید رمز همگانی بطور نسبی کار ارسال پیـام رمزگـذاری شده را برای افراد آسان می کند.(منبع 43)

رمزنگاری کلید عمومی Public key Encryption

فرآیند رمزنگاری کلید عمومی عبارت است از ایجاد همزمان کلید اختصاصی و عمومی، که این کار با استفاده از همان الگوریتم فراهم شده از سوی مقام مجاز صورت می‌پذیرد. کلید اختصاصی تنها با تقاضای بخش درخواست‌کننده ارایه می‌شود، در حالیکه کلید عمومی در فهرستی که همه بخش‌ها به آن دسترسی دارند و با هدف شناخت و درک مبادلات الکترونیکی، ارایه می‌شود. کلید اختصاصی، از طریق مقام معتبر، مخفی نگه داشته می‌شود که به کسی جزء تقاضادهنده واقعی ارائه نمی‌شود و هیچگاه نیز از طریق اینترنت ارسال نمی‌شود.

رمزهای چند الفبایی

در روش های جانشینی که در بخش های گذشته مطرح شد با وجود تغییر حرف های متن اصلی، ویژگی حروف باقی می ماند. برای از بین بردن توزیع ظاهری حرف ها در متن ، روش چند الفبایی را به کار می برند که در آن هر نماد از متن رمز شده می تواند متعلق به بیش از یک نماد در متن اصلی باشد. اما با توجه به اینکه کشف رمز می باید بطور یگانه صورت گیرد نماد رمز شده و محل قرار گرفتن آن در متن بطور یگانه نماد متن اصلی متناظر را بیان می کنند (منبع 30)

روت کیت Root kit

یکی از بی شمار ابزار در دسترس هکرها هستد که نفوذ آنها به یک سیستم را از دید صاحب واقعی آن پنهان می دارد. این ابزار برای نفوذ به یک سیستم استفاده نمی شود بلکه برای اطمینان از اینکه یک سیستم شکسته شده، هنوز در دسترس نفوذ باقی مانده است، به کار می رود.

روت کیت ها شامل مجموعه ای از ابزارها هستند که روی ماشین هدف نصب می شوند، که به ایجاد اصلاحاتی در برنامه هایی که بیشترین کاربرد را دارند می پردازند به گونه ای که انجام عملیات مشکوک در اختفا قرار گرفته و پنهان بماند.عبارتند از: اسب های تراوا، درهای پنهانی، برج های مراقبت /چراغ های دریایی، دریچه های تله. (منبع 23)

روش های آلوده سازی رایانه Infect methods

1) نصب مستقیم :در این شیوه فرد نفوذگر یا عوامل او به صورت مستقیمم به رایانه دسترسی پیدا نموده و نرم افزار را بر روی رایانه اجرا می نماید. 2) نصب غیر مستقیم : در این روش از طریق سی دی های آلوده که از بازار و از افراد ناشناخته تهیه می شود یا این که به صورت برنامه ریزی برای یک بار در رایانه (به هر دلیلی) اجرا شود نرم افزار ثبت کننده به رایانه منتقل شود.3) نفوذ از طریق شبکه‌های

اینترنتی 4) نفوذ از طریق نصب نرم‌افزارهای جاسوسی5) نفوذ از طریق دانلود نرم‌افزار از اینترنت .(منبع 43)

رویداد امنیتی (اطلاعاتی) security event

یک یا مجموعه ای از حوادث امنیتی ناخواسته یا غیرمنتظره در حوزه امنیت اطلاعات که احتمال زیادی می رود عملیات کسب و کار سازمان را به خطر انداخته و امنیت اطلاعات را تهدید نماید.(منبع43)

زیر ساخت کلید عمومی Public Key Infrastructure

به عنوان استانداردی که عملا برای یکی کردن امنیت محتوای دیجیتالی و فرایند های تجارت الکترونیک و همچنین پرونده ها و اسناد الکترونیکی مورد استفاده قرار می گرفت ظهور کرد.این سیستم به بازرگانان اجازه می دهد از سرعت اینترنت استفاده کرده تا اطلاعات مهم تجاری آنان از رهگیری ، دخالت و دسترسی غیر مجاز در امان بماند.یک PKI کاربران را قادر می سازد از یک شبکه عمومی ناامن مانند اینترنت به صورتی امن و خصوصی برای تبادلات اطلاعات استفاده کنند.این کار از طریق یک جفت کلید رمز عمومی و اختصاصی که از یک منبع مسؤل و مورد اعتماد صادر شده و به اشتراک گذارده می شود، انجام گیرد .

سامانه اسکادا SCADA system

امروزه سامانه های اسکادا به طور گسترده و همه جانبه ای در اتوماسیون صنعتی و کنترل فرآیندهای خاص مورد استفاده قرار می گیرند و بطور ویژه برای خودکار کردن سیستم هایی نظیر کنترل تبادلات انرژی، مدیریت شبکه برق و پردازش تلفات طراحی شده اند.سیستم های موجود بر پایه سخت افزار، نرم افزار و پروتکل های ارتباطی که دارای قابلیت تشخیص و اصلاح خطا هستند، استوار می باشند ولی قابلیت ارتباطات امن که امروزه برای اتصال سیستم ها و شبکه های مختلف موردنیاز می باشد را دارا نمی باشد.(منبع 43)

سرریزی بافر Buffer Overflow

یک نقص نرم افزاری که زمانی رخ می دهد که برنامه داده ها را به فضایی در حافظه می برد، اما در آن قسمت از حافظه فضای کافی برای ذخیرهٔ آن داده ها وجود ندارد. این کار می تواند انواع مشکلات

را به بار آورد و معمولا به اتفاقاتی منجر می شود که امنیت برنامه را خدشه دار می کند. می توان پیش از انتقال هر داده به حافظه ،یک بررسی ساده برای اطمینان از وجود حافظهٔ کافی انجام داد و بدین ترتیب از وقوع سرریزی buffer پیشگیری کرد.

سرور پراکسی Proxy Server

این سرور، خدمات شبکه کامپیوتری را ارائه می دهد به مشتریان اجازه می دهد تا روابط شبکه ای غیر مستقیمی را نسبت به خدمات شبکه ای دیگر، ایجاد کنند و به عنوان رله خدمات عمل می کند، مثل: توانایی های فیلترسازی و پنهان کردن (برای مثال: پراکسی وب که از دسترسی به سایت های لیست سیاه ممانعت می کند).

سیستم رمز خودکار Auto Encryption system

در این نوع سیستم رمز تمامی مراحل رمز و ارسال و دریافت و کشف پیام بصورت خودکار و اتوماتیک توسط ماشین های گیرنده و فرستنده انجام می گیرد که نمونه این نوع از سیستم های رمزی را می توانیم دستگاه های تلکس با کد مخصوص را نام ببریم.(منبع 30)

سیستم رمز نیمه خودکار Semi-auto Encryption system

در این سیستم ماشین های رمز در خارج از مدار ارسال و در اتاق رمز قرار داشته وپیام بوسیله متصدی ماشین رمز از وضعیت کشف بصورت رمز درآمده و پیام رمز شده برای ارسال به مرکز پیام برده شده و در آنجا توسط یکی از وسایل ارتباطی بوسیله اپراتور ارسال می گردد و عکس همین عمل در طرف مقابل که گیرنده پیام می باشد اجرا می شود.(منبع 30)

سیستم اشتراک اطلاعات Information Joint System

طبق طرح پاسخ گویی، اطلاعات موجود برای مخابره شدن به وسیله تلفن ایمیل و فکس جمع آوری می شوند.

سیستم مدیریت امنیت اطلاعات Information Security Management Systrm(ISMS)

بخشی از سیستم مدیریت یکپارچه و سراسری در یک سازمان است که هدف آن پایه گذاری ، پیاده سازی ، بهره برداری ، نظارت ، بازبینی ، نگهداری و بهبود امنیت اطلاعات است . سیستم مدیریت امنیت اطلاعات در مجموع یک رویکرد نظام مند به مدیریت اطلاعات حساس به منظور حفاظت از آن هاست. (منبع 43)

سیستم کشف نفوذ Intrusion Detection System

سیستم‌های کشف نفوذ موسوم به IDS برای پایش ترافیک شبکه به منظور کشف تهدیدات احتمالی بکار می‌روند. سیستم کشف نفوذ اشاره به سیستم‌هایی دارد که حملات احتمالی را با مقایسه داده‌های پایش شده با علائم حملات شناخته شده کشف می‌کنند. ترکیبی از اجزا شامل سنسورها، واحد های کنترل ،خطوط انتقال و واحدهای مونیتوری می باشند که برای کشف نفوذ استفاده می شوند.

سیستم کلید عمومی Public key system

سیستم کلید عمومی چیزی است که از دو کلید استفاده می کند، یک کلید عمومی، که برای هرکسی شناخته شده است و کلید خصوصی که تنها گیرنده پیام بکار می برد. (منبع 23)

شبکهٔ خصوصی مجازی Virtual Private Network

یک اتصال خصوصی میان دو ماشین است که داده های ترافیکی خصوصی را از طریق اینترنت ارسال می کند. VPN فناوری سازمان را قادر می کند که بتواند از طریق اینترنت خدمات شبکه ای خود را بطور محرمانه به کاربران راه دور، دفاتر شعب و شرکت های همکار برساند.

شبکیه نگاری Retina-Scan

هر شبکیه هم مانند عنبیه دارای الگوی منحصر بفردی از عروق خونی است که می تواند برای شناسایی های1 :N بکار رود. استفاده از شبکیه‌نگاری به موارد بسیار امنیتی که راحتی یا ناراحتی کاربران اهمیت ندارد محدود است. شبکیه نگاری نیز سیستم بسیار فریب ناپذیری است.

شمارهٔ هویت شخصی Personal Identification Number

یک رشته از اعداد یا حروف که برای تصدیق هویت یک کاربر سیستم یا سرویس بکار می رود. شمارهٔ هویت شخصی مشابه رمز عبور است اما عمومًا مربوط به معاملات مالی (حساب های بانکی یا کارت های اعتباری) یا دسترسی فیزیکی به یک مکان می باشد.

شناسایی و تصدیق هویت Ratification & reconnaissance identification

شناسایی، ارتباط دادن یک هویت با یک موضوع است. تصدیق هویت، اعتبار یک هویت را به اثبات می رساند و تصدیق اختیار،ارتباط دادن حقوق یا امتیازات به یک هویت می باشد.شناسایی و تصدیق هویت ممکن است به تنهایی بوسیلهٔ یک ایستگاه کاری که فرد از آن استفاده می کند انجام شود، یا ممکن است یک سیستم مبتنی بر شبکه تصدیق هویت را بر عهده داشته باشد که در آن هویت های

کاربران در یک سرویس دهنده مرکزی ذخیره شده و توسط گروه های سرویس گیرنده ها بـه اشـتراک گذاشته شده است.(منبع 43)

شنود Wiretapping

در این نوع، نفوذگر تنها به پایش اطلاعات رد و بدل شده می پردازد. برای مثال شنود ترافیک روی یک شبکه ی محلی یا یک شبکه ی بی سیم (که مد نظر ما است) نمونه هایی از این نوع حمله به شمار می آیند.(منبع 43)

شنود (قانونی) Wiretapping

شنود ترافیک شبکه و ترافیک مخابراتی که توسط آژانس‌های امنیت ملـی و سـازمان‌هـای قضـایی صورت می‌گیرد. شنود باید توسط یک مقام ذیصلاح بر طبق قوانین ملی قابل اعمال، مجاز شناخته شده باشد.

صحت داده Integrity of data

خصوصیتی از داده است که فارغ از تغییرات صورت گرفتـه در آن، دقـت و یکنـواختی اش حفـظ می شود. به عبارت دیگر ، حفظ تمامیت داده به معنی دریافت درست داده ها در مقصد می باشد.

ضد امنیتی انتقال Transfer security Counter

یک پروتکل که هدف آن برقراری امنیت و ارتباطات معتبـردر شـبکه هـای عمـومی بـا اسـتفاده از رمزنگاری داده ها است. امنیت لایه انتقال از SSLV3 مشتق شده و یـک اسـتاندارد پیشـنهادی اینترنتـی است.(منبع 23)

عنبیه نگاری Iris –Scan

هر عنبیه دارای یک الگوی پیچیده منحصر بفرد است. بطوریکه عنبیه چپ و راست یک فرد کاملاً متفاوت هستند. ادعـا مـی‌شـود سیسـتم هـای عنبیـه نگـاری خطاناپـذیر (foolproof) هسـتند. زیـرا کپی برداری مصنوعی از عنبیه بخاطر ویژگی ها و تعداد خصوصیات قابل سنجش آن غیرممکن اسـت. عنبیه نگاری دارای سطح امنیت بسیار بالا می باشد.

فن آوری اطلاعات و ارتباطات Information and Communication Technology(ICT)

به مجموعه فن آوری هائی که امکان ذخیره سازی ، پردازش ، ارائه و انتقال اطلاعـات را از طریـق محیط های انتقال فراهم می نماید ، اطلاق می گردد.مواردی از قبیل ذخیره سازی اطلاعات، پـردازش و ارائه اطلاعات ، سیستم ها ی عامل، زبان ها ی برنامه نویسی ، مهندسـی پروتکـل هـا ، نـرم افزارهـای کاربردی شبکه، شبکه های ذخیره سازی داده ، فـن آوری هـای رمزنگـاری و امنیتـی، سـخت افـزار ، زبان های ارائه محتوا در وب و ... (منبع 5)

فن آوری بیومتریک Biometric tecnology

این فناوری که در واقع روش های تعیـین یـا تأییـد هویـت افـراد بـه صـورت خودکـار، طبـق شناسه های فیزیولوژیکی یا رفتاری است در سال های گذشته، بیشتر در فیلم های سـینمایی بـه عنـوان یک فناوری پیشرفته علمی- تخیلی نمود داشته است و در عین حال در تعدادی از مراکـز حسـاس کـه نیازمند به ضریب امنیتی بالایی بوده اند نیز بکار گرفته شده است. انواع بیومتریک ها عبارتند از:

بیومتریک های فیزیولوژیکی عبارتند از: عنبیه نگاری - شبکیه نگـاری- انگشـت نگـاری- چهـره نگاری- دست نگاری- صوت نگاری. بیومتریک های رفتاری عبارتند از: امضا نگاری- نحـوه ی تایـپ کردن

فنون شناسایی reconnaissance technicals

رایانه ها سیستم های شناسایی مختلفی را بکار می برند. ساده ترین آنها بر اساس اسامی کاربری و رمزهای عبور کار می کنند، و بقیه بر اسـاس سـخت افزارهـای مخصوصـی هسـتند کـه مـی تواننـد مشخصات ممیزهٔ انسان های مختلف را بسنجند. سیستم هایی نیز وجود دارند که بر اسـاس رمزنگـاری کلید عمومی کار می کنند. این فنون عبارتند از: 1) شناسایی فیزیکی

۲) فنون شناسایی توسط رایانه(مثل: سیستم های مبتنی بر رمز عبور- معیارهای زیستی مثل DNA ، اثر انگشت - شناسایی مکان - استفاده از کلیدهای عمومی) (منبع 43)

قابلیت دسترسی Accessibility

خصوصیت داده یا منبع که به موجب آن به محض درخواست یک کاربر مجاز، آن داده یا منبع قابل دسترسی و استفاده باشد.

قفل شکن cracker

شامل افرادی مجرب و خطرناک تر از گروه تازه کار هستند.تفاوت آنها با تازه کاران این است که این گروه قادرند حملات جدیدی را پی ریزی و اجرا کنند.(منبع 43)

کرم رایانه ای Computer worm

کرم ، برنامه مخربی است که از اتصالات شبکه برای انتشار خود از یک سیستم به سیستم دیگر استفاده می‌کند. کرم‌ها به برنامه میزبان نیازی ندارند و با اتکاء به خود می‌توانند منتشر شوند. به محض فعال شدن در یک سیستم کرم می‌تواند مانند یک ویروس یا یک باکتری عمل نماید. کرم‌ها به منظور تکثیر خودشان از امکانات شبکه از قبیل پست الکترونیکی استفاده می‌کنند (منبع 11)

کمین سایبری Ambush Cyber

کمین سایبری یک جرم تروریستی نسبتاً جدید در حوزه سیستم‌های کامپیوتری می‌باشد هرچند که در مقایسه با تروریسم سایبری از اولویت کمتری برخوردار است، یک سری کارها که در آن یک شخص، گروهی از اشخاص یا سازمان‌ها، از فناوری اطلاعات و ارتباطات استفاده می‌کند تا یک تعداد بیشتری از افراد را مورد آزار قرار دهد. چنین کارهایی می‌تواند در برگیرنده رفتارهایی مانند انتقال دادن تهدیدات و اتهامات کاذب، به سرقت بردن هویت، دزدی اطلاعات، آسیب رساندن به اطلاعات یا تجهیزات، تحت نظر قرار دادن رایانه ای فرد، جلب افراد رده پایین به منظور ایجاد ترس و جبهه‌گیری باشد ولی محدود به آنها نیست. (منبع 23)

کنترل فیزیکی دسترسی Access physical control

استفاده از ساز و کارهای فیزیکی برای تأمین کنترل دسترسی. مثال: نگهداری از رایانه در اتاقی که درب آن قفل شده است.(منبع 43)

لایه سوکت امن security socket layer

پروتکل رمزنگاری برای داده ها که در واسط (سطح مشترک) سوکت به کار رفته و اغلب به کاربردها متمرکز شده است و به طور وسیعی جهت محافظت نقل و انتقال در شبکه گسترده جهانی به کار می رود. (منبع 23)

ماهواره های مخابراتی Communication satellites

سیگنال های رادیویی ماکروویو در ماهواره ها تأمین کننده ارتباطات جهـانی در فضـا (خـارج جو) بوده و متقابلا عمل رهگیری این گونه اطلاعات در فضا و زمین میسر مـی گـردد. در سـال 1999 شبکه ماهواره های جهانی اینتل ست ، 19 ماهواره را هدایت می کرد که آخرین مدل آن ظرفیتی معادل 90000 کانال تلفن، تلکس، تلگراف، تلویزیون، دیتا و فاکس را بطور همزمان دارا بود. (منبع 47)

مجوز کاربری User Privilege

تعریف و استفاده از مجوزها یکی از جنبه های اساسی در مقوله امنیـت سیسـتم هـای پایگـاه داده است. بطور کلی کاربران سیستم های پایگاه داده پس از آنکه مورد تصدیق قـرار گرفتـه و بعنـوان یـک کاربر معتبر شناخته شدند تنها در حیطه ای که به آنها مجوزهای مورد نظر داده شده است قادر به انجام عملیات می باشند.مدیر سیستم (و یا فرد صاحب اطلاعات ذخیـره شـده) مجـوز مـورد نظـر را بـرای کاربران مذکور صادر کند.(منبع 23)

مجوزهای سیستم System Privileges

مجوزهای سیستم تنها توسط مدیر سیستم قابل تعریف و واگذاری هستند. این مجوزها امکان انجام عملیات سیستمی و امکانات اولیه آن را در اختیار کاربران قرار می دهد. بطور کلـی بـا اسـتفاده از ایـن امکان در سیستم های مدیریت پایگاه داده می توان حیطه عمل کاربران را تعریف و دسترسـی آنـان بـه منابع سیستم را کنترل نمود. (منبع 23)

محافظت از جامعیت داده ها Protecting of data Integrity

در سیستم هایی که با استفاده از مدل های سه لایه و چند لایه طراحی و پیاده سازی می شوند یک مرحله دیگر از حفاظت داده ها در بحث جامعیت مورد استفاده قرار می گیرد. در این نوع سیستم ها بـا توجه به این که ارتباط کاربران با پایگاه داده تنها ازطریق لایه وسطی برقرار می شود و سیسـتم پایگـاه داده تنها به درخواست هایی که از طرف رایانه لایه وسطی(با یک IP مشخص دریافت شده اند) پاسـخ داده، لذا چنانچه مهاجمی قصد اتصال مستقیم بـه سیسـتم پایگـاه داده را داشـته باشـد بهـیچ وجـه بـه درخواست او پاسخ داده نمی شود. (منبع 30)

محرمانگی Confidentiality

خصوصیتی از داده است که میزان عدم دسترسی افراد، فرآیندها یا موجودیت های غیرمجاز و عدم

افشای داده برای آنها را نشان می دهد. به عبارت دیگر ، حفظ محرمانگی بدین معنی است که فقط کاربران خاصی از داده بتوانند استفاده کنند.

مدیریت واکنش اضطراری management of Computer Emergency Response

مراحل پاسخگویی به رخدادهای امنیتی عبارتند از:

1) آمادگی 2) شناسایی: تشخیص این موضوع که اولا آیا یک رخداد امنیتی رخ داده است یا خیر و ثانیا در صورت وقوع ، طبیعت این رخداد چیست؟

3) کنترل و محدود سازی: محدود کردن دامنه رخداد و جلوگیری از بدتر شدن آن است.

4) پاکسازی: حذف یا کاهش عواملی که باعث وقوع این رخداد امنیتی شده اند.

5) بازیابی: بازگرداندن سیستم به وضعیت عادی و کاربردی.

6) پیگیری: یادگیری از این تجربه و استفاده از آن در هنگام وقوع رخدادهای آتی. (منبع 43)

معماری امنیت شبکه Network security architecture

در معماری امنیت شبکه، هدف ارائه مدلی است که بر اساس آن بتوان نحوه آرایش تدابیر حفاظت سایبر در شبکه را مورد قضاوت قرار داد.

ممیزی و ثبت وقایع Audit and registration of event

بعد از نصب سیستم های دفاعی روی رایانه، باید مطمئن شوید که این سیستم های دفاعی به درستی عمل می کنند و همچنین باید از هرگونه رفتار غیرعادی و سایر مشکلات آگاهی یابید ، این فرآیند را نظارت یا ممیزی می نامند. دو نوع متداول ممیزی عبارتند از :

بررسی جامعیت فایل ها، و بررسی فایل های ثبت سیستمی.(منبع 43)

مهندسی امنیت Security Engineering

مهندسی امنیت مجموعه فعالیت‌هایی است که برای حصول و نگهداری سطوح مناسبی از : محرمانگی - صحت - قابلیت دسترسی- حساب پذیری - اصالت - قابلیت اطمینان به صورت قاعده مند در یک سازمان انجام می‌شود. (منبع 43)

مهندسی اجتماعی Sosial Engineering

در حوزه امنیت کامپیوتر، اصطلاح مهندسی اجتماعی برای توصیف اهداف شوم افرادی که درصدد دسترسی به داده ها و اطلاعات حساس از طرق غیرقانونی هستند، بکار می رود. فرایند بدست آوردن اطلاعات از طریق تکنیک های مهندسی اجتماعی بر نبود مهارت های فنی دلالت دارد اما بر اساس آن،

داشتن مهارت های اجتماعی از اهمیت زیادی برخوردار بوده. مهندسی اجتماعی فرایندی است که بوسیله آن یک نفر دیگران را برای انجام خواسته های خود اجیر می کند (منبع 23)

نامه های الکترونیکی جعلی Counterfeit e-mails

در این نوع حمله مهندسی اجتماعی کامپیوتری، مهاجمین، پیام هایی از طریق پست الکترونیک به قربانیان فرستاده و ادعا می کند که یک نهاد معتبر می باشند. این نامه های الکترونیکی تلاش دارند تا قربانیان را برای ارائه اطلاعات محرمانه به سایت شبکه خرابکاری ارائه کرده یا برنامه های مخربی را نصب کنند.

نبردهای دیجیتالی Digital warfares

در عصر نبردهای دیجیتالی و جنگ‌های شبکه محور امروزی، توجه به برنامه‌ریزی ،فرماندهی، هدایت و کنترل عملیات دفاعی با استفاده از فناوری‌های ارتباطات و اطلاعات به واقعیتی انکارناپذیر مبدل شده است.

نرم افزار اسنیفر sniffer software

این نرم افزاری است که از ترافیک داده ها در شبکه کامپیوتری استراق سمع می کند؛ برای سیستم های کشف- تجاوز مستقر در شبکه ضروری ولی برای مهاجمان نیز مفید است. (منبع 23)

نرم افزار ثبت کننده صفحه کلید keylogger

صفحه کلید رایانه ها نیز در «گلوگاه ورودی» قرارگرفته اند و می توانند همانند نگهبانان این کار را در فضای مجازی انجام دهند. با هر بار فشردن بر روی دگمه های صفحه کلید پالسی تولید می شود. حال اگر فردی به صورت غیر مجاز از این پالس های عبوری، تصویر تهیه نماید می تواند همگام با رایانه در جریان کلیه اطلاعات تولید شده قرار گیرد. این نرم افزار ثبت کننده صفحه کلید نام دارد که توسط افراد غیر مجاز به نحوی در سیستم نصب می شود. (منبع 43)

نفوذ Intrusion

دسترسی غیرمجاز به یک سامانه پردازش داده می باشد.(منبع 43)

هرزنامه(اسپم) Spam

« اسپم » به ایمیل ناخواسته ای با حجم انبوه اطلاق می شود که افراد تمایلی به دریافت آن ندارند. امروزه این ایمیل های ناخواسته بتدریج در حال تبدیل به مشکلی جدی است .رویکردهای ضد اسپم

کلیدی شامل فیلترینگ، پست مجدد، هشکش، و تصدیق اصالت فرستنده می باشد.(هشکش: این رویکرد راه حل دیگری برای اسپم است در اوایل دهه1990 ارائه شد، ایده آن شبیه پست الکترونیک است، یعنی الصاق یک تمبر الکترونیک به هر ایمیل ارسالی).

هکر Hacker

هکر در دنیای کامپیوتر کسی است که با سیستم های رایانه ای آشناست و میتواند با روش هایی خاص ،بدون اجازه وارد آن ها شود .یکی از ابزار های متداول برای هک کردن ، استفاده از نرم افزارها و سخت افزارهای جاسوسی جهت ورود غیر مجاز به سیستم های هدف و بهره گیری غیر مجاز از اطلاعات آن ها می باشد . (منبع 11)

هندسه دست Hand-Scan

این تکنیک از تصاویر3 بعدی دست و اندازه گیری پهنا، عرض و طول انگشتان و بند انگشتان استفاده می کند.به این ترتیب که کاربر دست خود را در فضای مشخص شده قرار می دهد و دوربین از بالا و کنار با تهیه تصاویر لازم اطلاعات خواسته شده را دریافت می کند. از این تکنولوژی بیشتر در کاربردهای 1:1 استفاده می شود و یکی از ساختاریافته ترین تکنولوژی های تجاری روز به شمار می رود که بعلت استفاده آسان و راحت از آن ،کاربردش رشد سریعی دارد.

هکر کلاه سفید with hat Haker

یک هکر که در امر ایمن سازی سیستم های اطلاعاتی تمرکز داشته واز نظر اخلاقی با سوء استفاده از سیستم های اطلاعاتی مخالف می باشد (منبع 23)

ویروس های رایانه ای Computer Viruse

ویروس برنامه ای غیر مجاز و ناخواسته است که توسط یک برنامه ی دیگر و یا به صورت مستقل با نام های مجازی در سیستم هدف وارد شده و باعث ایجاد تغییرات نامطلوب در عملکرد آن می شود.بنابراین از نظر امنیت رایانه و شبکه های رایانه ای ویروس ها نیز می توانند اختلالاتی در عملکرد سیستم ایجاد نمایند. توانایی ویروس‌های کامپیوتری عبارتند از :

از بین بردن اطلاعات - در اختیار گرفتن منابع سیستم و هدر دادن آن ها - ایجاد صدمات نرم افزاری- ایجاد صدمات سخت افزاری - مختل کردن سیستم عامل و برنامه‌های دیگر (منبع 11)

کارت خوان Card Reader

وسیله ای است که وقتی کارتی که دارای اطلاعات است در آن قرار داده می شود دستگاه آن اطلاعات را خوانده و آن ها را تشخیص می دهد.(منبع 44)

کلید خصوصی رمز Encryption private key

کلید به کار رفته در رمزنگاری کلید عمومی که به یک هویت فردی تعلق دارد و باید به طور سری نگه داشته شود. (منبع 43)

کنترل دستیابی مجاز

ابزاری برای اطمینان یافتن از این که «دسترسی به منابع یک سامانه ی پردازش داده، تنها توسط کاربر های مجاز و به روش های مجاز قابل انجام است». به بیان ساده تر ، یعنی فقط کاربران مجاز بتوانند به داده ها دستیابی داشته باشند.(منبع 43)

کوکی Cookie

یک فایل که به درخواست یک پایگاه وب راه دور، روی دیسک سخت رایانهٔ شما نوشته و یا از روی آن خوانده می شود . پایگاه وب درخواست می کند که فایل نوشته شو د و در دفعات بعد دو باره محتویات آنرا می خواند .در بعضی موارد ممکن است حریم خصوصی کاربران را نقض کنند.

2- واژگان جنگ الکترونیک

اقدامات پشتیبانی الکترونیک Electronic Suport Measures(ESM)

کلیه اقدامات رهگیری ، تعیین موقعیت ، ضبط و ارزیابی و شناسایی انرژی الکترومغناطیس منتشر شده دشمن به منظور شناسایی و کسب اطلاعات از انتشار دهنده و پشتیبانی از عملیات نظامی خودی انجام می گیرد را اقدامات پشتیبانی الکترونیکی یا ESM می گویند .(منبع 12)

اقدامات ضد الکترونیکی Electronic Counter Measures (ECM)

اقدامات متقابل یا ضد الکترونیکی عبارت است از اقداماتی که برای جلوگیری ، درهم گسیختن یا کاهش استفاده دشمن از طیف امواج الکترومغناطیس انجام می شود .(منبع 12)

اقدامات ضد پارازیت ECM

اساسی ترین اقدام جهت مقابله با پارازیت رسانی ایجاد قابلیت انتقال سریع فرکانس (Frequency Agility) در رادار است . در رادارهایی که از این قابلیت بهره مند هستند فرکانس انتشار رادیویی ثابت نیست و بطور مداوم تغییر می کند (منبع 12)

اقدامات ضد ضد الکترونیکی Electronic Counter-Counter Measures

جلوگیری از تضییع انتشاراامواج خودی بوسیله دشمن که به اقدامات ضد- ضد الکترونیک (ECCM) مشهور است . .(منبع 12)

پارازیت اغتشاشی Noise Jamming

در این روش یک سیگنال اغتشاشی که همانند فرکانس رادار هدف می باشد ارسال می شود تا گیرنده رادار را اشباع کند و در نتیجه نمایش دهنده رادار با رنگ سفید یک دست پوشیده می شود . در این حالت کاربر رادار سردرگم می شود و قادر به تشخیص هیچ هدفی نیست . (منبع 12)

پارازیت رسانی الکترونیکی Electronic Jamming

عبارت است از ایجاد تشعشعات و یا تجدید انتشارات عمدی انرژی الکترومغناطیسی جهت مختل نمودن سیستم ها و تجهیزات الکترونیکی دشمن (منبع 12).

جاسوسی سیگنالی Signaling Intelligence

جمع آوری و ضبط اطلاعات حاصل از رهگیری و تجزیه و تحلیل این امواج که ممکن است از سیستم های راداری و تسلیحات وابسته به آنها و یا از سیستم های مخابراتی باشد، جاسوسی سیگنالی می گویند. (منبع 12)

جاسوسی مخابراتی Commiucation Intelligence

جمع آوری و ضبط اطلاعات حاصل از رهگیری و تجزیه و تحلیل این امواج آن بخش از اطلاعات که مربوط به سیستم های مخابراتی است را جاسوسی مخابراتی می گویند (منبع 12)

جنگ الکترونیک Electronic warfare

اقداماتی است جهت کاهش یا ممانعت از بهره برداری دشمن از طیف امواج الکترومغناطیس در عین حال حراست از بهره برداری نیروهای خودی از این طیف .جنگ الکترونیک شامل سه عنصر اصلی زیر است : جنگ الکترونیک فعالECM - اقدامات ضد-ضد الکترونیک ECCM - اقدامات پشتیبانی الکترونیکی ESM (منبع 12)

چف Chaff

چف عبارت است از رشته های فلزی یا پوشش داده شده با فلز که تقریبا نصف طول موج امواج راداری است که قصد فریب آن را دارد و بصورت یک ابر در فضا رها می شود تا انعکاس راداری فریبی فراهم کنند چف های مدرن امروزی از جنس فایبر گلاس یا Mylar است و با روکش آلومینیومی پوشانده می شوند . (منبع 12)

خفیه کاری Stealth

تکنیک های خفیه کاری هنوز بصورت اسنادی با طبقه بندی بسیار سری نگهداری می شوند و اطلاعات فنی بسیار جزئی در این رابطه در دسترس است برای یگانهای هوایی این اقدامات شامل

کاهش سطح مقطع راداری ، کاهش انتشارات حرارتی در محدوده مادون قرمز و ماوراء بنفش و پوشش بدنه با مواد جاذب امواج راداری است. (منبع 12)

ژیروسکوپ Gyroscop

یکی از مسائل مهم در کنترل پرواز موشک و هدایت آن به سمت هدف (یا نقطه مورد نظر) اطلاع از موقعیت پروازی موشک (مسیر پروازی) و میزان حرکت و چرخش در سه محور دوران، سمت و ارتفاع می باشد. اما پس از شلیک موشک با توجه به چرخش کره زمین و حرکت موشک در محورهای سه گانه خود، تعیین و تشخیص میزان انحراف موشک از مختصات و محورهای تعیین شده و مقایسه ی آن با مختصات نقطه ی پرتاب و موقعیت هدف بسیار مهم می باشد. از طرفی امکان انجام این کار و هدایت صحیح موشک بدون وجود یک مبنا و مرجع که همه مختصات با آن سنجیده شود، میسر نمی باشد. ژیروسکوپ یک وسیله ای است که امکان این امر را فراهم می آورد.

سامانه فرماندهی و کنترل C4 I

این اصطلاح به محدوده ای از عملیات و تجهیزات و ساز و برگ نظامی جهت تحت نظر داشتن مداوم موارد مشکوک و حرکات دشمنان، ارتباطات در زمان جنگ و صلح و بهره برداری از امکانات ماهواره های جنگی، ارتباطات رادیویی و راداری ، امکان ایجاد اختلال در ارتباطات دشمن و شناسایی حملات احتمالی و آمادگی برای ضد حملات و استفاده از تجهیزات هدایت کننده عملیات گفته می شود . سامانه های فرماندهی (Command) ، کنترل (Control) ، ارتباطات (Communication) ، کامپیوتر (Computer) و اطلاعات نظامی (Intelligence) » یا C4I نامیده می شود. (منبع 29)

سیستم هدایت موشک Missile guidance system

منظور از سیستم های هدایت، چگونگی دریافت یا ارسال فرامین به موشک به منظور تصحیح خطا

و هدایت به سمت مسیر اصلی می باشد. تمامی انواع موشک های هدایت شونده (با هر نوع سیستم هدایتی) دارای سیستم حلقه بسته کنترل می باشند.

سیستم هدایت ناوبری با GPS GPS Navigational guidance

این سیستم هدایت بر اساس اطلاعات دریافتی از GPS استوار می باشد.GPS با دریافت اطلاعات از حداقل 4 ماهواره و انجام محاسبات لازم، موقعیت نقطه ی استقرار خود را با دقت بالا تعیین می نماید.با نصب سیستم GPS در موشک های هدایت شونده (بالستیک، کروز) کامپیوتر موشک، موقعیت دقیق موشک را محاسبه و آنرا در مسیر صحیح هدایت می کند.

فریب الکترونیک فعال Active Electronic Deception

با استفاده از پارازیت و نویز می توان تعداد زیادی هدف کاذب الکترونیکی در اطراف یگان دشمن ایجاد نمود و کاربر رادار را که سعی در انتخاب هدف برای شلیک سلاح دارد را گیج نمود . حضور این اهداف الکترونیکی کاذب در نمایش دهنده رادار حالتی کاملا حقیقی دارد و اپراتور یا کنترل کننده رادار را سردرگم خواهد کرد . (منبع 12)

فریب الکترونیکی غیر فعال Passive Electronic Deception

استفاده از فریب دهنده ها (Decoys) بخشی دیگر از اقدامات ضد الکترونیک فریبی است پس از دریافت هشدار حمله حتمی یک موشک ، یگان مدافع شروع به پراکندن الگویی از فریب دهنده های مختلف پیرامون خود می کند که به این ترتیب یگان حمله کننده تعدادی هدف را به شکل گروهی مشاهده می کند مهمترین فریب دهنده ها عبارتند از :1- چف یا باریکه (Chaff) برای فریب راداری 2- فلیر (Flare) برای فریب مادون قرمز 3- فریب دهنده های سه کنج. (منبع 12)

فریب تقلیدی Imitative Deception

عبارت است از پخش و ارسال انتشارات روی کانال دشمن به گونه ای که انتشارات خود دشمن تقلید شود . (منبع 12)

فریب جعلی Manipulative Deception

عبارت است از تغییر و یا وانمود سازی انتشارات الکترومغناطیسی خودی به منظور فریب دشمن. (منبع 12)

فریب دهنده فلیر Flare deceptor

رایج ترین اقدام مقابله برای فریب جستجوگر مادون قرمز استفاده از نوعی فریب دهنده به نام شراره یا فلیر (Flare) است که پس از پرتاب مشتعل شده و منبع حرارتی جذاب تری را برای موشکی که در حال حمله است فراهم می نماید . (منبع 12)

فریب دهنده های سه کنج Triangle deceptor

انعکاس دهنده های یکی دیگر از وسایل منعکس کننده امواج الکترومغناطیس هستند که از سطوح صیقلی تخت به شکل هرم ساخته می شوند و علی رغم کوچک بودن سطح انعکاس راداری بزرگی دارند و مقدار زیادی از انرژی رادار را پس از دریافت منعکس می نمایند . این وسایل پس از پرتاب در هوا چرخش و نوسان نموده و روی صفحه رادار بصورت یک هدف متحرک بسیار بزرگ ظاهر می شوند (منبع 12)

فریب مخابراتی تقلیدی Simulative Communication Deception

عبارت است از وارد شدن به سیستم مخابراتی دشمن و تقلید کردن انتشارات جهت گمراه کردن کاربر مخابرات و یا مختل کردن سیستم های مخابراتی. انواع تکنیک های فریب تقلیدی مخابراتی عبارتند از: 1- اختلالات در سیستم ترافیک 2- قطع متناوب پیام 3- مختل نمودن مدار کنترل فرکانس اتوماتیک (AFC) و... (منبع 12)

فریب مخابراتی جعلی imitation Communication Deception

در اقدامات فریب جعلی باید فعالیت نیروهای خودی و دوست را که فرضی بوده و وجود خارجی ندارند به روشهای زیر به تصویر بکشیم :

- ناوی که در ساحل و یا بندر است می تواند روی مدار عملیاتی و یا اجرای پیام های رد و بدلی وانمود کند که در حال شرکت در عملیات است . (منبع 12)

فریب الکترونیکی Electronic Deception

عبارت است از ایجاد تشعشعات ، تغییر جهت ، جذب ، انعکاس و پخش مجدد انرژی الکترومغناطیسی بطور عمدی به گونه ای که دشمن را در تفسیر و بکار بردن اطلاعات دریافتی از طریق سیستم های الکترونیکی مربوطه گمراه نماید (منبع 12)

کاهش امکان شناسایی رادار Radar detecting reduction

کاهش امکان شناسایی رادار دربرگیرنده اقداماتی است که مانع دسترسی دشمن به اطلاعات هدف

می‌گردد. این اقدامات عبارتنداز: استتار، کاهش سطح صدا، کاهش میزان حرارت، تقلیل سیگنال‌های الکترومغناطیس، استتار از دید رادار و ابزارهای استتار

کاهش سطح مقطع راداری Reduction of radar cross section (RCS)

هدف از آن به حداقل رساندن انرژی امواج انعکاسی رادار دشمن و انحراف امواج بازگشتی در راستای نامناسب می باشد . به این منظور اقداماتی انجام می شود که مهمترین آنها به شرح زیر می باشد:

1-مخفی نمودن تسلیحات درون دهلیزهایی داخل بدنه شناور و یا هواپیما

2-انتقال دادن تجهیزات از قبیل آنتن رادارها به داخل بدنه . ,...

موشک هدایت شونده Guidance missile

موشکی است که اطلاعات نقطه ی پرتاب و اطلاعات نقطه ی اصابت (هدف) و مسیری را که باید طی کند دریافت کرده و به سمت هدف پرواز می کند.

هدایت ناوبری Navigational guidance

مشخصه اصلی هدایت ناوبری اینست که موشک، کامپیوتر هدایت و اطلاعات مربوط به موقعیت موشک را که از تجهیزات یا سنسورهای مربوطه (درون موشک) بدست می آید را درون و همراه خود حمل می کند. اگرچه در مورد اهداف متحرک نیز سیستم هدایت ناوبری بکارگیری می شود که این حالت تا فاز هدایت نهایی ادامه می یابد.رایج ترین نوع هدایت ناوبری (NG)، هدایت اینرسی می باشد دو نمونه زیر مجموعه هدایت ناوبری عبارتند از : هدایت ناوبری صفحه پایدار (stable table) و **هدایت ناوبری اینرسی** strap down . (منبع 38)

هدایت هومینگ غیرفعال Passive Homing

اساس هدایت غیر فعال بر دریافت انرژی طبیعی که از هدف منتشر یا منعکس می شود، قرار دارد. سنسور (حساسه) درون موشک از این انرژی جهت ردیابی و تعقیب هدف استفاده می نماید.مانند موشک های ضد رادار (که از تشعشع صادر شده از رادار جهت هدف یابی و انهدام آنها استفاده می کند) . (منبع 38)

هدایت هومینگ فعال Active Homing

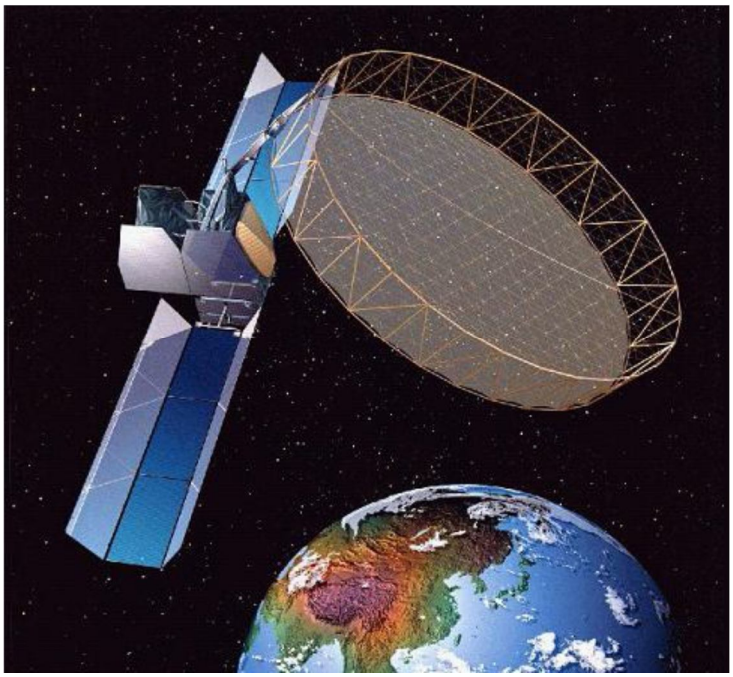
یک سیستم هدایت آشیانه یاب فعال، دارای منبع انرژی داخلی در موشک می باشد بخش فرستنده امواج راداری را به سمت هدف ارسال می نماید. این امواج پس از برخورد به هدف (هواپیما، یا ...) منعکس شده و بخشی از امواج برگشتی توسط آنتن و گیرنده موشک دریافت می گردد. (منبع 38)

فصل سوم
واژگان اطلاعات، امنیت و تهدیدات نرم
(جنگ روانی، رسانه و...)

۱- واژگان اطلاعات،امنیت

۲- واژگان تهدیدات نرم(جنگ روانی، رسانه و...)

۳- واژگان فرهنگی



1- واژگان اطلاعات و امنیت

ارزیابی آسیب پذیری امنیتی

فرآیند ارزیابی آسیب پذیری امنیتی، متدولوژی مبتنی بر ریسک و اجرا می باشد. کاربر می تواند مفاهیم مختلفی از شکل گیری روش کلی ارزیابی آسیب پذیری امنیتی را بر اساس ضوابط اجرایی انتخاب نماید. راه حل 5 مرحله ای متدولوژی ارزیابی آسیب پذیری امنیتی به شرح زیر می باشد:

مرحله 1: شناسایی زیرساخت - مرحله 2: ارزیابی تهدید - مرحله 3 : تحلیل آسیب‌پذیری- مرحله 4: ارزیابی ریسک مرحله 5: تحلیل اقدامات پدافند غیرعامل و مدیریت بحران در زیرساخت

استراتژی Strategy

استراتژی(راهبرد) مجموعه برنامه‌های کلی و جامعی است که با توجه به منابع و امکانات سازمان، طریق نیل به آرمان ها و اهداف عالی سازمان را معین می‌سازد.«دکتر سیدمهدی الوانی»

راهبرد عبارت است از برنامه جامع و کاملی که بر مبنای آن نیل به اهداف اساسی سازمان تضمین می گردد.«دکتر علی رضائیان»

استراتژی ملی National Strategy

علم و هنر بکارگیری قدرت ملی تحت هر شرایطی جهت پشتیبانی از سیاست‌ها و اهداف ملی.

