HSE News

خبر نامه علمی- آموزشی ایمنی ، بهداشت کار و محیط زیست

شرکت مدیریت تولید برق بعثت

ویژه نامه هفته پدافند غیر عامل