استراتژی نظامی Military Strategy

هنر و علم بکارگیری نیروهای مسلح یک کشور به منظور نیل به اهداف سیاسی ملی از طریق کاربرد زور یا تهدید به زور. (منبع 28)

استراق سمع Overhear

استراق سمع می تواند از طریق خطوط تلفن (شنود از طریق کابل)، پست الکترونیکی، پیام های لحظه ای، و هر نوع روش ارتباطات که خصوصی محسوب می شود، انجام گردد. می توان با بکارگیری یک سرویس امنیت حریم خصوصی، از استراق سمع پیام ها جلوگیری کرد. (منبع 23)

اصول ضد شناسایی Reconnaissance Counter Tenets

درک این واقعیت که دشمن با بهره‌گیری از توان بالای اطلاعاتی و روش های مدرن شناسایی، قابلیت آن را دارد که فعالیت های ما را سریعاً مورد شناسایی قرار دهد، ما را بر آن می‌دارد که هر چه بیشتر و بهتر به شناخت روش ها، تاکتیک ها و مسائل شناسایی دشمن همت گماریم و در حفظ اطلاعات خویش نیز کوشا باشیم.این اصول عبارتند از:

(1) عملیات ضد شناسایی تنظیم و توجیه شود. (2) عناصر شناسایی دشمن، کشف و خنثی شوند. (3) نیروهای پردهء پوشش در عمق، رده‌بندی شوند. (منبع 33)

اطلاعات راهبردی Strategic Information

دانستنی هایی است مربوط به مقدورات، آسیب‌پذیری ها، راه کار های احتمالی کشورهای خارجی که مورد استفاده تعیین‌کنندگان خط‌مشی کلی یک مملکت و یا مسئولین طرح‌ریزی اقدامات امنیت کشور در زمان صلح و یا هدایت عملیات نظامی در زمان جنگ را فرا می‌گیرد. این اطلاعات در مورد کلیه کشورها جمع‌آوری شده و با داشتن آنها می توان قدرت نظامی کشورهای دوست و متفق و یا متخاصم را برآورد نموده و در موقع لزوم از آن بهره‌برداری کنیم.(منبع 28)

اطلاعات امنیتی خارجی Outsider Security Information

اطلاعات امنیتی خارجی معمولاً در خارج از قلمرو حاکمیتی یک کشور به دنبال اهداف، روش ها و شیوه‌های کاری سازمان های اطلاعاتی و امنیتی یا سازمان های جاسوسی سایر کشورها با اولویت دشمن، حریف و هدف می‌باشد.(منبع 35)

اطلاعات امنیتی داخلی Insider Security Information

اطلاعات امنیتی داخلی در صحنه داخل مرزهای یک کشور فعال می‌باشد. این نوع سازمان ها در اولویت اول به دنبال اهداف اطلاعاتی و امنیتی در ارتباط با گروه های معاند و مخالف نظام و سیستم حکومتی و در اولویت دوم به دنبال کنترل اقشار و صنوف جامعه، گروه ها و احزاب رسمی، کنترل شخصیت های حکومتی، جلوگیری از نفوذ بیگانگان و جاسوسان به داخل نظام حکومتی و ... می‌باشد .(منبع 35)

اطلاعات رزمی Military intelligence

اطلاعات رزمی (اطلاعات تاکتیکی) پیرامون سه موضوع جو، زمین و دشمن جمع‌آوری اطلاعات دارد. در جو موضوعات گوناگونی از قبیل شرایط آب و هوایی منطقه عملیات، درجه حرارت، فشار، باد (جهت، سرعت و میزان)، روشنایی، طلوع و غروب آفتاب و ماه و ... بحث می شود. (منبع 35)

اطلاعات نظامی Martail information

اطلاعات نظامی بر اساس قلمرو و کاربرد صحنهٔ عمل و سطوح جنگ به سه دستهٔ اطلاعات استراتژیکی، عملیاتی و تاکتیکی طبقه‌بندی می‌گردد. اطلاعات استراتژیکی برای برنامه‌ریزی در وسیعترین سطح یک کشور و یا سطوح بالاتر (یعنی سطح بین‌المللی) به کار می‌آید. اطلاعات عملیاتی برای برنامه‌ریزی در چارچوب صحنه جنگ در داخل یک کشور به کار می‌آید. اطلاعات تاکتیکی که گاه از آن به عنوان «اطلاعات رزمی» نیز یاد می‌شود، بر برنامه‌ریزی و هدایت نبرد در صحنه محدودی از یک جنگ تمرکز دارد.(منبع 35)

اقدام پنهان Secret Action

اقدام پنهان، در فرهنگ لغت اطلاعاتی ، عبارت از تلاش یک کشور در دنبال نمودن اهداف سیاست خارجی خود، از طریق انجام برخی اقدامات مخفیانه به منظور تأثیرگذاری بر رفتار کشور دیگر یا تأثیر بر حوادث و شرایط سیاسی، نظامی، اقتصادی و اجتماعی آن است. (منبع 36)

اقدامات جاسوسی intelligence Measures

جمع آوری اطلاعات و فعالیت های حفاظتی مربوط به آن مانند :جاسوسی و فعالیت های زیرکانه دیگر، خرابکاری یا ترور افراد مهم؛یا فعالیت های خرابکانه تروریستی در مورد مقامات کشورها.

اقدامات ضد امنیتی

اقدامات ضد امنیت را می‌توان به اقدامات ضد امنیتی خارجی و داخلی تقسیم کرد اما گاهی کشیدن مرز بین اقدامات ضد امنیتی خارجی و اقدامات ضد امنیتی داخلی و تعیین این که فلان اقدام دقیقاً خارجی است یا داخلی، کار دشواری است . با این حال برخی از اقدامات ضد امنیتی را می‌توان خارجی تلقی کرد حتی اگر از زمینه‌های داخلی استفاده شود از آن جمله می‌توان از اقدامات نظامی یا مداخله نظامی و تبلیغات نام برد. در مقابل، ضعف بنیان‌های اقتصادی و بی ثباتی سیاسی و اجتماعی را می‌توان در درجه‌ی اول در زمره اقدامات ضد امنیتی داخلی محسوب داشت. (منبع 28)

اقدامات ضد تروریستی Antiterrorism Measures

اقدامات پیشگیرانه برای کاهش آسیب پذیری اشخاص، نیروها و اموال از حملات تروریستی.(منبع 44)

امنیت خارجی Outsider security

به مجموعه توانایی های یک کشور اعم از سیاسی، اجتماعی، فرهنگی، اقتصادی، جغرافیایی، نظامی

و در حفظ تمامیت ارضی اقتدار و حاکمیت ملی، استقلال سیاسی در مقابل تهدیدات خـارجی در حضور منطقی و مناسب در عرصهٔ بین‌المللی بیان می‌شود. (منبع 28)

امنیت داخلی Insider security

به توانایی دولت یـا حکومـت جهـت برقـرار نمـودن نظـم، قـانون، آرامـش و بـرآوردن نیازهـا و خواسته‌های منطقی مردم کشور گفته می شود..(منبع 28)

امنیت عملیات Operation Security

عبارت است از اقداماتی که به منظور حفظ امنیت و افـزایش تـوان غـافلگیری تـاکتیکی صـورت می‌پذیرند. این اقدامات شامل امنیت اطلاعات مخابره شـونده، کـاهش امکـان شناسـایی بـر روی رادار، امنیت فیزیکی و اطلاعات می‌باشد. امنیت عملیات هم چنین شناسایی، حفظ یا کنترل شاخص‌هایی کـه ممکن‌است توسط سازمان‌های جاسوسی دشمن مورد استفاده قرارگیرند را نیز در بر می گیرد (منبع 23)

امنیت اطلاعات Information security

اصطلاحی که به تضمین امنیت، نه تنها در سیستم های اطلاعات، بلکه در تمام جوانب حفاظتی بـر تمام انواع اطلاعات دلالت دارد. (منبع 23)

امنیت فیزیکی Physical security

سیستم های امنیتی و مشخصات معماری که بهبود سیستم های حفاظتی را سبب مـی شـود. بطـور مثال: شامل حصار کشی، درها، دروازه ها، دیوارها، گردان درها، قفل ها، ردیـاب هـای حرکتـی، موانـع وسیله نقلیه و شیشه های سخت شده.(منبع 22)

اهداف تدافعی Defence goals

اهداف تدافعی به آن دسته از اهدافی گفته می‌شود که دشمن یا حریف، همواره به دنبال ضـربه زدن به این اهداف یا شناخت نقاط آسیب‌پذیر آن است. در صورتی که اینگونه اهداف مورد تعـرض دشـمن قرار بگیرند، به امنیت و منافع ملی در ابعاد مختلف سیاسی، اجتمـاعی- فرهنگـی، اقتصـادی، نظـامی و اطلاعاتی خدشه وارد می‌شود. مثل: تأمین امنیت ملی کشور .(منبع 35)

اهداف تهاجمی Attack goals

به آن دسته از اهداف گفته می‌شود که از دشمن یا حریف مورد شناسایی قرار می‌گیرد تا در هنگـام لزوم بتوان بر او ضربه زد. این قبیل اهداف در کشورها به ترتیب اولویت دشـمنی آن هـا بـا مـا، مـورد

جمع‌آوری اطلاعات قرار می‌گیرد تا بتوان با شناخت دقیق از آسیب‌پـذیری هـا، بـر او هجـوم نمـوده و موجب شکست آن کشور شد.(منبع 35)

برآورد اطلاعات استراتژیکی Estrategy Informations Estimat

برآورد تهدیدات داخلی و خارجی، تعیین ضعف ها، آسیب پذیری ها، قابلیت ها و توانایی‌های ملی و بهره گیری از فرصت هـای موجـود در عرصـه داخلـی وخـارجی، مسـتلزم تهیـه بـرآورد اطلاعـات استراتژیکی از محیط ملی و محیط بین المللی است. برآورد اطلاعات استراتژیک به عنوان پایه و اساس تهیه خط مشی ها و طرح های ملی (سیاسی، اقتصادی، اجتماعی و فرهنگی و نظامی) یک کشور به کار می رود.(منبع 36)

برخورد با اقدامات تروریستی Counterterrorism

جلوگیری ،حفاظت برای پاسخ به اقدامات تروریستی.

پرورش اخبار News nurture

پرورش اخبار یکی از مهمترین مراحل مدار اطلاعاتی است که طی آن اخبـار بـه اطلاعـات تبـدیل می گردد. پرورش اخبار در سه مرحله صورت می گیرد: ثبت اخبار - ارزیابی- تفسیر (منبع 35)

پنهان نگاری Steganography

به طور کلی، این فرایند پنهان کردن اطلاعات یا « پوشیده نوشتن» است. به شکل تخصصی تـر، در محیط دیجیتال، پنهان نگاری شامل داده ها یا عکس های پنهان در فایل های دیگر است به طوریکـه از منظر افرادی که از مضمون سری (مخفیانه) آنها بی اطلاعند، بدون تغییر به نظر می رسند. (منبع 23)

تجهیزات بدون سرنشین دریایی Equipment of Without Director

تجهیزات آبی خودکار یا کنترل از راه دور می‌باشند که می‌توانند بر روی آب شناور باقی بمانند. این وسایل بدون سرنشین طولی حدود 1/5 تا 16 متر و وزنی در حدود 450 الی 900 کیلوگرم دارند.از این شناورها می‌توان برای جستجو و نقشه‌برداری دریایی و عملیات اقیانوس‌شناسی اسـتفاده کـرد. ایـن دستگاه ها دارای تجهیزات صوتی و تصویری و سیستم ممانعت از برخورد با مانع می‌باشد.(منبع 33)

تروریست حرفه‌ای Vocation terrorism

تروریست حرفه‌ای کسی است کـه تـرور، شـغل و حرفـهٔ وی محسـوب مـی‌شـود. ایـن دسـته از تروریست ها بسیار خطرناک هستند و دارای روش کار مخصوص به خود مـی‌باشـند. تروریسـت هـای حرفه‌ای بر دو دسته‌اند. دستهٔ اول این افراد، عموماً یا عضو سـرویس هـای اطلاعـاتی برخـی کشـورها هستند یا از پشتیبانی این سازمان ها برخوردارند و به صورت مقطعی برای آنها مأموریت انجام می‌دهند. (منبع 35)

تروریسم جهانی Global Terrorism

اهداف آن بین المللی است و مجریان آن در نقاط مختلف دنیا می‌توانند به شکل زنجیره ای، بـرای نیل بـه اهـدافی مشـترک تـلاش کـرده، از آخـرین پیشـرفت‌هـای فنـاوری در کسـب اطلاعـات بهـره گیرند.تروریست‌های بین المللی از روش های به دقت طراحی و سازماندهی شده استفاده می‌کنند. آنهـا دارای ارتباطی گسترده با سازمان های جنایتکار مختلف بوده و از طرف آنها حمایت مالی می‌شوند. این گروه‌ها به دنبال ایجاد حداکثر تخریب ممکن به منظور جلب نظر رسانه‌ها بـرای گسـترش وحشـت در میان مردم هستند. بارزترین نمونه این گروه‌ها، سازمان القاعده به رهبری اسامه بن لادن است. (منبع 14)

تروریسم ناسیونالیستی Nationalist terrorism

عاملان این نوع تروریسم، افراد یا گروه‌هایی با ایده و اهداف استقلال طلبی متعصـبانه هسـتند کـه گاهی خواستار ایالتی خود مختار یا در دسـت گـرفتن کنتـرل منطقـه ای خـاص و در مـواردی در پـی سرنگونی دولت یک کشور یا براندازی کامل یک رژیم سیاسی به منظور جایگزینی آن با رژیمی دیگر و یا صرفاً روی کارآوردن رژیمی دیگر هستند. (منبع 14)

تهدیدات اجتماعی و فرهنگی Cultueral & social Threats

تهدیداتی هستند که به صورت رفتارهای جمعی ،مبتنی بر باورها و یا واکنش های فرهنگی در یک جامعه یا اجتماع معین در زمان و یا مکان معین بصورت رفتار های مغایر با ارزش های حاکم بر جامعه بروز می کند. مثال: (1) خود باختگی: یعنی اینکه انسان‌ها آداب و سنن کشور و ملت خود را فرامـوش کنند و تحت تأثیر و فرهنگ بیگانگان قرار گیرند (2)تبعیض نژادی و اختلاف قومی، مذهبی (منبع 28)

تهدیدات اقتصادی Economic Threats

خطراتی که رشد و توسعه پایدار اقتصاد جامعه را به هر نحوی مختل سازد مثل تحریم ، رکود و ...

یا به موازات رشد جمعیت در یک کشور ، چنانچه توسعه اقتصادی متوازن نباشد و مسئولین آن کشور هم قادر به پاسخگویی مردم نشوند، جامعه با تهدید اقتصادی مواجه خواهد شد. (منبع 28)

تهدیدات سایبری آب Water syber Threats

اختلال فیزیکی در یک شبکه کنترل نظارتی و جمع آوری داده - حمله به یک سامانه کنترل مرکزی با ایجاد تخریب های همزمان - حملات الکترونیکی با استفاده از کرم ها یا ویروس ها - انسداد شبکه - اطلاعات فریبنده برای از بین بردن اثر کلر یا اضافه نکردن مواد گندزدا برای فراهم کردن شرایط رشد میکروب ها.

تهدیدات سیاسی Politic Threats

عوامل سیاسی که عبارت است ازنوع، ماهیت، روش و نحوه برقراری و اداره کشور از نظر قانون اساسی و قوای سه گانه(مجریه، مقننه، قضائیه)می‌باشد، ممکن است در یک کشور عوامل زیر مورد تهدید قرار بگیرد.(1) حکومت از نظر نحوه اداره (2) حکومت از نظر نحوه برقراری (منبع 28)

تهدیدات فرامنطقه‌ای Transterritorial Threats

برخی مواقع امنیت یک کشور از سوی قدرت‌های جهانی تهدید می‌شود، این تهدید اغلب به بهانه حمایت از متحد یا متحدین این قدرت‌ها و در قالب یک ائتلاف نظامی، امنیتی و بیشتر تحت عنوان حفظ امنیت جهانی و بین‌المللی و مقابله با ناامنی صورت می‌گیرد مثل : حضور نظامی امریکا در منطقه خلیج فارس به بهانه دفاع از کشورهای هم پیمان خود (منبع 28)

جاسوسی Intelligence

عمل تجسس با بدست آوردن اسرار محرمانه از دشمنان یا رقبا برای رسیدن به مقاصد نظامی، سیاسی یا تجاری. پیشرفت های رخ داده در فناوری اطلاعات و توسعه و تکامل ابزار ذخیره سازی کوچک و پنهان به مخاطرات جاسوسی به شکل قابل ملاحظه ای افزوده اند(منبع 22)

جرائم سازمان یافته Organaze Crimes

فعالیت های غیر قانونی که توسط سازمان های خلاف کار رسمی بصورت سیستماتیک انجام می شود. فناوری اطلاعات پیشرفته اشکال بدیهی از جرائم سایبری سازمان یافته را تعریف می نماید.(منبع 23)

جمع‌آوری پنهانی Secret Collection

منظور جمع‌آوری اخباری است که حریف می‌خواهد آنها را مخفی نگه‌داشته و به وسیله اقدامات مختلف حفاظتی از آن حفاظت کند.

جمع‌آوری اخبار به دو صورت آشکار (جراید، صدا و سیما و....) و پنهانی (مواردی که در دسترس عده ای خاص است) انجام می‌گیرد. (منبع 36)

جنگ اطلاعات Information warfare

جنگ اطلاعاتی یک نوع درگیری‌های نظامی است که سیستم‌های اطلاعاتی به طور مستقیم یا غیرمستقیم مورد تهاجم واقع شده یا از آنها دفاع می‌شود تا بدین ترتیب داده‌ها، دانش، باورها یا پتانسیل جنگجوئی دشمن افت کرده یا کاملاً نابود شود و در عین حال داده‌ها، دانش، باورها، و میل جنگجوئی نیروهای خودی حفظ شود. (منبع 5)

جنگ محیطی Invironment warfare

جنگ محیطی، جنگی است که در آن محیط به منظور اهداف نظامی و خصومت آمیز دست کاری می شود. جنگ محیطی شامل آسیب های وارد شده در اثر دست کاری های ایجاد شده در حوزه های اتمسفر –لیتوسفر و .... است .

برای مثال آتش سوزی های نفتی یک فاجعه اکولوژیکی بود که شاید بتوان آن را بعد از حادثه چرنوبیل از بزرگترین و مهمترین فجایع اکولوژیکی محسوب نمود که تاثیر بسیار زیادی در تخریب اکوسیستم ، آلودگی آب های جاری و زیر زمینی و از بین رفتن گونه های گیاهی به عهده داشت. (منبع 14)

حریم امنیتی Security sanctum

عبارت است از محدوده و منطقه ی بعد از حریم حفاظتی که در آن امنیت مورد نیاز جهت استقرار اهداف دفاعی و حفاظتی تأمین می گردد.

حریم ایمنی Safty sanctum

عبارت است از محدوده ی داخلی یک مجموعه ی حفاظت شده که می بایست استاندارد ایمنی و حفاظتی در آن رعایت گردد.

حریم حفاظتی Protection sanctum

عبارت است از محدوده خارجی و پیرامونی یک مجموعه حفاظت شده که اقـدامات تـامین در آن، به منظور مراقبت و حراست از اهداف حفاظتی و ممانعت از ورود عناصر غیـر مجـاز بـه مرحلـه اجـرا گذارده می شود (منبع 12)

حمله مهندسی اجتماعی Social engineering attack

روش به دست آوردن اطلاعات محرمانه با استفاده از کاربرا ن مجاز. یک مهندس اجتماعی به طور کلی از تلفن و اینترنت برای فریب یک شخص جهت آشکار کردن اطلاعات حساس استفاده می کند یا آنها را وادار به انجام کاری می کند که مخالف قوانین اداری باشد. (منبع 23)

دکترین Doctorin

عبارتست از اصول اساسی است که نیروهای مسلح یا عناصر تابعه اقدامات خود را در پشـتیبانی از هدف های ملی بر مبنای این اصول هدایت می‌نمایند. (منبع 28)

دکترین نظامی Military Doctorin

دکترین نظامی عبارت است از بیان نظریات پذیرفته شده دولت در رابطه با مسائل مربوط به ارزیابی سیاسی جنگ آینده. محتوا و ماهیت دکترین نظامی یک کشور تا اندازه‌ای متأثر از وضـعیت جغرافیـایی، ویژگی‌های ملی مردم، اقتصادی، سیاسی و همچنین موضعگیری‌های دول همسایه و روابط متقابل با آنها می باشد. (منبع 28)

دیپلماسی عمومی public diplomacy

عبارت است از کاربرد ابزارهای بین فرهنگی وارتباطات بـین المللـی در سیاسـت خـارجی، و بـه عبارتی " برنامه های مورد حمایت دولت " . (منبع 16)

زیرساخت های حیاتی Critical Infrastructure

سیستم ها و دارایی های فیزیکی یا مجازی، برای کشور بسیار حیاتی است که فقـدان یـا تخریـب چنین سیستم ها و دارایی ها اثرات زیادی بر امنیت، امنیت و اقتصاد ملی، امنیـت و سـلامت عمـومی و هرگونه ترکیبی از این موارد را دارد.(منبع 22)

سنسور سیم خاردار Grid-Wire Sensor

سنسوری شامل سیم های الکتریکی پیوسته که به یکدیگر متصل شده اند.از سیم ها یک جریان الکتریکی عبور می کند و وقتی که جریان سیم ها قطع می شود سنسور آن را تشخیص می دهد.این سنسورها نیروهای ورودی به دیوارها،درها،پنجره ها،سقف ها،و قسمت های دیگر را می توانند تشخیص دهند.

سنسور فیبر نوری Optical fiber Sensor

سنسوری که به تغییر و کشش در فیبرهای نوری حساس است.اما این سنسور بیشتر روی سیگنال های الکتریکی که از فیبرهای نوری ایجاد می شود، حساس است و تغییر در این سیگنال ها توسط سنسور تشخیص داده می شوند.

سیاست امنیتی Security policy

عبارتی است که مشتمل بر تمامی مقررات، قوانین ، روش ها، و تمریناتی که یک سازمان برای برقراری و حفظ قابلیت اعتماد و امنیت اطلاعات با آنها سروکار دارد، می باشد. (منبع 23)

سیستم مدیریت صحنه نبرد Combat management system

سیستم عامل نرم افزاری- مغز افزاری مدیریت در صحنه نبرد را می توان C4I گفت ،که زمینه برتری اطلاعاتی و شناختی را از طریق تعامل پذیری و شبکه سازی تمام عناصر اطلاعاتی و دانشی دخیل در فرماندهی وکنترل فراهم آورده وامکان برقراری ارتباطی سالم و امن در بهترین زمان ممکن بین نیروهای صحنه نبرد و فرماندهی را ایجاد می کند تا تصویر همه جانبه ای از فضای نبرد پدیدارشده و مدیریت جبهه امکان پذیر گردد.

شبکه جاسوسی اشلون Ashlon Spy Network

اشلون نام اختصاری یک سیستم نظارت جهانی بر ارتباطات بین المللی است، پنج کشور امریکا ،انگلیس، کانادا، استرالیا و نیوزلند عضو این شبکه عظیم جاسوسی الکترونیکی در جهان هستند. شبکه اشلون حدود 120 ماهواره ارتباطی ، اکتشافی و نظارت، در مدار های ثابت دور زمین دارد. شنود همه وسایل ارتباطی اعم از انواع تلفن ، فکس ، اینترنت و ایمیل در سطح جهانی جزء مأموریت های این شبکه است. اطلاعات به دست آمده به حافظه مدرن ترین رایانه های قوی در امریکا ارسال می شود.این اطلاعات از «دیکشنری های اشلون» عبور کرده که شامل پایگاه داده کلمات کلیدی مرتب است.

تجهیزات ویژه اشلون قادر است بطور خودکار اطلاعات دریـافتی را طبقـه بنـدی و پـردازش نمـوده و گزارش تهیه نمایید.سیستم نظارت جهانی بر ارتباطات موسوم به اشلون را آژانس امنیـت ملـی امریکـا اداره می کند.(منبع 43)

شناسایی روی نقشه reconnaissance in map

این نوع شناسایی یکی از روش هـای سـریع و قابـل دسـترس مـی‌باشـد کـه طـی آن بـا بررسـی نقشه،مواضع دشمن و خودی، جاده‌ها، معابر وصولی، نحوهٔ گسترش و... را مشخص نموده و تصـویری از نحوهٔ گسترش نیروهای خودی و دشمن را مشخص می‌نماید. (منبع 33)

شنودهای زیرآبی under water sonics

تجهیزات شنود زیرآبی در کف اغلب دریاهای جهان مستقر گردیـده‌انـد. معبرهـا و گـذرگاه هـای حساس دریایی زیر پوشش کامل اینگونه تجهیزات می‌باشند. این سیسـتم هـا ضـمن ارسـال اطلاعـات مربوط به عبور زیردریایی‌ها و کشـتی هـا در زمینـهٔ مطالعـات سـاختاری دریاهـا نیـز فعـال و کارآمـد می‌باشند.(منبع 33)

ضد اطلاعات Counter- intelligence

شامل کلیه اقداماتی است که به منظور مقابله و مبارزه با فعالیت های سازمان های اطلاعاتی حریف انجام می‌پذیرد (ضد جاسوس و....). (منبع 36)

طرح‌ریزی Planning

طرح‌ریزی عبارت از ترسیم و تصویر دورنمای آینده سازمان است یا تلاشی هدایت شده به سـوی جهتی خاص است.

طرح‌ریزی شامل اقدامات مداوم در خصوص پرسنل، اطلاعات، لجستیک و عملیات مـی‌باشـد کـه معمولاً قبل از انجام عملیات و گاهی هنگام عملیات صورت می‌پذیرد. (منبع 36)

عملیات پنهان سیاسی Poletic cryptic operation

عملیات پنهان سیاسی نیز یکی از طرق نفوذ کشوری در کشور دیگر و خدشه‌دار کـردن حاکمیـت ملی آن کشور و احیاناً به خطر انداختن امنیت ملی آن است. عملیات پنهان سیاسی اشکال مختلفی دارد

که برخی از آنها ممکن است امنیت یک کشور را به طور جدی تهدید کند. از جمله عملیات پنهان سیاسی بیشتر شیوه تطمیع دولتمردان یک کشور، فعالیت تبلیغاتی مخفی و ترور رهبران سیاسی کشور مورد نظر را می‌توان نام برد.(منبع 28)

عملیات اطلاعاتی information operation

عملیات اطلاعاتی عبارت است از هر گونه اقدامی که برای پشتیبانی از اهداف سیاسی و نظامی انجام می‌شود و از طریق تأثیرگذاری بر اطلاعات دشمن و بهره برداری و حفاظت کامل از اطلاعات خودی، تصمیم‌گیران را تحت تأثیر قرار می دهد. (منبع 11)

فیبر نوری Optical fiber

کابلی برای انتقال اطلاعات به وسیله عبور و شکست نور از درون رشته های پلاستیکی شفاف یا شیشه ای.

قدرت نرم Soft power

قدرت نرم، استفاده‌ی بهینه از فناوری‌های نرم در صحنه ی نبرد جهت تسلط بر اوضاع و کنترل صحیح نیروها و ابزارآلات نظامی و دفاعی است به گونه‌ای که در سایه‌ی اثربخشی این فناوری‌های نرم ،توازن قوا را به سود خود و علیه دشمنان بر هم زده و به کیفیتی دست یابیم که موازنه‌ی قوا بر مبنای "قدرت نرم" به شیوه‌ای دلخواه فراهم آید. (منبع 11)

مؤلفه‌های امنیت ملی National security implemens

مؤلفه‌ها عبارتند از :

مؤلفه سیاسی : منظور از مؤلفه سیاسی در شکل گیری امنیت ملی بیان نوع نظام، حکومت، قانون اساسی، شیوهٔ اداره و هدایت کشور، سیاست گذاری در جهات مختلف، روابط و سیاست داخلی و خارجی می‌باشد چنانچه نظام سیاسی یک مملکت مورد حمایت و پشتیبانی مردم باشد و پیوندی عمیق و اساسی بین مردم و هیئت دولت برقرار گردد.

- مؤلفه اجتماعی و فرهنگی : عواملی که در مؤلفه اجتماعی و فرهنگی نقش اساسی داشته و موجب استقرار امنیت ملی در یک کشور می‌شود عبارتند از :جمعیت - وحدت ملی و انسجام - روحیه ملی- ایدئولوژی - ارزش‌های دینی و مذهبی (منبع 28)

مدیریت امنیت اطلاعات Information Security Management

مدیریت امنیت فضای تبادل اطلاعات یکی از مدیریت‌های سازمان ها و شرکت ها خواهد بود که مسؤولیت حفظ امنیت فضای تبادل اطلاعات (رایانه‌ای و غیر رایانه‌ای) را منطبق بر خط مشی امنیتی بر عهده دارد.

مرز و محدوده کنترلی Controlled Perimeter

یک مرز و محل عبور فیزیکی که در آن قسمت ورود و خروج وسایل نقلیه و افراد کنترل می شود.

منابع کلیدی(حیاتی) Key Resources

در قانون امنیت ملی، منابع کلیدی، منابع کنترل شده اختصاصی یا عمومی هستند که برای عملیاتهای اقتصادی و دولتی حیاتی می باشند.(منبع 22)

نارکوتروریسم narco terrorism

نارکوتروریسم از سال 1983 که توسط «فرناندو بلاند تری» رئیس جمهور پرو ابداع شده،معانی متفاوتی داشته است. در ابتدا به خشونت بکارگرفته شده توسط قاچاقچیان مواد مخدر برای متأثر کردن دولتمردان یا جلوگیری از تلاش‌های دولت در توقف قاچاق مواد مخدر اطلاق می‌شد. در سال‌های اخیر تروریسم مواد مخدر توصیف‌گر شرایطی است که در آن، گروه‌ها از قاچاق مواد مخدر برای نیل به دیگر اهداف خود بهره می‌جویند. (منبع 14)

نرده حفاظ Protection Fence

نرده هایی که با تکنولوژی هایی ساخته شده اند که اگر شخصی بخواهد با روش های مختلف مانند بالارفتن،خزیدن،یا بریدن از آنها عبور کند تشخیص داده و زنگ خطر به صدا در می آید.

کلید مغناطیسی درب Balanced Magnetic Switch

سوئیچی که برای تشخیص باز بودن در استفاده می شود.این سنسورها همچنین می توانند برای پنجره ها،دروازه ها یا وسایل دیگر که در محل ورود و خروج هستند، استفاده شوند.(منبع 44)

2- واژگان تهدیدات نرم(جنگ روانی، رسانه و...)

ابزار رسانه ای Media tools

ابزار رسانه ای همان رسانه های مورد استفاده در عملیات روانی جهت انتقال پیام هستند که به پنج دسته عمده شامل تلویزیون (عادی، خبری و ویژه)، رادیو ، خبرگزاری ها، مطبوعات (نوشتاری) و اینترنت تقسیم می شوند و هر کدام قابلیت های مؤثری در امر انتقال پیام دارند و بطور مجزا قادر به اجرای بخش های تأثیرگذار هستند. این ابزارها به دلیل برد زیاد و فراگیر بودن، در تلقین و القای تحلیل ها، اخبار سیاسی و اجتماعی هدفمند، بیشترین تأثیرگذاری را بر طرز فکر و اراده مخاطبان دارند.(منبع 16)

اقدام روانی Psychological action

به فعالیتی گفته می شود که در راستای عملیات روانی صورت گیرد و سعی در تأثیر گذاری بر افکار و رفتار طرف مقابل دارد.

افکار عمومی Public Opinion

پدیده‌ای روانی ـ اجتماعی و خصلتی جمعی می باشد و عبارت است از ارزیابی و نظر مشترک گروهی اجتماعی در مسئله‌ای که همگان به آن توجه و علاقه دارند و در لحظه‌ی معینی، بین عده‌ی زیادی از افراد و اقشار مختلف جامعه نسبتاً عمومیت می‌یابد و عامه مردم آن را می‌پذیرند. افکار عمومی به صورت تأیید یا مخالفت با یک عمل، نظر، شخص و واقعه با خواسته، مطالبه، پیشنهاد و توصیه تجلی می‌یابد.

بر چسب زدن tally

بر اساس این تکنیک، رسانه ها واژه های مختلف را به صفات مثبت و یا منفی تبدیل می کنند و آنها را به افراد و یا نهادهای مختلف نسبت می دهند. گاهی هدف از این عملکرد آن است که ایده، فکر و یا گروهی محکوم شوند بی آنکه استدلالی در محکومیت آنها آورده شود

تبلیغات Propagation

واژه «تبلیغات»، در فارسی زمانی در مقابل واژه «Propagation» قرار می‌گیرد که به معنای اشاعه، ترویج، تکثیر و رساندن صحیح یک مطلب است .از نظر «رابرتز» تبلیغات عبارت است از تـلاش بـرای تأثیر گذاشتن بر دیگران، به منظور اقناع آنان و تغییر آرای آنان در قبال مسائلی معین .(منبع 11)

تبلیغات خاکستری Gray propaganda

تبلیغاتی است که از منبعی بی‌هویتی منتشر می‌شود(منبع انتشار، هیچ هـویتی بـرای خـود مشـخص نمی‌کند). قابلیت های آن عبارت است از:

1) اگر تبلیغات خاکستری، ماهرانه بکار گرفته شود می‌تواند با پرهیز از برچسب تبلیغات دشـمن ، مقبولیت کسب کند.2) می‌تواند بدون تأثیر مخرب بر حیثیت منتشر کننده، از تم های احساسـی اسـتفاده کند.

تبلیغات سیاه Black propaganda

تبلیغاتی است که به منبع غیرواقعی نسبت داده می‌شود. این تبلیغات وانمود می‌کنـد کـه از داخـل سرزمین دشمن(یا سرزمین تحت اشغال دشمن) و یا نزدیکی های آن پخش می‌شود و البته گـاهی نیـز واقعاً همین طور است. نمونه‌های تبلیغات سیاه عبارتند از:1) ایجاد شایعه 2)پخش تصـاویر مسـتهجن 3) شعار و ...

جنگ رسانه ای Media war

استفاده از رسانه برای تضعیف کشور هدف و بهره گیـری از تـوان و ظرفیـت رسـانه هـا (اعـم از مطبوعات ، خبرگزاری ها، رادیو، تلویزیون، اینترنت) و اصول تبلیغات به منظور دفاع از منافع ملی است. (منبع 16)

جنگ روانی Psychological Warfare

به صورت‌های متعددی تعریف شده، وجه اشتراک تمام این تعـاریف آن اسـت کـه جنـگ روانـی تلاشی آگاهانه و نظامند برای تخریب یا تضعیف روحیه حریف یا دشمن است.(منبع 11)

مجموعه اقدامات تبلیغی - روانی است که کشور یا گروهی برای اثر گـذاری و نفـوذ بـر عقایـد و رفتار دولت و مردم در جهت مطلوب به پشتیبانی زمینه ها و ابزارهای سیاسـی ،اقتصـادی ، فرهنگـی و نظامی انجام می دهد (منبع 16)

جنگ نرم Soft warfare

شامل هر گونه اقدام روانی و تبلیغات رسانه ای می شود که جامعه هدف و گروه هدف را نشانه می گیرد و بدون درگیری نظامی رقیب را به انفعال یا شکست وا می دارد. جنگ روانی، جنگ اینترنتی ، براندازی شبکه های رادیویی و تلویزیونی و شبکه سازی از اشکال جنگ نرم هستند.

البته تعاریف دیگری نیز از جنگ نرم بعمل آمده که جهت مزید آگاهی ایفاد می گردد:

1- جنگ تغییر باورها ،استحاله عقایدو جابجایی دیدگاه ها با نگاه های رسانه های استکباری است!

2- جنگ مغزهاست، نه مرزها! جنگ دیدگاه هاست، نه قرارگاه ها!

3- جنگ تقدس زدایی از ارزش ها و شبهه افکنی در اذهان است!

4- جنگ تخریب اعتمادهای موجود به ارکان و مسئولان حاکمیت در ابعاد مشروعیت و کارآمدی! (منبع 16)

عملیات روانی Psychological operation

عملیات روانی عبارت است از اقدامات برنامه ریزی شده برای انتقال اطلاعات و شاخص‌های منتخب به طرف های مقابل با هدف تأثیرگذاری بر احساسات، انگیزه‌ها، قدرت تفکر و استدلال و در نهایت تغییر رفتار حکومت‌ها، سازمان‌ها، گروه‌ها، و افراد خارجی. به طور کلی هدف از انجام عملیات روانی القاء یا تشدید آندسته از نگرش‌ها و رفتارهای هدف است که مطابق میل نیروهای عمل کننده می‌باشد.(منبع 10)

عملیات‌روانی استراتژیک Estrategic Psychological Operation

این عملیات، عموماً برای پیشبرد اهداف گسترده یا درازمدت و در هماهنگی با طرح‌ریزی استراتژیک کلی طراحی شده و معمولاً دارای تأثیراتی درآینده دور است. مخاطبان این عملیات ، شهروندان و نظامیان دشمن که خارج از منطقه جنگی بسر می‌برند و همچنین کل جمعیت کشورهای دوست می باشند. (منبع 10)

عملیات‌روانی پنهان Covert Psychological Operation

عملیات روانی پنهان عملیاتی است که منبع انتشار آن فاش نمی‌شود. این عملیات به گونه‌ای طراحی و اجرا می‌شود که دولت مسئول آن معلوم نباشد و یا اگر هم کشف شد، آن دولت بتواند

هرگونه دخالتی را انکار کند. عملیات‌روانی پنهان، معمولاً به وسیله تبلیغات سیاه و خاکستری بـه اجـرا درمی‌آید.(منبع 10)

عملیات‌روانی تاکتیکی Tactical Psychological Operation

این عملیات در منطقه جلویی نبرد و در پشتیبانی از عملیات نظـامی تـاکتیکی، طراحـی و اجـرا می‌گردد. مقاصد آن عبارتند از:

1- کاهش روحیه و کارآیی رزمی دشمن. 2- افزایش تأثیر سلاح های سنگین از جمله بمب ها.

3- آشفته کردن و سردرگم کردن دشمن.(منبع 10)

عملیات روانی psychological Operation

عملیات روانی شاخه ای از جنگ روانی است که به منظور تأثیر یا حصول تغییـر در برداشـت هـا، عقاید و احساسات فرد یا گروه معین (دوست یا دشمن) در جهت پشتیبانی از اهداف و منافع کشور بـه کار می رود.(منبع 16)

3- واژگان فرهنگی

آئین مندی ritualism

یک رفتار اجتماعی است ،آئین مندان برعکس نوآوران وسایل نهادی جامعه را ارج می نهند و پاس می دارند، بدون آنکه هدف را بشناسند و برای دستیابی به آن تلاش نمایند. اینان نسبت به هدف بی تفاوت بوده و با وسواس فرهنگی در خدمت وسیله در می آیند.(منبع 31)

آسیب‌شناسی Pathology

آسیب‌شناسی عبارت است از "مطالعه و شناخت ریشه بی‌نظمی‌ها در ارگانیسم انسانی" بنابراین در مشابهت کالبد انسان با کالبد جامعه، اصطلاح آسیب‌شناسی اجتماعی برای مطالعه و ریشه‌یابی بی‌نظمی‌ها، انحرافات و مشکلات اجتماعی بکار می‌رود.(منبع 31)

آسیب‌شناسی اجتماعی Social Pathology

رفتار اجتماعی و آسیب‌شناسی اجتماعی را می‌توان بوسیله شرایط سخت اقتصادی، تعارضات طبقاتی، تبعیض، سیاست‌های حکومتی یا تغییرات فناوری تبیین نمود.(منبع 31)

آسیب‌شناسی فردی Individual Pathology

در این رویکرد، برای تبیین رفتارها و آسیب‌های اجتماعی تجربه‌های منحصر به فرد افراد در دوران کودکی، توانایی‌ها،انگیزه‌ها و صفات شخصیتی افراد مورد بررسی قرار می‌گیرد. براساس این نقطه نظر ویژگی‌ها و صفحات شخصیتی و انگیزه‌های افراد می‌تواند برای توصیف و چرایی رفتار افراد نسبت به دیگران و آسیب‌شناسی اجتماعی مورد استفاده قرار گیرد.(منبع 31)

آسیب‌شناسی نظامی Military Pathology

آسیب‌شناسی نظامی نیز حوزه‌ای از آسیب‌شناسی و علوم اجتماعی است که به توصیف، تبیین، پیش‌بینی و کنترل بی‌نظمی‌ها، مشکلات و انحرافات اجتماعی مانند، دزدی، اعتیاد،خودکشی و خودزنی،فرار انحرافات جنسی در سازمانهای نظامی می‌پردازد.(منبع 31)

انحراف از هنجارهای اجتماعی Deviation from social malformation

از این دیدگاه، رفتار نابهنجار رفتاری است که به طور مشخص بامعیارها یا هنجارهای اجتماعی

مورد قبول جامعه متفاوت باشد. بدیهی است هنجارهای اجتماعی محدودیت‌های زمانی و مکـانی خاص خـود را دارنـد و اکثـر هنجارهـای اجتمـاعی قابـل تعمـیم بـه جوامـع و زمـا ن هـای مختلـف نمی‌باشند.(منبع 31)

اهریمن سازی Demiurgeing

در این تکنیک جنگ رسانه، مبلغ تلاش دارد تا تنفر و دشمنی جمعیت مخاطب را نسبت به عقیده، گروه و یا کشورهای خاص برانگیزد بنحوی که اگر گروهی منفور (از دیدگاه رسانه)،سیاست خارجی را پشتیبانی کند، صرفنظر از درست و یا نادرست بـودن آن، وجهـه منفـی گـروه حـامی ایـن سیاسـت را بزرگنمایی می کند و از این طریق بر مواضع جمعیت مخاطب اثر می گذارد.

پردازش زبان طبیعی Natural Languag Process

زیر شاخه ای از اطلاعات و زبانشناسی مصنوعی می باشد، که بر مطالعـه علـوم مربـوط بـه زبـان، سخن گفتن و مکانیزم تبدیل اطلاعات از بانک های اطلاعاتی کـامپیوتر بـه زبـان آوای طبیعـی انسـان، دلالت دارد. (منبع 23)

تشخیص ناهنجاری Malformation Recognation

عمل یا درکی است که یک عمل یا حالت مخفی، پوشیده یا انحرافی یک شخص از حالت نرمـال، شامل هم تمایلات خوب و هم بد را نمایش می دهد و رفتارهای غیرعـادی را داخـل سـازمان هـا، بـه عنوان شاخص های اولیه اخطار، نمایان می کند. (منبع 23)

عزلت گزینی Retreat

کسانی که نه هدف های ارجدار جامعه را می پذیرند و نه وسایل مقبول دستیابی بـه آن اهـداف را، ناگزیر یا کنج عزلت برمی گزینند و یا از جامعه می گریزند تا "برند گـوهر خـود را بـه خریـدار دیگـر بفروشند.(منبع 31)

ناهنجاری Abnormal

عمل انحراف یا جدا شدن از نظم نرمال یا معمول، شکل، یا قانون می باشد که غیرعادی، عجیب و یا غیرنرمال باشد، تا حدی که هر دو تمایلات خوب و بد را در بر گیرد. (منبع 23)

نظریه فرصت افتراقی segregat Opportunity theory

براساس دیدگاه فرصت افتراقی، جامعه و نهادهـای حکـومتی مسـئول اصـلی پدیدآمـدن و شـیوع نابهنجاری ها و آسیب های اجتماعی هستند. جامعه با توزیع ناعادلانه فرصت ها و امکانات دستیابی بـه موفقیت های مختلف، موجب پدیدآمدن "احساس تبعیض" در گروهی از افراد خود می شود. احسـاس تبعیض نیز افراد را برمی انگیزد تا برای تحقق اهداف خود، و زدودن فاصله خویش با افراد و گروه های برخوردار، به روش های نامشروع متوسل شوند و به کجروی های اجتماعی روی آورند. (منبع 31)

فصل چهارم

واژگان تهدیدات نیمه سخت

(تهدیدات :NBC ، بمب گرافیتی و EMP)

۱- واژگان تهدیدات NBC (بیولوژیک،شیمیایی و هسته ای)

۲- واژگان تهدیدات EMP ، بمب گرافیتی

– نمایی از قوطی‌های خارج شده از بمب اصلی ورشته‌های گرافیت

1- واژگان تهدیداتNBC (بیولوژیک، شیمیایی و هسته ای)

آلودگی زدایی بیولوژیک Biologic decontamination

شامل راهکارها و ابزارهای توزیعی به منظور خنثی سازی عوامل سلاح‌های بیولوژیک در آب، بـاد، خاک یا از روی مردم و لباس‌های آنها می شود و آگاهی دادن به کارکنان که در معرض آلـودگی قـرار نگیرند.(منبع 14)

آگاهی ازحملات بیولوژیک:

علایم زیر می تواند در شناخت وقوع حمله بیولوژیک کمک نماید:

- مشاهده انفجار بمبی که بخارهایی از آن خارج می گردد.
- مشاهده ابر و بخار بدون بو و رنگ مشخص.
- بروز بیماری های شبه سرماخوردگی در غیر فصل خود.
- مشاهده اجساد جانداران و جوندگان.
- افزایش ناگهانی میزان حشرات و ناقلین.
- ابتلاء به طور غیرمستقیم به بیماری‌هایی که اغلب در حالت طبیعی از طریق ناقل منتقل می‌شوند.
- همه گیری‌های متعدد و هم زمان از بیماری‌های عفونی مختلف.
- مشاهده همه گیری بیماری های گوارشی پس از مصرف آب و غذا از یک منشأ مشترک.

(منبع 45)

آگرو تروریسم Agroterrorism

«حملات تروریستی علیه محصولات کشاورزی» به مفهوم «تولید هدفمند آفات و بیماری های گیـاهی و جانوری به منظور ایجاد ترس و زیان‌های اقتصادی و کاهش ثبات (سیاسی و اجتماعی)» در نظر گرفتـه می‌شود.

سوء استفاده از عوامل شیمیایی و بیولوژیک علیه دام و کشاورزی با هدف، ایجاد رعب و وحشـت در اذهان عمومی و .... از مصادیق اگروتروریسم می باشند. بطور کلی طراحی هر عمل تروریستی جهت آسیب رسانی به محصولات کشاورزی را اگروتروریسم گویند (منبع 14)

آنفولانزای مرغی

آنفولانزای مرغی ماکیان را مبتلا می کند و عامل آن ویروس است .که با ساختار فیزیکی پرندگان سازگار شده است. با وجود اینکه این بیماری مخصوص ماکیان بوده، اما در سال های اخیر ظاهر این ویروس به گونه های دیگر جانداران نیز منتقل شده و موجب ابتلای انسان ها به این بیماری شده است. در مقابل، ویروس آنفولانزای فصلی بویژه با بدن انسان سازگار می شود. بر خلاف آنفولانزای مرغی، آنفولانزای فصلی به آسانی از فردی به فرد دیگر منتقل می شود .این ویروس اغلب در فضولات پرندگان یافت می شود و مرغدارانی که این ویروس را تنفس می کنند به آن مبتلا می شوند.

انتقال بیماری از انسان به انسان بسیار به ندرت اتفاق می افتد. آنچه این بیماری را برای انسان خطرناک می کند، این است که ویروس آن به شکلی دچار جهش ژنتیکی و تغییر رفتار شود که بتواند از انسان به انسان دیگر منتقل شود. در نتیجه این امر، شیوع بیماری بسیار گسترده خواهد شد.

خطرناکتر از این وضعیت آن است که ویروس مرغی بتواند فردی را آلوده کند که همزمان به بیماری آنفولانزای انسانی مبتلا است در صورتی که ژن های ویروس های مرغی و انسانی در این شرایط با یکدیگر ترکیب شوند ویروس می تواند از فردی به فرد دیگر منتقل شود و درنتیجه یک آنفولانزای عالم گیر شایع خواهد شد.

اپیدمیولوژی Epedemulogy

به علم مطالعه رخداد، پخش و کنترل بیماری‌ها و فاکتورهای مرتبط با سلامت در یک جمعیت انسانی، حیوانی یا گیاهی اپیدمیولوژی گویند (منبع 14)

اجتناب از آلودگی شیمیایی Chemical decontamination

آگاه‌سازی زودهنگام در اجتناب از آلودگی شیمیایی و بیولوژیک یک امر بنیادی است. هدف از اجتناب از آلودگی در حوزه‌های جنگی تأمین بلادرنگ توانمندی ها به منظور تعیین و تشخیص، ترسیم‌کردن و کیفیت‌سنجی و اجتناب از مواد شیمیایی و یا بیولوژیک است (منبع 14)

اشعه گاما Gamma Ray

فوتون هایی با انرژی زیاد که از هسته اتم ها ساتع می شوند،شبیه اشعه ایکس هستند.این اشعه می تواند به درون بافت های بدن و همچنین بسیاری از مواد دیگر نقوذ کند.کبالت60 و سزیم137 دو ماده ای هستند که اشعه های قوی از خود ساتع می کنند.

اقلیم شناسی حمله زیستی Bio-att Climatology

این متغیر از فاکتورهای مربوط به هواشناسی مانند سرعت باد ، میزان نور فرابنفش و امکان واژگونی دما تشکیل شده است در آمریکا یک مدل هواشناسی رایانه‌ای بدون مشکل اساسی در یکی کردن اطلاعات مربوط به این فاکتورها ایجاد شده است که از این طریق احتمال یک وضعیت آب و هوایی خاص را برای توزیع موفقیت آمیز یک عامل بیولوژیک جهت تحت پوشش قرار دادن فرودگاه یا سایر تجهیزات نظامی برای ایجاد تلفات وسیع، پیش بینی می کنند (منبع 14)

امنیت زیستی bio security

به مجموعه اقدامات و سیاست های اعمال شده جهت حفاظت در برابر آسیب های بیولوژیک را گویند که در بر گیرنده تخفیف یا حذف بیماری ها، آفات و بیوتروریسم در زمینه های اقتصاد، محیط زیست و سلامت اجتماعی می باشد و شامل عرضه و تامین آب و غذا، منابع کشاورزی و تولید، مدیریت آلودگی و ... می گردد (منبع 14)

امنیت غذایی Food security

دسترسی به غذا برای افراد جامعه را امنیت غذایی گویند. زمانی یک جامعه دارای امنیت غذایی می باشد،که در گرسنگی یا ترس از مرگ بدلیل گرسنگی نباشند(فائو 2007)، بدلیل افزایش قیمت سوخت : سطح زیر کشت برای تولید سوخت های زیستی Bio fuel افزایش یافته است (منبع 14)

ایمنی زیستی Biosafety

ایمنی (سلامت) زیستی بیانگر بکارگیری راهکارها و یا استفاده از تجهیزات، وسایل و تأسیسات مناسب برای کاهش پتانسیل پخش عوامل عفونی یا مواد مشتق از ارگانیسم‌های زنده به محیط می شود. این اقدامات برای نمونه شامل استفاده از وسایل ایمن نگهدارنده به منظور جلوگیری از رها شدن مواد مضر در اتمسفر، پوشیدن لباس‌های محافظ برای جلوگیری از آلودگی هنگام کار با بیماری‌های عفونی (منبع 14)

ایمنی غذا Food safety

حفاظت از منابع غذایی در برابر خطرات و آلودگی های میکروبی ، شیمیایی و فیزیکی خشک شدن،فاسد شدن، ترشیدگی که ممکن است در طول مسیر تولید، توزیع، بسته بندی و انبار داری حادث گردد (منبع 14)

باکتری ها Bacterias

باکتری ها ارگانیسم های تک سلولی هستند که به وسیله تقسیم ساده یا دوتایی شدن تکثیر می‌یابند. بیشتر آن ها زندگی آزاد داشته، اطلاعات ژنتیکی، تولید انرژی و سیستم های بیوسنتز لازم را برای رشد و تولید مثل دارند. تعداد کمی از آن ها نظیر کلامیدیا و ریکتزیا، انگل های داخل سلولی اجباری هستند.

بر چسب هشدار خطر بیولوژیک Biohazard warning symbol

بر چسب های هشدار خطر بیولوژیک روی درب ورودی اتاق هایی که در آن ها اصول ایمنی زیستی باید رعایت شود.(منبع 34)

بیو تروریسم bio terrorism

سوء استفاده از عوامل بیولوژیک یا مواد حاصل از آنها را علیه موجودات زنده بیوتروریسم گویند. (منبع 14)

پاکسازی Eradication

از نظر زیست شناسی، پاکسازی به معنای محو کردن کامل یگ گونه از یک ناحیه جغرافیایی خاص می باشد.

پناهگاه حفاظت شیمیایی Chemical protected shelter

یکی از آخرین و مجهزترین پناهگاه هایی که هم به عنوان بیمارستان های نظامی و هم پناهگاه‌های رفع آلودگی عوامل شیمیایی و میکروبی بکار می رود، سیستم پناهگاه حفاظت و شیمیایی است.این

پناهگاه نوع پیشرفته از این خانواده بوده و با خصوصیات قابلیت حمل بالا، حفاظت از آلودگی بسیار مناسب، قابلیت برپایی و کنترل در سطوح سخت محیطی و بسیار مناسب و مجهز برای عملیات پزشکی در شرایط جنگی می باشد. (منبع 15)

پناهگاه های سیار Mobile shelter

کاربرد دیگر پلیمرها استفاده در پناهگاه های سیار است که می تواند در مواقع ضروری و خطر مانند زمان جنگ، زلزله، بلایای طبیعی و غیره مورد استفاده قرار گیرد. این پناهگاه های سیار می‌توانند به دو صورت بادی و خیمه ای مورد استفاده قرار گیرند. روکش این پناهگاه ها از جنس PVC بوده و به راحتی در پشت یک خودروی نظامی جاسازی می‌شود.این پناهگاه ها به دلیل سبکی، سرعت بالای نقل و انتقال، قابلیت استتار، مقاوم در مقابل عوامل شیمیایی، مقاوم در مقابل رطوبت، برف، باران و غیره بعنوان قرارگاه های ستادی، فرماندهی، رزمی و جان پناه انفرادی مصارف متعددی را دارند (منبع 15)

پیشگیری مصدومین بیولوژیک Biologic sickest prevent

پیش گیری قبل از تماس: این بخش شامل کسب آمادگی قبل از بروز حوادث در گروه های پر خطر و یا قبل از ورود به مناطق آلوده گروه های مختلف مانند گروه های پزشکی مداخله گر در روند امداد و درمان می باشد.مهمترین فعالیت در این بخش استفاده از برنامه های واکسیناسیون اختصاصی (ایمونو پروفیلاکسی فعال) تایید شده، موجود می باشد.

پیش گیری پس از تماس: به دنبال بروز حادثه بیولوژیک و یا پس از ورود به مناطق آلوده را شامل شده که در این بخش خدمات پزشکی و پروتکل های مربوطه به دو قسمت تقسیم می گردد: ایمونولوژیک- پیش گیری دارویی.

تروریسم Terrorism

ادارۀ بازرسی فدرال امریکا ،تروریسم را به این صورت تعریف می کند که به عنوان یک عمل حساب شده و یا تهدید، توسط فرد و یا گروهی، برای موضوعات سیاسی و یا اجتماعی، انجام می گیرد.

تروریسم بیولوژیکی Biological Terrorism

تهدید یا استفاده از عوامل بیولوژیکی توسط افراد یا گروهی با انگیزۀ سیاسی اکولوژیکی و یا سایر موضوعات ایدئولوژیکی می باشد.(منبع 14)

تروریسم شیمیایی Chemical terrorism

کموتروریسم؛ بکارگیری مواد شیمیایی به عنوان سلاح توسط افراد یا گروه‌ها برای تهدیدکردن، آسیب رسانی یا کشتن مردم بی گناه به منظور دستیابی به اهداف سیاسی، ایدئولوژیک یا ... است.دسته‌بندی عوامل شیمیایی :دانشمندان عوامل شیمیایی را برحسب نوع یا اثر آن‌ها روی بدن انسان دسته‌بندی می‌کنند:

بیوتوکسین‌ها- عوامل تاول زا - عوامل خونی- عوامل سوزاننده - عوامل تنفسی - عوامل ناتوان کننده - ضدانعقادهای طولانی اثر- فلزات -عوامل عصبی- حلال‌های آلی- گازهای اشک آور.(منبع 14)

تریاژ (مصدومین بیولوژیک) biological sickest

اولویت بندی مصدومین؛ به معنی طبقه بندی کردن و یک روش کلی برای تقسیم بندی بیماران بر اساس فوریت نیاز به درمان است. این روش در وضعیت های مصدومین انبوه که امکان برخورد کلاسیک با تک تک بیماران وجود ندارد، استفاده می شود. فردی که مسئولیت این کار را بر عهده داشت افسر تریاژ خوانده می شد و دوره های خاصی را بدین منظور طی می کرد.

• معیارهای برخورد تریاژ : 1) فوریت (وضعیت مصدوم) 2) احتمال بقاء 3) دسترسی به منابع مراقبت های پزشکی. (منبع 44)

تریاژ انتقال sickest transfer

این تریاژ قربانیان را برای انتقال به مراکز درمانی که از پیش هماهنگ و آماده شده اند اولویت بندی می کند. مدیر پست مراقبت های پیشرفته با هماهنگی پست فرماندهی و بیمارستان و بر اساس وضعیت قربانیان و مقصد، نوع وسیله نقلیه و اسکورت درمانی را تعیین می کند.(منبع 44)

تریاژ در صحنه

غالباً توسط امدادگران انجام می شود. در این نوع تریاژ مصدومین به دو گروه تقسیم می شوند :

– حاد (با علامت نوار قرمز) نیازمند مراقبت های پزشکی فوری می باشند.

– غیر حاد (با علامت نوار سبز) می توانند منتظر بمانند.

تریاژ مدیکال Medical sickest

در محل ورودی پست مراقبت های پزشکی پیشرفته (اورژانس صحرایی) و توسط نیروهای مجرب درمانی صورت می گیرد. در این مرحله روی کارت های تریاژ (Tag) که با رنگ کدبندی شده اند اطلاعات دقیقتری از مصدومین ثبت و در چهار سطح درمانی طبقه بندی می شوند:

- قرمز (درمان فوری) - زرد (درمان تأخیری) - سبز (درمان سرپایی) - سیاه (فوت شدگان).

تسلیحات بیولوژیک Biological Weapon

سلاح بیولوژیک عبارت است از وسایلی که باعث پخش و گسترش عوامل بیولوژیک می‌شود نظیر موشک، بمب، حشرات ناقل و...

- بمب های میکروبی R400 عراق که در سال 1991توسط مامورین خلع سلاح سازمان ملل تصویر برداری شده است

تقسیم‌بندی عوامل بیولوژیک Biologic agent groups

نوع دیگر طبقه‌بندی عوامل بیولوژیک از لحاظ نوع اثر است. از این دیدگاه، عوامل بیولوژیک را به دو دسته تقسیم می‌کنند: (1) عوامل کشنده (Lethal agents) (2) عوامل ناتوان‌کننده

یک نوع طبقه‌بندی عوامل بیولوژیک از لحاظ نوع ارگانیسم است. از این دیدگاه، عوامل بیولوژیک به 6 دسته تقسیم می‌شوند که عبارتند از: باکتری ها، ریکتزیاها، ویروس ها، قارچ ها، پروتوزوئرها و

توکسین ها - نوع دیگر طبقه‌بندی عوامل بیولوژیک از لحاظ نوع هدف است. از این دیدگاه عوامل بیولوژیک را به چهار گروه تقسیم می‌نمایند:

ضد انسان - ضد حیوان- ضد انسان و حیوان - عوامل بیولوژیک ضد گیاه

نوع دیگر طبقه‌بندی عوامل بیولوژیک بر اساس راه ورود عامل به بدن میزبان است. بر این اساس عوامل بیولوژیک را به سه گروه تقسیم می‌کنند:ورود عوامل بیولوژیک از طریق دستگاه تنفس- ورود از طریق دستگاه گوارش - ورود از طریق پوست و مخاط.

تهدیدات بیولوژیکی آب Waret Biological Threats

عوامل بیماری زا و بیوتکسین های زیادی وجود دارد که می توانند به صورت سلاح های جنگی در آینده و به طور بالقوه در مقابل گندزدایی کلر مقاوم باشند و برای مدت های نسبتا طولانی در آب پایدار هستند. خاصیت رقیق سازی آب شرایطی فراهم می کند که یک ذره شناور با هر اندازه ای می تواند برای انتشار عوامل بیماری زا درون سامانه های آب آشامیدنی به کار رود

تهدید عوامل زیستی Biological agents treat

عامل زیستی عبارت است از میکروب زنده و یا سم تولید شده توسط میکروب‌ها که قادر به ایجاد بیماری یا مرگ در انسان‌ها، حیوانات و یا گیاهان است. میکروب‌ها توانایی رشد تدریجی در بدن میزبان را برای ایجاد بیماری دارند.ویروس‌ها اغلب به عنوان مادهٔ ژنتیکی شناخته می‌شوند و اغلب حاوی DNA و همچنین RNA می‌باشند که با پوششی از پروتئین احاطه شده‌اند. ویروس عامل آنسفالیت، تب طوطی، تب زرد و تب دنگو از عواملی هستند که بالقوه در ساخت سلاح‌های کشتار جمعی می توانند بکار روند.بروز بیماری‌های انگلی در دام‌ها و گیاهان کشاورزی به عنوان خطری قابل توجه محسوب می شود. ریکتزیا جزء مواردی است که توانایی القای بیماری در انسان‌ها و دام‌ها را داراست و به عنوان عاملی زیستی برای حمله مورد توجه است.(منبع 14)

توکسین ها (Tocsins) به مواد سمی تولیدشده یا مشتق ازمیکروارگانیسم ها، حیوانات و گیاهان زنده توکسین می‌گویند. در برخی از باکتری ها، وجود جسم باکتری در بدن فرد دلیل ایجاد بیماری نیست بلکه تولید توکسین توسط باکتری در شرایط مناسب باعث ایجاد بیماری می‌شود. با توجه به این محاسن و خصوصیات منحصر به فرد توکسین ها، گرایش به، به کارگیری آنها در جنگ های بیولوژیک و بویژه عملیات های تروریستی بیشتر است.

جنگ بیولوژیکی Biological warfare

کشت و یا تولید عمومی باکتری ها، قارچ ها ، ویروس ها ،... و سایر محصولات زهرآگین بیماریزا، همانند ترکیبات شیمیائی به عنوان سلاح های بیولوژیکی بالقوه معرفی شده اند. در زمرهٔ عوامل بیولوژیکی، سیاه زخم و جنون دارای بیشترین پتانسیل برای تلفات و تخریب کلی می باشند.(منبع 14)

جنگ شیمیایی chemical warfare

جنگی است که در آن بجای استفاده از جنگ افزارهای متعارف ، از مواد منفجره ممنوع ، گازهای سوزاننده ، خفه کننده ، دودزا و آتش‌زا استفاده می‌شود. این گازها در ساختمان بدن انسان موجب مرگ انسان یا از کار انداختن دائمی اعضای بدن یا سلب موقت و اختیار آن می‌گردند.

حفاظت پزشکی شیمیایی Chemical medic Protection

محافظت پزشکی از سه کارکرد اولیه تشکیل شده است :

تدابیر پیشگیری‌کننده قبل از مواجهه - درمان‌های بعد از مواجهه - قابلیت های تشخیصی.

این عملکرد به منظور دفاع در برابر حملات شیمیایی و بیولوژیک بکاربرده می‌شود. تلاش‌های تکنولوژیک زمانی که آئروسل های مواد شیمیایی و مواد بیولوژیک در میادین جنگی استفاده می شوند، تعدادی از محصولات پزشکی را برای پیشگیری از بیماری ها یا کاهش ابتلای سربازان فراهم می آورند و یا برای سربازانی که در معرض مواد شیمیایی یا بیولوژیک قرارگرفته ، شرایطی را فراهم می کنند که میزان مرگ و میر و دورهء نقاهت کاهش یابد.(منبع 14)

حسگرهای زیستی (بیوسنسور) Bio sensor

حسگرهای بیولوژیک تلفیقی از زیست شناسی و الکترونیک است با به کارگیری گیرنده‌های اختصاصی که می‌تواند مبتنی بر سیستم های آنزیمی و یا واکنش های آنتی‌ژن و آنتی‌بادی باشد. استفاده از گیرنده بسیار اختصاصی عوامل بیولوژیک و پیوند آن با نشانگرهای الکترونیک می‌تواند به عنوان یک آشکارساز فوق حساس و اختصاصی عمل کند. به نحوی که با حضور غلظت بسیار کمی از عامل و پیوند آن با گیرنده اختصاصی، با ارسال امواجی موجب فعال شدن بخش الکترونیک حسگر شده و در نتیجه هشدار حضور عامل به دستگاه ها و مراکز کنترل صادر گردد.

حصر بیولوژیکی Biological Containment

عبارتی است که برای توصیف روش های ایمن مدیریت عوامل مخاطره آمیز زیستی در آزمایشگاه و محیط اطراف آزمایشگاه مورد استفاده قرار می گیرد و هدف از حصر کاهش میزان تماس کارکنان آزمایشگاه ، افراد دیگر و محیط خارجی با عوامل بالقوه خطرناک است. (منبع 34)

دفاع بیولوژیک Biological defence

به مجموعه وسیعی از اقدامات و فعالیت‌ها که به منظور جلوگیری، به حداقل‌رسانی پیامدها و مواجهه با حوادث زیستی نظیر پاندمی ها و حملات بیوتروریسم کشاورزی بکار می روند، دفاع زیستی گفته می شود. این اقدامات شامل موارد ذیل می باشند: - آگاهی از خطر که دربرگیرنده جمع آوری، آنالیز و پخش اطلاعات با ماهیت موضوعات امنیت زیستی و پیش‌بینی آنها است - جلوگیری و محافظت، که دربرگیرنده محافظت از زیرساخت‌های حیاتی، توسعه رویه ها و روندهای مدیریت کردن تهدیدات نو پدید - پاسخ دهی و بازیابی که برای کاهش اثرات منفی رهاسازی میکروارگانیسم‌های بیمارگر، طرح های پاسخ دهی، مراقبت کشتار دست جمعی و رفع آلودگی از مردم و حیوانات و گیاهان. (منبع 14)

رفع آلودگی Decontamination

رفع آلودگی روند پاک کردن هرگونه چیزی از روی انسان، حیوان یا سطح برای رفع آلودگی یا آلودگی بالقوه به‌وسیله ماده ای خطرناک است. برای نمونه رویه های آلودگی زدایی در تأسیسات ایمنی زیستی سطح چهار نیازمند روندی بسیار خاص برای اطمینان از این امر است که مردم با موادی که با آنها کار می کنند تماس نخواهند داشت.

- چمدان آزمایشگاهی تشخیص عوامل

رفع آلودگی شیمیایی Chemical decontamination

رفع آلودگی به عنوان روندی به منظور رفع یا خنثی کردن مواد خطرناک ناشی از حملات شیمیایی یا بیولوژیک از روی سطوح، تعریف می شود. هدف از تلاش‌های تکنولوژیک رفع آلودگی، توسعه روش‌های مؤثر و ایمن و افزایش واکنش پذیری با مواد شیمیایی یا ضدعفونی کننده مواد بیولوژیک است که برروی سطوح اثر چندانی ندارند. از جمله نقاط ضعف این اقدام این است که مواد رفع کننده آلودگی رایج، سوزاننده هستند و روش‌هایی که برای رفع آلودگی استفاده می شوند، نمی توانند سطوح حیاتی وسیعی را پوشش دهند (دریا ، فرودگاه ها ، داخل دریاها) (منبع 14)

رها سازی در محیط زیست shooting

هر گونه استفاده غیر محصور از سازواره های دستورزی شده ژنتیکی زنده.(منبع 34)

روش ایمونولوژیک تشخیص عوامل Diagnosis emonologic method

روش ایمونولوژیک از قدیم ترین روش های شناسایی و تعیین هویت عوامل بیولوژیک است.میکروارگانیسم ها اعم از باکتری ها، ویروس ها، قارچ ها و همچنین توکسین ها دارای ساختمان آنتی‌ژنی همچون کپسول، تاژک، و... می‌باشند. ورود عوامل واجد این ساختار آنتی‌ژنی به بدن، موجب تولید آنتی‌بادی علیه آنها می‌شود. این آنتی‌بادی تولید شده براساس نوع میکروب، اختصاصی است. از این آنتی‌بادی ها می‌توان برای تشخیص عوامل بیولوژیک استفاده کرد.

روش تراشه‌های ژنی Gene chip method

روش کاملاً نوینی در عرصه تشخیص بسیار سریع عوامل بیولوژیک، سرطان ها و بیماری های ژنتیکی است. در این روش با استفاده از تراشه‌های الکترونیکی که روی آن، ده ها تا صدها هزار کاوشگر (که بر اساس ردیف DNA عوامل بیولوژیک طراحی شده است) نصب گردیده، امکان شناسایی انواع عوامل بیولوژیک وجود دارد.

روش تشخیص عوامل بیولوژیک Biological diagnosis method

(1) روش آزمایشگاهی قدیمی و متداول تشخیص عوامل فونی (کلاسیک)

(2) روش کشت و تشخیص میکروب ها با کمک تست های بیوشیمیایی

(3) کیت های تشخیصی دستی و دستگاهی

(4) روش بیوشیمیایی خاص

(5) روش ایمونولوژیک

(6) روش های تشخیص نوین:

کاوشگرهای ژنی - تراشه‌های ژنی - حسگرهای زیستی یا بیوسنسورها- فلوسیتومتری

سلاح شیمیایی Chemical weapon

سلاح های شیمیایی بسیار کشنده بوده و قادرند ده ها هزار آسیب ایجاد نمایند. این دسته شامل گازها، مایعات و جامداتی می شود که اثرات سمی بر انسان ها، حیوانات و نباتات دارند. اغلب سلاح های شیمیایی باعث ایجاد جراحات جدی و یا مرگ می شوند. خطرناک ترین عامل های شیمیایی عبارتند از: سارین، وی ایکس، وگاز خردل.

سلاح های زیستی Biological weapons

جزئی از دسته سلاح های شیمیایی، زیستی، رادیولوژیک یا هسته ای بوده. این سلاح های کشتار جمعی در برگیرنده استفاده از یک عامل زیستی در یک روش تهاجمی و خصمانه می باشند. اگ رچه پروتکل ژنو، استفاده از سلاح های زیستی را در جنگ و توسعه آنها را توسط کنوانسیون سلاح های زیستی و سمی (BTWC) ممنوع کرده است. (منبع 14)

سلاح های کشتار جمعی Mass destruction weapons

سلاح‌هایی که قادر به تخریب وسیع بوده ویا به شیوه ای استفاده می شوند که سبب مرگ و میر و آسیب شمار زیادی از مردم می گردند. سلاح های کشتار جمعی می توانند شامل مواد منفجره با دامنه وسیع انفجار و یا سلاح های هسته‌ای، زیستی، شیمیایی یا رادیولوژیک باشند (منبع 14)

سلاح های نا متعارف MDW weapons

سلاح های شیمیایی، زیستی، رادیولوژیک و هسته ای (CBRN) را شامل می‌شود که به‌عنوان سلاح های کشتار جمعی قلمداد می شوند.(منبع 14)

عقیم گذاری Thwarting

اقداماتی که بعد از شناسایی حمله زیستی یا قریب الوقوع بودن آن به‌منظور جلوگیری از ابتلا یا تهاجم عامل صورت می‌گیرد. (منبع 14)

عوامل بیولوژیک Biological Agents

عوامل بسیار مؤثر سلاح های بیولوژیکی، می توانند بسیار مسری، واگیر و مهلک باشند و بطور مؤثر پراکنده شده به آسانی و به مقدار زیادی تولید شوند و پایداری انبار شدن داشته باشند ودر مقابل کاهنده های محیط زیست مقاومت کنند و فاقد واکسن و یا معالجه مؤثر باشند. ممکن است عوامل بیولوژیکی که توسط تروریست ها بکار برده می شوند بطور مستقیم و یا از طریق جلدی و موضعی، تزریق شوند، بر علیه محصولات کشاورزی، احشام، ماکیان و ماهی ها بکار گرفته شوند. یا توسط غذا و آب آشامیدنی مورد استفاده قرار گیرند. عوامل بیولوژیکی را می توان بی سر و صدا ، غیر قابل دید ، میکروسکوپی، بدون بو ،بدون هیاهو و بی خبر تولید نمود و چون میکرو ارگانیسم ها در میزبان به آسانی در نرخ های بالائی تکثیر پیدا می کنند یک مقدار جزئی بیماریزا به سرعت می تواند موجب سرایت عفونت ویران کننده شود. (منبع 14)

این عوامل را به طرق مختلفی **طبقه بندی** نموده اند که به برخی از آنها اشاره می گردد:

1) براساس انواع عوامل که شامل: پاتوژن های تکثیریابنده، توکسین ها یا تعدیل کننده های بیولوژیک .

2) براساس هدف مورد نظرشان که ضد انسانی، ضد حیوانی و یا ضد گیاهی ویا حتی محیط های بیجان (استفاده از باکتری های فلز دوست جهت تخریب صنایع استراتژیک) باشد.

3) براساس دارا بودن یا فقدان قدرت انتقال ثانویه ..(منبع 45)

عوامل بیوتروریسم کشاورزی Agro terrorism Agents

همان گونه که تعداد زیادی میکروارگانیسم و ماکروارگانیسم، وجود دارند که در جنگ های بیولوژیکی، علیه انسان ها، بکار گرفته می شوند، گروه متفاوتی از عوامل ، وجود دارند، که می توانند بر علیه کشاورزی، مورد استفاده قرار گیرند. این ها، شامل بیمارگرهای میکروسکپی ، پروانه ها، علف های هرز و سایر ارگانیسم ها یا مواد بیولوژیکی هستند. فعالیت تروریسم کشاورزی از طریق انتشار آلودگی های مسری در احشام یا آلوده سازی زنجیره مزرعه و فروشگاه با عوامل باکتریایی می تواند به پیامدهای مخربی منجر شود که نه تنها سلامت عمومی را به خطر می اندازد بلکه بر اعتماد مصرف کنندگان به سلامت محصولات غذایی مورد عرضه تأثیر منفی چشمگیری داشته و ممکن است اعتماد و حمایت مردم نسبت به دولت را کاهش دهد.

عوامل زیستی Biological Agents

عامل زیستی؛ یک ویروس، میکروارگانیسم یا ماده سمی مشتق از یک ارگانیسم زنده یا تولیدات آن است. برخی از عوامل زیستی، اثرات منفی روی سلامت انسان دارند و در نتیجه تهدید امنیت زیستی محسوب می شوند. بیماری‌های عفونی به‌واسطه عوامل زیستی ایجاد می شوند. نمونه هایی از آنها شامل آنتراکس، آبله، آنفلوآنزای پرندگان و بوتولیسم هستند. از طرف دیگر برخی از عوامل زیستی مانند آنتی بادی ها، اینترلوکین ها و واکسن ها برای جلوگیری، تشخیص یا درمان بیماری‌ها استفاده می شوند منبع 14)

عوامل عصبی Neurotic agents

سارین (یا GB) جزء عوامل عصبی و سمی‌ترین و سریع الاثرترین ماده شیمیایی جنگی به شمار می‌رود. سارین مایعی بدون رنگ، بو، مزه و محلول در آب نیز می‌باشد. سارین بعنوان عاملی بالقوه و مورد توجه در آلوده سازی مواد غذایی و آب آشامیدنی بشمار می‌رود. (منبع 14)

عوامل ناتوان‌کننده Incapacitating agents

در تقسیم‌بندی عوامل بیولوژیک از نظر نوع اثر ، عوامل ناتوان‌کننده یکی از تقسیمات است.هر یک از این عوامل نیز خود به دو دسته مسری و غیر مسری تقسیم می‌شوند. گفتنی است که ترسیم مرز مشترک بین عوامل کشنده و ناتوان‌کننده کاری مشکل است و به شرایط مختلف از جمله شرایط عامل و میزبان، مثل سوء تغذیه، سلامت جسم، سن، دوز عامل، محیط، ژنتیک، راه ورود عامل به بدن و ... بستگی دارد.

فلزات سمی Toxic metals

آرسنیک و آرسین ترکیبات سمی هستند که باعث بروز نقص های جنینی شده و با تجمع تدریجی در بدن سبب بروز مخاطرات دراز مدت سلامتی از جمله افزایش احتمال ابتلا به سرطان می‌شود. ترکیبات آلی آرسنیک سمیت بیشتری نسبت به ترکیبات معدنی آن دارند. اثر عمدۀ آن‌ها، تخریب گلبول‌های قرمز خون است. استنشاق آرسنیک باعث خراش گلو و ریه می‌شود. بلع سبب تهوع، استفراغ، آسیب به عروق و بافت قلب، ضربان غیرطبیعی قلب و کاهش تولید سلول‌های قرمز و سفید خون می‌شود. (منبع 14)

فن‌آوری زیستی Biotechnology

کنوانسیون سازمان ملل متحد در تنوع زیستی، فن‌آوری زیستی را چنین تعریف مـی کنـد: «هرگونـه کاربرد فن‌آوری که از سامانه‌های زیستی، ارگانیسم‌های زیستی یا مشتقات آنها برای ساختن یـا اصـلاح محصولات یا روندهایی با کاربرد خاص استفاده می کند» (منبع 14)

ماسک محافظت protection mask

ماسک های محافظت فردی جزء کلیدی محافظت فـردی، محافظـت از چشـم، دسـتگاه تنفسـی و بافت‌های زیرجلدی است. فن‌آوری پیشرفته فیلتراسیون و غشاهای نفوذ ناپذیر نسبت به مـواد، مـانع از تنزل کارایی افراد می‌شود. (منبع 14)

محافظت فردی از عوامل شیمیایی personal protection of chemical agents

تجهیزاتی شامل انواع ماسک و لباس‌ها می‌باشند شرایط مشکلی که به همراه استفاده از ایـن اجـزاء می باشد اثربخشی مؤثر آنها را کاهش داده و در شـرایط آب و هـوایی متعـدد، تنهـا بـرای بـازه زمـانی محدودی قابل استفاده هستند یک ماسک تجاری که تنها از طریق سامانه تنفسی عمل می کنـد بـه طـور مشخصی باعث کاهش استشمام مواد بیولوژیک می شود و حفاظت مناسب و خوبی را برعلیه تحریکات مواد سلاح‌های بیولوژیک فراهم می‌آورد.در اغلب موارد، این میزان از حفاظت بدون کاهش فعالیت‌های عملیاتی و سختی های ناشی از ماسک های شیمیایی سنتی،باعث جلوگیری از عفونت می شود(منبع14)

محافظت جمعی از عوامل شیمیایی Collective protection of chemical agents

تجهیزاتی از طریق فیلتر کردن هـوای ورودی، نـواحی عـاری از سـلاح‌هـای بیولوژیـک را فـراهم می‌آورند. مناطقی وجود دارد که مردم بدون آسیب‌پذیری نسبت به عوامل سـلاح‌هـای بیولوژیـک و یـا داشتن اجبار نسبت به پوشیدن چکمه، دستکش، ماسک و لباس‌هـای رویـی سـنگین و گـرم محافظـت کننده، می‌توانند به راحتی زندگی کنند. بسیاری از امکانات بـا کمـی بهبـود یـافتن و ترفیـع مـی تواننـد حفاظت خوب و لی نه کامل را بر علیه سلاح‌های بیولوژیک فراهم آورند (منبع 14)

همه گیری های غیر طبیعی Unnatural epidemic

این نوع همه گیری ها به دلیل دخالت انسان و مسایل بهداشتی ایحاد می شود و لیکن عمدی در

کار نیست مانند آلوده شدن آب به فاضلاب های انسانی و یا عدم رعایت اصول بهداشتی که سبب بروز بیماری های عفونی می گردد..(منبع 45)

همه گیری های مشکوک suspicious epidemic

این نوع همه گیری های مشکوک با منشأ نامشخص هستند که شک برانگیزند نه دلایل همه گیر شناسی قاطعی بر طبیعی بودن آن وجود دارد و نه استنادی بر بکارگیری عمدی آن، بنابراین جزء همه گیری های مشکوک قرار می گیرند..(منبع 45)

همه گیری هایی با منشأ طبیعی Natural epidemic

در بروز حوادث بیولوژیک سناریو های مختلفی مطرح است: - همه گیری هایی با منشأ طبیعی: اکثر همه گیری ها بدین طریق رخ می دهند و منشأ آنها عوامل طبیعی است مانند انتقال عوامل بیماری زا از طریق حشرات، حیوانات و تغییرات عوامل جوی که در بروز همه گیری ها نقش دارد..(منبع 45)

****

2- واژگان هسته ای

انواع راکتور اتمی Kinds of Nuclear reactor

راکتورهای اتمی را معمولا برحسب خنک کننده ، کند کننده ، نوع و درجه غنای سوخت در آن طبقه بندی می‌کنند. معروفترین راکتورهای اتمی ، راکتورهایی هستند که از آب سبک به عنوان خنک کننده ،کند کننده و از اورانیوم غنی شده 2 تا 4 درصد U235 (به عنوان سوخت) استفاده می‌کنند. این راکتورها عموما تحت عنوان راکتورهای آب سبک (LWR) شناخته می‌شوند. راکتورهای PWR، BWR و WWER از این دسته‌اند. نوع دیگر راکتورهای آب سنگین (HWR) که از آب سنگین بعنوان مدولاتور و هم خنک کننده استفاده می کنند. نوع دیگر، راکتورهایی هستند که از گاز به عنوان خنک کننده ، گرافیت به عنوان کند کننده و اورانیوم طبیعی یا کم غنی شده به عنوان سوخت استفاده می‌کنند. این راکتورها به گاز - گرافیت معروفند. راکتورهای GCR، AGR و HTGR از این نوع می‌باشند.

اورانیوم Uranium

اورانیوم یکی از عناصر شیمیایی جدول تناوبی است که نماد آن ، U و عدد اتمی آن 92 می‌باشد. اورانیوم که یک عنصر سنگین ، سمی ، فلزی ، رادیواکتیو و براق به رنگ سفید مایل به نقره‌ای می‌باشد،

به گروه آکتیندها تعلق داشته و ایزوتوپ 235 آن برای سوخت راکتورهای هسته‌ای و سلاح های هسته‌ای استفاده می‌شود.

اورانیوم با غنی سازی بالا Highly Enriched Uranium

اورانیومی که غنی سازی آن بالای 20 درصد اورانیوم 235 انجام شده است . برای ساخت سلاح های اتمی غنی سازی اورانیوم 235 بالای 90 درصد صورت می گیرد.

بمب هسته‌ای Nuclear Bomb

یکی از سلاح های انفجاری با نیروی بسیار خوب است که براساس واکنش های خودبخودی زنجیری شکست هسته U235 یا Pu239 انجام می گیرد. از واکنش یک نوترون حرارتی با U235 دو هسته نسبتا سبک پایدار و Mev200 انرژی حاصل می‌شود. اجزای اصلی این بمب شامل مقداری سوخت هسته‌ای ، ماده انفجاری به عنوان چاشنی و یک پوسته می‌باشد. انفجار بمب اتمی با یک موج بسیار قوی ، روشنایی بسیار شدید و تشعشعات نافذ همراه است که باعث آلودگی رادیو اکتیو محیط اطراف ، هوا و آب می‌گردد.

تروریسم هسته ای Nuclear terrorism

تروریسم هسته‌ای به راه‌هایی که مواد هسته ای ممکن است به عنوان تاکتیکی تروریستی مورد سوء استفاده قرار گیرند گفته می‌شود. این نوع تروریسم دربرگیرنده حمله به تأسیسات هسته‌ای، خرید یا تولید اسلحه هسته‌ای و یافتن راهی برای پخش تشعشعات رادیواکتیو است. (11)

با اسلحه هسته‌ای یا «ماشین‌های پخش کننده تشعشعات رادیواکتیو» امنیت همه کشورهای جهان به طور جدی تهدید خواهد شد. (منبع 14)

تیم مقابله با حوادث هسته ای Nuclear Incident Respons Team

این تیم به استناد قانون امنیت ملی تشکیل تا قابلیت مقابله با حوادث هسته ای را در بخش امنیت ملی تامین کند. در زمان فعال سازی، این تیم شامل تیم های مقابله ملی می باشد(منبع 22)

ساختمان بمب هسته‌ای Nuclear bomb structur

ساختار سلاح هسته‌ای به این صورت است که هر گاه مقدار عنصر قابل شکافت ، که از اندازه

بحرانی بیشتر باشد، پدیده شکافت شروع می شود. این پدیده خیلی سریع پیشرفت می‌کند و با آزاد شدن مقادیر عظیم انرژی در مدت بسیار کوتاه ، انفجار مهیبی رخ می‌دهد. ولی از آنجایی که بمب باید در لحظه دلخواه منفجر شود، مقداری از U235 ، یا Pu239 را که خالص بوده و حجم کلی آن از اندازه بحرانی بیشتر باشد، به چند قسمت مجزا ، که هر یک از آنها از اندازه بحرانی کمتر است، تقسیم می‌کنند و این قسمت ها را در محفظه‌ای طوری قرار می‌دهند تا نوترون هایی که ممکن است هر یک از آنها آزاد شوند، در قسمت دیگر نفوذ نکنند.

سوخت راکتور هسته‌ای Nuclear reactor fuel

ماده‌ای که به عنوان سوخت در راکتورهای هسته‌ای مورد استفاده قرار می‌گیرد باید شکاف پذیر باشد یا به طریقی شکاف پذیر شود.U235 شکاف پذیر است ولی اکثر هسته‌های اورانیوم در سوخت از انواع U238 است. این اورانیوم بر اثر واکنش هایی که به ترتیب با تولید پرتوهای گاما و بتا به Pu239 تبدیل می‌شود. پلوتونیوم هم مثل U235 شکافت پذیر است. به علت پلوتونیوم اضافی که در سطح جهان وجود دارد نخستین مخلوط های مورد استفاده آنهایی هستند که مصرف در آنها منحصر به پلوتونیوم است.

شکافت هسته‌ای nuclear gap

یک نوع بمب از طریق شکافت هسته‌ای یعنی شکسته شدن هسته‌های سنگین به هسته‌های سبکتر تولید می شود که همزمان با شکستن هسته مقدار قابل توجهی انرژی آزاد می‌شود.

غنی سازی اورانیوم Uraniom enrichment

ایزوتوپ های اورانیوم می‌توانند از هم جدا شوند تا تمرکز یک ایزوتوپ بر دیگری را افزایش دهند. این فرایند ، غنی سازی نام دارد. وزن U-235 برای غنی شدن باید 0,711 درصد افزایش یابد. اورانیوم م235 برای استفاده در سلاح های هسته‌ای و نیروگاه های اتمی مناسبتر است.

غنی سازی با سانتریفیوژ Enrichment with Centrifuge

سانتریفیوژ دستگاهی است که برای جدا سازی مواد از یکدیگر بر اساس وزن آنها استفاده می‌شود. این دستگاه مواد را با سرعت زیاد حول یک محور به گردش در می‌آورد و مواد متناسب با وزنی که دارند از محور فاصله می‌گیرند. در واقع در این روش برای جدا سازی مواد از یکدیگر از شتاب ناشی از نیروی گریز از مرکز استفاده می‌گردد، کاربرد عمومی این دستگاه برای جداسازی مایع از مایع و یا مایع

از جامد است. سانتریفیوژهایی که برای غنی سازی اورانیوم استفاده می‌شود حالت خاصی دارند که برای گاز تهیه شده‌اند که به آنها Hyper-Centrifuge گفته می‌شود.

گونه‌های اورانیوم kinds of Uranium

-آلفا (Orthohombic) که تا دمای 667,7 درجه پایدار است.

- بتا (Tetragonal) که از دمای 667,7 تا 774,8 درجه پایدار است.

- گاما (Body-centered cubic) که از دمای 774,8 درجه تا نقطه ذوب پایدار است. (این رساناترین و چکش‌خوارترین گونه اورانیوم می‌باشد)

دو ایزوتوپ مهم ان U235 و U238 می‌باشند که U235 مهمترین برای راکتورها و سلاح های هسته‌ای است. چرا که این ایزوتوپ تنها ایزوتوپی است که در طبیعت وجود دارد و در هر مقدار ممکن توسط نوترون های حرارتی شکافته می‌شود. ایزوتوپ U238 نیز از این جهت مهم است که نوترونها را برای تولید ایزوتوپ رادیواکتیو جذب کرده و آن را به ایزوتوپ Pu239 پلوتونیوم تجزیه می‌کند. ایزوتوپ مصنوعی U233 نیز شکافته شده و توسط بمباران نوترونی Thorium232 بوجود می‌آید.

واحد سنجش قدرت هسته‌ای Nuclear power unit

قدرت انفجارهای هسته‌ای بر حسب T.N.T (تری نیترو تولوئن) می‌باشد. وقتی گفته می‌شود یک بمب هسته‌ای 20 مگاتنی ، منظور این است که انرژی حاصل از این بمب برابر انرژی حاصل از 20 مگاتن تی ان تی است. یعنی باید 20 مگا تن T.N.T منفجر شود تا انرژی معادل بمب هسته‌ای مذکور تولید شود.

کاربرد حرارتی انرژی هسته ای Thermal Application of Nuclear energy

گرمای حاصل از واکنش هسته‌ای در محیط راکتور هسته‌ای تولید و پرداخته می‌شود. بعبارتی در طی مراحلی در راکتور این گرما پس از مهارشدن انرژی آزاد شده واکنش هسته‌ای تولید و پس از خنک سازی کافی با آهنگ مناسبی به خارج منتقل می‌شود. گرمای حاصله آبی را که در مرحله خنک سازی بعنوان خنک کننده بکار می‌رود را به بخار آب تبدیل می‌کند. بخار آب تولید شده ، همانند آنچه در تولید برق از زعال سنگ ، نفت یا گاز متداول است، بسوی توربین فرستاده می‌شود تا با راه اندازی مولد ، توان الکتریکی مورد نیاز را تولید کند. در واقع ، راکتور همراه با مولد بخار ، جانشین دیگ بخار در نیروگاه‌های معمولی شده است.

کاربردهای اورانیوم غنی شده

شرایطی ایجاد کرده اند که نسبت U235 به U238 را به 5 درصد می‌رساند. برای این کار و تخلیص کامل اورانیوم از سانتریفوژهای بسیار قوی استفاده می‌کنند.

برای ساختن نیروگاه اتمی ، اورانیوم طبیعی و یا اورانیوم غنی شده بین 1 تا 5 درصد کافی است.

برای تهیه بمب اتمی حداقل 5 تا 6 کیلوگرم U235 صد درصد خالص نیاز است. در صنایع نظامی از این روش استفاده نمی‌شود و بمب های اتمی را از Pu239 که سنتز و تخلیص شیمیایی آن بسیار ساده‌تر است، تهیه می‌کنند.

3- واژگان تهدیدات EMP و بمب گرافیتی

اثرات EMP روی تجهیزات موشک EMP Efective on device

نتیجه اثر مستقیم پرتوهای گاما و X حاصل از انفجار هسته‌ای روی سیستم ها می‌باشد. چون پرتوهای گاما و X در اتمسفر زمین تضعیف می‌شوند، این پرتوها روی سیستم های خارج از جو نظیر ماهواره‌ها و موشک های در حال پرواز اثر می‌گذارند. SGEMP، مدهای تزویج پیچیده‌ای برای هر سیستم دارد که با توجه به شرایط فیزیکی و الکتریکی سیستم، می‌تواند میدان های الکتریکی با قدرت تا چند kV/m100 تولید کند. (منبع 4)

الیاف کربنی Carbon fibers

الیاف کربنی به گروه‌های زیر تقسیم‌بندی می‌شوند:

1- پلی‌اکلریلونیتریلی 2- قطران میان فاز 3- قطران 4 P.V.C- ریونی

الیاف گرافیتی Graphit fibers

الیاف گرافیت از الیاف آلی، مانند الیاف ابریشم مصنوعی تولید می‌شوند. این الیاف طی فرآیندهایی در دمای 3000 گرافیتی و منظم می‌شوند. الیاف بدست آمده دارای درجه خلوص بالایی هستند.

انتشار از روی پوشش Propagation of cover

میدان های حاصل از EMP از دیواره‌های هادی غیر ایده‌آل قفسه‌های پوشش به دلیل اثر پوستی عبور می‌کنند، دلیل این مسأله دامنه بسیار بالای این میدان ها و قدرت نفوذ آن ها خصوصاً در فرکانس های پایین می‌باشد (منبع 4)

انفجار هسته ای در سطح زمین SBEMP

انفجار هسته ای در ارتفاع کمتر از km2/0 از سطح زمین که ناحیه‌ای با شعاع تقریبی حدود km3 تا km5 دارد را یک SBEMP می نامیم. چنین انفجاری می تواند ناحیه ای به شعاع km10 و بیشتر را با میدان های الکترومغناطیسی بسیار قوی تحت تأثیر قرار دهد. (منبع 4)

بمب الکترومغناطیسی Electro-Magnetic pulse(EMP)

یک پالس الکترومغناطیسی بسیار باریک با دامنه بسیار بزرگ است و در حوزه فرکانس محدوده زیادی را پوشش می‌دهد. یک بمب الکترومغناطیسی به خاطر پهنای باند فرکانسی زیاد و انرژی فراوان، قادر است تجهیزات الکترونیکی و مخابراتی زیادی را از کار انداخته و یا بسوزاند. همانطور که ذکر شد یکی از روش‌های تولید پالس الکترومغناطیسی انفجار هسته‌ای است. روش‌هایی غیر از انفجار هسته‌ای نیز وجود دارد.این پالس ها ممکن است توسط انفجارهای هسته‌ای در ارتفاعات مختلف نیز بوجود آیند. (منبع 4)

پاکسازی آلودگی‌های گرافیتی Cleaning of graphit bomb

دمش هوای فشرده – مکش - استفاده توآم از دمش و مکش - استفاده از آب، حلال و مواد شیمیایی - پاکسازی دستی

پالس الکترومغناطیسی هسته ای HEMP

پدیدهHEMP حاصل از یک انفجار هسته‌ای در ارتفاع بالاتر از 30 مایلی سطح زمین می‌باشد که در پی این انفجار، پرتوهای گاما در خارج از اتمسفر و یا جاهایی که اتمسفر رقیق می‌باشد، شروع به تابیدن از محل انفجار می‌کند. پرتو گاما در واقع تابش فوتون های پرانرژی می‌باشد که پس از انفجار به طرف خارج از صحنه انفجار پرتاب می‌شوند. (منبع 4)

تداخل الکترومغناطیسی Electromagnetic Interferenc

تداخل الکترومغناطیسی، فرایندی است که بوسیله ارسال انرژی الکترومغناطیسی ناخواسته و درهم گسیخته (نویز) از یک قطعه، مدار یا سیستم، به قطعه، مدار یا سیستم دیگر، توسط مسیرهای تشعشعی (مانند فضا)، هدایتی (مانند سیم‌ها و مسیرهای روی برد مدار چاپی) و یا هر دو ایجاد می شود (منبع 4)

تداخل الکترومغناطیسی داخلی insider EMI

اجزاء یا عوامل مختلف موجود در داخل یک سیستم یا مدار، سبب ایجاد تداخل الکترومغناطیسی در قسمتهای مختلف دیگر می شوند.

گروه تداخل داخلی می تواند به خاطر وجود بازتاب یا افت سیگنال در طول یک مسیر انتقال، تداخل سیگنالی و ... ایجاد گردد (منبع 4)

جداسازی زیر سامانه‌ها Segregation subsystem

هدف اولیه از جداسازی زیر سامانه‌ها رسیدن به خودسازگاری الکترومغناطیسی در سامانه بر مبنای جداسازی بخش‌های حساس از بخش‌های نویزی سامانه می‌باشد.با اولویت بندی سامانه های حساس در پوشش‌ها و بسته‌بندی‌های مناسب قرار گرفته و پوشش بخش های مختلف به دقت زمین می‌شوند (منبع 4)

حساسیت پذیری Susceptibility

تداخل ناشی از حساسیت پذیری(یا عدم ایمنی) نیز همان تداخلی است که دیگر سیستم ها روی همان سیستم مورد نظر ایجاد می کنند. این تداخل از طریق تشعشع مستقیم به قسمت های مختلف یک سیستم یا مدار، ایجاد شده است (منبع 4)

حفاظت در برابر EMP Protection of EMP

عبارتند از: الف- اصل جداسازی زیر سامانه‌ها ب- زمین کردن ج- فیلترهای EMI
د- استفاده از پوشش ح- استفاده توأم از فیلتریگ و پوشش (منبع 4)

روش‌های تولید EMP (غیر هسته ای) EMP Generation method

فناوری اساسی که تولید پالس های الکترومغناطیسی در سلاح ها توسط آن ها صورت می گیرد، غالباً عبارتند از: مولد های فشرده سازی شار (FCG) ، ژنراتور های Magnet-Hydrodynamic و دسته ای از وسایل پرقدرت مایکروویو (HPM) که در رأس آن ها نوسان ساز با کاتد مجازی یا ویرکتور (Vircator) قرار دارد (منبع 4)

زمین کردن Grounding

هدف اولیه در زمین کردن سامانه‌ها، تضمین امنیت پرسنل و حفاظت دستگاه‌ها می‌باشد. عوامل اصلی برای لزوم استفاده از زمین امنیتی، نقص های سامانه توان و صاعقه می‌باشد که نوعاً جریان های تا دهها کیلوآمپر در محدوده فرکانسی تا چند مگاهرتز دارد و ممکن است حتی امنیت جانی پرسنل را به خطر بیندازد (منبع 4)

سازگاری الکترومغناطیسی Electromagnetic Compatibility

منظور از سازگاری الکترومغناطیسی در یک سیستم یا مدار آن است که دارای سه شرط اساسی ذیل باشد: الف- باعث ایجاد تداخل در دیگر سیستم ها نشود؛

ب – سیستم‌های اطراف در آن تداخل ایجاد نکنند؛ ج – در خودش تداخل ایجاد نکند. (منبع 4)

سیستم تولید کننده EMP EMP Generator System

نتیجه اثر مستقیم پرتوهای گاما و X حاصل از انفجار هسته‌ای روی سیستم ها می‌باشد. چون پرتوهای گاما و X در اتمسفر زمین تضعیف می‌شوند، این پرتوها روی سیستم های خارج از جو نظیر ماهواره‌ها و موشک های در حال پرواز اثر می‌گذارند (منبع 4)

عملکرد بمب گرافیتی operation of graphit bomb

فناوری به کار گرفته شده در این بمب ها مشابه بمب های خوشه‌ای است که حاوی تعدادی بمب کوچک می باشددر هر یک از این بمب‌های کوچک تعداد زیادی قرقره (147 عدد) وجود دارد که با انفجار بمب، الیاف گرافیت از قرقره ها باز شده و در هوا پخش می شود و بر روی هدف فرود می آید و در سیستم های تولید و انتقال برق ایجاد اتصال کوتاه نموده و سبب قطع برق می شوند.

فیلترهای EMI EMI filters

فیلترها برای تضعیف و تلف کردن سیگنال‌های موجود روی سیم‌های هدایت کننده جریان ناخواسته به کار می‌رود، حال آن که اثری در کاهش توان سیگنال در فرکانس‌های اصلی ندارد.(منبع)

قفس فارادی Cage of Faraday

یکی از روش های مؤثر ، برای حفاظت سیستم ها و تجهیزات در برابر EMP ، قراردادن کل

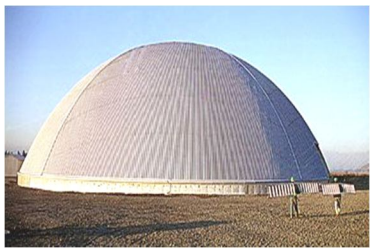
تجهیزات در داخل یک پوشش است که به قفس فارادی معروف می باشد، اگـر ایـن پوشـش بـه درستی طراحی شده باشد می تواند تا مقـدار زیـادی از ورود امـواج مخـرب بـه تجهیـزات جلـوگیری نماید(منبع 4)

گرافیت Graphit

گرافیت از جنس کربن بوده و خاکستری رنگ است.گرافیت دارای رسانایی نسبتاً بالایی است. علت این امر را نیز می‌توان در ساختار لایه‌ای گرافیت و الکترون چهارمی جستجو کرد که ارتباط بین لایه‌هـا را برقرار می‌سازد. از طرف دیگر گرافیت دیرگداز است و همانطور که اشاره شد تا دمای 3890 درجـه سانتیگراد دچار تحول نمی‌شود.رسانایی بسیار بـالا و مقاومـت الکتریکـی خیلـی کـم یکـی از بهتـرین گزینه ها برای استفاده در بمب های خاموشی به منظور ایجاد اتصال کوتاه در خطوط فشار قـوی شـبکه برق می‌باشند و در آینده نزدیک نیز ماده اولیه هر بمب خاموشی در هر کشور پیشرفته‌ای خواهد بود.

مقابله با بمب گرافیتی Protection of Graphit bomb

1- آشکارسازی و ره‌گیری ادوات و سیستم های حمل و پرتـاب ایـن بمـب‌هـا 2-اسـتفاده از سقف‌های فلزی، توری یا پلاستیکی برای جلوگیری از تماس الیاف گرافیت 3- استفاده از چتر بـرای جمع‌کردن الیاف گرافیت.



یک نمونه از سقف‌های محافظ مدور بدون درز

نشت از روزنه‌ها Leakage of slot

هر پوششی ناچار دارای درها، پنجره‌ها، حفره‌ها، درزها و ... می‌باشد که می تواند منشأ ورود میدان های EMP به داخل پوشش گردد. روزنه‌ها هم به میدان های الکتریکی و هم به میدان هـای مغناطیسـی اجازه نفوذ می‌دهند. نشت میدان از یک روزنه به سایز، نوع ساختار و مکان روزنه روی پوشش بسـتگی دارد (منبع 4)

فصل پنجم

واژگان مدیریت بحران

۱- واژگان مدیریت بحران

آب گرفتگی حاصل از باران Flood

به آب گرفتگی گفته می شود که از بارش باران به وجود آمده است و جریان می یابد تا بـه منطقـه وسیعی برسد و خود به خود خشک شود یا به دریا یا رودخانه ای متصل ریخته شود.

آگاه سازی از وضعیت مردم Notification of people

توانایی به دست آوردن اطلاعات در کوتاه ترین زمان ممکن در مورد سـاختمان هـا و افـرادی کـه ممکن است تحت تهدید حوادث قرار بگیرند.

آلاینده Pollutant or Contaminant

هرگونه عنصر، ماده، ترکیب یا مخلوطی که محتوی عاملان بیماری زا هسـتند و بعـد از رهـایی بـه محیط زیست و به محض بلعیدن، تنفس یا جذب آن توسط هر جانداری، چه بصورت مستقیم از محیط یا بصورت غیرمستقیم با بلعیدن آن از طریق زنجیره غذایی انتظار می رود که منجر بـه مـرگ، بیمـاری، ناهنجاری های رفتاری، سرطان، جهش ژنتیکی، کژکاری فیزیولوژیکی یا دگردیسـی فیزیکـی در چنـین جاندارانی یا اولادشان شود. (تعریف شده درسند ملی مدیریت بحران) (منبع ۲۲)

آمادگی قبل از بحران Pre- crisis preparedness

شامل کلیه عملیات و اقداماتی است که دولت ها، جوامع و همچنین افراد را قادر به انجـام عکـس العمل سریع و کارا در مواقع بروز بحران می نماید. اقدامات آماده سازی در کل شامل تهیه یـک برنامـه ضد بحران، برآورد دقیق منابع و هم چنین آموزش پرسنل می باشد. (منبع ۵)

اتاق وضعیت Status room

هدف از ایجاد اتاق وضعیت، ایجاد مکانی برای تمرکز فعالیت های مرتبط با همـاهنگی فرمانـدهی حادثه جنگی، با در نظر گرفتن تمهیدات خاص معماری و فراهم آوردن تجهیزات و امکانات مناسـب و مورد نیاز در آن تا مدیران در شرایط وقوع بحران بتوانند در این مکان امن گرد هم آمده و با اسـتفاده از تجهیزات و اطلاعات فراهم شده در ساختمان بـه تحلیـل شـرایط موجـود بپردازنـد و همـاهنگی‌هـای

ضروری را بر اساس اصول مقابله با بحران با هدف کنترل سریع بحران انجـام داده و دسـتورات لازم را صادر نمایند. (منبع ۲۲)

ارزیابی و تشخیص هشدار Alarm Assessment

ارزیابی و شناخت علائم خطری که هنگام وقوع یا احتمال بحرانی از تلویزیون برای مـردم پخـش می شود.سیستم هایی که برای اعلام هشدار طراحی می شوند باید در هنگام احتمال خطر به سـرعت و به صورت اتوماتیک عمل کنند.

اطلاعات عمومی شرایط اضطراری Emergency Public Information

اطلاعاتی که بطور ابتدایی در پیش بینی یک حادثه یا در طول یک حادثه منتشر می شود. علاوه بـر تأمین اطلاعات وضعیتی برای عموم مردم، فعالیت هایی که باید توسط مردم انجام گیرد نیز اطلاع رسانی می شود.(منبع ۲۲)

امداد رسانی Helping

فعالیت های مربوط به امداد رسانی به کلیه عملیـات و اقـداماتی کـه قبـل و بعـد از وقـوع بحـران می بایست صورت بگیرد را شامل می شوند این عملیات و اقدامات در جهت حفاظت از جان مـردم و تأسیسات و دارایی های موجود انجام می گردد. (منبع ۵)

انواع رزمایش kinds of drill

انواع رزمایش ها عبارتند از:

رزمایش های مباحثه‌ای – رزمایش های کارکردی – رزمایش های میدانی (منبع ۲۲)

باران اسیدی Aside Rain

یکی از جدی‌ترین مشکلات زیست محیطی که امروزه بسیاری از مناطق دنیا با آن روبه‌رو هسـتند، باران اسیدی است .باران اسیدی دارای انواع نتایج زیان‌بار بوم شناختی است وجـود اسـید در هـوا نیـز احتمالا بر روی سلامتی انسان اثر دارد. پدیده باران اسیدی در سـال هـای آخـر دهـه ۱۸۰۰ در بریتانیـا کشف شد، باران اسیدی به نزولات جوی که قدرت اسیدی آن بطور قابل توجهی بیش از بـاران طبیعـی باشد، اطلاق می‌شود.

بازسازی Reconstruction

بازسازی عبارت است از تأمین کل خدمات و زیرساخت های تخریب شده، جایگزینی کالبدی

بناهای منهدم شده، احیا کردن و توانمند ساخت مجاری اقتصادی و در نهایت بهبود شرایط زیست جامعه مصیبت زده. (منبع ۵)

بازسازی اجتماعی Community Recovery

فرآیند ارزیابی اثرات یک حادثه ملی، تعیین منابع و توسعه و اجرای روش کار برای ترمیم و احیای ساختارهای اجتماعی اقتصادی و فیزیکی جامعه را گویند (منبع ۲۲)

بازیابی Recovery

عبارت است از پاکسازی، تولید مجدد محصول، ذخیره سازی مجدد و کمک به افـراد، خـانوادههـا، گروهها و نواحی آسیب دیده برای بازگشت به وضعیت عادی (منبع ١٤)

بازیابی (پس از بحران)

مجموعه عملیات پس از مرحله امداد اضطراری را بازیابی می نامند، که شامل دو مرحله ساماندهی و بازسازی است. (منبع ۵)

بحران Crisis

بحران رویدادی است که به طور طبیعی یا بوسیله بشـر، بـه طـور ناگهـانی (Emergensy) یـا بـه صورت فزاینده (Crisis) بوجود آید و سختی و مشقتی را به جامعه انسانی تحمیل کند که برای برطرف کردن آن نیاز به اقدامات اضطراری، اساسی و فوق العاده باشد.

به عبارتی بحران فرآیندی است که در نتیجه یکسری عوامـل طبیعـی و غیرطبیعـی شـامل: انفجـار، زلزله، فوران، آتشفشان، تسونامی، زمین لغزش، سیل، طوفان، آتش سوزی های مهیب، نشـت گازهـا یـا مواد خطرناک، ناکارآمدی های فناوری، هجوم، بیماری های واگیردار، اپیدمی ها، ناکارآمدی ها یـا عـدم کاربری های خدمات اوراژنس، حملات احتمالی یا واقعی یا چیزی شبیه جنگ و... اتفاق افتاده است و سبب به خطرافتادن جان انسان ها یا آسیب پذیری، بیماری، فاجعه یا به خطر افتادن امنیـت جوامـع یـا اموال ملی و مردمی می شود.(منبع ۵)

بسیج کردن Mobilization

فرآیند و روندی که بوسیله تمام سازمان ها ی ملی، استانی و محلی- برای فعال کردن، جمع آوری و انتقال منابع برای مقابله و پشتیبانی حوادث انجام می گیرد.(منبع ۲۲)

بهبودی Recovery

این بخش از چرخه مدیریت بحران شامل کلیه عملیاتی است که به منظور عادی سازی شرایط وقوع بحران صورت می پذیرد. مرحله بهبودی و عادی سازی اوضاع معمولا توأم با بهسازی و بازسازی نیز می باشد. (منبع ۵)

بیماران تخلیه شده از صحنه Evacuees

افرادی که از محیط خطرناک یا حادثه دیده خارج شده باشند یا از زیر آوار به بیرون کشیده شده باشند.

پرسنل ستاد فرماندهی Staff personal commander

شامل مأمور اطلاعات عمومی، مأمور امنیت، رابط مناصب دیگر بر حسب نیاز، که بطور مستقیم به فرماندهی گزارش می دهند. آنها ممکن است همیار یا همیارانی داشته باشند. (منبع ۲۲)

پیشگیری Mitigation

کلیه اقداماتی که موجب پیشگیری از وقوع بحران ها و همچنین سبب جلوگیری از اثرات مخرب آن برجامعه شود. به عنوان مثال احداث سدها و یا اقدامات انجام شده جهت جلوگیری از طغیان رودخانه ها، مقاوم سازی ساختمان ها برای مقابله با زلزله و... را می توان به عنوان اقدامات پیشگیرانه نامید. همچنین پیشگیری شامل آموزش دولت مردان، مشاغل و مردم مرتبط با اقداماتی که می تواند برای کاهش تلفات و خسارات انجام گیرد، می شود.(منبع ۵)

تخلیه مردم people Evacuation

عقب نشینی، پراکندگی و جابجایی سازمان دهی شده و سرپرستی شده شهروندان از مناطق خطرناک و یا بالقوه خطرناک و پذیرش و مراقبت از آنها در مکان های امن را تخلیه گویند.(منبع ۲۲)

تشخیص و سندیت Identificat & Authenticatio

افراد و سازمان هایی که به سیستم مدیریت اطلاعات سامانه مدیریت بحران کشور دسترسی دارند، خصوصا آن هایی که اطلاعات را به سیستم وارد می کنند. (نظیر گزارشات وضعیت)، باید بطور دقیق برای اهداف امنیتی تأیید و تصدیق شوند.(منبع ۲۲)

تشعشع سنج Dosimeter

یک دستگاه قابل حمل برای اندازه گیری میزان تشعشع رادیواکتیو.

چارچوب مدیریت ریسک Risk management Framework

یک متدولوژی برنامه ریزی شده که فرآیندی را برای استقرار اهداف امنیتی؛ تشخیص عملکردها، شبکه ها، سیستم ها و اموال؛ ارزیابی ریسک ها؛ اولویت بندی و اجرای طرح های حفاظتی؛ارزیابی اجرا؛ و انجام عملیات اصلاحی طراحی می کند(منبع ۲۲)

چک لیست Checklist

لیست موضوعاتی که بر اساس تجربیات قبلی توسعه یافته اند و بعنوان راهنما در اجرای سطح استانداردی از مراقبت از فعالیت های موضوع و یا در تکمیل فعالیت در سرتاسر یک روش کمک می کند.(منبع ۲۲)

حادثه فاجعه انگیز Catastrophic Incident

هرگونه حادثه طبیعی یا انسان ساز، ازجمله تروریسم، که منجر به تلفات، خسارات یا اختلالات شدید و گسترده می شود و افراد، زیرساخت ها، محیط زیست، اقتصاد، روحیه ملی و یا عملکردهای دولت را به شدت تحت تاثیر قرار می دهد. فاجعه منجر به اثراتی در سطح ملی و در یک دوره زمانی طولانی مدت می شود. تقریبا بلافاصله بعد از حادثه، منابعی که به صورت عادی در مراکز استانی، محلی، ناحیه ای یا بخش خصوصی موجود هستند، روانه مناطق تحت تاثیر می شوند. فعالیت های دولتی و خدمات اورژانسی در اثر گستردگی حادثه بصورت مشخصی مختل می شود و امنیت ملی می تواند تهدید شود (منبع ۲۲)

حادثه، واقعه Incident

در فرهنگ آریان پور این لغت به معانی اتفاق، حادثه، واقعه، رویداد ورخداد آورده شده است.

به معنی یک حادثه دردرون مجموعه ای از حوادث پشت سرهم است (منبع ۲۲)

دفاع غیرنظامی Civil Defense

مجموعه فعالیت هایی که می‌توان با انجام آن از بروز و استمرار سوانحی که جان و مال مردم را تهدید می‌کنند مانند سیل، زلزله، آتشفشان، آتش‌سوزی، طوفان و ... جلوگیری نمود و یا در صورت بروز، آثار ناشی از آن را کاهش داد. تأکید اصلی دفاع غیرنظامی، حفاظت از مردم و انجام اقدامات اضطراری برای تعمیر و راه‌اندازی مجدد خدمات و تأسیسات جهت ادامه فعالیت‌های روزمره می‌باشد.

حفاظت شهروندان در مقابل خطرات ناشی از جنگ و دیگر بلایا، کمک به افراد برای بازیابی از عواقب آن حوادث، و فراهم نمودن شرایط لازم برای بقای افراد در زمان وقوع آنها.(منبع ۲۲)

رزمایش Drill

مانور یک روش متداول برای پایش و ارزشیابی بخش‌های مختلف یک برنامه آماده‌سازی، انجام تمرین و مانور است .انجام مانور در اصل برای ارزیابی میزان اثربخشی و کارایی برنامه مقابله و آمادگی یک جامعه برای شرایط حوادث اعم از حوادث طبیعی یا جنگ استفاده می‌شود.(منبع ۲۲)

رزمایش میدانی Field Drill

مشخصات رزمایش های میدانی:

در این رزمایش ها، نیروها وارد تمرینی می‌شوند که شبیه حادثه واقعی است. این حادثه می‌تواند یک تصادف بازسازی شده یا یک کارخانه منفجر شده باشد.

در این نوع از رزمایش ، اجزایی از رزمایش های کارکردی به علاوه هماهنگی‌های کنترلی و همچنین مهارت‌های میدانی ارزیابی می‌شوند.معمولا قبل از رزمایش های میدانی، رزمایش های مباحثه ای یا کارکردی زیادی انجام می‌شوند. (منبع ۲۲)

رزمایش مباحثه‌ای Controversy Drill

مشخصات رزمایش های مباحثه ای:

- در این رزمایش ها بحث بر روی سناریو انجام می‌شود.
- در این نوع از رزمایش ، افراد، موارد توافق شده قبلی را با هم مرور می‌کنند و از این راه، اثربخشی برنامه‌ها را آزمایش می‌کنند، ارتباط‌ها را شکل می‌دهند و به دنبال ایده‌های جدید هستند.چهار نوع شایع از رزمایش های مباحثه ای عبارتنداز: رزمایش های آگاه سازی، رزمایش های معرفی سازمان‌ها از خود، رزمایش های فرضی و رزمایش های تیمی (منبع ۲۲)

رزمایش کارکردی Operation Drill

مشخصات رزمایش های کارکردی:

این نوع از رزمایش هم از رزمایش های مباحثه‌ای است ولی در یک محیط عملیاتی اجرا می‌گردد و به شرکت‌کنندگانی نیاز دارد که واقعا کارکردهای مربوط به نقش‌های خود را بازی می‌کنند.

این نوع از رزمایش را به نام رزمایش های دورمیزی و یا مانورهای تاکتیکی بدون سپاه نیز می‌گویند. (منبع ۲۲)

سازمان غیردولتی Nongovernmental Organi zati

نهادی که بر اساس تمایل و علاقه اعضا، افراد یا موسساتی ایجاد می شود. این سازمان ها به وسیله دولت به وجود نیامده اند ولی ممکن است با دولت همکاری داشته باشند. چنین سازمان هایی نه به دلایل شخصی بلکه برای اهداف عمومی خدمت می کنند. نمونه ای از NGO ها شامل سازمان های خیریه و صلیب سرخ می باشد.(منبع ۲۲)

ساماندهی Organiz

ساماندهی دلالت دارد بر بازگرداندن خدمات بنیادی به عملکردهای پیش از سانحه، کمک به مردم در جهت خودکفایی و خودباوری، مرمت خرابی ها، اعطای تسهیلات مالی، احیای فعالیت ها ی اقتصادی و فراهم آوردن زمینه های حمایت از بازماندگان در زمینه های روانی، اجتماعی. مرحله ساماندهی به طور عمده برتوانمند کردن آسیب دیدگان متمرکز است، تا جامعه آمادگی بازگشت به الگوهای زیست قبل از بحران را بیابد. (منبع ۵)

سناریو Senario

یک سناریو، تنها پیش بینی یک آیندهٔ خاص نیست، بلکه توصیف همهٔ احتمالات است. در واقع، سناریو تصویری از آیندهٔ ممکن و محتمل است.سناریو ابزاری برای تحلیل سیاست ها و شناخت شرایط، تهدیدات، فرصت ها، نیازها، و ارزش های برتر آینده است (منبع ۲۲)

سیستم فرماندهی سانحه Incident Command System

ترکیبی از تسهیلات، تجهیزات، پرسنل، روندها و ارتباطات می باشد که تحت یک ساختار سازمانی معمول عمل می کند و برای کمک به مدیریت منابع در طول حوادث تعیین می شوند. ICS برای انواع شرایط اضطراری و انواع حوادث از بزرگ تا کوچک و پیچیده قابل استفاده است (منبع ۲۲)

سیستم ملی مدیریت حادثه Incident Managment National System

این سیستم بعنوان سیستم فرماندهی حادثه؛ سیستم هماهنگی سازمانها؛ آموزش؛ تشخیص و مدیریت منابع (نظیر سیستم های طبقه بندی انواع منابع)؛ کیفی سازی و تصدیق و جمع آوری، ردیابی و گزارش دهی اطلاعات و منابع حادثه عمل می نمایید.(منبع ۲۲)

سیستم هماهنگی سازمان ها Organization Coordination System

تأمین ساختار برای پشتیبانی از هماهنگی برای اولویت بندی حوادث، تخصیص منابع حیاتی، یکپارچگی سیستم های ارتباطی و هماهنگی اطلاعات، مؤلفه های سیستم های هماهنگی سازمانها شامل

تسهیلات، تجهیزات، پرسنل، روندها و ارتباطات است. دو مؤلفه مهم عبارتند از مراکز عملیاتی (EOC) و گروه های هماهنگی (MAC). این سیستم ها، آژانس ها و سازمان ها را در مقابله با حوادث کمک می کنند. (منبع ۲۲)

شرایط اضطراری Emergency term

شرایط اضطراری عبارتست از هرگونه حادثه اتفاقی یا لحظه ای که کمک های ملی برای تکمیل فعالیت ها و توانایی های محلی یا استانی نیاز می شود تا به کمک آنها از جان و اموال انسان ها و سلامت و امنیت عمومی حفاظت شود.(منبع ۲۲)

عملکرد پشتیبانی اضطراری Emergency Support Function

گروهی از ظرفیت های حکومتی و بخش خصوصی در یک ساختار سازمان دهی شده برای تأمین پشتیبانی، منابع، اجرای برنامه و خدمات که بیشتر برای نجات انسان ها، حفاظت از اموال و محیط زیست، ترمیم خدمات ضروری و زیرساخت های حیاتی و کمک به قربانیان و جامعه برای بازگشت به حالت عادی در ادامه حوادث داخلی نیاز می شوند. (منبع ۲۲)

عملیات ایمن سازی Continuity of Operations

کنترل ها ی ایمن سازی برای جلوگیری از وقوع اتفاقات ناخوشایند و به حداقل رساندن خسارات.

فاجعه، بلا Disaster

در فرهنگ آریان پور این لغت به معانی مصیبت، فاجعه، بلا و سانحه آورده شده است. در دیکشنری Random House Unbridged، این لغت به معنی یک پدیده فاجعه بار نامیده شده است که ناگهانی رخ داده و باعث مرگ انسان ها و صدمات جدی در زندگی آنها می گردد. حوادثی مانند سیل و سقوط هواپیما مثال هایی از این نوع حوادث هستند. طبق تعریف سازمان بهداشت جهانی، بلایا (Disaster)، به هرحادثه ای اطلاق می شود که باعث ایجاد صدمات، اختلالات زیست محیطی، مرگ ومیر انسان ها و به هم ریختن خدمات نظام سلامت در مقیاسی شود که نیاز به کمک های خارج از جامعه برای اداره حادثه باشد.(منبع ۲۲)

فرآیند مدیریت بحران Crisis management procese

فرآیند مدیریت بحران در یک تقسیم بندی کلی به سه مرحله تقسیم می شود:

مرحله قبل از بحران، حین بحران و پس از بحران.

هریک از این مراحل خود شامل بخش های مختلفی می شود این بخش ها فرایند مدیریت بحران را تشکیل می دهد که عبارت است از: **پیشگیری، آمادگی، پاسخگویی و امدادرسانی(خدمات اضطراری) بهبودی، بازسازی و سازماندهی** می باشد. (منبع ۵)

فرماندهی سانحه Incident Commander

مسئول تمام بخش های مدیریت سانحه و شامل فرمانده سانحه ، فرماندهی یکپارچه یا یگانه و هرگونه پرسنل پشتیبانی می باشد.(منبع ۲۲)

گزارش‌های مدیریتی رزمایش Drill managment Reports

نکات مهمی که در گزارش های مدیریتی رزمایش باید مورد توجه قرار گیرد:

میزان دقت و جزئی‌نگری در گزارش‌نویسی‌ها، خیلی متغیر هستند و به اندازه و پیچیدگی رزمایش مرتبط می‌باشند.حداقل گزارش می‌تواند یک صفحه باشد و شامل محتویات زیر باشد:

هدف – یک یا دو نتیجه – یک سناریو با چندین ایده خاص – جزئیات محل رزمایش – تجهیزات لازم – زمان لازم . (منبع ۲۲)

لایه ازن Ozone layer

یکی از مسائلی که در سال های اخیر باعث نگرانی دانشمندان شده ، مسئله تهی شدن لایه ازن و ایجاد حفره در این لایه در قطب جنوب است. لایه اوزون در فاصله ١٦ تا ٤٨ کیلومتری از سطح زمین قرار گرفته و کره زمین را در برابر تابش فرابنفش نور خورشید محافظت می‌کند. هر گاه از مقدار لایه ازن ، ۱۰ درصد کم شود، مقدار تابشی که به سطح زمین می‌رسد تا ۲۰ درصد افزایش می‌یابد. تابش فرابنفش موجب بروز سرطان پوست در انسان می‌شود و به گیاهان صدمه می‌زند. مولکول های کلروفلوئورکربن ها (CFC) در از بین بردن لایه ازن موثرند. از این ترکیبات بطور گسترده در دستگاه های سرد کننده و در افشانه‌ها (اسپری‌ها) استفاده می‌شود.

مخاطره Hazard

به هر پدیده، ماده یا موقعیتی گفته می شود که به طور بالقوه توان آسیب رساندن یا ازبین بردن زیرساخت ها را داشته باشد ویا موجب اشکال یا قطع در سیستم های ارائه خدمات گردد و مردم، سرمایه و محیط زیست را تهدید نماید.(منبع ۲۲)

مدیریت بحران Crisis management

براساس تعریف برنامه عمرانی سازمان ملل متحد(UNDP) عبارت است از سیاست گذاری، اخذ تصمیمات مدیریتی وانجام اقدامات اجرایی به منظور آمادگی، کاهش اثرات مخرب بحران، پاسخگویی (Response) وبازسازی و بازتوانی وترمیم اثرات ناشی از بلایای طبیعی یا انسان ساخت.(منبع ۲۲)

مدیریت بحران علمی است کاربردی که به وسیله مشاهده سیستمایک بحران های پیشین و تجزیه و تحلیل آن ها درجستجوی یافتن ابزاری است که به وسیله آنها از یک سو بتوان از وقوع فجایع پیشگیری نمود و یا برای مقابله با آن ها آماده شده و از سوی دیگر در صورت وقوع آنها نسبت به امداد رسانی و بهبود اوضاع اقدام نمود (منبع ۵)

مدیریت پیامد Consequence Management

اقدامات پیشگیرانه محافظت از سلامت عمومی و امنیت،که این اقدامات می بایست از طرف سازمان های دولتی صورت گیرد و نمایندگان دولتی مسئولیت حفاظت از مردم را در حمله های خرابکاری یا ...دارند.(منبع ٤٤)

– مدیریت شرایط اضطراری و اقدامات مرتبط برای حفظ سلامت و ایمنی عمومی، ترمیم و تداوم خدمات حیاتی دولت و رها شدن دولت، مشاغل و افراد تحت تأثیر پیامدهای واقع شده در شرایط اضطراری موجب می شود مدیریت پیامدها و مدیریت بحران در برنامه مقابله ملی ،ترکیب شوند. (منبع۲۲)

مراقبت آسیب دیدگان(مردم) Mass attend

فعالیت هایی که برای حفاظت و پناه دادن به آسیب دیدگان حادثه صورت می گیرد.این فعالیت ها شامل ایجاد پناهگاه موقتی،تأمین غذا،خدمات پزشکی،لباس و پوشاک و نیازهای ضروری و اولیه زندگی برای مردمی که خانه هایشان در اثر حادثه از دست داده اند.

مراقبت اپیدمیولوژیک Epidemiulogic surveillance

پایش اپیدمیولوژیک یک سامانه مداوم شامل جمع آوری، تجزیه و تحلیل و تفسیر داده های سلامتی مهم برای طرحریزی، اجرا و ارزیابی و ارزشیابی اقدامات حفظ کننده سلامت انسانها،حیوانات و گیاهان می باشد (منبع ١٤)

مرکز ارتباطات/ اعزام Communic/ Dispatch Center

مراکز ارسال کننده سازمانی یا بین سازمانی، مراکز ارسال فرمان یا کنترل شرایط اضطراری یا هرگونه مرکزی که تماس های اضطراری را از مردم و وسایل ارتباطی دریافت می کند. این مرکز به عنوان هماهنگ کننده و پشتیبان اولیه و اصلی سیستم های هماهنگ کننده سازمان ها برای یک حادثه انجام وظیفه می کند تا المان های دیگر سیستم های هماهنگ کننده سازمان ها بصورت رسمی ایجاد گردند. (منبع ۲۲)

مرکز بازسازی بلایا Disaster Recovery Center

تسهیلاتی که در یک مکان متمرکز شده در نزدیکی منطقه حادثه دیده قرارگرفته اند تا جوابگوی درخواست های قربانیان حادثه (افراد، خانواده ها و مشاغل) برای کمک باشند(منبع ۲۲)

مرکز بازیابی در حوادث Disaster-Recovery Center

مکانی که در نزدیکی محیط های مهم مانند مجلس احداث می شود تا در هنگام وقع حادثه به سرعت مجروح ها وزخمی ها را به سرعت به محل های درمانی ببرند و همچنین این مرکز مسئول جمع آوری اطلاعات حادثه است.

مرکز بسیج منابع Mobilization Center

یک مرکز تسهیلات موقتی خارج از سایت که پرسنل و تجهیزات مقابله را از محل ورود دریافت می کند و برای پخش به مناطق محلی یا مستقیما به محل حادثه براساس نیاز و قوانین موجود عمل می کند. مرکز بسیج منابع، همچنین خدمات پشتیبانی موقت، نظیر غذا و اسکان را برای پرسنل مقابله قبل از انجام خدمات و مأموریتشان تأمین می کند.(منبع ۲۲)

مرکز عملیات شرایط اضطراری Emergency Operations Center

مکانی فیزیکی که برای هماهنگی اطلاعات و منابع برای پشتیبانی از فعالیت های مدیریت حادثه (عملیات های در صحنه) ایجاد می شود. یک مرکز عملیات ممکن است موقتی باشد و یا بصورت

دایمی و مرکزی مستقر شود. (منبع ۲۲)

مرکز ملی هماهنگی زیرساخت ها Infrastructure Coordinat Center

مرکزی است که زیرساخت های حیاتی ملی و منابع کلیدی را بصورت مداوم مانیتور می کند. در اثر وقوع یک حادثه، این مرکز وظیفه هماهنگی تقسیم اطلاعات با نهادهای مرتبط با منابع کلیدی و زیرساخت های حیاتی را دارد.(منبع ۲۲)

مزایای انجام رزمایش Drill performance premius

انجام رزمایش می‌تواند در موارد زیر ارزشمند باشد:

ارزیابی برنامه مقابله و آمادگی یک جامعه درشرایط جنگ – بررسی میزان اثربخشی و کارآیی برنامه آمادگی و مقابله درشرایط جنگ – افزایش آگاهی پرسنل و مدیران – افزایش مهارت‌ها– آشکارنمودن کارایی‌ها – ارزیابی کارایی افراد – ارزیابی استراتژی‌های مدیریت خطربرای شرایط جنگ. (منبع ۲۲)

مقابله کنندگان اولیه First Responder

پلیس، آتش نشانی و پرسنل اورژانس غیردولتی و محلی که در مراحل اولیه حادثه در حفاظت از زندگی، اموال، مدارک و محیط زیست جوابگو می باشند همانند پرسنل مدیریت بحران، سلامت عمومی، مراقبت بالینی، کارهای عمومی و دیگر پرسنل خبره پشتیبانی (نظیر اپراتورهای تجهیزات) که خدمات پشتیبانی ضروری را در حین عملیات های جلوگیری، مقابله و بازسازی تأمین می کنند. (منبع ۲۲)

نقش اطلاعات در مدیریت بحران information impress in crisis managment

پیش نیاز هریک از مراحل چهارگانه مدیریت بحران ایجاد شبکه ارتباطی، اطلاع رسانی و تهیه اطلاعات جامع و کامل از وضعیت موجود ارائه یک برآورد عملیاتی جهت ارائه فعالیت های امدادرسانی و ایجاد یک شبکه ارتباطی جهت اطلاع رسانی سریع و صحیح است این سامانه سبب افزایش دقت تصمیمات مدیریتی و شبیه سازی نتایج حاصل از این تصمیم گیری های مختلف، استاندارد بودن اطلاعات و اطلاع رسانی سریع به مسؤلان و امدادگران شده است (منبع ۵)

نهاد هماهنگی سازمان ها Multiagency Coordination Entity

دارای عملکردهایی فراتر از سیستم هماهنگی سازمان ها میباشد. اولویت بندی بین حوادث و

اختصاص منابع وابسته، سازگاری سیاست های سازمانی و تدارک راهبردهای استراتژیک برای پشتیبانی فعالیت های مدیریت بحران از جمله عملکردهای این نهاد می باشد.(منبع ۲۲)

هماهنگ کردن Coordinate

توسعه سیستماتیک یک آنالیز یا مبادله اطلاعات در بین رؤسا، کسانی که نیاز به دانستن اطلاعات موثق برای اجرای مسئولیت های مدیریت حادثه دارند. (منبع ۲۲)

کاهش خطر Hazard Mitigation

هر فعالیتی که باعث کاهش خطر زندگی افراد شود . این تعریف گاهی اوقات در مورد اینکه کسی این حس خطر را قبل از وقوع حادثه احساس کند به کار می رود

کاهش اثرات سانحه Incident Mitigation

فعالیت هایی که در طول یک حادثه اجرا می شوند تا اثرات و خسارت به اموال یا محیط زیست را به حداقل برساند.(منبع ۲۲)

کاهش اثرات مخرب Destroyer effect reduction

کلیه عملیات و اقداماتی که تحت یک برنامه منسجم و جامع جهت کاهش اثرات بحران در یک کشور و یا برای منطقه خاصی انجام می گیرد را می توان به عنوان کاهش اثرات بحران نام برد.

به عنوان مثال تهیه و کاربرد کدهای ساختمانی به منظور کاهش خسارات و آسیب های ناشی از زلزله برای ساختمان ها. (منبع ۵)

کاهش مخاطرات Hazard mitigation

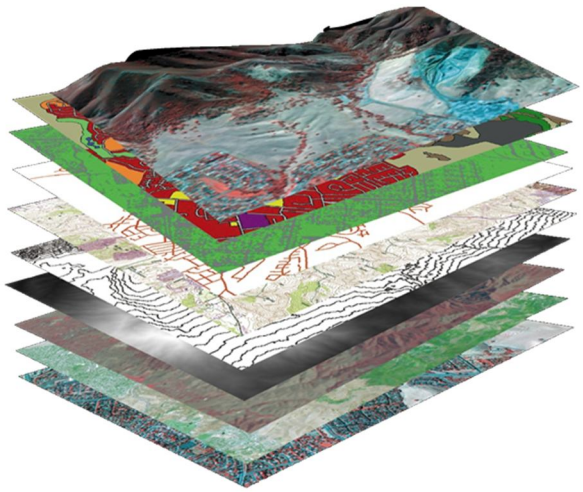
هرگونه اقدام توجیه شده از نظر اقتصادی که سبب کاهش پتانسیل خسارت به تسهیلات می شود.(منبع ۲۲)

فصل ششم

واژگان استتار ،اختفا و فریب(CCD)
و سنجش از دور

۱- واژگان استتار ،اختفا و فریب(**CCD**)

۲- واژگان سنجش از دور




ATF
NOAA

۱- واژگان استتار ،اختفاء و فریب(CCD)

اثرات دود Smoke efects

اثرات ناخواسته دود را می توان به دو دسته تاثیرات روانی و تاثیرات فیزیولوژیکی تقسیم کرد .

تاثیرات فیزیولوژیک دود بسته به نوع استفاده شده متفاوت است . دود ها می توانند سبب ایجاد عوارض زیر شوند:

ایجاد تنگی نفس - تحریک سیستم تنفسی - سرگیجه و تهوع - سردرد - ایجاد مشکلات دیگر در صورت استفاده از عوامل شیمیایی به همراه دود .

تاثیرات روانی دیگر دود بر افراد و نیروهای خودی عبارتند از : اغتشاش و دستپاچگی - ترس و اضطراب (منبع ۲)

اختفاء Concealment

اختفاء یا پنهان کاری به کلیه اقداماتی اطلاق می گردد که مانع از قرار گرفتن تأسیسات و تجهیزات در دید دشمن گردیده و یا تشخیص تأسیسات و تجهیزات و هم چنین انجام فعالیت های خاص رابرای او غیر ممکن یا مشکل می سازد. دشمن همواره تلاش می کند تا نقاط حیاتی، حساس و مهم کشور مورد نظر را کشف و نشانه گذاری نموده و یا از فعالیت های مهم مطلع گردد تا در زمان مناسب با هدف گیری دقیق، تأسیسات و تجهیزات را منهدم و فعالیت ها را مختل نماید .(منبع ۲)

اختفاء با فضای سبز Concealment. Green cover

مهمترین مواردی را که باید در اختفا در نظر گرفت عبارتند از شکل زمین، موقعیت مکانی، نوع وسایل، شکل وسایل، رنگ وسایل، مدت زمان اختفاء و اتخاذ تدابیر و تمهیدات مناسب در رعایت فاصله ایمنی جهت جلوگیری ا ز سرایت اتش سوزی های احتمالی به تجهیزات با ارزش است.

با توجه به مواردی که در بالا ذکر گردید، نسبت به نوع به کارگیری پوشش گیاهی مناسب باید توجه کافی شود. تغییر رنگ و بافت زمین و پوشش آن از ابزار مهم جهت نامشخص شدن وسایل و ادوات است.

استتار Camouflage

مفهوم کلی استتار، هم رنگ و هم شکل کردن نیروی انسانی ،تأسیسات و تجهیزات با محیط اطراف است. روش های استتار عبارتند از : مخفی سازی – همگون سازی – بدل سازی (منبع ۲)

استتار چند طیفی Multi spectral Camouflage

در سیستم های شناسایی مدرن از چندین حسگر به طور هم زمان استفاده شده جهت استتار در مقابل این سیستم ها، یکی از بهترین روش ها استفاده از پوشش های استتار چند طیفی مدرن است.پوشش های استتار چند طیفی مدرن حداقل از پنج لایه تشکیل شده است. یک لایه به عنوان پایه و نگه دارنده در وسط قرار گرفته است. در طرفین این لایه ذراتی ازآلیاژ فلزات بازتاب کننده به ضخامت چند نانومتر با استفاده از فناوری نانو نشانده می شود. بعداز لایه فلزی لایه رنگی و عبوردهنده پلیمری قرار می گیرد. رنگ و بافت لایه رویی باید مطابق رنگ و بافت محیط باشد. هرکدام از لایه فلزی و لایه ها رویه در طیف الکترومغناطیسی نقش استتاری خویش را بر عهده دارند.(منبع ۲)

استتار حرارتی Thermal Camouflage

استتار در مقابل شناسایی حرارتی با کاهش اختلاف دمای حرارتی بین شیء و زمینه یا محیط اطراف آن صورت می گیرد . بدین منظور باید اقداماتی در جهت کاهش میزان گرمای جذب شده از نور خورشید و کاهش میزان گرمای حرارتی خود شیء صورت گیرد. در این صورت کنتراست حرارتی هدف نسبت به زمینه کاهش یافته و احتمال شناسایی آن به حداقل خواهد رسید

استتار دود Smoke Camouflage

عملیات دود برای ایجاد پوشش استتاری به عنوان فرایندی تعریف می‌گردد که طی آن انتشار امواج الکترومغناطیسی بین منبع گسیل‌کننده (یعنی هدف) و سیستم گیرنده (یعنی تهدید) متوقف یا تضعیف گردد. (منبع ۲)

استتار راداری Radar Camouflage

حسگرهای راداری بر خلاف حسگرهای ماوراء بنفش، مریی، مادون قرمز نزدیک و مادون قرمز حرارتی به صورت فعال عمل می کنند. بدین صورت که رادار امواج راداری را به سمت هدف ارسال نموده و از میزان امواج برگشتی، نوع و موقعیت هدف را تشخیص می دهد. جهت استتار در مقابل سیستم های راداری از روش های متفاوتی استفاده می شود.روش ها عبارتند از : روش تغییر شکل

هندسی – پوشش هایی از دود ضد رادار – رنگ های جاذب – پوشش های ضد بازتاب راداری و ... (منبع ۲)

اصول منظره سازی Viewing Principle

جهت ارتقای فضای سبز در محیط زیست و برای هماهنگی و همگامی مجموعه فعالیت ها، اصولی باید مورد توجه قرار گیرد که جایگاه ویژه ای در افزایش کیفیت طراحی و زیبا سازی محیط دارد که تعدادی از اصول مهم در امر فضا سازی و منظره سازی در فضای سبز ذکر می شود : اصل یکنواختی– اصل تنوع– متحرک بودن منظره– قابل رویت بودن منظره

انضباط استتار Camouflage discipline

دومین اصل و شرط اساسی، دست یابی به استتار و موفقیت آن رعایت شدید و قاطع و دقیق انضباط استتاری به صورت فردی و گروهی است. انضباط استتار، پرهیز از کارهایی است که ظاهر طبیعی یک منطقه را تغییر داده و یا موقعیت و میزان تجهیزات را بدون این که حتی دیده شوند برای دشمن آشکار می سازد. وجود ردّ لاستیک خودروها، ضایعات و قطعات مستعمل از علائم متداولی است که حاکی از وجود یک منطقه نظامی می باشد (منبع ۲)

انواع سنجنده kinds of sensor

سنجنده ها از نظرتفکیک طیفی به چهار دسته تقسیم می گردند:

(۱) طیف سیاه و سفید(PAN (Pancromatic با توجه به بازتاب انرژی اجسام، پدیده هارا در محدوه ۰/٤ میکرومتر تا محدوده ۰/۹ میکرومتر بصورت تک باند نشان می دهد. دراین تصاویر رنگ قابل تشخیص نبوده و این تصاویر تفکیک مکانی خوبی دارا است.

(۲) طیف رنگیRGB(Red Green Blue) در محدوده نور مرئی کار می کند و عکس ها بصورت رنگی قابل تهیه است.

(۳) چند طیفیMSS(Multi Spectral Scanner) فراتر از محدوده مرئی کار می کند و در نواحی مادون قرمز(نزدیک، میانی و حرارتی) و مایکروویو قابلیت سنجش دارد بطوریکه در باند های مختلف انرژی دریافت شده را تجزیه و در هر باند یک تصویر می دهد.

(٤) ابرطیفی HSS(Hyper Spectral Scanner) سنجده های با چند صد باند است بطوریکه اهداف مشابه را به کمک آن می توان جدا کرد با توسعه علم سنجنده از دور سنجنده های ابر طیفی یا Hyper

Spectral نیز تولید شدند که اطلاعات حاصل از آن در محدوده داخل آن ولی به تعداد زیاد دریافت می شود(منبع ۲)

اهداف ماکت فریب Deception maquette Goals

حفظ جان نیروی انسانی خودی از طریق منحرف نمودن آتش دشمن.

فریب دشمن در خصوص تعداد و آمار تسلیحات، نیروها و یا تجهیزات خودی در جهت بیشتر نشان دادن توان خودی. – جایگزین نمودن تجهیزات و تسلیحات تخلیه شده به عقب.

واقعی جلوه دادن اقدامات فریب گیج و مغشوش نمودن دشمن در خصوص نقاط حساس و کلیدی و نقاط شاخص. –تحمیل هزینه بیشتر به دشمن (مقابله با دشمن در دستیابی به اصل صرفه جویی قوا). – غافلگیر نمودن دشمن و سلب ابتکار عمل از وی. (منبع ۲)

بافت Texture

به فرکانس تغییر تن در تصویر بافت گفته می شود. به عبارت دیگر، بافت به وسیله تغییر تن یا رنگ در گروههایی از اهداف و اشیاء که تشخیص اجزاء تشکیل دهنده آنها به دلیل کوچکی بیش از حد بسیار مشکل است، ایجاد می گردد. بافت سطوح اجسام و تجهیزات با توجه به صافی و یا ناهمواری آنها در شناسایی نقش مهمی ایفا می کند . سطوح صاف و مسطح در عکس های هوایی، روشن و سطوح ناهموار به علت پراکنده نمودن امواج، تیره وتار دیده می شوند. (منبع ۲)

بدل سازی Hiding

عبارت است از تغییر قیافه هدف و استفاده از تجهیزات کاذب و فریبنده در فاصله ای منطقی از هدف به عنوان مثال تغییر شکل یک نفربر نظامی به یک ساختمان مسکونی نمونه ای از بدل سازی است

پرده دود Smoke screen

دودهای دیواره ای در سه دسته دودهای روکشی یا پوشاننده، دودهای بخارگونه یا مه‌گونه ، و پرده دود استفاده می شوند.(منبع ۲)

پوشش Cover

پوشش، پنهان سازی و حفاظت تأسیسات، تجهیزات و نیروی انسانی در برابر دید و تیر دشمن می‌باشد.

پوشش های استتار مدرن modern Camouflag Covers

پوشش های استتاری چند طیفی بسته به نوع کاربرد در ابعاد و اشکال متفاوتی تولید می شوند که عبارتند از: پوشش های استتاری اهداف متحرک – چترهای استتاری – چادر استتار نفرات(منبع۲).

تلویزیون مدار بسته Closed-Circuit Television

یک سیستم الکترونیکی از دوربین ها،کنترل تجهیزات،ضبط کننده ها،و وسایل مربوط به نظارت و کنترل.(منبع ٤٤)

تور استتار Camouflage screen

تور ها، ساختارهایی هستند که برای مخفی سازی نیروها و پروژه ها در مقابل دشمن و یا تغییر شکل خارجی آنها استفاده می شوند. تور ها به دو صورت طبیعی (جنگل و ناهمواری های زمین، شاخه های درختان و....) و مصنوعی (ساختارهای مهندسی استتاری) وجود دارند (منبع ۲)

تور افقی Horizantal screen

این دسته از تور ها تجهیزات و پروژه ها و هم چنین حرکت پروژه ها را تنها در مقابل شناسایی هوایی و عکسبرداری مخفی می سازند. ابعاد این تور در تمامی جهت ها باید از ابعاد پروژه بزرگ تر باشد تا علاوه بر تمامی پروژه، حرکت آن را نیز استتار نماید. (منبع ۲)

تور پوششی Covering screen

تور های پوششی پروژه را در مقابل دید هوایی و عکس برداری های دشمن مخفی می کند و به طور عمده برای استتار پروژه هایی استفاده می شوند که دارای ارتفاع می باشند. جهت استتار این نوع پروژه ها از تور های پوششی منحنی شکل استفاده می شود. برای اهداف و تجهیزاتی که در دره ها، شیارها و کمین گاه ها مستقر هستند، از تور های پوششی مقعر استفاده می شود(منبع ۲)

تور تعلیقی Suspension screen

این تور ها پروژه را در مقابل نظارت هوایی و عکسبرداری هوایی مخفی می کنند و برای استتار تجهیزات ویژه جنگی، مواد ذخیره شده و سایر پروژه ها به کار گرفته می شوند. برخلاف تور های افقی، تور های تعلیقی می توانند نه تنها به شکل افقی بلکه در زوایای مختلف نصب شوند. در اغلب مواقع تور های تعلیقی از مجموعه تور ها تشکیل شده است (منبع ۲)

تور تغییر شکل یافته Deforme screen

تورهای تغییر شکل یافته برای مخفی سازی و استتار شکل پروژه و سایه های آن به کار گرفته می‌شود. این تور ها برای استتار پروژه های ثابت و بزرگ استفاده می شود در صورتی که به صورت ترکیبی با تکنیک رنگ آمیزی به کار روند تاثیر بسزایی در استتار دارند.

تور طبیعی Natural screen

تور های طبیعی، همان طور که از نامشان پیداست با استفاده از مواد موجود در طبیعت ساخته می شوند، نظیر شاخه های بریده درختان و بوته ها، خشت چمنی، علف، خاک و برف. شاخه های درخت افرا، بلوط، توس، زبان گنجشک، اقاقیا، تبریزی (صنوبر) در فصل تابستان رنگ سبز خود را بیشتر از چند روز حفظ می کنند. (منبع ۲)

تور عمودی Vertical screen

تور های عمودی از پروژه ها در مقابل عکسبرداری هوایی و نظارت زمینی محافظت می کند. با توجه به اهداف به کارگیری تور های عمودی به سه دسته تقسیم می شوند:

تور های جاده ای – تور های کمین گاهی – تور های حصاری (منبع ۲)

تور ماکتی Maquette screen

به تور هایی گفته می شود که به شکل نمای خارجی ساختمان ها و استحکامات و.. بوده و در زیر آنها تجهیزات مورد نظر استتار می شود. از این تور ها برای مخفی سازی فرودگاه ها، مراکز کنترل هدایت، مناطق استقرار نیروهای موشکی و ضد هوایی استفاده می شود.(منبع ۲)

تور مایل Oblique screen

این تور ها اغلب برای مخفی ساختن سایه ها و در مورد استتار پروژه ها و اهداف ثابت به کار می رود. این نوع تور ها از نظر ساختاری مشابه تور های تعلیقی هستند با این تفاوت که این تور ها در مرزهای پایینی خود به زمین متصل می شوند. معمولا این تور ها در زوایای ۳۰ تا ٦۰درجه نصب می شوند (منبع ۲)

تور پارازیتی Noise screen

این تور ها سبب ایجاد پارازیت در دستگاه راداری دشمن می شود. در ساخت این تور ها از مواد ویژه ای استفاده می شود که یا به طور مؤثر امواج راداری را بازمی تاباند و یا آن را جذب نماید. یکی از متداول ترین مواد مورد استفاده بازتاب کننده های کربنی است (منبع ۲)

تور های مصنوعی Artificial screen

ساختار مهندسی هستند که برای مخفی سازی نیروها و پروژه های به طور عمده ثابت به کار گرفته می شوند. در واقع این تور ها در حکم پرده ای هستند که بین پروژه و دشمن نصب می شوند. این تور ها پروژه را مخفی کرده و یا آن را استتار می کنند و سبب می شوند دشمن نتواند پروژه را کشف و یا برآن نظارت داشته باشد. (منبع ۲)

جذب جوّی atmospheric absorption

در مقایسه با پخش ،جذب جوّی منجر به انتقال قابل توجهی از انرژی ذرات موجود در جوّ می شود. این پدیده معمولا شامل جذب انرژی در یک طول موج می گردد. در این رابطه مؤثرترین جذب کننده تابشهای خورشیدی عبارتند از: بخار آب ،دی اکسید کربن و ازن .

حسگر Sensor

هر وسیله‌ای که تغییرات محیطی مانند انرژی الکترومغناطیسی، حرارتی، نوری، خواص مغناطیسی، امواج رادیویی، سوپرسونیک و غیره را آشکار کرده و آنها را به شکل سیگنال های الکترونیکی یا شکل مناسبی برای کسب اطلاعات از محیط اطراف ارائه دهد، حسگر یا سنجنده نامیده می شود. حسگرها بر اساس منبع انرژی به دو دسته حسگرهای فعال و غیر فعال تقسیم می شوند (منبع ۲)

حسگر مادون قرمز حرارتی Thermal Infra- red sensor

حسگرهای حرارتی با دریافت تشعشعات حرارتی از افراد، تجهیزات، سلاح ها و تأسیسات ،توانایی آشکار سازی و کشف آنها را دارند. از این حسگرها در انواع سیستم های تصویربردار حرارتی و موشک های هدایت شونده استفاده می شود . تسلیحات هدایت شونده حرارتی برای شناسایی و نشانه گیری دقیق در شب و در شرایط آب و هوایی مختلفی (بارانی ،دود آلود، غبارآلود)به کار می رود.

حسگر مادون قرمز نزدیک Near Infra- red sensor

این حسگرها نیز همانند حسگرهای مریی بازتاب امواج را آشکار می کنند و عوامل شناسایی مشابه ناحیه مریی درکارایی آنها مؤثر است . این حسگرها غالبا در بردها و فواصل کوتاه مؤثرند .(حدودا۹۰۰ متر). از این حسگرها در ساخت دوربین های دید در شب استفاده می شود. رعایت

انضباط استتاری و جلوگیری از انتشار نور و استفاده از تجهیزات استتاری مناسب از جمله اقدامات مؤثر در جلوگیری از تشخیص، شناسایی، رد گیری و انهدام اهداف خودی توسط این حسگرها است.

حسگر ماوراء بنفش Ultraviolet sensor

این حسگرها در محیط برفی مورد استفاده قرار می گیرند. این حسگرها مشابه دوربین های مریی بوده که در لنز آنها فیلتر ماوراء بنفش استفاده شده است. این فیلتر ها فقط اجازه عبور امواج ماوراء بنفش را به دوربین می دهند

حسگرهای راداری Radar sensors

حسگرهای راداری در محدوده فرکانسی بین MHZ3 تا GHZ 300 طیف الکترومغناطیسی قرار دارند و بسته به نوع رادار مورد استفاده بازه ای از این محدوده فرکانس را پوشش می دهند . سیستم های راداری و نحوه مقابله با آنها از نظر تکنیک های CCD در بخش جداگانه ای توضیح داده خواهد شد. برخی از حسگرها راداری طوری طراحی شده اند که قادر به شناسایی اهداف متحرک می باشند.

حسگرهای غیر فعال Passives sensor

حسگرهای غیر فعال خود مولد انرژی الکترومغناطیسی نیستند، بلکه انرژی بازتابی و یا گسیلی از پدیده های زمینی را آشکار می کنند. برخی از این حسگرها اشعه الکترومغناطیس خورشید را در باندهای مریی و مادون قرمز نزدیک جمع آوری می نمایند. شناسایی حسگرهای غیر فعال بسیار مشکل است و عملیات CCD در مقابل این حسگرها نیاز به تدابیر خاص دارد.(منبع ۲)

حسگرهای فعال Active sensors

این حسگرها خود دارای مولد انرژی الکترومغناطیس هستند . امواج به طرف هدف مورد نظر فرستاده شده و بازتاب آن جمع آوری و ثبت می گردد (نظیر عکسبرداری با فلاش). این حسگرها از امواج لیزر (LIDAR) و میکروویو(RADAR) و.... استفاده می کنند.

حسگرهای مرئی Visible sensors

فاکتورهای مهم شناسایی، عواملی مانند: فرم، بافت، سایه، حرکت، درخشش و رنگ در عملکرد این حسگرها مؤثر است. این عوامل می توانند مشاهده کننده را به نمایان کردن و مشخص نمودن ماهیت اشیاء محیط و هدف قادر سازد.

درخشندگی Brightness

درخشندگی نوری است که از یک سطح صاف بازتابیده می شود . نوری که به سقف ساختمان ها، پنجره ها، سقف خودروها، سطوح صیقلی یا کلاهک های آهنی می تابد به طور درخشانی به چشم دیده بان یا سیستم شناسایی می رسد و عامل مهمی در شناسایی و کشف اهداف است.

دود Smoke

به ذرات بسیار ریز مایع، جامد و مه گونه معلق در هوا دود گفته می شود. ابعاد ذرات دود از قطر یک میکرومتر تا بیش از ۱۰ میکرومتر متغیر است. این ذرات سرعت سقوط بسیار کمی دارند و معمولاً در هنگام حرکت در هوا، بار الکتریکی را جذب می کنند. حرکت ذرات در اثر جریان هوا صورت می گیرد. دود با ذرات ریز معلق در هوا، پنهان سازی را انجام می دهد. ذرات دود نور را جذب کرده و یا باز می تابانند.

دودهای دیواره ای screening Smokes

دودهای دیواره ای به عنوان پوشش استتاری بکار می روند . دودهای دیواره ای در سه دسته دودهای روکشی یا پوشاننده، دودهای بخارگونه یا مه‌گونه ، و پرده دود استفاده می شوند .(منبع ۲)

ردپا Track

ردپا عامل مهمی در شناسایی اشیاء و نیز مسیر حرکت می باشد. ردپای گروه های سربازان و وسایل نقلیه و تانک ها در زمین های خاکی در تصاویر ماهواره ای با قدرت تفکیک بالا و دیگر سیستم های شناسایی اهداف قابل تشخیص بوده و مورد استفاده قرار می گیرد.

رنگ آمیزی استتاری Camouflage painting

رنگ آمیزی پروژه ها یکی از ساده ترین و در دسترس ترین روش های استتاری است و به طور گسترده از آن استفاده می شود. از این روش می توان به طور مستقل و یا در ترکیب با سایر روش های استتاری استفاده کرد.رنگ آمیزی استتاری به منظور تغییر تباین زمینه و پروژه به کار گرفته می شود. (منبع ۲)

رنگ استتار حرارتی Thermal camouflage paint

رنگ هایی وجود دارد که به عنوان جاذب حرارت عمل کرده و با استفاده از رنگ آمیزی اهداف با

ضخامت مناسب از این رنگ ها، استتار حرارتی صورت می گیرد.(منبع ۲)

روش های استتار Camouflage Techneque

مخفی سازی: که در آن یک شیء کاملا توسط پوشش های فیزیکی نظیر تور استتار مخفی می گردد.

همگون سازی : در همگون سازی از وسایلی در اطراف و بالای شیئ استفاد می شود بطوری که هدف جزیی از زمینه گردد . نمونه بارز همگون سازی استفاده از شاخ و برگ درختان است .

بدل سازی : عبارت است از تغییر قیافه هدف و استفاده از تجهیزات کاذب و فریبنده در فاصله ای منطقی از هدف به عنوان مثال تغییر شکل یک نفربر نظامی به یک ساختمان مسکونی نمونه ای از بدل سازی است. (منبع ۲)

سازگاری Adaptation

تغییرات تدریجی ظاهری، هورمونی و رفتاری در ساختار یک موجود برای هماهنگ شدن با طبیعت را گویند.

سنجنده Sensor

سنجنده دستگاهی است که بر روی ماهواره نصب شده و امواج الکترو مغناطیس بازتابی و گسیل شده پدیده ها را دریافت می کند و بصورت داده های رقومی برای کاربر قابل استفاده می نماید.

شاخص های توانمندی حسگر sensor power indexs

شاخص های توانمندی این حسگرها عبارتند از :

– قدرت تفکیک مکانی – قدرت تفکیک طیفی – قدرت تفکیک رادیومتریک– قدرت تفکیک زمانی .

شناسایی Reconnaissance

فرماندهان نظامی به طور مداوم نیازمند اطلاعات به موقع از دشمن، زمین ، شرایط آب و هوایی می باشند. اصول فعالیت های شناسایی عبارتند از : تمرکز – پیوستگی– تهاجمی – استتار،اختفاءو فریب و قابلیت اطمینان . شناسایی عموما با سنجش از دور انجام می گیرد و می تواند در زمان صلح یا جنگ یا تهدید با اهداف متفاوتی صورت گیرد. (منبع ۲)

طراحی پوشش گیاهی Vegetation Design

استفاده از ویژگی های ذاتی پوشش گیاهی و بکارگیری مهندسی آن با توجه به نـوع طـرح پدافنـد غیرعامل را طراحی پوشش گیاهی گویند.

طرح کلی اشیاء Objects Pattern

منظور از طرح کلی یا الگو، ترتیب یا آرایش مکانی اشـیاء اسـت . الگوهـا مـی تواننـد طبیعـی یـا مصنوعی باشند مانند الگوی خیابان های منظم و ساختمان های تشکیل دهنده در شـهر و نیـز الگوهـای زهکشی (شبکه ای، شعاعی و...). با شناسایی الگوها امکان تشخیص اهداف میسر می گردد (منبع۲)

طیف الکترو مغناطیس Electromagnet Spectral

مفهوم انرژی الکترومغناطیسی توسط ماکسول در دهه ۱۸٦۰ میلادی بیان شد. بر اساس این نظریـه انرژی الکترومغناطیسی به صورت هارمونیک و سینوسی و با سرعت نور حرکت می‌کند. علت ایجاد این انرژی حرکت یک ذره باردار است که تولید میدان الکتریکی و مغناطیسی عمود برهم موسوم به میـدان الکترومغناطیس می نماید. بسـته بـه تعـداد فرکـانس و یـا طـول مـوج، امـواج الکترومغناطیسـی را بـه بخش های زیر تفکیک می کنند.به هر یک طیف الکترومغناطیس گفته می شود:

(۱) اشعه گاما: طول موج های بین بین$^{-٦}$۱۰–$^{-٥}$۱۰ میکرومتر

(۲) اشعه X : طول موج های بین $^{-٥}$۱۰– $^{-٢}$۱۰ میکرومتر.

(۳) اشعه ماوراء بنفش: طول موج‌های ۰/۰۱ تا ۰/٤ میکرومتر

(٤) محدوده مرئی: طول موج‌های بین ۰/٤ تا ۰/۷ میکرومتر

(۵) محدوده مادون قرمز: محدوده مادون قرمز بازتابی که از طول موج ۰/۷ تا ۳ میکرومتر

عایق های حرارتی Thermal insulators

در استتار حرارتی استفاده از عایق های حرارتی و سیستم های دو جداره برای کنترل انتقال گرمای داخلی هدف به سطح آن انجام می گیرد . در این سیستم ها از جریان هوا جهت خنک نگه داشتن بدنـه منبع حرارتی استفاده می شود (منبع ۲)

عملیات دود Operation of smoking

عملیات دود به علت تاثیرات اجتناب ناپذیر عوامل و مؤلفه هـای زمـانی، مکـانی، آب و هـوایی، عوارض محیطی و توپوگرافی منطقه، رطوبت، تغییرات دما در ارتفاع، سمت و سرعت باد، وسعت هدف و منطقه عملیاتی، نوع مواد دودزا و تجهیزات مورد اسـتفاده، میـزن مهـارت و آمـوزش کارکنـان دارای

پیچیدگی خاص خود بوده ، موفقیت و یا عدم موفقیت در عملیات وابستگی نزدیکی به رعایت یا عـدم رعایت ملاحظات، موازین و مؤلفه های یاد شده و انجام هماهنگی های دقیق دارد .(منبع ۲)

عوامل شناسایی reconnaissance Agents

صرف نظر از نوع حسگر مورد استفاده، وجود عواملی خاص ضرورت دارد تا به چشم و مغز انسان در شناسایی هدف کمک و یاری کند این عوامل در اصطلاح عوامل شناسایی نـام دارنـد. در صـورتی می توان به نحو صحیح و مؤثر خود را از دید تیر دشمن مخفـی داشـت کـه عوامـل شناسـایی را درک نموده و روش ها و اقدامات مناسـب را در جهـت ایـن عوامـل و محـروم نمـودن دشـمن از کشـف و شناسایی آنها اتخاذ نمود. عوامل شناسایی عبارتند از :

وضعیت – بافت – شکل – صدا – سایه– ردپا – حرکت – ارتباط – طرح کلی– حرارت– رنگ – درخشندگی– اندازه

عوامل مخرب استتار Camouflage destroyer Agents

منظور از مشخصه های شناسایی، مشخصاتی است که دشمن توانـایی تشـخیص وجـود نیروهـا و دسته جات نظامی و آماده سازی آنها برای عملیات جنگی و هم چنین پروژه هایی با اهداف مختلـف را داده و سبب ناکارآمدی استتار می گردد. بر اساس این مشخصه ها دشمن مـی توانـد مکـان، چگـونگی استقرار و هدف از پروژه ها را تعیین نماید. این مشخصه ها شامل موارد زیر است:

– حصار بندی های ویژه– زمینه ویژه حرارتی– زمینه تابش راداری– رنگ سـطح پـروژه و فـرم و ابعاد آن و ...

فریب Deception

فریب به مجموعه اقداماتی اطلاق می گردد که به طور کلی موجب گمراهی دشمن گردیـده و او را در تشخیص هدف و هدف گیری با شک و تردید مواجه نماید.(منبع ۲)

فریب نظامی Military Deception

اقداماتی که به منظور گمراه ساختن فرماندهان تصمیم‌گیرنده دشمن انجـام مـی‌شـود تـا دشـمن از تواناییها، اهداف و عملیات نیروهای خودی آگاه نشود، در نتیجه به اقدام (یا عدم اقدام) خاصی مبادرت ورزد که به انجام مأموریت نیروهای خودی کمک خواهد نمود.

فضای سبز و استتار Vegetation &Camouflage

یکی از مهمترین کاربردهای فضای سبز، کاربرد آن در استتار اماکن و استتار محیط هـای نظـامی از دید افراد غیر نظامی و دشمن با بهره گیری از فضای سبز می باشد توجه به ایـن کـه هـر گیـاهی دارای فصل رویش، خاک، اقلیم، و سازگاری اکولوژیکی خاصی در محیط می باشد باید بر اساس طرح پدافند غیرعامل، نوع کاربری و استقرار گیاهان مناسب برای طرح استتار مشخص شود.

قدرت تفکیک رادیومتریک radiometric resoulation

منظور از قدرت تفکیک رادیومتریک، توانـایی تشـخیص اختلافـات خیلـی کـم در انـرژی ثبـت شـده می باشد، حساسیت آن نسبت به آشکار سازی اختلافات کوچک تر در انرژی گسیلی یا بازتابیـده شـده بیشتر است حسگرهای ابر طیفی دارای قدرت تفکیک رادیومتریک تا ١٦ بیت می باشند

قدرت تفکیک زمانی timing resolution

منظور از قدرت تفکیک زمانی یک حسگر، مدت زمانی است که طول مـی کشـد تـا حسـگر یـک سیکل مداری تصویربرداری را کامل کند.

قدرت تفکیک طیفی Spectral resolution

منظور از قدرت تفکیک طیفی، فواصل طول موجی مشخص در طیـف الکترومغنـاطیس اسـت کـه حسگر می تواند ثبت نماید. اصولا هر چه تعداد باندهای طیفی حسگر بیشتر باشد، قدرت تفکیک طیفی نیز بیشتر خواهد بود.

قدرت تفکیک مکانی locational resolution

عبارت است از اندازه کوچکترین عارضه ای که می تواند در تصویر حسگر مشخص گردد . سطوح شناسایی و تشخیص اشیاء عبارتند از :

۱-آشکار سازی : به معنی تعیین محل و کلاس واحد ها، شی یا فعالیت مورد نظر ۲- تشخیص : تعیین کلی نوع هدف است ۳-شناسایی: تعیین دقیق نوع هدف . با قدرت تفکیک مکانی یک متر، شناسایی ساختمان ها و تشخیص وسایل نقلیه انجام می شود.

کاربردهای پوشش گیاهی Vegetation application

کارکرد طبیعی و محیطی : انعکاس نور و تابش مجدد نور خورشید، تعدیل بارش باران، مه و نزول برف ، تولید اکسیژن،, ..

کارکرد بهداشتی : بعضی درختان و گیاهان با ترشح بعضی از اسانس ها و ترشحات و تولید ترکیبات شیمیایی به سایر موجودات زنده که اغلب میکروارگانیسم ها می باشند صدمه زده و سبب ایجاد شرایط مناسب محیطی برای رشد و حیات خود می شوند ولی این عمل سبب از بین رفتن بسیاری از آلودگی های میکروبی می شود.

کارکرد معماری و اقتصادی : استفاده عمده از فضای سبز در محیط از نظر منظر و زیبا شناختی است که می تواند با معماری و طراحی صحیح، خود را نمایان سازد. تنوع شکل، رنگ، بافت درختان، درختچه های زینتی و ... کارکردهای دفاعی و نظامی: ایجاد پوشش فضای سبز در مسائل نظامی بویژه از لحاظ استتار، اختفاء، جلوگیری از اثرات انفجارات بمبارانها و سایر موارد که می توان از فضای سبز در طرحهای نظامی یاری گرفت و از آن بهره برد، از نقش استتار در خشکی، سواحل دریا و هوایی به کمک فضای سبز بیان نمود. از نظر تاکتیکی فضای سبز، پناهگاه و نقطه اتکا مهمی در هنگام نبرد می باشد.

گیاهان شاخص Index vegetable

پوشش گیاهی که در طول زمان و تحت شرایط اکولوژیکی موجود سیمای رستنی های منطقه ای را شکل می دهد و در مناطق مشابه نیز با این خواص مشاهده شود را گویند مثلا گون در اطراف معادن آلومینیوم زیاد می روید.

ماکت فریبنده Deceptor maquette

ماکت ها را در جهت فریب و گمراهی دشمن به کار می برند. ماکت های فریب اسلحه دفاع غیرعامل محسوب می گردند . استفاده از ماکت موجب انحراف توجه دشمن از هدف های اصلی به

سمت اهداف کاذب می باشد (منبع ۲)

ماهواره های جاسوسی Spy satellites

مدار ماهواره های جاسوسی که در فاصله ۲۰۰ تا ۲۵۰ کیلومتری قرار دارند، این ماهواره ها قدرت تفکیک مکانی بالا و در حدود ۱۰ سانتی متر دارند. با توجه به سرعت بسیار بالای آن ها نمی توانند بالای یک منطقه توقف نمایند و بنابراین برای تصویر برداری Real- Time نامناسب هستند

منابع تابش الکترو مغناطیس electromagnet Radiation Resource

بهترین و اصلی ترین منبع الکترو مغناطیس، خورشید است . تابش خورشیدی از طول موج ماوراءبنفش تا محدوده مادون قرمز را شامل می شود. تمام مواد در دمای بالاتر از صفر مطلق (73 C–) به طور پیوسته از خود امواج الکترو مغناطیس گسیل می کنند . میزان انرژی گسیل شده از هر ماده، تابعی از درجه حرارت سطحی آن است.

مواد دود زا Smoking metal

مواد دود زا بر اساس نوع تولید، نوع واکنش و کاربرد آن تقسیم بندی می شوند. انواع مواد دود زا بر اساس تولید :

مواد دودزا یا به صورت مکانیزه توسط توپخانه، خمپاره، نارنجک، موشک و... تولید می شود. و یا به صورت موتوریزه با انواع سیستم های مختلف موتوری. مواد دود زای مکانیزه عبارتند از :

هگزاکلوتان، فسفرسفید، فسفرقرمز و ترکیبات آن، پودر برنج، ترکیبات گرافیت – مواد دودزا بر اساس واکنش آنها در مقابل بخار آب به دو نوع مواد دودزای بدون جذب آب و مواد دودزای با جذب آب تقسیم می شوند.

مواد دودزای بدون جذب آب عبارتند از: فسفر فید، ترکیبات پیروتکنیکی شامل پرکلرات آمونیوم.

انواع مواد دود زا بر اساس کاربرد: از مواد دودزا جهت استتار در مقابل حسگرهای شناسایی مختلفی استفاده می شود. بسته به این که ماده دودزا در مقابل چه حسگری مؤثر است به چهار نوع

مختلف تقسیم بندی می شود که عبارتند از : الف- مواد دودزای مؤثر در برابر حسگرهای ناحیه مریی - ب- مواد دودزای مؤثر در برابر حسگرهای مادون قرمز

ج- مواد دودزای مؤثر در برابر حسگرهای چند طیفی: این مواد در برابر دو یا چند بازه طیفی مؤثرند مانند: (مرئی و IR نزدیک) (منبع ۲)

نگهداری پوشش گیاهی Vegetation miantenance

پوشش گیاهی زنده می‌تواند در اکثر اقلیم‌ها و محیط‌ها با شرایط گوناگون، وجود داشته باشد. رنگ و بافت این پوشش‌ها موجب یکنواختی در منطقه می‌گردد. در عین حال، درختچه‌ها و درختان به طور دائمی نیازمند مراقبت و نگهداری هستند تا در شرایط خوب و شاداب قرار داشته باشند. اگر شاخه‌ها در موقعیت رشد مناسب خود قرار نداشته باشند، ممکن است باعث لورفتن موقعیت نیروهای خودی در برابر مشاهدات دشمن گردند.

همگون سازی Blending

در همگون سازی از وسایلی در اطراف و بالای شیئ استفاده می شود بطوری که هدف جزیی از زمینه گردد. نمونه بارز همگون سازی استفاده از شاخ و برگ درختان است .(منبع ۲)

۲- واژگان سنجش از دور

انواع سنجنده های راداری

انواع سنجنده های راداری عبارتند از: رادار با روزنه دید ترکیبی(SAR) که بر روی ماهواره ها نصب می‌گردد. رادار هوائی پهلونگر (SLAR) که بر روی هواپیما نصب می‌گردد و رادار تصویر بردار شاتل(SIR) که بر روی شاتل فضائی نصب می‌شود.(منبع ٤٧)

انواع سیستم های شناسایی kinds of reconnaissance system

سیستم های نوری و الکترواپتیکی که شامل دوربین های چشمی و بر روی سلاح می باشند .

– سیستم های تقویت تصویر (دید در شب)– سیستم های تصویر بـرداری نـور مریـی – سیسـتم های تصویر برداری حرارتی (مادون قرمز) – سیستم های راداری – سیسـتم هـای لیـزری یـا لیـدار – سیستم های چند حسگری که ترکیبی از سیستم های ذکر شده قبلی است.

باند فرکانسی راداری Radar freqency band

اصلی ترین عاملی که نقش ها و وظایف انواع رادارها را مشخص می کند، فرکانس عملیـاتی ایـن رادارها می باشد . به طوری که رادارهای با فرکانس پایین به منظور نظارت، تجسس و شناسایی هدف از راه دور مورد استفاده قرار می گیرند. این رادارها دارای آنتن های بزرگی بـوده و معمـولاً در تأسیسـات ثابت و معینی قرار دارند. رادارهای با فرکانس بالاتر در ردّ گیری هـدف و هـدایت تسـلیحات اسـتفاده می شوند. این رادارها اطلاعات با ارزش موقعیت هدف از قبیل زاویه و ارتفاع را نشان می دهند.

پایونیر Pioneer

آغاز آماده سازی این پرنده در سال ۱۹۸۵ بود تا اطلاعات تصویرسازی را برای فرماندهان تاکتیکی در خشکی و دریا تا مسافت ۱۸۵ کیلومتر تهیه نماید.(منبع ۲)

پوشش های سرامیکی seramic Cover

پوشش های سرامیکی، سرامیک هایی با ساختار فریت هستند که بازتابش امواج راداری را کاهش داده و باعث استتار راداری شده برای پوشش نقاط داغ مانند اگزوزها مورد استفاده قرار می گیرد. استفاده از سرامیک ها در موارد ویژه کاربرد داشته و برای قسمت های خاصی استفاده می گردد.(منبع۲)

پوشش های ضد بازتاب راداری Redar Antiradiat coating

پوشش های ضد بازتاب راداری در انواع مختلف موجود می باشد. برای ساخت ایـن پوشـش هـا ترکیب لایه های مرکب در یک جاذب مـایکروویو بـا اسـتفاده از لایـه‌ای غیررسـانا و دارای ثابـت دی الکتریک نسبتاً بالایی صورت می گیرد و سپس لایه ای از مواد مغناطیسی با ضریب نفوذ پـذیری نسـبتاً بالا به کار می رود (منبع ۲)

تجسس زمین فضایی ground Spatial Search

استفاده از داده ها و برنامه های زمین فضایی از قبیل سیستم های اطلاعات جغرافیایی و نرم افزار

پردازش تصویر در کاربرهای نظامی.

تصویر سازی ابر طیفی Hyper Spectral Imagery

با استفاده از بیش از ٦٠ باند طیفی (از قبیل مادون قرمز، حرارتی، ماورای سنجش، رادیو . . .)، شکل، چگالی، دما، تغییر مکان و ترکیب شیمیایی اشیاء را آشکار می سازد .(منبع ٤٧)

تصویر سازی چند طیفی Multi-Spectral Imagery

در این حالت یک تصویر دیجیتال الکترواپتیکی مبتنی بر داده های جمع آوری شده همزمان، در باندهای متفاوت با نواحی طیفی مختلف تولید می گردد .(منبع ٤٧)

توپولوژی در GIS Topologi in GIS

هنگامی که داده های جغرافیایی را به منظور استفاده در سیستم های GIS به صورت مدل درمی آورید متوجه می شوید که بعضی از داده های مدل شده می بایست دارای روابط مکانی با دیگر داده های موجود در مدل باشند. در واقع توپولوژی مدلی است که اشتراک هندسی داده های موجود در یک مدل با هم را شرح می دهد و همچنین مکانیزمی را برای استقرار و نگهداری روابط مکانی بین داده های موجود در مدل ایجاد می نماید.(منبع ۲)

حساسه های لرزه

حساسه های لرزه به دو نوع اساسی بشرح زیر تقسیم بندی می شوند:

- لرزه نگارهای تنظیم از پیش که حرکات زمینی را در مقایسه با یک مرجع تنظیم از پیش اندازه گیری می کند.
- نوع دیگر لرزه نگارها، سازکاری کششی دارد که از نوع قبلی ساده تر ولی از نظر فنی پیچیده تر است.(منبع ٤٧)

حساسه های مغناطیسی magnetic sensors

شناسایی اهداف دریایی از طریق سامانه تاکتیکی ماهواره ای صورت می گیرد.این سامانه نیز مشابه سامانه های چند سنسوری قبل با تاکید بر حساسه مغناطیس، به صورت مجموعه های سه الی چهار دستگاهی با استفاده از سامانه GPS فاصله بیشتری را تحت پوشش قرار داده و اهداف زمینی، هوایی و دریایی را شناسایی می کند.(منبع ٤٧)

حساسه های تصویری راداری Redar videoing sensors

تهیه عکس و تصویر بوسیله فناوری راداری با انتشار امواج الکترومغناطیسی بر روی منطقه هدف امکان‌پذیر می باشد. هواپیماهای مجهز به سامانه راداری با فرستادن یک پالس بـر روی هـدف، انـرژی انعکاس داده شده همان پالس از هدف را دریافت می نماید. از محاسبه، میزان انرژی بازگشـتی و زمـان انعکاس، تصویر راداری بدست می آید.(منبع ٤٧)

حسگر لیزر Laser sensors

یکی دیگر از سامانه های تشخیص سلاح های هوشمند، رادار لیزری است که با بهره گیری فناوری پرش شکل و طول موج و با بکار گیری حساسه های غیر عامل قـادر اسـت اهـداف زمینـی، هـوایی و فضایی را در فواصل بسیار دور (بالای هزار کیلومتر) ردیابی و شناسایی کند.(منبع ٤٧)

حسگر اپتیکی Optical sensors

تفاوت اصلی سنجنده های الکترواپتیکی یا تصـویربرداری بـا دوربـین هـای عکسـبرداری در نـوع محصول یا خروجی آنهاست. خروجی دوربـین هـای عکسـبرداری، عکـس آنـالوگ اسـت در حالیکـه خروجی سنجنده های تصویربرداری، تصویر رقومی (دیجیتالی) است. لذا سنجنده هـای تصـویربرداری مشکلات دوربین های عکسبرداری را ندارند. اما مشکل اصلی آنها امنیت پـائین تـر، بـدلیل اسـتفاده از ارتباطات مخابراتی جهت ارسال تصاویر، می باشد. استفاده از ماهواره ها و هواپیماهای عکـس بـرداری مدرن باعث جمع آوری عکس‌هایی می شود که از قدرت تفکیـک بـالائی برخوردارنـد و بـا جزئیـات بیشتری اهداف را مشخص می‌کنند.امروزه ابزار رایانه‌ای بسیار پیشرفته‌ای اعم از نرم‌افزار و سخت‌افـزار برای پردازش عکس‌ها وجود دارد که بکار گیری این ابزارها باعث می شود تا تمام این امکانـات بـرای یک تفسیر کامل از سوی متخصصین تفسیر عکس صورت پذیرد.(منبع ٤٧)

حسگر تصویری مادون قرمز Infera-red videoing sensor

حساسه‌های سامانه عکس‌برداری مادون قرمز، انرژی خارج شده از هر شیء را دریافت می‌کننـد. در حقیقت این حساسه‌ها امواج الکترومغناطیس ما بین نور مرئی و امواج مایکروویو را دریافت و سپس آن را تبدیل به تصویر می نماید.از جمله قابلیت‌های مهم این نوع عکس برداری را می‌توان به بی‌اثر کـردن عمل اختفاء و یا تجهیزات آنها بدون توجه به شب و روز ، اشاره نمود.(منبع ٤٧)

حسگر تصویری الکترواپتیکی Electro optical videoing sensors

این سامانه در حوزهٔ طیف نور مرئی با استفاده از چند آشکارساز که هر کدام نور دریـافتی را در نقطه ای متمرکز می کنند، عمل می نماید. در نهایت عکس از منطقهٔ مورد نیاز، با ارسال به موقع تمـامی اطلاعات به محدودهٔ ترمینال حساسه و تمرکز تمامی نقاط بدست خواهد آمد.(منبع ٤٧)

رادار SAR Synthetic Aperture Radar

با بکارگیری رادارهای پیشرفته فوق می توان تصاویری دریافت نمود کـه تـاکنون امکـان آن میسـر نبوده است. تصاویری که به کمک پرش امواج رادیویی از یک ناحیه یا یک شیء تولید می شود.یکی از ویژگی های رادار SAR تشخیص اهداف بصورت خودکار است. سامانه FOPEN با نفوذ از شاخ و برگ درختان و بکارگیری تکنیک های رادار SAR، قادر است اهداف پنهان شده بوسیله شاخ و برگ درختـان و یا سایر وسایل اسـتتاری و اختفـا و یـا فریـب راداری بـا اسـتفاده از Clutter راداری را شناسـایی و موقعیت یابی نماید.

رنگ جاذب راداری radar absorbing paint

رنگ های ضد بازتابش با تغییر فاز امواج راداری و کاهش سطح مقطع (RCS) سبب کمینـه شـدن مقدار امواج بازتابی می گردند. این رنگ ها شامل رزین های مخصوص رنـگ و پودرهـای فریـت مـی باشند. این پوشش می تواند بازتاب امواج راداری را تا حدی که رادار قادر به تشخیص آن نباشد کاهش دهد . (منبع ۲)

روش های استتار راداری radar Camouflag techniques

در این روش ها به نحوی بازتابش و میزان پراکندگی امـواج راداری از هـدف را کـاهش داده و یـا ایجاد پارازیت های مختلف مانع از تشخیص امواج بازتابی می گردند. این روش ها عبارتند از :

روش تغییر شکل هندسی – پوشش هایی از دود ضد رادار – رنگ های جـاذب – پوشـش هـای ضد بازتاب راداری – پوشش های سرامیکی – تور های پارازیتی (منبع ۲)

سامانه چند طیفی هوایی Airborne multi spectral

سامانه چند طیفی هوایی با بکارگیری چندین دوربین از داخل به یکدیگر متصل شده تا قادر باشـد بطور همزمان داده را دریافت کند.(منبع ٤٧)

سطح مقطع راداری RCS (Radar Cross Section)

سطح مقطع راداری با میزان شناسایی هدف توسط رادار نسبت مستقیم دارد. هرچه سطح مقطع راداری یک هدف بزرگتر باشد به همان نسبت مقدار انرژی راداری بیشتری به طرف محل سیگنال ارسالی بازتابیده می شود و در نتیجه هدف بسیار آسانتر توسط رادار مورد شناسایی قرار می گیرد و هرچه سطح مقطع راداری یک هدف کوچکتر باشد به همان نسبت انرژی بازتابیده آن کمتر و شناسایی آن مشکل تر خواهد بود (منبع ۲)

سطح مقطع راداری کاهشی Reduce RCS

چهار روش اساسی کاهش سطح مقطع راداری وجود دارد : تغییر شکل (shaping) – استفاده از مواد جاذب رادار(RAM) – حذف غیر فعال – حذف فعال (منبع ۲)

سکوهای شناسایی Recognizing lanchers

برای داشتن استتاری موفق، علاوه بر دانستن نوع سیستم شناسایی، تعیین این که سیستم بر روی چه سکویی قراردارد نیز ضروری است در سنجش از دور از سکوهای متفاوتی استفاده می شود که شناسایی انجام شده توسط هر یک دارای ویژگی های خاص خود بوده و در نتیجه در انتخاب نوع استتار مؤثر است. سکوهای شناسایی می توانند زمینی، هوایی، دریایی و فضایی باشند

سنجش از دور Geographic Information System(GIS)

سنجش از دور علم دست یابی به اطلاعات از محیط پیرامون بدون تماس مستقیم (فیزیکی) با آنها است. عکس برداری هوایی، تصویر برداری ماهواره ای و راداری از انواع مختلف داده های سنجش از دور می باشند. داده های سنجش از دور عموماً از طریق حسگرهای ثبت تابش الکترومغناطیسی بازتاب یافته و یا گسیل شده از اشیاء در سطح یا زیرزمین به دست می آید. این حسگرها می تواند در هواپیماها، ماهواره ها و یا دیگر سکوهای سنجش از دور قرار گیرد. هر سیستم سنجش از دور شامل **اجزاء مختلفی** است که عبارتند از:

منبع انرژی یا روشنایی– تابش و محیط انتقال (اتمسفر) – تعامل انرژی با هدف مورد سنجش – ثبت انرژی توسط حسگر – ارسال، دریافت و پردازش اطلاعات – تفسیر و آنالیز – ارسال جهت کاربرد مشخص – **مزایای** استفاده از سنجش از دور عبارت است از :

پوشش دهی مناطق وسیع با هزینه نسبتا پایین –قابلیت ثبت تابش الکترومغناطیسی در بازه های طیفی مختلف – دقت بسیار بالا – سرعت بالای کسب اطلاعات و منظم بودن – قابلیت تصویر برداری

در شرایط زمانی و آب و هوایی متفاوت – دریافت اطلاعات سودمند از اهداف با کمترین احتمال آسیب –قابلیت دریافت اطلاعات از اهداف دور از دسترس .

سنجنده‌های غیر تصویری

منظور از سنجنده‌های غیرتصویری، آن دسته از سنجنده ها است که ابزار سنجش آنها مستقیما تصویر تهیه نمی کنند، بلکه حاصل سنجش آنها اطلاعاتی از شدت و ضعف انرژی بازتابی از عوارض زمین است. شدت و ضعف انرژی بازتابی بوسیله سنجنده‌های ماهواره ها دریافت و پس از عملیات مخصوص به صورت علایم رادیویی به زمین مخابره می‌شود.(منبع ٤٧)

سیستم موقعیت یاب جهانی Global Positioning System(GPS)

آرایشی از ٢٤ ماهواره که توسط ایالات متحده در مدار۲۰ هزار کیلومتری زمین قرار گرفته اند و سیگنال های آنها به هر دریافت کننده سیگنالGPS در هر نقطه از زمین امکان می دهد محل خود را شناسایی نماید. این سیستم در ناوبری، نقشه برداری و بسیاری کاربردهای دیگر مورد استفاده قرار می گیرد.

سیستم شناسایی reconnaissan system

عموما شناسایی توسط تکنیک های سنجش از دور انجام می گیرد . بسته به نوع حسگر مورد استفاده در سنجش از دور؛ اطلاعاتی که از اهداف بدست می آید متفاوت است. گاه یک سیستم شناسایی هم زمان از چند حسگر جهت تکمیل اطلاعات استفاده می کند . سیستم های مورد استفاده در سنجش از دور و فرایند شناسایی بسته به نوع حسگر مشخص می شوند. (منبع ۲)

شناسایی راهبردی strategic Reconnaissan

این شناسایی هم در زمان صلح و هم در زمان جنگ انجام می گیرد .هدف آن کسب اطلاعات لازم از تسلیحات و سیستم های جدید دشمن، شناسایی پادگان ها و پایگاه های جدید الاحداث و نیز نقل و انتقالات عمده، اطلاعات آب و هوایی و نظارت بر مراکز مهم، حساس و حیاتی است. (منبع ۲)

شناسایی تاکتیکی tactical reconnaissan

این شناسایی در زمان جنگ انجام می گیرد و هدف آن شناسایی تحرکات دشمن، شناسایی مراکز تجمع قوای دشمن و شناسایی اهداف است . این نوع شناسایی به منظور تکمیل اطلاعات جهت طراحی و انجام عملیات جنگی انجام می گیرد (منبع ۲)

شناسایی دریایی naval reconnaissan

این شناسایی توسط نیروهای دریایی و مکان های استقرار دریایی انجام گیرد. هدف از این شناسایی پایگاه های جنگی دریایی، مراکز استقرار، مراکز تمرکز نیروها و بخش های مناسب ساحلی جهت هماهنگی نیروهای دریایی است. از ناوچه ها و قایق های اکتشافی در این شناسایی استفاده می شود (منبع ۲)

شناسایی زمینی ground reconnaissan

شناسایی های زمینی به دو صورت دیده بانی مستقیم و غیر مستقیم صورت می گیرد. دیده بانی مستقیم معمولا توسط فرد با دوربین های چشمی و در نزدیکی پروژه های ویژه و مشخص انجام می شود. هدف این شناسایی جمع آوری اطلاعات جهت فعالیت های اولیه انهدامی است. دیده بانی غیر- مستقیم عموما توسط دوربین های عکسبرداری مریی ،حرارتی و سیستم های راداری صورت می گیرد. (منبع ۲)

شناسایی فضایی spacing reconnaissan

این شناسایی در ارتفاع بالاتر از ۲۰۰ کیلومتری انجام می شود . انواع سکوهای فضایی عبارتند از:

- راکت ها: که تا ارتفاع ۹۰۰ کیلومتری اوج می گیرند و مدت زمان پروازی در حدود یک الی دو ساعت دارند. شاتل ها: در ارتفاع ۲۰۰ تا ۳۰۰ کیلومتری عملیات شناسایی را انجام می دهند، دارای سرنشین بوده و پس از انجام ماموریت به زمین بر می گردند .
- ایستگاه های فضایی- ماهواره ها: انواع ماهواره ها در عملیات شناسایی شرکت دارند .

شناسایی هدایت نهایی Fainal guidance reconnaissan

این شناسایی که برای هدایت موشک ها و بمب های هوشمند انجام می گیرد مشابه شناسایی هدف یابی با تجهیزات راداری، حسگرهای حرارتی و لیزری و GPS صورت می گیرد (منبع ۲)

شناسایی هدف یابی Target detection reconnaissan

هدف از این نوع شناسایی تعیین موقعیت (مختصات)،جهت و سرعت هدف (به منظور قفل نمودن روی هدف) است . این شناسایی با تجهیزاتی نظیر رادار، حسگرهای حرارتی و لیزری و GPS (سیستم تعیین موقعیت جهانی) انجام می شود.(منبع ۲)

شناسایی هوایی Air reconnaissan

شناسایی هوایی با استفاده از بالون، هلی کوپتر، هواپیماهای بـدون سرنشـین و بـا سرنشـین انجـام می گیرد. سیستم های پروازی تا ارتفاع ۳۰ کیلومتری عملیات شناسایی را انجام می دهند. این شناسایی بیشتر برای شناسایی تاکتیکی استفاده می شوند و می توانند بر اساس اطلاعات از پیش تعیین شده و یـا با اطلاعات اپراتوری کنترل شوند. این شناسایی از تجهیزات تخصصی که بدون ورود به منطقـه هـوایی دشمن و یا وارد شدن به مرزهای پدافند هوایی قادر به شناسایی است بهره می برد.

عکس هوایی Air picture

هر گونه عکسی که از طریق وسیله نقلیه هوایی مثل بالون، هواپیما و بالگرد از سطح بخشی از زمین برداشت شود، عکس هوایی نامیده می شود.برای استفاده و کاربرد آن در تهیه نقشه از اصول خـاص و استاندارد استفاده می شود.عکس هوایی ممکن است قائم و یا مایل باشد. برای کاربری های تولید نقشه از نوع استاندارد قائم استفاده می شود.(منبع ٤٧)

کاربردی حسگرهای مسنت Application of MASINT sensor

مسنت قادر خواهد بود تا سامانه سلاح های ویژه را شناسایی، نوع ماده را تعیین، ترکیب مواد شیمیایی را مشخص وتوانایی های دشمن بالقوه را در میزان بکارگیری این سلاح ها تا حد بسیار بالایی تعیین نماید.

- مسنت بعنوان شیوه ای منحصر بفرد جهت جمع آوری و تجزیه و تحلیل همراه بـا راه کارهـای ویژه تجزیه و تحلیل با روش های سنتی متفاوت است . - اطلاعـات مسـنت جهـت تـامین نیازهـای اطلاعات ملی به منظور کسب اطلاعاتی در زمینهٔ تکثیرسلاح های کشتار جمعی، شیمیایی ومیکروبـی حیاتی می باشد. شناسایی سلاح های هوشمند متکی به اطلاعات مسنت است . (منبع ٤٧)

مسنت راهبردی strategic MASINT

یکی از منابع جمع آوری اطلاعات مسنت راهبردی، هواپیمای کبرابال است که دارای حساسه های مختلف و امکانات جمع آوری اطلاعات آن چند منظوره بوده و شامل امکانات اطلاعات تصویری نیـز میشود. محصول تولید شده، حاصل تجزیه و تحلیل اطلاعاتی است که از طریق این شیوه بدسـت آمـده است .(منبع ٤٧)

مسنت Measurement & Signature INTelligence (MASINT)

مسنت یا اطلاعات سنجش و علایم، در دهه۱۹۸٦ بعنوان روش هایی از تشریح عملیات و منابع نظامی ، متفاوت با اغلب منابع دیگر اطلاعاتی از قبیل اطلاعات سیگنالی، اطلاعات انسانی و اطلاعات تصویری پا به عرصه جامعه اطلاعاتی نهاد مسنت به اطلاعات جمع آوری شده بوسیله ابزارها و تجهیزاتی همچون رادار، لیزر، حسگرهای الکترواپتیکی، آشکارسازهای تشعشی، حسگرهای ارتعاشی و . . . اطلاق می گردد . این اطلاعات، اهداف یا رویدادها را از روی آثار شان می سنجد. در واقع **مسنت** شامل اطلاعات علمی و فنی می گردد که از طریق تجزیه وتحلیل کیفی و کمی اطلاعات (مقیاس،زاویه، مکانی طول موج، زمان،مدولاسیون، پلاسما، هیدرومغناطیسی و ...) توسط حسگرهای ویژه بکار می رود.(منبع ٤٧)

مواد جاذب رادار Radar Absobent Metals

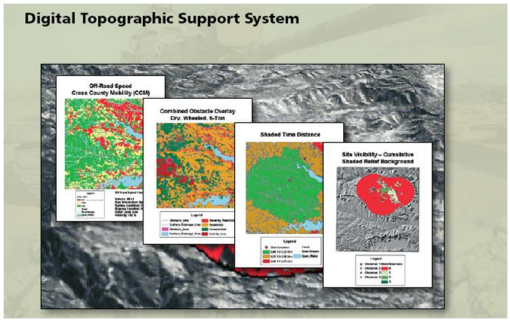
این مواد بازتاب انرژی را با جذب قسمت عمده انرژی کاهش می دهند جذب انرژی از طریق مکانیسم های مختلفی امکان پذیر است که می تواند ناشی از خواص الکتریکی یا مغناطیسی ماده باشد. در حقیقت تلفات ایجاد شده در انرژی به حرارت تبدیل می شود. یکی از دی – الکتریک های جاذب معروف کربن است. جاذب های الکترومغناطیسی از لحاظ علمی دارای کاربرد بیشتری هستند. از جمله مواد جاذب مغناطیسی Iron Carbony1 و اکسید آهن (فریت) هستند (منبع ۲)

هواپیمای بدون سرنشین تاکتیکی tactical UAV

هواپیمای مذکور برای تصویربرداری تا مسافت ۲۰۰ کیلومتر طراحی شده بود تا از این طریق از فرماندهان تاکتیکی پشتیبانی نماید (منبع ۲)

هواپیمای بدون سرنشین Unmanned Aerial Vehicle(UAV)

یکی از ابزارهای بسیار مهم در شناسایی، هواپیماهای بدون سرنشین هستند. این هواپیماها مجهز به دوربین‌های الکترواپتیکی ، تجهیزات مخابراتی یا محموله های دیگر می‌باشند.(منبع ۲)



نوعی از لایه های پشتیبانی در محیط GIS

کاربردهای سنجش از دور GIS Application

این دانش در زمینه‌های مختلفی از جمله برنامه‌ریزی شهری و منطقه ای، زمین شناسی و معادن، کشاورزی، در صنعت خودرو، بررسی موضوع حریم و مدیریت زمین وآنالیز پهنه بندی ،معماری ساختمانها ، منابع طبیعی و غیره کاربرد داشته و قادر است امر مدیریت و برنامه ریزی را بهبود بخشد. همچنین به کارگیری GIS علاوه بر سود آوری می‌تواند باعث تسریع در روند انجام کارهای برنامه‌ریزها در تشخیص موارد بحرانی و غیره گردد.

کاربردهای سیستم GPS Application of GPS

کاربرد های عبارتند از :پیش بینی زلزله ،نقشه برداری ، کاداستر ، کنترل امور مربوط به حمل و نقل و ترافیک ، کنترل حرکات تکتونیکی زمین ، کنترل جابجایی سدها و برج های بلند، پیش بینی وضع هوا ، ناوبری (زمینی،هوایی،دریایی) ، هیدروگرافی(آبنگاری) ، تعیین موقعیت سکوهای دریایی نفتی،تعیین موقعیت جزیره های مرجانی، مین یابی ، SCAN کردن دریا ، بروز رسانی سیستم های تعیین موقعیت اینرشیال ، استفاده جهت کنترل ماهواره های سنجش از دور و....

فصل هفتم

واژگان سازه امن – تهدیدات سخت

۱- واژگان سازه امن

۲- واژگان تهدیدات سخت

- بمب هدایت شونده لیزری GBU-27

موشک تام هاوک مجهز به سرجنگی خوشه‌ای

اولین نوع هواپیمای آواکس درسال ۱۹۷۷

۱- واژگان سازه امن

آثار انفجار بر ساختمان Blast effects of building

در یک انفجار، انرژی پتانسیل مواد منفجره در مدت زمان بسیار کوتاهی (در حد چند میکرو ثانیه) آزاد شده و انرژی آزاد شده به دو پدیده مجزا، تشعشعات حرارتی و امواج شوک (در هوا و زمین) تبدیل می گردد. در این بین امواج انفجاری در هوا عمده ترین دلیل خسارات وارده بر ساختمان ها می باشد. این امواج با سرعت مافوق صوت منتشر شده، موجب افزایش فشار محیطی می گردد. پس از برخورد امواج انفجار به نزدیک ترین دیوار خارجی ساختمان، پنجره ها شکسته شده، دیوارها و ستون های خارجی تحت فشار امواج پژواکی تغییر شکل داده و با گسترش امواج سایر وجوه ساختمان نیز تحت تأثیر قرار می گیرد.

ارتعاش پایه Basis tremble

در اثر انفجار، سازه به لرزش در می آید. اگر لرزش وارده شدید باشد، می تواند به تجهیزات نصب شده بر روی سازه آسیب جدی وارد کند، و باعث شکستن و یا لق شدن نگهدارنده ها و اتصالات شود. هم چنین لرزش باعث ایجاد ضربه قوچ در خطوط انتقال آب، و ضربه در مخازن می شود.

استحکامات Fortification

ایجاد هرگونه حفاظ که در مقابل اصابت مستقیم بمب ، راکت ، موشک ، گلوله ، توپخانه ، خمپاره و یا ترکش آنها مقاومت نموده ، مانع صدمه رسیدن به نفرات و یا تجهیزات گردد . (منبع ٤٠)

الگوی بارگذاری Loading Pattern

الگوی بارگذاری در واقع تبدیل اثرات ناشی از انفجار به سازه به شکلی ساده و قابل فهم می باشد، که طراح بتواند به سادگی ممکن سازه را در برابر آن به صورت مقاوم طراحی نماید. این الگوی بار به عواملی همچون نوع سازه، فاصله از محل انفجار، شرایط خاک، مشخصات منبع انفجار و ... بستگی دارد.

بارگذاری انفجاری Explosive loading

تعیین بارگذاری انفجاری سازه ها در حالات مختلف نظیر انفجار در هوا، انفجار در سطح زمین، انفجار زیر زمین از نوع محبوس یا غیر محبوس می باشد. فرمول های مربوط به تعیین فشار در فواصل مقیاس شده ارایه می شود. سپس تعیین بار وارد بر سطوح مختلف سازه (سطح جلویی, پشتی , جانبی و سقف) مطرح شده همچنین در مورد نحوه بارگذاری در داخل زمین روابط و فرمول هایی ارایه می گردد (منبع ۳)

بارگذاری سازه Structure loading

مقدار نیروهای استاتیکی معادل نیروهای دینامیکی ناشی از انفجار که بر اعضاء مختلف سازه وارد می شود، مورد بحث قرار می گیرد. نیروهای استاتیکی معادل، مانند بار مرده ناشی از وزن اعضاء به صورت گسترده و یکنواخت توزیع می شود. برای بدست آوردن تنش های بحرانی در هر نقطه از سازه لازم است کلیه بارگذاری هایی را که منطقی و محتمل به نظر می رسند بر سازه اعمال گردد.

بارهای انفجاری Explosive loads

انفجارها از نظر موقعیت به دو دسته انفجار خارجی و داخلی تقسیم می شوند:

انفجار خارجی با نام های انفجار غیرمحبوس و انفجار آزاد نیز خوانده می شود که به دو نوع انفجار در هوا و انفجار در سطح زمین تقسیم می گردد. در انفجار هوایی، امواج انفجار مستقیما به سازه برخورد کرده و نحوه گسترش آن نیز به صورت کروی می باشد.در صورتی که امواج ناشی از انفجار در سطح زمین ابتدا به زمین برخورد کرده و سپس به سازه برسند ،انفجار را، در سطح زمین گویند.

انفجارهای داخلی، بسته به شرایط ساختمان و نحوه تهیه آن به دو دسته محبوس و نیمه محبوس تقسیم می گردد. علاوه بر بارهای ناشی از انفجار، باید اثر ترکش های ناشی از انفجار و همچنین شوک ناشی از انفجارات خارجی نیز در نظر گرفته شود.

بالا بردن مقاومت ساختمان(مقاوم سازی) Building Hardening

بالا بردن مقاومت ساختمان ها برای کاهش خسارت های ناشی از انفجارها.(منبع ٤٤)

پناه‌گاه از نظر سطح محافظت shelter due level protection

پناه‌گاه‌ها بر مبنای میزان مقاومتی که از خود در برابر انفجار و پیامدهای آن(موج انفجار، ترکش...) نشان می‌دهند در سطوح مختلفی طبقه‌بندی می‌گردند این سطوح محافظت در برابر انفجار معمولاً در

ارتباط با میزان تخریب ایجاد شده در فضای امن پناه‌گاهی و میزان آوار ناشی از انفجار تعریف می‌شود. بر همین مبنا سطوح محافظت یک فضای پناه‌گاهی در برابر انفجار به سه دسته تقسیم می‌شود:

سطح محافظت کمینه – سطح محافظت متوسط – سطح محافظت بیشینه .

به عبارت دیگر میزان مقاومت یک سازه در برابر انفجار با میزان تخریبی کـه در اثـر انفجـار در آن ایجاد می‌شود سنجیده می‌شود.(منبع ۵۱)

پناه‌گاه چند منظوره Multitask Shelter

توانایی استفاده‌ی چندگانه از یک فضا علاوه بر کاربری پناه‌گاهی،طراحی و سـاخت یـک پنـاه‌گـاه داخلی یا مستقل را برای مالک یا کارفرمای ساختمان از نظر اقتصادی مقرون به صرفه‌تر می‌کند .

پناه‌گاه هسته‌ای، شیمیایی و.. chemical biological shelter

به فضای بسته‌ای است که افراد خودی (نیروهای داخل پناهگاه) را در برابر خطر آلودگی ش. م. ه. که به شکل بخار و آئروسل (ذرات ریزمایع و جامد) می‌باشد، حفاظت می‌کنـد، پناهگـاه ش. م .ه گفتـه می شود.عوامل شیمیایی و میکروبی نیز اگر چه دارای مدت اثر و شعاع اثر بسیار محدودتری می‌باشند، ولی از طریق هوا قابل انتقال بوده و دفاع در برابر آن‌ها نیز مانند دفاع در برابر ریزش‌هـای هسـته‌ای بـه تدابیر مشابهی نیازمند می‌باشد. (منبع ۵۱)

پناه‌گاه تک منظوره singletask shelter

پناه‌گاه‌های تک منظوره پناه‌گاه‌هایی هستند که با هدف استفاده در مواقع بحـران طراحـی و سـاخته می‌شوند. (منبع ۵۱)

پناه‌گاه خصوصی وخانوادگی family Shelter

این پناه‌گاه‌ها فاقد دستگاه‌های هوا دهی و فیلتر بوده و حفاظت در مقابل عوامل شیمیایی، میکروبی و هسته ای در آن‌ها، صرفاً از طریق هوابندی و درزبندی و به طـور کلـی جـدا کـردن فضـای آلـوده و غیرآلوده، برای مدت محدود حداکثر ۵ ساعت، فراهم می‌شود. تهویه در این پناه‌گاه‌ها در حالت عادی به صورت طبیعی انجام می‌شود؛ ولی دریچه‌های لازم به گونه‌ای طراحی می‌گردند کـه در هنگـام حملـه و بسته شدن آن‌ها، امکان ورود هوای آلوده به داخل پناه‌گاه وجود نداشته باشد. (منبع ۵۱)

پناه‌گاه عمومی و شهری public Shelter

برای حفاظت از جان مردمی که هنگام حملات هوایی در خانه نبوده یا دسترسی به پناه‌گاه‌هـای خانوادگی ندارند ایجاد پنـاه‌گـاه‌هـای عمـومی ضـروری مـی‌باشـد در همـین راسـتا در ادارات دولتـی،

فروشگاه‌ها، کارخانه ها، مساجد، مدارس، رستوران‌ها و سایر مراکز فعالیت‌های شهری می‌توان فضاهایی با کاربری دوگانه به عنوان پناه‌گاه‌های چند منظوره احداث نمود . (منبع ۵۱)

پناه‌گاه نظامی Military Shelter

این پناه‌گاه‌ها انواع مختلفی داشته و از نظر مقاومت و سطوح حفاظت طیف وسیعی را شامل می‌شوند وبه منظورهای نظامی به کار برده می‌شوند مانند آشیانه های حفاظتی هواپیماها، انبارهای مهمات و تسلیحات استراتژیک، ستادهای فرماندهی نظامی و ... (منبع ۵۱)

پناهگاه Shelter

حفاظ و پوششی است جهت مخفی شدن از دید و مصون ماندن از آتش دشمن با استفاده از مواد طبیعی یا مصنوعی. (منبع ۸)

یک پناهگاه استتار شده با استفاده از پوشش گیاهی بر روی سقف و زیر درخت

پناهگاه بتنی پیش ساخته Ready-mixed concrete Shelter

این پناهگاه به طول ۳ متر و عرض ۱/۵ متر بوده و ظرفیت این پناهگاه که تماماً بتنی می باشد بین ۱۲ تا ۱۵ نفر است. (منبع ۵۰)

پناهگاه طاق بتنی Concrete floor shelter

این پناهگاه با دیوار آجری و طاق بتنی مسلح احداث می شود، ظرفیت آن نیز بین ۱۲ تا ۱۵ نفر می باشد. (منبع ۵۱)

پناهگاه زیرزمینی Under ground shelter

بیشتر سازه های زیر زمینی به دلیل عمق قرارگیری نسبت به سطح، احاطه شدن توسط ضخامت قابل توجهی از مصالح زمین مثل سنگ و خاک و قابلیت استفاده از انواع سیستم های نگهداری جهت افزایش ضریب پایداری به نوعی در برابر انواع حملات هوایی و موشکی مقاوم هستند .به طور کلی پناهگاه ها به چند دسته تقسیم می شوند:

الف: پناهگاه های ضد تهاجمات اتمی ب: پناهگاه های ضد حملات هوائی ج: پناهگاه های ضد بلایای طبیعی(منبع ۵۱)

پو شش مقاوم hardeling cover

پوشش های مقاوم در محیط هایی که برای جلوگیری از صدمات انفجار به مواد با ارزش به کار می رود.(منبع ٤٤)

سازه امن درجه دو Two degree safe structure

این سازه ها در مقابل آثار ناشی از سلاح های متعارف دشمن (برخورد، نفوذ و انفجار) مقاومت کافی دارند ولی در برابر حملات هسته ای آسیب پذیر می باشند. از جمله این سازه های امن می توان پناهگاه های عمومی را نام برد.(منبع ۸)

سازه امن درجه سه Three degree safe structur

این سازه امن در مقابل آثار موج ناشی از انفجار و ترکش سلاح های متعارف مقاومت کافی دارند، ولی برای اصابت مستقیم طراحی نمی شوند. از جمله این سازه های امن می توان پناهگاه های خانوادگی را نام برد. (منبع ۸)

– یک نمونه سازه امن

سازه امن درجه یک one degree safe structure

مقاوم در برابر اصابت مستقیم سلاح های غیر متعارف دشمن،

مقاوم در برابر آثار ناشی از انفجار سلاح های هسته ای، شیمیایی و میکروبی،

سازه امن شیمیایی، هسته ای و میکروبی توسط درب های مخصوص هوابندی شده اند و هوای آلوده ورودی به داخل آن ها تصفیه می گردد. (منبع ۸)

سازه حفاظت کننده Protective structure

این سازه با توجه به سطوح مختلف حفاظتی، ویژگی های خاص خود را دارا بوده و براساس خصوصیات سامانه دهنده و سامانه گیرنده طراحی می گردد. به همین دلیل به منظور طراحی مناسب و بهینه ساختمان پایدار در برابر انفجار ، پیش از هر چیز، باید اطلاعات کافی در مورد سامانه های دهنده و گیرنده موجود باشد.

سازه رو زمینی Ground structure

طراحی سازه های امن روزمینی که در معرض آثار سلاح ها قرار می گیرد، بایستی به گونه ای انجام بگیرد که نفرات و تجهیزات را در برابر تهدید محتمل محافظت نمایند. عموما طرح این سازه ها برای مقاومت در برابر انفجار در هوا صورت می پذیرد. (منبع ۸)

سازه های زیر زمینی underground structures

سازه های زیرزمینی سازه هایی هستند که برای مقاومت در برابر آثار سلاح های نفوذ کننده و دقیق دشمن احداث می شوند. مجموعه های زیر زمینی جزو بهترین گزینه ها برای احداث قرارگاه های فرماندهی و کنترل، پناهگاه ها و انبار سلاح ها و تجهیزات مهم و صنایع دفاعی می باشند. (منبع ۸)

سازه های نیمه مدفون و مدفون Buried & semi bureid structures

سازه های نیمه مدفون و مدفون در خاک برای آثار ناشی از انفجار سلاح ها در هوا، در سطح و اصابت مستقیم طراحی می شوند. این گونه سازه ها به شکل های زیر وجود دارند:

۱- سازه سطحی که اطراف و روی آن با خاک پوشیده می شود و ورودی آن با استفاده از موج گیرهای مناسب و دربهای ضد انفجار مقاوم می شود. ۲- سازه ای که قسمتی از آن درون خاک است و قسمت روی سطح با خاک پوشیده می شود. این گونه سازه ها می توانند به صورت چند طبقه نیز احداث شوند. ۳- سازه ای که تمام آن درون خاک است. در واقع ابتدا زمین کنده شده، سازه احداث

می شود و سپس روی آن به طور کامل با خاک پوشیده می شود. ورودی این سازه ها بایستی بـا دقـت انتخاب شود و حتما از درب های ضد انفجار استفاده گردد. (منبع ۸)

سامانه گیرنده Receiver system

این سامانه شامل افراد، تجهیزات، سرمایه ها و ... بوده که نیازمند سطحی از حفاظت در برابر سامانه دهنده و آثار خروجی آن می باشد. با تعیین سطح آسیب پذیری قابـل پـذیرش در سـامانه گیرنـده، کـه براساس میزان حساسیت اجزای سامانه صورت می گیرد، سطح حفاظتی مورد نیاز مشخص می گردد.

سامانه حفاظتی انفجار Blast protective system

هر سامانه حفاظتی شامل سه جزء اصلی می باشد که عبارتند از: سامانه دهنده – سامانه گیرنـده – سازه حفاظت کننده

سطح محافظت بیشینه Maximum protection level

میزان تخریب و آسیب وارده به پناهگاه جزیی و کاملاً قابل تعمیر خواهد بود. به فضای پناهگاهی ممکن است در قسمت‌های پیرامونی آسیب‌های جزیی وارد شود.در این سطح، فاکتور محافظت در طراحی سازه برای پناهگاه بیش از200psi در نظر گرفته می‌شود. (منبع ۵۱)

سطح محافظت کمینه پناهگاه Minimum protection level of shelter

فضاهای پناهگاهی با سطح محافظت کمینه در برابر انفجار دچار تخریب‌های گسترده می‌شوند ولـی فروریزی کامل در آن‌ها اتفاق نمی‌افتد. امکان ایجاد جراحات جسمانی به پناه جویان وجـود دارد و بـه تجهیزات پناهگاه نیز آسیب جدی وارد می‌شود.دراین سطح، فاکتورمحافظت در طراحی سازه‌یـا تقویـت آن برای پناهگاه بین3-2(25 – 50 psi اتمسفر) در نظر گرفته می‌شود که حتی المقدور (چنان چه موانع اقتصادی وجود نداشته باشد) عدد 50 psi در طراحی لحاظ می‌گردد. در پناهگاه‌های مستقل یا خـارجی میزان پوشش خاک برای این سطح محافظت ۷۰ سانتی‌متر در نظر گرفته می‌شود. (منبع ۵۱)

سطح محافظت متوسط پناهگاه

در این حالت میزان تخریب و آسیب وارده به سـاختمان متوسـط و قابـل تعمیـر خواهـد بـود. بـه ساختمان پناهگاه آسیب‌های جدی وارد خواهد شد ولی سازه‌ی پناهگاه قابل استفاده مجدد خواهد بود.

مانع مقاوم Hardeling Curtain

یک مانع بزرگ که از مواد مقاوم ساخته شده و برای حفاظت از تخریب و ریزش آوار ناشی از انفجار به کار می رود.(منبع ٤٤)

مبحث ۲۱ مقررات ملی ساختمان Topic 21 of building national regulations

مبحث ۲۱ مقررات ملی ساختمان نیز تحت عنوان "پدافند غیر عامل" تدوین گردیده و ویرایش نخست آن مدون شده است. فصول این آیین نامه شامل موارد زیر می باشد:

فصل ۱- کلیات فصل۲- ملاحظات معماری فصل ۳- بارهای ناشی از انفجار فصل ٤- مشخصات مکانیکی و دینامیکی مصالح فصل ۵- ساز و کار آسیب دیدگی ساختمان و تاثیر انفجار بر سیستم های سازه ای فصل٦- روش های تحلیل و طراحی فصل۷- ملاحظات تاسیسات مکانیکی و برقی و ... (منبع ٤٠)

مقررات ملی ساختمان Building national regulations

مجموعه‌ای است از ضوابط فنی، اجرایی و حقوقی لازم‌الرعایه در طراحی، نظارت و اجرای عملیات ساختمانی اعم از تخریب، نوسازی، توسعه بنا، تعمیر و مرمت اساسی، تغییر کاربردی و بهره‌برداری از ساختمان که به‌منظور تأمین ایمنی، بهره‌دهی مناسب، آسایش، بهداشت، و صرفه اقتصادی فرد و جامعه وضع می‌گردد.

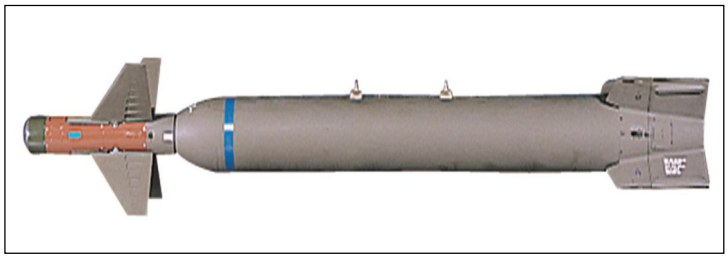
مقررات ملی ساختمان حاوی ضوابط حداقل برای طراحی، نظارت و نگهداری ساختمان است که باید در کلیه عملیات ساختمانی از قبیل تخریب، نوسازی، تغییر کاربری، توسعه بنا، افزایش یا کاهش طبقات، جابجایی، تغییرات و تعمیرات اساسی رعایت شود.

مقررات ملی ساختمان شامل ۲۱ مبحث بوده که تا کنون ۲۰ مبحث از طرف شورای تدوین مقررات وزارت مسکن و شهرسازی ارائه شده است. (منبع ٤٠)

۲- واژگان تهدیدات سخت

بمب لیزری

پیشرفت و توسعه چشمگیری که در زمینه جنگ افزارهای هدایت شونده لیزری صورت گرفته باعث پیشرفت و ارتقای دقت سلاح های هدایت شونده شده است. بمب های هدایت شونده لیزری قابلیت انهدام بالایی برخوردارند .سرجنگی های بکارگیری شده در بمب های هدایت شونده لیزری به منظور نفوذ بیشتر عمدتا از نوعBlu-109 و Blu-113 می باشد. جنس بدنه این بمب از فولاد با کیفیت عالی و پرچ شده با آلیاژ ۴۳۲۰ می باشد.اگرچه بمب های هدایت شونده ی لیزری برای اصابت به اهداف مورد نظر از دقت فوق العاده ای برخوردار می باشند با این حال نفوذ به سنگرهای زیرزمینی و استحکامات سخت دشمن می باید با دقت صورت گیرد. در این نوع نفوذ پذیری از Blu-109 و Blu-113استفاده می شود.از جمله بمب های هدایت شونده لیزری می توان به GBU-12, GBU -16 27 GBU-28, GBU اشاره نمود که در جنگ های اخیر به شدت مورد بهره برداری و توجه واقع شده اند .این بمب ها قابل حمل توسط انواع سکوهای هوابرد از قبیل هواپیماهای هریر، جگوار، تورنادو و کفیر می باشند.



- بمب GBU-28

بمب افکن استیلث B2 Spirit

بمب افکن استیلث که قادر به حمل ۲٤ بمب ۵۰۰ کیلویی GBU-31 می باشد . سرعت پروازی آن در حدود ۷۵۰ مایل بر ساعت است.هواپیمای B2 به علت داشتن قابلیت رادار گریزی امکان رسوخ در مواضع پدافندی طرف مقابل را دارد .

بمب خوشه‌ای Cluster bomb CBU-55/B

دارای بدنه‌ای استوانه‌ای و پیشانی دوکی همراه با فیوز بخش جلویی به طول ۱٤٤میلی‌متر وعقبه همراه چهار بال صلیبی به شکل مستطیل است. در این بمب بال در جهت خلاف بدنه و به صورت تا شونده می‌باشد. بمب با قلاب‌های آویز به طول ۳٥٦ میلی‌متر متناسب شده است. طول این بمب ۲/٤متر، قطر آن ۳٦۰ میلی‌متر و در صورتی که سه بمب BLU-73/B در داخل آن قرار گیرد وزن آن ۲٥۰کیلوگرم می‌شود.

بمب اتمی Atomic bomb

بمب اتمیB-61 در طول سال‌های ۱۹٦۳ تا ۱۹٦۸ به عنوان یک سلاح هسته‌ای حرارتی با مقاصد تاکتیکی و با هدف حمل و به کارگیری آن در اغلب هواپیماهای نیروی هوایی ساخته شد.

این بمب که از شکل آئرودینامیکی برخوردار است، دارای وزن کمی بوده و در شش وضعیت و مدل مختلف وجود دارد.مدل های مختلف بمب B-61 دارای سامانه مسلح کنندگی در حین پرواز هستند و انتخاب توان عمل بمب‌ها با چرخاندن یک سوئیچ امکان پذیر می‌باشد. محدوده توان بمب‌ها بین ۱۰ تا ٥۰۰ کیلوتن است که می‌توان آنها را با فیوز چند حالته، انفجار در هوا، بر روی زمین و به صورت تأخیری پرتاب نمود.

تهدید هوایی airy thraet

این تهدیدات شامل حملات جنگ افزار و سلاح های هوایی می باشند.به منظور شناسایی و بررسی توان عملیاتی هوایی تعدادی از جنگ افزار های هوایی را نام می بریم: هواپیماهای عملیاتی و جاسوسی مثل : بمب افکن استیلث – هواپیما های جاسوسی U–2 و آواکس – موشک های هوا به زمین و ...

خرج پلاستیک (C4)

این ماده خالص نیست بلکه از مخلوط ۹۱درصد RDX و ۹درصد مواد پلیمری ساخته شده است، حساسیت آن کمتر از RDX بوده و جزء مواد تندشکن غیر حساس است در نتیجه ایمنی آن بالاتر است. یکی از بهترین مواد منفجره نظامی برای انواع تخریب‌هاست حالت فیزیکی آن خمیری و شکل پذیر است، سرعت انفجار آن m/s8100 و قدرت آن ۱/۳٤ است به همین جهت برای قطع و برش فولاد و تخریب اجسام سخت بسیار مناسب است.(منبع ۲٥)

سرجنگی ترکشی Quiver warhead

در این نوع کلاهک ها پوسته را از جنس فولاد ضخیم می سازند و آن را طوری طراحی مـی کننـد که پس از انفجار، پوسته به ترکش های بسیار زیادی تبدیل شود. ترکیبی از ترکش و انفجار عاملی برای نتیجه بهتر در این سرجنگی است. انفجار ابتدا درون بدنه و در حجم کم انجام شده و بـه محـض آنکـه قدرت آن به حد معینی رسید بدنه از قسمت های ضعیف متلاشی و تکه تکه شده و با شتاب به بیـرون رانده یا پرتاب می شوند.

سرجنگی خوشه ای Cluster warhead

در این کلاهک ها بجای مواد انفجاری یک پارچه از بمب های کوچکی که به بمبلـت معـروف هستند، استفاده می شود. پوسته کلاهک را طوری می سازند که در هنگام نزدیـک شـدن آن بـه زمـین پوسته باز شده و بمبلت ها شعاع معینی را پوشش می دهند بسته به نوع مأموریت تعداد بمبلتها می تواند متغیر باشد .

سرجنگی گرافیتی Graphitie warhead

گفته می شود که اساس کار آن،پخش ریز مهمات هایی محتوی الیاف کربن است که با پخش شدن در انتقال دهنده ها و پست های برق باعث اتصال کوتـاه در آن هـا مـی شـود. مشـابه بـا سـلاح هـای خوشه ای پس از رسیدن موشک به ناحیه مورد نظر ، سرجنگی که حاوی چنین جعبه اسـت از موشـک جدا شده و سرجنگی های کوچکتر به ابعاد تقریبی یک قوطی نوشابه را در هوا پخش می کند. هر کدام از این زیر مهمات شامل مقدار کمی مواد منفجـره و نیـز الیـاف کـربن هسـتند. پـس از جـدا شـدن از سرجنگی اصلی مواد منفجره عمل کرده و باعث پخش الیاف در هوا می شوند. پس از قرار گرفتن الیاف بر روی پست های فشار قوی مدار اتصال کوتاه ایجاد شده و معمولاً یک قوس الکتریکـی بـا حـرارت زیاد تولید می کند، که خود الیاف را تبخیر می کند.

سلاح های متعارف standard weapons

بطور کلی، سلاح هایی که دشمن قادر است در جنگ های محدود از آن به راحتی بهره برداری کند را سلاح های متعارف یا کلاسیک می نامند. برخی از این تسلیحات عبارتند از :

– سلاح های با قدرت تخریب بالا که از هواپیما پرتاب می‌شوند. (مانند : بمب‌هـای ۵۰ تـا ۲۰۰۰ پوندی) سلاح های کلاسیک که شامل انواع گلوله های انفجاری، بمـب هـا و موشـک هـا مـی‌باشـند

بواسطه عوامل ذیل قادرند به نفرات، تجهیزات و تاسیسات خسارت وارد سازند. این سه عامل عبارتند از : اصابت (ضربه حاصله از برخورد) – موج انفجار – ترکش

موشک کروز Cruise missile

موشک کروز یک پرنده با خصوصیات بدون سرنشین، مسلح شده، آیرودینامیک، کنترل خودکار و اغلب دارای موتور تنفسی با هوا می‌باشد.»

هدایت موشک کروز معمولا در سه فاز صورت می‌گیرد: فاز پرتاب، فاز میانی و فاز نهایی. در فاز پرتاب موشک تنها به وسیله سیستم ناوبری اینرسی هدایت می‌شود. در فاز میانی موشک از هدایت اینرسی و یک یا چند روش دیگر که با هدایت اینرسی در ارتباط بوده، استفاده می‌کند.

مین‌های هوشمند Smart mine

این مین‌ها توسط بالگرد و هواپیما به سمت زمین رها می‌شوند و مین پس از قرار گرفتن در زمین فعال شده و به‌صورت یک راکت اتوماتیک آماده شلیک می‌گردد، به محض اینکه خودروی دشمن به محدوده برد رادار آن قرار گیرد راکت به سمت آن نشانه رفته و شلیک می‌شود.(منبع ۲۷)

نیتروگلیسیرین NG

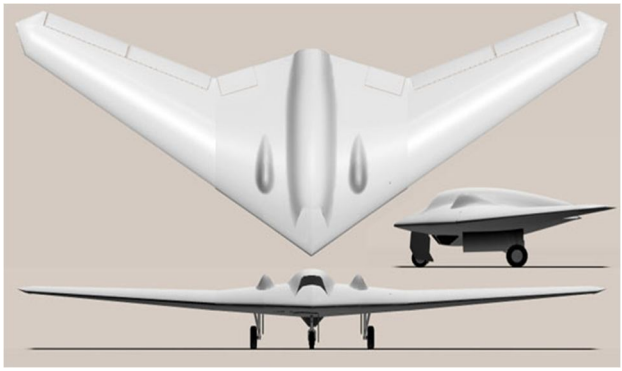
ماده ای است به شکل مایع بی رنگ مانند روغن مایع یا گلیسیرین است، مقدار بسیار کم آن با شعله می‌سوزد ولی اگر مقدار آن زیاد باشد و یا در محیط بسته قرار گیرد به شدت منفجر می‌شود، به ضربه به شدت حساس است، سرعت انفجار آن m/s8400 و قدرت انفجار آن ۱/٦۳ یعنی برابر RDX است، در حال حاظر خالص آن کاربرد انفجاری ندارد ولی به صورت مخلوط در ساختن دینامیت ها و خرج های پرتاب و خرج های جامد موشک استفاده می‌شود، دستکاری و استنشاق بخار آن مسمومیت و سردرد شدید ایجاد می‌کند.(منبع ۲۷)

هواپیمای RPV Remote-Piloted Vehicle

پرنده‌های هدایت پذیر از راه دور که در بعضی منابع علمی به RPV ، UAV نیز شهرت دارند، در سیستم دفاعی کشورهای دنیا جایگاه ویژه‌ای کسب نموده‌اند. آنها قادرند عملیات های شبانه روزی در نقاط دوردست بر علیه اهداف ساکن و متحرک در تمام شرایط آب و هوایی را انجام دهند.پرنده های

بدون سرنشین به طورکلی از دیدگاه های مختلفی مورد بررسی قرار می گیرند و بـه دسـته بنـدی هـای مختلفی تقسیم می شوند شاید بتوان این ادعا را نمود یکی از این دسته بندی ها که بیشـتر مـورد تاییـد کارشناسان هوایی بوده عبارت است از: ریز پهباد ، Drone ، RPV، RPH هواپیمای RPV

این پرنده ها برخی از محدودیت های ذاتی وطبیعی Drone را برطرف می نمایند و قابل کنترل از ایستگاه زمینی یا توسط خلبان هواپیمای سرنشین دار دیگـر ، مـی باشـند. پرنـده هـای RPV قـادر بـه جوابگویی به فرامین هدایت وکنترل در طول مسیر پروازی می باشند .



تصویر هواپیمای کنترل از راه دور RQ-۱۷۰ امریکا

هواپیمای جاسوسی U–2

هواپیمای U-2 یک هواپیمای جاسوسـی سرنشـین دار اسـت کـه دارای تجهیـزات عکـس بـرداری پیشرفته جهت انجام ماموریت‌های جاسوسی و شناسایی می‌باشد. مشهورترین مدل این نـوع هواپیماهـا SR–71 یا «پرنده سیاه» است که هنوز سریع ترین هواپیمای جاسوسی جهان به شمار می‌رود. هواپیمای U2 قادر است تا انواع تجهیزات جاسوسی از قبیل حسـگرهای الکترونیکـی، رادیـویی و دوربـین‌هـای مختلف را با خود حمل کند . این دوربین‌ها به گونه‌ای طراحی شده‌اند که بتوانند در سخت‌ترین شرایط جوی بهترین بازده را داشته باشد. این هواپیما،ارتفاع پروازی بسیار بـالا در حـدود ۷۵۰۰۰ پـا داشـته و دارای جنس بدنه خاصی است که از چشم رادار مخفی می‌ماند.

U–2 دارای سیستم شناسایی الکترواپتیکی«SYEARS» است ، این سیستم شناسایی در واقع سیستم مرکبی از دو سیستم تصویر برداری مادون قرمز و سیستم تصویر برداری الکترواپتیکی می‌باشد.

هواپیمای شناسایی آواکس

آواکس با استفاده از یک سیستم مراقبتی دوربرد پیشرفته باعث ایجاد یک فرماندهی دفاع جوی قوی خواهد شد. که قابلیت دوام و بقاء بخش‌های فرماندهی، کنترل و مراقبت سیستم دفاعی امریکا را افزایش داده و همچنین پوشش راداری اهداف را در تمام ارتفاعات و بلنـدی‌هـا، چـه در زمـین و چـه در آب، فراهم می‌آورد.آواکس می‌تواند یک لینک کنترل‌ترافیک را بطور موقت برقرار سازد که استتار متحرک‌های هوائی را در نواحی جغرافیائی، به حداقل می‌رساند. در یـک چنـین وضـعیت‌هـای اضـطراری، آواکـس می‌تواند یک رابط مخابراتی برای هدایت عملیات، کمک ناوبری و ادامه مراقبت هوائی، ایجاد کند.

هواپیمای عمود پرواز هاریر Harrier plane

هواپیماهای عمود پرواز نوعی از هواپیماها هستند که دارای دو موتور مجزا می باشند کـه یکـی در هنگام بالا رفتن هواپیما و دیگر برای حرکت رو به جلوی آن طراحی شده است.هواپیماهای قائم پـرواز به باند نیاز ندارند؛ بنابراین می توان آنها را در دسته های کوچک در نقاط مختلفی که هیچ گونه شباهتی به فرودگاه نداشته باشد مستقر نمود. این قرار گاه ها میتواند حتی در میـان جنگـل یـا در دل کوهسـتان جایی که دشمن گمان آنرا هم نمی برد،پنهان نمود.اولین مدل هواپیمای هاریر پی ۱۱۲۷ نام داشت که در ۳۱ اوت ۱۹٦٦ اولین پرواز خود را انجام داد

فصل هشتم

مدیریت ریسک ،
مواردی از زیرساخت ها و ...

۱- مدیریت ریسک

۲- مواردی از زیرساخت ها و ...

۱- واژگان مدیریت ریسک

آنالیز خطر فرآیند Process Hazard Analysis

ارزیابی خطر در محدوده وسیعی که اهمیت موقعیت های خطرناک مرتبط با یک فرایند یا فعالیت را شناسایی و آنالیز می کند.(منبع ۲۲)

ارزیابی ریسک Risk Evaluation

ارزیابی ریسک کل فرایند تجزیه و تحلیل ریسک و برآورد ریسک را شامل می‌شود. ارزیابی ریسک شامل تحلیل تهدیدها، ارزش دارایی و آسیب پذیری برای تعیین درجه ریسک هر کدام از دارایی‌های مهم در مقابل تهدیدها بالفعل می‌باشد.(منبع ۲۱)

انتقال ریسک Risk Transfer

مسؤلیت ریسک از طریق تمهیدات مدیریتی به سازمان دیگر منتقل می‌شود. برای مثال بیمه یک نوع سامانه، انتقال ریسک است. (منبع ۲۱)

انواع مخاطرات kinds of hazards

مخاطرات را می‌توان به انواع مختلفی دسته بندی کرد :

مخاطرات طبیعی: مخاطرت طبیعی ، خود به انواع مخاطرات زمین شناختی، مخاطرات جوی، مخاطرات زیستی و مخاطرات بیولوژیک، تقسیم‌بندی می شوند.

مخاطرات انسان‌ساخت: این مخاطرات شامل دو دسته تصادفی و یا عمدی هستند.(منبع ۲۱)

اولویت بندی ارزیابی ریسک avaluation Prioritize of Risk

در برنامه حفاظت زیرساخت ها، اولویت بندی فرآیند ارزیابی ریسک است که منجر به تشخیص این موضوع می شود که کجا تلاش های پیشگیری یا کاهش ریسک ضروری تر است و در نتیجه تعیین اینکه کدام فعالیت های حفاظتی برای داشتن بیشترین تاثیر باید انجام گیرد.(منبع ۲۲)

برآورد ریسک Risk Estimation

بعد از اتمام پروسه تجزیه و تحلیل ریسک، بایستی بین ریسک‌های تخمین زده شده و معیارهای ریسک، مقایسه صورت‌گیرد. می‌توان گفت، برآورد ریسک، مرحله‌ای است برای تصمیم‌گیری درباره اینکه چه ریسک‌هایی برای سازمان مهم است و اینکه کدام ریسک‌ها قابل قبول و کدام نیاز به کنترل و اصلاح دارد، می‌باشد(منبع ۲۱)

پذیرش ریسک Risk Acceptance

وقتی ریسک‌ها کاهش پیدا کردند، تحت کنترل قرار گرفته و در همان سطح نگاه داشته می‌شوند. (منبع ۲۱)

تجزیه و تحلیل ریسک Risk Analysis

استفاده نظام مند از اطلاعات، به منظور شناسایی منابع ریسک و برآورد ریسک.(منبع ۲۱)

تخمین ریسک Risk Estimation

تخمین ریسک می‌تواند کمی، نیمه کمی و یا کیفی باشد که براساس احتمال یا تکرار و پیامدهای احتمالی آن بیان می‌شود. سازمان‌های مختلف بسته به نیازشان ممکن است ، معیارهای متفاوتی برای طبقه‌بندی پیامدها و احتمال وقوع ، تنظیم کنند. مثلاً بسیاری از سازمانها ترجیح می‌دهند که پیامدها و احتمال را به صورت بالا، متوسط، پایین تنظیم کرده و آن را به صورت یک ماتریس ۳ در ۳ نمایش می‌دهند.(منبع ۲۱)

حذف ریسک Risk Elimination

به این معنی که فعالیتی که دارای ریسک خاصی می‌باشد انجام نگیرد، یا اینکه به طریق دیگری انجام گیرد تا ریسک آن حذف شود. (منبع ۲۱)

دارایی Asset

دارایی به معنای هر چیزی است که برای سازمان دارای ارزش باشد. شناسایی و اولویت بندی دارایی های مهم، گام حیاتی در فرایند مدیریت ریسک پدافندغیرعامل، یعنی افزایش درجه محافظت در برابر حملات دشمن می‌باشد. (منبع ۲۱)

روش دلفی Delfy method

امروزه بسیاری از تحقیقات و پژوهش‌ها با استفاده از این روش انجام می‌شود و خصوصاً در مدل‌ها و تحلیل‌های بین رشته‌ای، رهنمودهای حاصل از این روش بسیار کارگشا می‌باشد. تعاریف و برداشت‌های متعدد از روش دلفی عبارتند از : روشی برای توسعه و بهبود اجماع گروهی است

فرایندی ارتباطی است که اجازه می‌دهد تا گروه برای حل مسأله‌ای پیچیده بدون کنش متقابل رو در رو یا مراجعه تک‌تک اعضای گروه به توافق برسد. روش دلفی برای حل مسائل و تصمیم‌گیری بکار می رود. (منبع ۲۱)

ریسک Risk

به پتانسیل خرابی یا از بین رفتن دارایی‌ها اطلاق می‌شود و براساس رابطه تجمعی ارزش دارایی و تهدیدها و خطرات و آسیب‌پذیری محاسبه می‌شود. ریسک براساس احتمال وقوع تهدید و خطر و نتایج وقوع آن تعریف می‌شود. (منبع ۲۱)

ریسک قابل تحمل Bearable risk

به ریسکی که میزان آن تا حد قابل قبول توسط سازمان، با درنظر گرفتن الزامات قانونی کاهش یافته باشد، ریسک قابل تحمل گویند.(منبع ۲۱)

ریسک قابل قبول Acception risk

وضعیتی است که در آن خطر و یا تهدید به روش‌های ایمنی و فنی حذف شده یا خنثی گردیده و یا اصولا عواقب آن به هر دلیل مورد پذیرش است.(منبع ۲۱)

ریسک باقیمانده Residual Risk

آن مقدار از ریسک که پس از مقابله با ریسک ها، هنوز وجود داشته باشد و یا در اثر مقابله با ریسک بوجود آید.(منبع ۲۱)

شناسایی ریسک Risk Identification

شناسایی ریسک، بیانی برای شناسایی عدم قطعیت‌ها در توان مقابله با تهدیداتی است که سازمان با آنها ممکن است مواجه باشد. این امر نیازمند داشتن آگاهی از سازمان، نحوه تعاملات، قوانین حقوقی، اجتماعی، سیاسی و فرهنگی محیط بر سازمان، که سازمان مربوطه با آن سروکار دارد، می‌باشد شناسایی ریسک باید از طریق یک مدل روشمند انجام شود، به طوری که در این روش تمام جوانب فعالیت‌های مختلف شناسایی شده و طبقه‌بندی شده باشد. (منبع ۲۱)

شناسایی تهدیدات Treats Identification

اطلاعات مورد نیاز که برای تعیین یا توصیف یک تهدید لازم است شامل موارد زیر می باشد:

نوع دشمن – فعالیت های بالقوه دشمن – انگیزه های دشمن – قابلیت های دشمن (منبع ۲۱)

کاهش ریسک Risk Reduction

ریسک در صورتی کاهش می‌یابد که احتمال، فراوانی و یا پیامد آن کاهش یابد. رویکرد عمده ترمیم ریسک، کاهش مقدار عناصر آن با بکارگیری اصول پدافند غیرعامل می‌باشد. و می‌توان شیوه‌هایی مانند کاهش اثرات ریسک و یا انتقال ریسک را مد نظر قرار داد.(منبع ۲۱)

کنترل ریسک Risk Control

فرایندی است که از طریق آن برای کاهش ریسک‌ها به یک سطح یا نگهداشتن ریسک‌ها در سطوح خاص تصمیم‌گیری و اقدام می‌شود.راهکارهایی که می‌توان برای کنترل ریسک در پیش گرفت، عبارتند از: حذف ریسک– کاهش ریسک – انتقال ریسک. (منبع ۲۱)

مدیریت ریسک Risk manegement

مدیریت ریسک، عبارت از فرآیندی است که عوامل اجتماعی، اقتصادی وسیاسی را درتجزیه وتحلیل ریسک مورد توجه قرار می دهد، میزان مقبول خسارت ناشی از حوادث راتعیین نموده و سپس روند تصمیم گیری رابرای به حداقل رساندن خسارت یا اختلال احتمالی تعیین می نماید. در واقع، مدیریت ریسک فرآیندی است که میزان قابل قبول یک ریسک را در جامعه شناسایی می کند و اولویت ها و راه حل هایی را درنظر می گیرد که مطابق با منابع مالی موجود باشد. (پژوهشکده سوانح طبیعی، ۱۳۸۵) مدیریت ریسک، هسته مرکزی هر مدیریت استراتژیک سازمانی است. فرایندی است که سازمان ها را به صورت روش‌مند به ریسک‌های مرتبط با فعالیت‌ها و نیز اهداف تعریف شده برای هر فعالیت آشنا می سازد. (منبع ۲۱)

نمایه ریسک Risk Profile

نتایج فرایند تجزیه و تحلیل ریسک، بایستی تبدیل به نمایه ریسک شود که در آن رتبه‌بندی بین ریسک‌ها انجام شده است که در اولویت‌بندی نحوه اصلاح و ترمیم ریسک‌ها استفاده خواهد شد. این رتبه‌بندی همچنین اهمیت ریسک‌ها را بیان می‌کند.(منبع ۲۱)

۲- واژگان مواردی از زیر ساخت ها

ایستگاه تقویت فشارگاز Gas pressure amplification Stations

با توجه به این که پس از طی کردن مسافت هائی، فشار گاز درون لوله کاهش پیدا می کند و جهت رساندن فشار گاز به فشار مطلوب، در مسیر خطوط انتقال از ایستگاه های تقویت فشار استفاده می شود. این ایستگاه ها شامل توربین ها و کمپرسورها می باشند و فشار گاز ورودی توسط کمپرسورها افـزایش پیـدا مـی کنـد. دسـتور در سـرویس قـرار گـرفتن کمپرسـورها توسـط مرکـز ارسـال و کنتـرل گـاز (DISPATCHIN) صادر می شود.

ایستگاه های تقلیل فشار Gas pressure reduction Stations

خطوط انتقال در نهایت به ایستگاه دروازه شهری (ایستگاه تقلیل فشـار) مـی رسـند جهـت تطبیـق شرایط فیزیکی گاز انتقال داده شده به مبادی مصرف کننده گان، نیاز به تاسیساتی است که بـه صـورت اتوماتیک این شرایط را کنترل و اندازه گیری نماید.فشار، درجه حرارت، میزان جریان گاز و میزان سطح مایعات در مخازن از عمده کمیتهای قابل کنترل واندازه گیری در ایستگاه های تقلیل فشار گاز می باشد.

ایستگاه تقلیل فشار با هدف اندازه گیری و تقلیل فشار گاز خط لوله و آماده بودن آن جهت اتصال به سیستم گازرسانی شهری ایجاد گردیده است و بر اساس پارامترهایی چون جمعیت منطقه ای ، میزان بهره مندی از صنایع کوچک و بزرگ و به عبارتی میزان مصرف دارای ظرفیت های مختلفی است.

بالانس آب به روش بالا به پایین Water Balance to up –down method

بالانس آب بالا به پایین یا همان ممیزی آب، یک ارزیابی از هـدررفت هـای واقعـی اسـت کـه در مبنای سالیانه انجام می شود و پس از آنکه حجم مصارف مجاز و هدررفت های ظاهری از کـل حجـم ورودی به سیستم کسر شده، به دست می آید.

بالانس سالیانهٔ آب Water yearly Balance

عبارتست از تجزیه و تحلیل مؤلفه های ورودی، خروجی و مصارف آب در سیستم توزیع.

هرقطره از آب ورودی به سیستم، به مؤلفه ای در بالانس آب تخصیص می یابد کـه ایـن موضـوع هماهنگی کامل با تعاریف " بالانس سالیانهٔ آب استاندارد " دارد. (منبع ٤٨)

پالایش گاز طبیعی Natural gas purge

به دلیل وجود شن ریز، گل رس، هیدروکربن های مایع، و سایر ناخالصی ها و به منظور جلوگیری از ورود این مواد به سیستم انتقال، گاز طبیعی پالایش می گـردد.و بـدین طریـق از ورود ایـن مـواد بـه سیستم انتقال جلوگیری بعمل می آید .ورود این مواد درخطوط لوله وایستگاه های تقلیل فشارگاز باعث بروز مشکلاتی می گردد که از آن جمله می توان به انسداد خطـوط لولـه گـاز، تخریـب رگلاتورهـا و کنتورهای توربینی ، ایجاد خوردگی و بروز خاصیت سمی در گاز و ... اشاره کرد.

تهدیدات آب آشامیدنی Water Threats

عبارتند از : تهدیدات فیزیکی – تهدیدات شیمیایی – تهدیدات بیولوژیکی– تهدیدات سایبری

تهدیدات فیزیکی آب آشامیدنی Water phisical Threats

۱) انهدام فیزیکی تجهیزات سامانه یا اختلال در تامین آب می توانـد احتمـال بیشـتری نسـبت بـه آلودگی داشته باشد. یک فرد تروریست به آسانی مـی توانـد کـل تأسیسـات یـک شـهر را بـا تخریـب تجهیزات سالم آن زمین گیر نماید.۲) اتلاف فشار آب با مخدوش کردن ظرفیت های آتش نشـانی کـه می تواند منجر به رشد باکتری در سامانه شود.

۳) پتانسیل ایجاد اثر ضربه با باز کردن یا بستن ناگهانی شیرفلکه های کنتـرل اصـلی و روشـن یـا خاموش کردن بسیار سریع پمپ ها می تواند منجر به شکستگی های گسترده همزمان شود.

خطوط انتقال گاز gas transmittal pipes

گاز خروجی از پالایشگاه توسط خطوط لوله جهت مصرف در شهر ها، صنایع یا صـادرات انتقـال می یابد. قطر خطوط انتقال از ۱۲ تا ٥٦ اینچ می باشد. در فواصل معین از خطوط انتقال، ایستگاه هـای شیر موجود است که عموما دارای یک شیر L.B.V بر سر مسیر اصلی، شیر های کنار گـذر (By pass) و شیر Blow Down یا تخلیه است. وظیفه شیر L.B.V بسته شدن آن در زمان احساس افت فشـار ناگهـانی در یکی از دو سمت آن می باشد. این امر باعث می شود در زمان انفجارات یا شکستگی لوله هر دو شیر L.B.V موجود در ۲ سمت محل حادثه بسته شوند و فقط گاز ما بین دو ایستگاه بسوزد یا تخلیه شود.

سطح اقتصادی نشت آب Economic Level of Leackage (ELL)

سطح اقتصادی نشت در واقع تعیین میزان هدررفت ها برای وضعیتی است که مجموع هزینه های کاهش هدررفت واقعی و هزینه های هدررفت آب دارای کمترین مقدار است، مشخص می شود.

سیستم های ایمنی ایستگاه تقلیل فشار گاز

در سیستم های تقلیل فشار گاز جهت جلوگیری از اعمال فشار نا مطلوب به شبکه های متصل به آن هنگام بروز اشکال در رگلاتور ها از سه نوع تجهیزات ایمنی استفاده می شود و اصولا در یک ایستگاه باید حداقل دو عامل از این سه نوع وجود داشته باشد. این سه عامل عبارت است از :بستن رگلاتورها به صورت ACT-Mon ، شیر قطع فشار ، شیر اطمینان.

شاخص نشت زیرساخت آب infrastucture leakage index

یک شاخص عملکرد درخصوص چگونگی مدیریت شبکهٔ توزیع از لحاظ کنترل هدررفت های واقعی در فشار بهره برداری موجود شبکه، می باشد . (منبع ٤٨)

شیر اطمینان Safety Valve

از تجهیزات ویژه ای که ایستگاه را در مقابل افزایش ناگهانی ایمن می سازد شیرهای اطمینان هستند. شیرهای اطمینان به عنوان وسیله ای مناسب جهت جلوگیری از ازدیاد فشار ناگهانی در ایستگاهها گاز مورد استفاده قرار می گیرند. محدودیت فشار در اینگونه کاربردها معمولاً ناشی از فشار قابل تحمل تجهیزات ، لوله ها ، محصولات تولیدی و همچنین مسائل مرتبط با حفظ ایمنی افراد می باشد که اصطلاحاً به محدوده فشار کارکرد امن معروف است.

شیرهای قطع فشار گاز shutoff valve

عامل مهم دیگری در سیستم های تقلیل فشار بوده که در فشار مورد نظر بسته شده و باز شدن آن به شکل دستی صورت می گیرد. هرگاه هنگام افزایش فشار شیر های اطمینان عمل ننمایند و یا با وجود عمل کردن نتوانند باعث افت فشار خط گردند، شیرهای قطع فشار به گونه ای تنظیم شده اند که موجب قطع گاز سیستم می گردند. ساختمان این نوع شیر ها از دو قسمت عمل کننده (Actuater) و شیر (Valve) ساخته شده است.

محاسبه هدررفت واقعی آب calculate of Water Real loss

حجم سالیانه ی هدررفت های واقعی عبارتست از بالانس بین ورودی سیستم و مؤلفه های زیر:

تمام عناصر مصرف – آب خروجی (فروخته شده) – هدررفت های ظاهری . (منبع ٤٨)

مصارف غیرمجاز آب Water unallowable consumpion

عبارت است از هر گونه استفاده ی غیرمجاز از آب. این مصارف شامل برداشت غیرقانونی از آب (مثلاً برای ساخت و ساز)، انشعاب غیرمجاز، نصب کنارگذار از کنتور مشترک و یا دستکاری کنتور می باشد. (منبع ٤٨)

نشت از انشعاب مشترک آب Leakage from customer offshoot

عبارت است از هدررفت آب ناشی از نشتی ها و شکستگی های انشعاب مشترک از نقطه شیرگذاری شده تا نقطه مصرف مشترک. (منبع ٤٨)

نشت در شبکهٔ انتقال آب Leakage in water transmittal network

عبارت است از هدررفت آب از نشتی ها و شکستگی های خطوط توزیع و انتقال . این مورد شامل نشتی های کوچکی است که هنوز گزارش نشده (مثل نشت از اتصالات) و یا شکستگی های بزرگی است که گزارش و تعمیر شده اند، امّا در دورهٔ زمانی مشخصّی قبل از گزارش، نشتی داشته اند.

هدر رفت آب water loss

عبارت است از اختلاف بین ورودی سیستم و مصارف مجاز. هدررفت های آب شامل هدررفت های واقعی و ظاهری می باشد. (منبع ٤٨)

هدر رفت ظاهری آب Water outward loss

شامل انواع بی دقتی در اندازه گیری مصارف مشترکین و خطای کار با داده ها (مربوط به قرائت کنتور و صدور صورتحساب) و مصارف غیرمجاز (غیرقانونی و سرقتی) می باشد. (منبع ٤٨)

هدررفت واقعی آب Water Real loss

عبارت است از هدررفت های آب از سیستم تحت فشار و همچنین مخازن ذخیره تا نقطه مصرف مشترک. این نقطهٔ مصرف در سیستم های دارای اندازه گیری همان کنتور مشترک است. (منبع ٤٨)

هدررفت ها در مخازن ذخیره

هدررفت های به دلیل نشت در تأسیسات ذخیره آب تصفیه، ناشی از مشکلات بهره برداری و یا فنی می باشد. این هدررفت ها شامل نشت از سازه های مخازن، سرریزها، تبخیر و غیره می باشد.

فصل نهم

واژگان سایر موضوعات

(آمایش سرزمینی، فناوری نانو، پزشکی و ...)

۱- واژگان آمایش سرزمینی

۲- واژگان فناوری نانو

۳- واژگان پزشکی

۱- واژگان آمایش سرزمینی

آمایش سرزمین Spatial planning

عبارت است از تنظیم روابط بین انسان، فضا و فعالیت های انسان، به منظور بهره برداری منطقی از تمام امکانات، برای بهبود وضعیت مادی، معنوی و اجتماعی، بر اساس ارزش های اعتقادی، سوابق فرهنگی و ابزار علم و تجربه در طول زمان.

دکتر مجید مخدوم، آمایش سرزمین را: تنظیم رابطه بین انسان، سرزمین و فعالیت های انسان در سرزمین به منظور بهره برداری در خور پایدار، از جمیع امکانات انسانی و فضایی در جهت بهبود وضعیت مادی و معنوی اجتماع در طول زمان، تعریف می نماید. (منبع ۱۸)

اجرای مکان یابی Site selection execution

با نظر به اینکه ویژگی های فعالیت شناخته شده، شاخص های مورد نیاز تعیین شده و اطلاعات و داده های مورد نیاز برای کاربرد در مدل و انتخاب نوع مدل هم جمع آوری گردیده، می بایست اطلاعات را وارد نرم افزارهای مرتبط با مکان یابی نمود و با توجه به دستورات و باید و نبایدهایی که کاربر برای نرم افزار تعیین می کند، نرم افزار به صورت خودکار و با توجه به پیش فرض های تعیین شده، بهترین سایت مورد نظر برای فعالیت را تعیین می کند و حتی چندین سایت با درجات اولویت مختلف را مشخص می کند. نرم افزارهای مختلفی امر مکان یابی را انجام می دهند که بهترین و پرکاربردترین نرم افزار جهت مکان یابی، نرم افزار GIS می باشد. (منبع ۱۸)

اجزاء آمایش سرزمینی Spatial planning Component

تعریف و مفهوم اولیه ای که از آمایش سرزمین داده شده بود مثلث معروف انسان- فضا- فعالیت را در کنار یکدیگر مطرح می سازد. این تعریف که حدود ٤٠ سال از ارایه آن برای نخستین بار می گذرد. در مفهوم اولیه ای که از آمایش بر اساس این مثلث مورد توجه بود، اینکه سه عنصر انسان، فضا و فعالیت در برنامه ریزی توسعه اعم از شهری و منطقه ای باید مورد مطالعه قرار گیرند. منظور از فضا،

همان سرزمین یک کشور است، یا کلیه زمین ها و مکان هایی که به هر نحوی در اختیار یک حکومت قرار دارد. در طرح های آمایش سرزمین، فضای ملی از نظر نقاط ضعف ، قوت و تهدیدها و فرصت ها مورد بازشناسی قرار می گیرد تا با توجه به پتانسیل و توان ، برای آن ها برنامه ریزی صورت گیرد .

برنامه‌ریزی Planning

«جان فریدمن » برنامه ریزی را چنین تعریف می کند: برنامه ریزی فرآیندی است که می کوشد دانش علمی و تکنیکی را به عمل در حوزه عمومی تسری دهد.

برنامه‌ریزی فرآیندی سازمان یافته، آگاهانه و مبتنی بر تصمیم‌گیری است که به منظور آینده نگری و حرکت کلیه روندهای موجود به سوی مطلوب‌های انسانی، که در چارچوب اهداف توسعه بیان شده‌اند صورت می‌پذیرد (منبع ۱۸)

برنامه‌ریزی توسعه منطقه‌ای Territ development planning

برنامه‌ریزی منطقه‌ای فرآیندی است از تنظیم و مکان‌یابی فعالیت‌ها در جهت اهداف اجتماعی و اقتصادی مشخص در یک فضای فراشهری. به تعبیری دیگر، برنامه‌ریزی منطقه‌ای عبارت است از فرآیندی که شامل شناخت امکانات و قابلیت‌های توسعه در هر منطقه و تعیین چگونگی کاربرد عقلانی آنها در چارچوب اهداف توسعه ملی و منطقه‌ای مناسب با خصوصیات و ویژگی‌های فرهنگی، اجتماعی و تدوین سیاست‌های اجرایی، که سهم مهمی در تقویت مبانی اقتصادی و بهبود نظام اجرایی دارد.(منبع ۱۸)

برنامه‌ریزی فضایی Spatial planning

برنامه‌ریزی فضایی به تشخیص، تشریح و تصویرگری ساختارهای فضایی، به عنوان بخشی از سیستم‌های متشکل از روابط دارای معنی می‌پردازد. به عبارتی دیگر، برنامه‌ریزی فضایی، مجموعه مفاهیم، دیدگاه‌ها و روش‌هایی است که در جهت ایجاد سازمان و ساختار فضایی مطلوب و دلخواه مورد استفاده قرار می‌گیرد. برنامه‌ریزی فضایی در واقع نام دیگری برای برنامه‌ریزی منطقه‌ای است. با این تفاوت که مفهوم فضا کلی‌تر از مفهوم منطقه است و مرزهای منطقه را قطع می‌کند و این یک فرآیند مداوم است که به حالت عمودی و افقی نمایان می‌شود و در سطوح گوناگون به کار می‌رود.(منبع ۱۸)

پراکندگی Dispersion

گسترش، باز و پخش نمودن و تمرکز زدایی نیروها، تجهیزات، تأسیسات یا فعالیت‌های خودی، به منظور تقلیل آسیب‌پذیری آنها در مقابل تهدیدات، به طوری که مجموعه‌ای از آنها هدف واحدی را تشکیل ندهند.

توسعه Development

گروه‌های مختلف، توسعه را بر اساس دیدگاه‌های خود تفسیر نموده‌اند. در شالوده همه سونگری و کل‌گرایی، تعریف توسعه را می‌توان چنین دانست: «روندی است فراگیر در جهت افزایش توانایی‌های انسانی- اجتماعی، برای پاسخ‌گویی به نیازهای انسانی- اجتماعی، ضمن آن که نیازها پیوسته در پرتو ارزش‌های فرهنگی جامعه و بینش‌های پایداری جهان، پالایش یابند». بر مبنای این تعریف «توسعه مفهومی است همه جانبه که به مجموع نیازمندی‌ها و ابعاد مختلف زندگی انسان توجه دارد. توسعه واقعی باید بتواند شرایط لازم را برای همه افراد جامعه صرف نظر از موقعیت استقرار مکانی در همه ابعاد، در جهت پویایی، رشد و تعالی مادی و معنوی آنان فراهم سازد». (عندلیب، ۹،۱۳۸۰).

فرآیند توسعه فرآیندی چندبعدی است که شناخت و تجزیه و تحلیل آن مستلزم یک برخورد کل‌گرا و استفاده از تمام ابزار علوم اقتصادی و اجتماعی است. (منبع ۱۸)

سازمان فضایی Spatial organization

منظور از سازمان فضایی، مجموعه‌ای از فعالیت‌های سازمان یافته در فضا است این سازمان را هنگامی مشاهده می‌کنیم که در ارتفاع ۳۰۰۰۰ پایی از سطح زمین پرواز نماییم. از چنین ارتفاعی تعدادی از گره‌گاه های شهری و روستایی قابل رویت می‌باشد. این نقاط گره‌گاهی به وسیله شبکه خطوط ارتباطی به یکدیگر مرتبط می‌باشند. شبکه شامل خطوط راه‌آهن، راه‌های اصلی و غیره می‌باشد. اگر ارتفاع پرواز خود را کمتر کنیم، جزئیات بیشتری از گره‌گاه‌ها و شبکه‌ها را مشاهده خواهیم کرد. گره‌گاه های بزرگتر اختصاص به فعالیت‌های ویژه‌ای دارند که مصرف کننده فضا نیست مثل بازرگانی، گره‌گاه های کوچک خاص فعالیت‌هایی است که مصرف کننده فضا است، مانند کشاورزی و گره‌گاههای بینابینی مانند شهرک‌ها دارای الگوی فعالیت‌های مختلط می‌باشند.(منبع ۱۸)

سامانه اطلاعات جغرافیایی Geographic Information System

عبارت است از سیستم سازمان یافته‌ای متشکل از سخت‌افزار، نرم‌افزار، نیروهای متخصص و مدل‌های طراحی شده جهت اخذ، ذخیره‌سازی، نمایش، پردازش، به‌هنگام‌سازی، بازیافت، تجزیه و تحلیل و ارائه اطلاعات زمین مبنا با اشکال جغرافیایی که هدف نهایی آن استفاده از اطلاعات به دست آمده جهت برنامه‌ریزی و تصمیم‌گیری هر چه صحیح‌تر و باتدبیر است.(منبع ۱۸)

شاخص های مکان یابی Site selection indexs

عبارتند از : شاخص های پدافند غیر عامل؛ شاخص های برنامه ای؛ شاخص های توسعه ای؛ شاخص های حریم ها؛ شاخص های ارتباطی؛ شاخص های زیرساخت های موجود؛ شاخص های اقلیمی؛ شاخص های محیطی؛(منبع ۱۸)

طرح پایه آمایش سرزمین basis plan of Spatial planning

طرح پایه آمایش سرزمین طرحی است که در چارچوب هدف ها و سیاست های کلی توسعه، سازماندهی فضای ملی را پایه‌گذاری می‌کند. از نظر تهیه کنندگان طرح، مطالعات و برنامه‌ریزی آمایش سرزمین، جزئی از نظام جامع برنامه‌ریزی توسعه ملی بوده و شامل مراحل زیر است:

- مرحله اول، تهیه طرح پایه آمایش سرزمین که پایه اقدامات آمایش سرزمین است.
- مرحله دوم، تهیه طرح‌های آمایش نواحی که از بررسی نقش ناحیه در مقیاس آن به دست می‌آید و جزئیات در سطح را طرح می‌کند. مرحله سوم، تهیه برنامه‌های توسعه نواحی بر پایه طرح‌های آمایش که شامل آن دسته از فعالیت هایی است که در یک دوره معین برنامه، بر اساس سهم ناحیه از سرمایه‌گذاری‌های ملی می‌تواند اجرا شود (منبع ۱۸)

مراحل تهیه طرح آمایش Process of spatial plan

فرآیند تهیه طرح آمایش به ۳ مرحله « ساماندهی مطالعات» ، «بررسی وضع موجود و قابلیت‌سنجی» و «آینده‌نگری» تقسیم می‌شود. این فعالیت‌ها در دو محور استانی و ملی انجام خواهد شد. بخش اعظم فعالیت‌های استانی این فرآیند انجام یافته است .(منبع ۱۸)

مکان یابی Site selection

فرآیندی است که از طریق آن می توان بر اساس شرایط تعیین شده و با توجه به منـابع و امکانـات موجود، بهترین محل مورد نظر برای یک فعالیت را تعیین کرد. مکـان یـابی در واقـع تجزیـه و تحلیـل توأمان اطلاعات فضایی و داده های توصیفی به منظور یافتن یک یا چند موقعیت فضایی بـا ویژگیهـای توصیفی مورد نظر کاربر می باشد.(منبع ۱۸)

مکان یابی بطور کلی یا از طریق انتخاب نقـاط نمونـه و پـردازش هـای آمـاری و ریاضـی انجـام می گیرد و یا با پردازش توأمان داده ها در سطح منطقه با تجزیه و تحلیل استعدادهای مکانی و توصیفی جهت انتخاب مکان مناسب برای کاربری خاصی صورت می گیرد.

منابع زیستی Bio resource

کنوانسیون سازمان ملل متحد در تنوع زیستی منابع زیستی را چنین تعریف می کند: «ذخایر ژنتیکی، ارگانیسم ها یا اجزاء آنها، جمعیت ها، یا هر جزء زیستی دیگری از اکوسیستم ها بـا اسـتفاده بالفعـل و بالقوه یا ارزشمند برای بشریت» (منبع ١٤)

وظایف آمایش سرزمین Task of spatial planing

در وظایف شش گانه زیر، مفهوم عملیاتی و تخصصی آمایش سرزمین به شرح زیر حاصل می‌شود:

١-مکان‌یابی برای فعالیت‌های معلوم؛

٢-فعالیت‌یابی برای مکان‌های معلوم؛

٣-تناسب بین جمعیت و ظرفیت توسعه‌پذیری در هر حوزه جغرافیایی؛

٤-ارائه گزینه‌های متناسب الگوی اسکان جمعیت؛

٥-ارائه گزینه‌های متناسب الگوی سازماندهی فضا؛

٦-ترتیبات حفاظت از محیط زیست؛ (منبع ۱۸)

۲- واژگان فناوری نانو

آرامیدها (پلیمر) aramids

آرامیدها ازخانواده نایلون ها بوده که معروفترین آنها شامل نومکس و کولار می‌باشند. کولار برای ساخت جلیقه های ضدگلوله و یا بعنوان الیاف کمکی در افزایش مقاومت لاستیک چرخ های دوچرخه در برابر پنچر شدن استفاده می‌شود. تصور می‌شود از الیاف کولار برای ساخت چرخ های ضدگلوله نیز در آینده استفاده شود. مخلوطی از نومکس و کولار برای ساخت لباس‌های ضدآتش نیز استفاده می‌شود.(منبع ۱۵)

الیاف نامرئی Invisible fibbers

دانشمندان در بریتانیا و ایالات متحده راه حل هوشمندانه‌ای برای نامرئی کردن اشیاء پیشنهاد کرده اند. این روش به کمک احاطه کردن شیء با ماده‌ای که متامتریال نام دارد، انجام می‌گیرد.

متامتریال، ماده‌ای است از ترکیب میله‌های ریز و مجموعه‌ای از حلقه‌های فلزی و مانند آن که برای اولین بار توسط دیوید اسمیت (استاد دانشگاه کالیفرنیا) ساخته شد.(منبع ۱۵)

بیومتریک Biometric

بیومتریک به روش های خودکار تشخیص یا تایید هویت یک شخص زنده از طریق اندازه گیری مشخصه های فیزیولوژیکی یا رفتاری وی اطلاق می شود. بدین ترتیب بیومتریک یک مجموعه فناوری محسوب می گردد. همچنان که در تعریف فوق ذکر شد، برخی از مشخصه های بیومتریکی افراد، فیزیولوژیکی و برخی نیز رفتاری هستند. اثرانگشت، الگوی عنبیه، الگوی خونی یا حرارتی صورت و یا الگوی فیزیکی چهره، الگوی عروق خونی شبکیه چشم، DNA ، هندسه دست و یا الگوی خطوط کف دست از جمله مثال های مشخصه های فیزیولوژیکی و در عین حال صدا و نحوه مکالمه، نحوه امضاء ، نحوه تایپ عبارات و نحوه راه رفتن از جمله مثال های مشخصه های رفتاری محسوب می گردند.

پلیمرهای هوشمند Smart polymers

پلاستیک های هوشمند ترکیباتی هستند که به طور خود به خود و هنگامی که حرارت داده می‌شوند به شکلی با اشتعال پذیری کم‌تبدیل می‌شوند. این پلاستیک ها یا پلیمرهای هوشمند نیاز به واکنشی

دارند که در دماهای بالا صورت گیرد مثالی از پلیمرهای هوشمند، پلی‌آمیدهای هوشمند هستند که در حال حاضر برای حفاظت لباس‌های حریق آتش نشانان استفاده می‌شود. (منبع ۱۵)

دیواره پارچه ای صداگیر sound trap screen

به تازگی، نوعی دیوار انعطاف پذیر صداگیرکه با الیافی از جنس ترویرا پوشش داده شده، به بازار عرضه شده است. قطعات این دیواره که بر روی چارچوبی ویژه نصب می‌شود. امکان نصب و برپایی سریع دیواره را فراهم می آورند. (منبع ۱۵)

میکرو نانو micro nano

سیستم‌های میکرو و نانو الکترو مکانیکی تحولی نوین در عرصه نانو بوده که با قیمتی کم و سرعتی بالا، با کمک فنآوری ساخت مدارات مجتمع ساخته می شوند. به این شکل که پدیده های مختلفی چون گشتاور، سرعت فشار، دما و غیره را حس کرده یا مخابره می کنند (منبع ۱۵)

نانو Nano

نانو از لغت یونانی نانوس به معنای کوتوله گرفته شده است و در اصل، علمی است که درباره اجسام بسیار کوچک مطالعه میکند. یک نانومتر یک میلیونیم میلیمتر و ده مرتبه کوچکتر از اتم هیدروژن است. تامسی کنی، محقق دانشگاه استنفورد آن را چنین توصیف می کند، "اندازه ای که ناخن شما در یک ثانیه رشد می‌کند". هر چند که تعریف دقیقی از این علم وجود ندارد. لیکن مؤسسه علوم طبیعی در آمریکا نیز آن را چنین تعریف می کند: "تحقیق وتوسعه ی علم درباره ی موادی به اندازه ی تقریبا ۱ تا ۱۰۰ نانومتر". (منبع ۱۵)

نانو الکترونیک nano electronic

با کوچکتر شدن میکرو الکترونیک به عرصه نانومتر، دیگر فنآوری لیتو گرافی سیلیکونی جوابگو نخواهد بود و فن آوری اطلاعات به ناچار توسط الکترونیک مولکولی و کوانتمی، احاطه خواهد شد. الکترونیک مولکولی که بر پایه مولکول‌های آلی بزرگ، پلیمرها و نانو لوله های کربنی و یا مولکول DNA می باشد، تا سال ۲۰۰۷ وارد بازار خواهد شد. این مواد سرعت‌هایی حداقل چند صد برابر

تراشه‌های امروزی خواهد داشت. البته لازم به ذکر است، که نانو الکترونیک علاوه بـر پـردازش، شـامل ذخیره سازی وانتقال اطلاعات نیز می‌شود. (منبع ۱۵)

نانو پودرها nano powder

چون اندازه نانو پودر در محدوده طول موج نوراست ، طول موج رنگ آن دقیقا با انـدازه آن برابـر است. لذا این طول موج،آن را با تلالو بسیار زیادی منتشر می کننـد. مـثلا فلوئورسـانس فلـز و طـلا در حالت نانو پودر بیش از ۱۰ برابر است .در منور ها یا موادی که نیاز به انتشار شدید طیف خاصی از نور مرئی یا مادون قرمز است، می توان از نانو پودرها اسـتفاده کـرد. همچنـین بـرای رنـگ آمیـزی خـاص هواپیما. (منبع ۱۵)

نانو حسگر های هوشمند nano smart sensor

نانو حسگرها ما را قادر خواهند ساخت تا بسیاری از متغیرها را با دقت بیشتری ارزیـابی کنـیم. بـا استفاده از ملکول های بیولوژیکی قادر خواهیم بود کـه نانوحسـگر بسـازیم. نانوحسـگرها کاربردهـای بسیاری در صنایع غذایی دارند.یکی از این کاربردها کنترل نقل و انتقال محصولات کشاورزی و غـذایی و نیز انبارهای غذایی می باشد. کاربردهای دیگر شامل شناسایی پروتئین ها و نیز آشکار سـازی سـریع عوامل بیماری زا برای کمک به حفظ سلامت غذا است.

نانو روکش‌ها nano Casing

نانو بتونه‌ها و روکش‌های تک مولکولی، یکی دیگر از زمینه های مورد توجه در نانو مواد است. این لایه‌های نازک را می توان روی سطوح فلزی یا پلاستیکی نشاند و مقاومت سایشـی و ضـربه‌ای آنهـا را بشدت ارتقاء داد. (منبع ۱۵)

نانو مواد nano materials

نانو مواد، مواد جدیدی هستند که دارای سبکی و مقاومت کششی بالا و عمر مفیدی چند برابر مواد متداول می‌باشند که به دو دسته نانو کامپوزیت‌ها و نانو روکش‌ها تقسیم می‌شوند. (منبع ۱۵)

۳- واژگان پزشکی

ارگانیسم زنده مدرن modified Living organism

ارگانیسم زنده ای که طی بهره گیری از بیوفناوری مدرن ، ترکیب جدید در ساختار مواد ژنتیکی آن ایجاد شده باشد.(منبع ۳٤)

افسردگی سیستم عصبی Nervous-System Depressant

ترکیبی که باعث اثرات زیاد در بدن می شود و باعث افسردگی و از کار افتادن سیستم عصبی می شود.اثرات مهم این ترکیب مختل کردن فکر،و کاهش انگیزه است.(منبع ٤٤)

آلودگی هوا Air pollution

آلودگی هوا عبارتست از حضور یک یا چند آلاینده در هوای آزاد مانند گردوغبار، دود غلیظ، مه آلوده، بوی نامطبوع، دود یا بخار با کمیت‌ها، ویژگی‌ها و تداوم که می‌تواند حیات انسان، گیاه یا جانوران و یا اموال انسانی را به مخاطره اندازد و یا به طور غیرقابل قبولی محل استفاده راحت از زندگی و اموال گردد.

بهداشت روانی Mental health concepts

به نظر کارشناسان سازمان جهانی بهداشت، بهداشت روانی شامل : سلامت فکر و روان، قابلیت برقراری ارتباط موزون و هماهنگ با دیگران، توانایی در تغییر و اصلاح محیط فردی، اجتماعی، توانایی در حل تضادها و تمایلات غریزی به طور منطقی، عادلانه و مناسب، می باشد.

بیماری های انسان و دام Human &animaln maladies

بسیاری از عوامل عفونی از انسان و حیوانات به یکدیگر قابل انتقال هستند. این دسته از بیماریها، از چنان تنوعی در راه های انتقال به انسان برخوردارند که مراقبت از آنها اقدامات گسترده و متنوعی را می‌طلبد. دسته‌ای از آنها از طریق آب و مواد غذایی انسان را مبتلا می‌کنند نظیر بیماری هایی چون تب مالت . برخی از آنها از طریق تماس مستقیم انسان با حیوانات اهلی و وحشی آلوده به آدمی‌منتقل می‌شوند. همانند بیماری های سیاه‌زخم.

پادزهر Atropine

ترکیبی دارویی که به عنوان پادزهر مورد استفاده قرار می گیرد.(منبع ٤٤)

چارچوب ملی ایمنی زیستی bio safety nation Framework

چارچوبی که در قالب پروژه توانمند سازی UNEP - GEF و بر اساس الزامات و نیازهای داخل کشور تهیه شده است.(منبع ٣٤)

زیست فناوری Bio technology

به معنای هنر بشر در استفاده از علم تشکیل شده است و به طور کلی براستفاده از موجودات زنده یا قسمت هایی از موجودات زنده برای ساختن یا اصلاح محصولات یا فرآیندها به یک منظور خاص اطلاق می شود. (منبع ٣٤)

زیست فناوری مدرن Modern Bio technology

شامل زیست فناوری های زیر می تواند باشد:

الف) کار با اسید نوکلئیک در خارج از بدن موجود زنده، شامل DNA نوترکیب و یا وارد کردن مستقیم اسید نوکلئیک به داخل سلول ها و اندامک ها

ب) آمیخته کردن سلول ها خارج از قرابت فامیلی، به استثناء روش های اصلاح سنتی.(منبع ٣٤)

عامل لخته کننده خون Blood cloting Agent

عامل ماده شیمیایی لخته کننده خون که باعث می شود حرکت خون متوقف شود.مثال های از این مواد عبارتند از : آرسین(SA)، کلراید سیانوژن(CK)،هیدروژن کلراید(HCL)،و سیانید هیدروژن(AC).

عوامل زیستی مخاطره آمیز bio hazard agents

شامل ویروس ها ، باکتری ها ، اسپورها، DNA های نوترکیب و محصولات آنها و حتی ذرات نمونه های بالینی و... می باشند.(منبع ٣٤)

فشار روانی پس از تروما Post Traumatic Stress

این اختلال از مجموعه ای از علایم که بدنبال مواجهه با عامل فشار آسیب‌زای فوق‌العاده شدید ایجاد شده و بقدری ناتوان کننده است که فرد را از پای در می‌آورد و بدنبال جنگ، شکنجه، بلایای طبیعی، حمله، تجاوز و سوانح جدی نظیر تصادفات رانندگی، آتش‌سوزی، بمباران و یا زندگی در اردوگاه های اسرای جنگی شروع می شود.

فشار روانی Stress

فشار روانی به شکلی که پژوهشگر مشهور ریچارد لازاروس آن را تعریف کرده، حالتی از اضطراب است که وقتی حوادث و مسئولیت ها افزون بر آن مقداری است که انسان بتواند با آن کنار بیاید، تجربه می‌شود. اما به زبان فیزیولوژی فشار روانی میزان استهلاک و فرسودگی بدن است.

فوریت های روان پزشکی Psychiatric Emergencies

فوریت های روان پزشکی پاسخ های رفتاری یا عاطفی، ورای طیف فعالیت خدمات مشاوره بحران بوده و نیازمند مداخله بهداشت روان از طریق منابع جامع تر است. این فوریت ها شامل پاسخ هایی در مقابل خطرهای تهدید کننده ایمنی فرد یا گروه سوء مصرف مواد ، موارد جدی اختلال عملکرد و علائم مهمی است که علیرغم مداخله ، ادامه می یابد.

کاربردهای دفاعی زیست فناوری Defensive application of Bio safty

تشیخص عوامل بیولوژیک خطرناک – تهیه واکسن بر علیه سموم وعوامل بیولوژیک

– تهیه بیوسنسورهای خاص جهت شناسائی عوامل بیولوژیک ومواد شیمیائی – تهیه مواد زیستی – شبکه های عصبی زیستی جهت پردازش اطلاعات – رایانه های زیستی– شبکه های اطلاعاتی پیشرفته بر اساس بیوانفورمتیک ها،سیستم های بیولوژیک و... (منبع ۳٤)

گازگرفتگی

گازهای خفه کننده به دو دسته تقسیم می‌شوند ، یکی گازهای غیرسمی خفه کننده که فقط هوا را رقیق نموده و اختلال در تنفس ایجاد می‌کنند و عبارتند از انیدریدکربنیک، متان، اتان، ازت و غیره و دیگری گازهای سمی خفه کننده که ضمن اختلال در سیستم تنفسی و جریان خون سیستم عضلانی و

اعصاب را نیز مختل می‌نماید و عبارتند از : اکسید کربن، گازهای نیتره، گاز ئیدروژن سولفوره، گاز کلر، آمونیاک و غیره.

منبع پرتو گاما Cesium-137

یک منبع پرتو گامای قوی که می تواند باعث آلوده شدن منطقه وسیعی شود.بطور معمول در اندازه گیری های صنعتی و تشعشع مواد بکار می رود.در نصف عمر دستگاه ۳۰/۲ سال است.

مهندسی ژنتیک Genetic enginnering

شاخه ای از علوم زیستی که امکان دستکاری و تغییر درژن های موجودات زنده و یا انتقال ژن های ویژه بین موجودات زنده را ایجاد کرده و از این طریق موجب تکثیر صفات دلخواه می شود.(منبع ۳٤)

موجودات دستورزی ژنتیکی زنده Genetical modified organism

به هر موجود زنده ای گفته می شود که با استفاده از زیست فناوری مدرن، واجد یک ترکیب جدید از ماده ژنتیکی باشد.(منبع ۳٤)

ویروس Viruses

به طور خلاصه می‌توان گفت که ویروس ها مولکول های بزرگ، پیچیده و استثنایی هستند که به طور اجباری برای عمل تکثیر و اعمال متابولیسمی خود به سلول میزبان نیاز دارند و به همین علت می‌توان آنها را به عنوان انگل یا پارازیت به حساب آورد. از طرف دیگر، ویروس ها ساده‌ترین میکروارگانیسم ها از نظر ساختمان می‌باشند

کتابنامه

۱- موحدی نیا ، جعفر، اصول و مبانی پدافند غیر عامل ،دانشگاه صنعتی مالک اشتر – مجتمع آمایش و پدافند غیـر عامـل ، سال ۱۳۸۶

۲- مجیدی داود ، مبانی استتار و اختفاء و پوشش، دانشگاه صنعتی مالک اشتر - مجتمع آمایش و پدافند غیـر عامـل ، سـال ۱۳۸۶

۳- دکتر جلالی غلام رضا و دکتر هاشمی فشارکی سید جواد ، پدافند غیرعامل در آئینه قـوانین و مقـررات ، سـازمان پدافنـد غیر عامل کشور ، ۱۳۸۹

۴- ابراهیم نژاد محمد ، سلاح های غیر کشنده دانشگاه صنعتی مالک اشتر – مجتمع آمایش و پدافند غیر عامل، سال۱۳۸۶

۵- ابهری مریم ، مدیریت بحران ، دانشگاه صنعتی مالک اشتر – مجتمع آمایش و پدافند غیر عامل، سال۱۳۸۶

۶- دکتر سهامی- حبیب الله، آمایش و مکان یابی، دانشگاه صنعتی مالک اشتر – مجتمع آمایش و پدافند غیر عامـل، سـال ۱۳۸۶

۷- موحدی نیا، جعفر، مفاهیم نظری پدافندغیرعامل، مرکز برنامه ریزی و تالیف کتابهای درسی سپاه ۱۳۸۶

۸- صفا پیمان ، استحکامات و سازه های امن ، دانشگاه صنعتی مالک اشتر – مجتمع آمایش و پدافند غیر عامل سال ۱۳۸۶

۹- محیط شناسی نظامی، دانشگاه صنعتی مالک اشتر – مجتمع آمایش و پدافند غیر عامل سال۱۳۶۸

۱۰- اصول و مبانی عملیات‌روانی ، دکتر حسینی حسین

۱۱- ابراهیمی عباس ، فناوری دفاعی ، مرکز تالیف کتابهای درسی سپاه ۱۳۸۸

۱۲- بی نام ، جنگ الکترونیک ، مرکز تالیف کتابهای درسی سپاه سال ۱۳۸۷

۱۳- جواهری علیرضا ، راهبرد ملی امریکا در حفاظت زیرساخت ها و منابع کلیدی ، مـؤ سسـه آموزشـی و تحقیقـاتی صـنایع دفاعی، سال ۱۳۸۶

۱۴- جمعی از اساتید ، پدافند غیرعامل- بخـش تهدیـدات دامـی و امنیـت زیسـتی ، وزارت جهـاد کشـاورزی- پژوهشـکده مهندسی

۱۵- دکتر حسینی سیّد حسین - شیمی پلیمر نظامی - مرکز برنامه ریزی و تالیف کتابهای درسی سپاه ، ۱۳۸۷

۱۶- جنت مکان شاد- حمید، عملیات روانی امریکا و دولت نهم ، دانشکده علوم و فنون فارابی ، ۱۳۸۸، تهران

۱۷- دانشنامه رشد ، سایت رشد، سازمان آموزش و پرورش ، ۱۳۸۸ ، تهران

۱۸- ستاره علی اکبر ، دکتر زنگنه شهرکی سعید ، حسینی سـید علـی ، آمـایش و مکـان یـابی از منظـر پدافنـد غیرعامـل ،دانشگاه صنعتی مالک اشتر – مجتمع آمایش و پدافند غیر عامل، سال ۱۳۸۹ ، تهران

۱۹- رضایی، سعید، مکان یابی با استفاده از سیستم اطلاعات جغرافیایی، مطالعه مـوردی: اسـکله بنـدرعباس، مجلـه پدافنـد غیرعامل، شماره ۱. سال ۱۳۸۸

۲۰- محمدنژاد، میرعلی و نوروزی محمدتقی ، فرهنگ استراتژی، انتشارات سنا، ۱۳۷۸، تهران

۲۱ - ستاره علی اکبر ، مدل سازی مدیریت ریسک برای تداوم حیات و فعالیتهای سـازمان در برابـر تهدیـدات-پایـان‌نامـه کارشناسی ارشد مهندسی پدافندغیرعامل ، دانشگاه صنعتی مالک اشتر- مجتمع دانشگاهی آمایش و پدافند غیرعامل، ۱۳۸۸

۲۲- دکتر علمداری ، الگوی مدیریت بحـران و دفـاع غیـر نظـامی ناشـی از جنـگ .. ، سـازمان پدافنـد غیـر عامـل کشـور

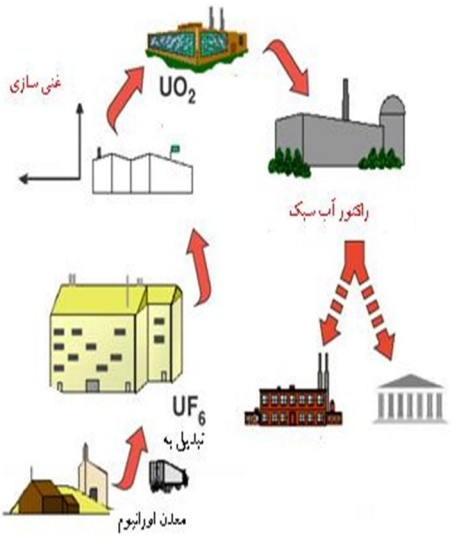
۲۳- ابراهیم نژاد شلمانی محمد ، جنگ سایبر و تروریسم سایبر ، پژوهشکده پدافند غیر عامـل دانشـگاه امـام حسـین (ع)

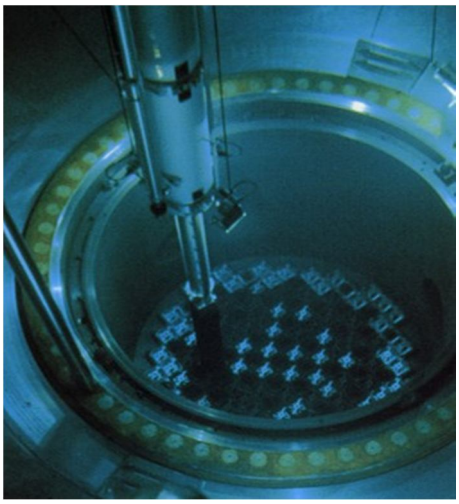
۲۴- بقایی نیا، مریم.. مدیریت دانش.پرتو ملت، نشریه داخلی بانک ملت.سـال دوم، شـماره۱۶. (۱۳۸۶)۲۵- مـک دانلـد،جان،

مدیریت دانش. ترجمه بدری نیک فطرت. تهران: کیفیت و مدیریت،(۱۳۸۱).۲۶- بهرنگی، محمد رضا.، مدیریت آموزشی و آموزشگاهی. انتشارات تابان. (۱۳۸۰)
۲۷ – طاهری عباس ، مهندسی رزمی ، ویژه دوره کارشناسی ، دانشگاه امام حسین (ع) ، ۱۳۸۶
۲۸- دانشپور حسن و همکاران مفاهیم و کاربرد نظامی و امنیتی اطلاعات – مرکز برنامه ریزی و تالیف کتابهای درسی سپاه
۲۹- دکتر رستمی ضرغام ، فرماندهی وکنترل در جنگ الکترونیک ، دانشگاه امام حسین (ع) ، سال ۱۳۸۵
۳۰- دکتر رستمی ضرغام ، امنیت مخابرات ، دانشگاه امام حسین (ع) ، سال ۱۳۸۵
۳۱- دکتر محمدحسین الیاسی و پرویز دباغی ، آسیب شناسی اجتماعی نظامی، مرکز برنامه ریزی و تالیف کتابهای درسی سپاه ، ۱۳۸۸
۳۲- امینی ، جنگ نوین (۲)، مرکز برنامه ریزی و تالیف کتابهای درسی سپاه، ۱۳۸۸
۳۳- چیذری امیر ، شناسایی، مرکز برنامه ریزی و تالیف کتابهای درسی سپاه، سال۱۳۸۶
۳۴- دکتر اسکندر امیدی نیا- دکتر سپیده اشرفی وند ، ایمنی زیستی وجنبه های حقوقی واخلاقی بیوفناوری ،مرکز برنامه ریزی و تالیف کتابهای درسی سپاه
۳۵- محمد رضا هدایتی، سازمان و مأموریت در اطلاعات (۱)، مرکز برنامه ریزی و تالیف کتاب های درسی سپاه ، ۱۳۸۶
۳۶- گرمابدری تقی ، طرح ریزی عملیات پنهان ، مرکز برنامه ریزی و تالیف کتاب های درسی سپاه ، ۱۳۸۶
۳۷- یوسف کریمی، برآورد اطلاعات، مرکز برنامه ریزی و تالیف کتابهای درسی سپاه ، ۱۳۸۶
۳۸ – محبی عباسعلی ، اطلاعات عمومی سیستم های موشکی و توپخانه ، مرکز برنامه ریزی و تالیف کتاب های درسی سپاه
۳۹- علی محمدی کامبیز ، پوشش گیاهی و پدافند غیر عامل، مرکز برنامه ریزی و تالیف کتاب های درسی سپاه ، ۱۳۸۹
۴۰- اسکندری حمید ، دانستنی های پدافند غیر عامل (ویژه مدیران و کارشناسان) ، بوستان حمید، ۱۳۸۹
۴۱- بی نام، پایگاه دانش مخاطرات امنیتی ICT ، مرکز پدافند عیر عامل فاوا ، سال ۱۳۸۹
۴۲- آریان پور منوچهر ، فرهنگ همراه پیشرو آریان پور، جهان رایانه ،۱۳۸۰
۴۳- اسکندری حمید - امیر صوفی رحمت اله ، تهدیدات فضای سایبر و امنیت اطلاعات، بوستان حمید، ۱۳۹۱
۴۴-ابراهیم نژاد محمد ، راهبرد های حفاظت از زیرساخت های حیاتی، بوستان حمید ۱۳۸۹
۴۵- کرمی دکتر علی ،پدافند غیرعامل و تهدیدات بیولوژیک ، بوستان حمید ، ۱۳۹۱ تهران
۴۶- اسکندری حمید ، تهدیدات سخت(آشنایی با انواع حملات و سلاح ها و ..)، بوستان حمید، ۱۳۹۰
۴۷- دکتر رزمخواه محمد رضا ، نقش حساسه ها در جمع آوری اطلاعات ، بوستان حمید ، ۱۳۹۰
۴۸- مزینانی عزت ا.. ، ارزیابی هدر رفت آب و راهبرد های کاهش آن ،بوستان حمید ،۱۳۹۱
۴۹- دکتر جلالی غلام رضا ، نگاهی به تهدیدات نوین و نقش بسیج در حوزه‌ی پدافند غیرعامل ، بوستان حمید ،۱۳۹۱
۵۰- گواهی مهندس تورج ، سازه‌های امن و استحکامات، دانشگاه امام حسین (ع)، ۱۳۹۰
۵۱- جوزبری ادوارد- کوین – دکتر هاشمی فشارکی(مترجم)، حفاظت و ایجاد پناهگاه های ضد بارش هسته ای ، بوستان حمید، ۱۳۹۱

بخش دوم

فرهنگ لغات
انگلیسی به فارسی


غنی سازی
UO_2
راکتور آب سبک
UF_6
تبدیل به
معدن اورانیوم



\

معادل فارسی	اصطلاحات
	A
ریسک قابل قبول	Acceptance risk
باران اسیدی	Acid rain
اقدام پنهان	Action secret
دفاع عامل	Active Defense
فریب الکترونیکی فعال	Active electronic Deception
هدایت هومینگ فعال	Active Homing Guidance
حسگرهای فعال	Active sensors
سازگاری	Adaptation
آگرو تروریسم	Agro terrorism
شناسایی هوایی	Air reconnaissance
تهدید هوایی	Air Threat
کمین سایبری	Ambush cyber
پوشش های ضد بازتاب راداری	Anti-radiate coating of radar
آرامیدها (پلیمر)	Aramid
تور های مصنوعی	Artificial screens
دارایی	Asset
جذب جوّی	Atmospheric absorption
اهداف تهاجمی	Attack goals
بازرسی در سطح شیيء	Auditing
سیستم رمز خودکار	Auto Encryption

معادل فارسی	اصطلاحات
	system **B**
درب پشتی	Backdoor
باکتری	Bacteria
اختلال کننده سدی	Barrage Gamer
طرح پایه آمایش سرزمین	Basis plan of Spatial planning
ارتعاش پایه	Basis tremble
ریسک قابل تحمل	Bearable risk
منابع زیستی	Bio resource
امنیت زیستی	bio security
حسگرهای زیستی	Bio sensors
زیست فناوری	Bio technology
بیو تروریسم	bio terrorism
اقلیم شناسی حمله زیستی	Bio-at Climatology
عوامل زیستی مخاطره آمیز	Biohazard agents
بر چسب هشدار خطر بیولوژیک	Biohazard warning symbol
روش تشخیص عوامل بیولوژیک	Biologic diagnosis method
تقسیم‌بندی عوامل بیولوژیک	Biologic agent groups
آلودگی زدایی بیولوژیک	Biologic decontamination
عوامل زیستی	Biological Agents

معادل فارسی	اصطلاحات
عوامل بیولوژیک	Biological Agents
تهدیدعوامل زیستی	Biological agents treat
حصر بیولوژیکی	Biological Containment
دفاع بیولوژیک	Biological defense
تروریسم بیولوژیکی	Biological Terrorism
جنگ بیولوژیکی	Biological warfare
تسلیحات بیولوژیک	Biological Weapons
سلاح های زیستی	Biological weapons
بیومتریک	Biometric
ایمنی زیستی	Bio safety
چارچوب ملی ایمنی زیستی	Bio safety nation Framework
فن‌آوری زیستی	Biotechnology
تبلیغات سیاه	Black propaganda
آثار انفجار بر ساختمان	Blast effects on building
بارگذاری انفجاری	Blast loading
سامانه های حفاظتی انفجاری	Blast protective systems
همگون سازی	Blending
درخشندگی	Brightness
مقررات ملی ساختمان	Building national regulation
سازه نیمه مدفون و مدفون	Buried semi buried structure

معادل فارسی	اصطلاحات
سامانه فرماندهی و کنترل	**C** C4 I
استتار	Camouflage
عوامل مخرب استتار	Camouflage destroyer Agent
انضباط استتار	Camouflage discipline
رنگ آمیزی استتاری	Camouflage painting
تور استتار	Camouflage screen
روش های استتار	Camouflage method
الیاف کربنی	Carbon fibbers
نانو روکش‌ها	Casing Nano
حادثه فاجعه انگیز	Catastrophic Incident
جمع‌آوری پنهانی	Secret collection
چف	Chaff
تالار چت(گفتگو)	Chat room
چک لیست	Checklist
رفع آلودگی شیمیایی	Chemical decontamination
پناهگاه حفاظت شیمیایی	Chemical protected shelter
حفاظت پزشکی شیمیایی	Chemical medic Protection
تروریسم شیمیایی	Chemical terrorism
جنگ شیمیایی	chemical warfare
سلاح شیمیایی	Chemical weapon

معادل فارسی	اصطلاحات
دفاع غیرنظامی	Civil Defense
حفاظت جمعی(شیمیایی	Collective protection
اطلاعات رزمی	Combat intelligence
سیستم مدیریت صحنه نبرد	Combat management system
رمز ترکیبی	Combined Encryption
جاسوسی مخابراتی	Communication Intelligence
مرکز ارتباطات/ اعزام	Communicate/ Dispatch Center
بازسازی اجتماعی	Community Recovery
ویروس رایانه ای	Computer Virus
کرم رایانه ای	Computer worm
اختلال سیستم های مخابراتی	Communication systems jamming
اختفاء	Concealment
اختفاء با فضای سبز	Concealment. Green with cover
پناهگاه طاق بتنی	Concrete floor shelter
پیامد	Consequence
مدیریت پیامدها	Consequence Management
رزمایش مباحثه‌ای	Controversy Drill
هماهنگ کردن	Coordinate
آنالیز هزینه- سود	Cost-Benefit analysis
ضد اطلاعات	Counter intelligence

معادل فارسی	اصطلاحات
اقدامات متقابل	Countermeasures
آنالیز اقدامات متقابل	Counter measures analysis
اصول ضد شناسایی	Counter reconnaissance Principal
پوشش	Cover
تور های پوششی	Covering screens
عملیات روانی پنهان	Covert Psychological Operation
بحران	Crisis
مدیریت بحران	Crisis management
فرآیند مدیریت بحران	Crisis management process
مراکز حساس	Critical Centers
زیرساخت حیاتی	Critical Infrastructure
تهدیدات اجتماعی و فرهنگی	Cultural & social Threats
حمله سایبری	Cyber Attack
جرم سایبری	Cyber Crime
تروریسم سایبر	Cyber terrorism
جنگ سایبری	Cyber warfare
فریب	**D** Deception
ماکت فریبنده	Deceptive model
رفع آلودگی	Decontamination
اهداف تدافعی	Defense goals

معادل فارسی	اصطلاحات
دفاع	Defense
انحراف از هنجارهای اجتماعی	Deflection due social formation
تور های تغییر شکل یافته	Deformed screen
روش دلفی	Delphi method
اهریمن سازی	Demerging
اتمام بسیج عمومی	Demobilization
انکار خدمات	Denial of Service
نماینده سازمانی	Deputy
کاهش اثرات مخرب	Destroyer effects reduction
آشکار سازی	Detection
بازدارندگی	Deterrence
توسعه	Development
روش ایمونولوژیک تشخیص عوامل	Agent Diagnosis immunologic method
نبرد دیجیتالی	Digital warfare
فاجعه، بلا	Disaster
مرکز بازسازی بلایا	Disaster Recovery Center
پراکندگی	Dispersion
دکترین	doctrine
رزمایش	Drill
گزارش مدیریتی رزمایش	Drill manage Report
E اعلام خبر	Early warning

معادل فارسی	اصطلاحات
اقدامات ضد ضد الکترونیکی	ECCM Electronic Counter-Counter Measures
اقدامات ضد الکترونیکی	Electronic Counter Measures(ECM)
اقدامات ضد پارازیت	ECM
تهدیدات اقتصادی	Economic Threats
جنگ اقتصادی	Economic warfare
منابع تابش الکترو مغناطیس	Electromagnetic Radiate Resources
طیف الکترو مغناطیس	Electromagnet Spectral
تداخل الکترومغناطیسی	Electromagnetic Interference
بمب الکترومغناطیسی	Electro-Magnetic Pulse
فریب الکترونیکی	Electronic Deception
پارازیت رسانی الکترونیکی	Electronic Jamming
جنگ الکترونیک	Electronic warfare
سازگاری الکترومغناطیسی	EM Compatibility
شرایط اضطراری	Emergency
مرکز عملیات شرایط اضطراری	Emergency Operations Center
اطلاعات عمومی شرایط اضطراری	Emergency Public Information
عملکرد پشتیبانی اضطراری	Emergency Support Function

معادل فارسی	اصطلاحات
فیلترهای EMI	EMI filters
سیستم تولید کننده EMP	EMP Generator System
رمزدارکردن	Encryption
رمزگذاری داده ها	Encryption data
کلید خصوصی رمز	Encryption private key
جنگ محیطی	Environment warfare
اپیدمیولوژی	Epidemiology
مراقبت اپیدمیولوژیک	Epidemiologic surveillance
پاکسازی	Eradication
اقدامات پشتیبانی الکترونیک	ESM
نرم افزار اسنیفر	Sniffer software
برآورد اطلاعات استراتژیکی	Strategic Information estimate
عملیات‌روانی استراتژیک	Strategy Psychology. Opera
شناسایی استراتژیک	Strategic Reconnaissance
مدیریت پیامدها	Event management
دانش صریح یا آشکار	Explicit Knowledge
چهره نگاری	**F** Facial-Scan
شناسایی هدایت نهایی	Final guidance reconnaissance.
عوامل بیوتروریسم	Pharmacy

معادل فارسی	اصطلاحات
کشاورزی	Bioterrorism. Agents
رزمایش میدانی	Field Drill
انگشت نگاری	Finger- Scan
دیواره آتش	Firewall
مقابله کنندگان اولیه	First Responder
فریب دهنده فلیر	Flare deceptive
ایمنی غذا	Food safety
امنیت غذایی	Food security
استحکامات	Fortification
	G
شکافت هسته‌ای	gap nuclear
روش تراشه‌های ژنی	Gene chip method
مهندسی ژنتیک	Genetic engineering
موجودات دستورزی ژنتیکی زنده	Genetically modified organism
سامانه اطلاعات جغرافیایی	Geographic Information System
سنجش از دور	GIS
کاربردهای سنجش از دور	GIS Application
تروریسم جهانی	Global Terrorism
سیستم موقعیت یاب جهانی	GPS
سیستم هدایت ناوبری با GPS	GPS Navigational guidance
گرافیت	Graphite

معادل فارسی	اصطلاحات
الیاف گرافیتی	Graphite fibers
تبلیغات خاکستری	Gray propaganda
تجسس زمین فضایی	ground Spatial Search
شناسایی زمینی	ground reconnaissance
سازه های رو زمینی	Ground structural
زمین کردن	Grounding
موشک هدایت شونده	Guidance missile
ژیروسکوپ	Gyroscope
هکر	**H** Hacker
هندسه دست	Hand-Scan
سیستم‌کشف نفوذ	Hank detect system
مخاطره	Hazard
کاهش مخاطرات	Hazard mitigation
انواع مخاطرات	hazards
امداد رسانی	Helping
پالس الکترومغناطیسی هسته ای	HEMP
بدل سازی	Hiding
تور افقی	Horizontal screen
بیماری های انسان و دام	Human &animal maladies
فن آوری اطلاعات و ارتباطات	**I** ICT

معادل فارسی	اصطلاحات
تشخیص و سندیت	Identification & Authentication
فریب مخابراتی جعلی	Imitation Communicate. Deception
فریب تقلیدی	Imitative Deception
دانش ضمنی یا پنهان	Implicit Knowledge
مراکز مهم	Important Centers
عوامل ناتوان‌کننده	Incapacitating agents
حادثه، واقعه	Incident
فرماندهی سانحه	Incident Command
سیستم فرماندهی سانحه	Incident Command System
کاهش اثرات سانحه	Incident Mitigation
سیستم ملی مدیریت حادثه	Incident National Manage. System
آسیب‌شناسی فردی	Individual Pathology
اطلاعات	Information
عملیات اطلاعاتی	information operation
امنیت اطلاعات	Information security
جنگ اطلاعات	Information warfare
زیرساخت	Infrastructure

Infrastructure Coordinate. National Center	مرکز ملی هماهنگی زیرساخت ها
insider EMI	تداخل الکترومغناطیسی داخلی
Insider security	امنیت داخلی
Insider Security Information	اطلاعات امنیتی داخلی
Intelligence	جاسوسی
intelligence satellite	ماهواره جاسوسی
International hosting	برون سپاری بین المللی
invisible fibers	الیاف نامرئی
J jamming	اختلال
Iris –Scan	عنبیه نگاری
K Key Resources	منابع کلیدی(حیاتی)
kind of drill	انواع رزمایش
knowledge	دانش
Knowledge Manage. Performa	منافع مدیریت دانش
Knowledge Management	مدیریت دانش
L Leakage of slot	نشت از روزنه‌ها
Loading Pattern	الگوی بارگذاری
vocational resolution	قدرت تفکیک مکانی

M Malformation Recognition	تشخیص ناهنجاری
Manipulative Deceptive.	فریب جعلی
Mass destruction weapons	سلاح های کشتار جمعی
massaging services	خدمات پیام رسانی
MDW weapons	سلاح های نا متعارف
Media tools	ابزار رسانه ای
media war	جنگ رسانه ای
Mental health	بهداشت روانی
Military Strategy	راهبرد نظامی
Military Deception	فریب نظامی
Military Doctrine	دکترین نظامی
Military information	اطلاعات نظامی
Military Pathology	آسیب‌شناسی نظامی
Missile guidance system	سیستم هدایت
Mitigation	پیشگیری
Mobile shelter	پناهگاه های سیار
Mobilization	بسیج کردن
Mobilization Center	مرکز بسیج منابع
Modern Biotechnology	زیست فناوری مدرن
modern Camouflage Covers	پوشش های استتار مدرن

Modern living organism	ارگانیسم زنده مدرن
Model screens	تور های ماکتی
Multi spectral Camouflage.	استتار چند طیفی
Multiagency Coordinate. Entity	نهاد هماهنگی سازمانها
Multiagency Coordination System	سیستم هماهنگی سازمان ها
Multi Alphabet encrypts	رمزهای چند الفبایی
N Nano	نانو
Nano materials	نانو مواد
Nano powder	نانو پودرها
Narco terrorism	نارکوتروریسم
National Leadership	رهبری ملی
National Security	امنیت ملی
National security implement	مؤلفه‌های امنیت ملی
National Strategy	استراتژی ملی
Nationalist terrorism	تروریسم ناسیونالیستی
Natural Language Process	پردازش زبان طبیعی
Natural screen	تور های طبیعی
naval reconnaissance	شناسایی دریایی
Navigational guidance	هدایت ناوبری

Nuclear reactor fuel	سوخت راکتور هسته‌ای
Near Infra-red sensor	حسگر مادون قرمز نزدیک
Neurotic agents	عوامل عصبی
News processing	پرورش اخبار
NG	نیتروگلیسیرین
Noise Jamming	پارازیت اغتشاشی
Noise screens	تور های پارازیتی
Nongovernmental Organization	سازمان غیردولتی
Nuclear power unit	واحد سنجش قدرت هسته‌ای
Nuclear Bomb	بمب هسته‌ای
Nuclear bomb structure	ساختمان بمب هسته‌ای
Nuclear Incident Respond Team	تیم مقابله با حوادث هسته ای
Nuclear reactor	راکتور اتمی
Nuclear terrorism	تروریسم هسته ای
O one degree safe structural	سازه امن درجه یک
Oblique screens	تور های مایل
Operation Drill	رزمایش کارکردی

operation graphite bomb	عملکرد بمب گرافیتی
Operation of smoking	عملیات دود
Opposition. Of Graphite bomb	مقابله با بمب گرافیتی
Operation Security	امنیت عملیات
Organize	ساماندهی
Organize Crimes	جرائم سازمان یافته
Outsider security	امنیت خارجی
Outsider Security Informant.	اطلاعات امنیتی خارجی
Overhear	استراق سمع
Ozone layer	لایه ازن
P Passive Deception	**فریب** الکترونیکی غیر فعال
Passive defense great goals	اهداف کلان پدافند غیرعامل
passive Defense in Russian	پدافند غیرعامل در روسیه
Passive defense principle	اصول پدافند غیرعامل
Passive Defense	دفاع غیرعامل ، پدافند غیرعامل
Passive Homing guidance	هدایت هومینگ غیرفعال
Passives sensor	حسگر غیر فعال

Pathology	آسیب‌شناسی
Pattern	طرح کلی اشیاء
people Evacuation	تخلیه مردم
Personnel protection of chemical agent.	محافظت فردی از عوامل شیمیایی
Personal Firewall	دیواره آتش شخصی
Physical security	امنیت فیزیکی
Planning	برنامه‌ریزی
Planning	طرح‌ریزی
plant Index	گیاهان شاخص
Politic cryptic operation	عملیات پنهان سیاسی
Politic Threats	تهدیدات سیاسی
Pollutant	آلاینده
Post-Traumatic Stress	فشار روانی پس از تروما
Pre- crisis preparedness	آمادگی قبل از بحران
Preparedness	آمادگی
Prioritization of Risk evaluate	اولویت بندی ارزیابی ریسک
Process Hazard Analysis	آنالیز خطرفرآیند
Process of spatial plan	مراحل تهیه طرح آمایش
Propagation	تبلیغات
Propagation of cover	انتشار از روی پوشش

protective Security layers	لایه های امنیتی حفاظت
Protecting of Data Integrity	محافظت از جامعیت داده
Protection of Critical Infrastructure	حفاظت از زیرساخت‌های حیاتی
protection mask	ماسک حافظت
Protection of EMP	حفاظت در برابر EMP
Protection sanctum	حریم حفاظتی
Protective structural	سازه حفاظت کننده
Psychiatric Emergencies	فوریت های روانپزشکی
Psychological Operation	عملیات روانی
Psychological action	اقدام روانی
Psychological operation	عملیات روانی
Psychological Warfare	جنگ روانی
public diplomacy	دیپلماسی عمومی
Public key encryption	رمزنگاری کلید عمومی
Public key system	سیستم کلید عمومی
purring with Centrifuge	غنی سازی با سانتریفیوژ
R Radar Absorbent Materials	مواد جاذب رادار
radar absorbing paint	رنگ جاذب راداری
Radar Camouflage technique	روش های استتار راداری

Radar Camouflage	استتار راداری
Radar Cross Section(RCS)	سطح مقطع راداری
Radar detecting reduction	کاهش امکان شناسایی رادار
Radar frequency bands	باندهای فرکانسی راداری
Radar sensors	حسگرهای راداری
radiometric resolution power	قدرت تفکیک رادیومتریک
Ready-mixed concrete shelter	پناهگاه بتنی پیش ساخته
Receiver system	سامانه گیرنده
Reconnaissance systems	سیستم های شناسایی
Reconnaissance launchers	سکوهای شناسایی
Reconnaissance Agents	عوامل شناسایی
Reconnaissance	شناسایی
reconnaissance on map	شناسایی روی نقشه
Reconstruction	بازسازی
Recovery	بازیابی (پس از بحران)
Recovery	بهبودی
Reduce RCS	کاهش سطح مقطع راداری
Residual Risk	ریسک باقیمانده
Retina-Scan	شبکیه نگاری

Retreat	عزلت گزینی
Risk	ریسک
Risk Acceptance	پذیرش ریسک
Risk Analysis	تجزیه و تحلیل ریسک
Risk Control	کنترل ریسک
Risk Elimination	حذف ریسک
Risk Estimation	برآورد ریسک
Risk Estimation	تخمین ریسک
Risk Evaluation	ارزیابی ریسک
Risk Identification	شناسایی ریسک
Risk management Framework	چارچوب مدیریت ریسک
Risk management	مدیریت ریسک
Risk Profile	نمایه ریسک
Risk Reduction	کاهش ریسک
Risk Transfer	انتقال ریسک
Root kit	روت کیت
S	
Safety sanctum	حریم ایمنی
SBEMP	انفجار هسته ای در سطح زمین
Security sanctum	حریم امنیتی
Security Countermeasure	اقدامات ضد امنیتی

Security policy	سیاست امنیتی
security socket layer	لایه سوکت امن
Segregation of subsystem	جداسازی زیر سامانه‌ها
Semi-auto Encryption system	سیستم رمز نیمه خودکار
Scenario	سناریو
Sensor	حسگر
sensor power indexes	شاخص های توانمندی حسگر
ceramic Covers	پوشش های سرامیکی
Shelter	پناهگاه
Shelter of Faraday	قفس فارادی
Shooting	رها سازی
Shun Chemical contamination	اجتناب از آلودگی شیمیایی
Signal Intelligence	جاسوسی سیگنالی
Site selection	مکان یابی
Site selection execution	اجرای مکان یابی
Site selection indexes	شاخص های مکان یابی
Smart mine	مین‌های هوشمند
Smart polymers	پلیمرهای هوشمند
smart Nano sensor	نانو حسگر های هوشمند

Smoke	دود
Smoke Camouflage	استتار دود
Smoke effects	اثرات دود
Smoke screen	پرده دود
Smoke screening	دودهای دیواره ای
Smoking metal	مواد دود زا
Social engineering attack	حمله مهندسی اجتماعی
Social Pathology	آسیب‌شناسی اجتماعی
Soft power	قدرت نرم
Soft warfare	جنگ نرم
Social engineering	مهندسی اجتماعی
spacing reconnaissance	شناسایی فضایی
Spam	هرزنامه(اسپم)
Spatial organization	سازمان فضایی
Spatial planning	برنامه‌ریزی فضایی
Spatial planning	آمایش سرزمین
Spatial planning Component	اجزاء آمایش سرزمین
Spectral resolution	قدرت تفکیک طیفی
Spot jammer	اختلال کننده نقطه‌ای
Spyware	جاسوس افزار
Status room	اتاق وضعیت
Stealth	خفیه کاری

Steganography	پنهان نگاری
Strategic Information	اطلاعات استراتژیک
Strategic of Warden	استراتژی پنج حلقه واردن
Strategy	راهبرد
Stress	فشار روانی
Structure loading	بارگذاری سازه
Susceptibility	حساسیت پذیری
Suspension screens	تور های تعلیقی
Sweep jammer	اختلال کننده جاروبی
Sweep Lock- on jammer	اختلال کننده جاروبی نقطه ای
System Privileges	مجوزهای سیستم
T Tactical Psychology. Operation	عملیات‌روانی تاکتیکی
tactical reconnaissance	شناسایی تاکتیکی
tally	بر چسب زدن
Target detection	شناسایی هدف یابی
Task of spatial planning	وظایف آمایش سرزمین
Thermal insulations	عایق های حرارتی
Thermal Camouflage	استتار حرارتی
Thermal camouflage paint	رنگ استتار حرارتی

Thermal Infra-red sensor	حسگر مادون قرمز حرارتی
Terri development planning	برنامه‌ریزی توسعه منطقه‌ای
Terrorism	تروریسم
Texture	بافت
Threat	تهدید
Three degree safe structure	سازه امن درجه سه
Thwarting	عقیم گذاری
timing resolution	قدرت تفکیک زمانی
Toxins	توکسین ها
Toxic metals	فلزات سمی
Topology in GIS	توپولوژی در GIS
Track	ردپا
Tran territorial Threats	تهدیدات فرامنطقه‌ای
Trap Door	درب مخفی
Treats Identification	شناسایی تهدیدات
triangle deceiver	فریب دهنده های سه کنج
Trojan Horse	اسب تروجان
Two degree safe structure	سازه امن درجه دو

U UAV	هواپیمای بدون سر نشین
Ultraviolet sensor	حسگر ماوراء بنفش
Underground shelter	پناهگاه های زیرزمینی
under water Sonics	شنودهای زیرآبی
underground structure	سازه زیر زمینی
Uranium pure	غنی سازی اورانیوم
Uranium	اورانیوم
User Privilege	مجوز کاربری
V Vegetation &Camouflage	فضای سبز و استتار
Vegetation Design	طراحی پوشش گیاهی
Vegetation maintenance	نگهداری پوشش گیاهی
Vertical screens	تور های عمودی
Viewing Principle	اصول منظره سازی
Vigenere Code	رمز ویژنر
Viruses	ویروس
Visible sensors	حسگرهای مریی
Vital Centers	مراکز حیاتی
Vocation terrorism	تروریست حرفه‌ای
Vulnerability	آسیب پذیری

W Water Biological Threats	تهدیدات بیولوژیکی آب
Water physical Threats	تهدیدات فیزیکی آب
Water cyber Threats	تهدیدات سایبری آب
Water Threats	تهدیدات آب آشامیدنی
Watermark Pattern	الگوگذاری دیجیتال سند
Wired Tapping	شنود قانونی
Wisdom	خِرد
with hat Hacker	هکر کلاه سفید
Without Director Equipment.	تجهیزات بدون سرنشین دریایی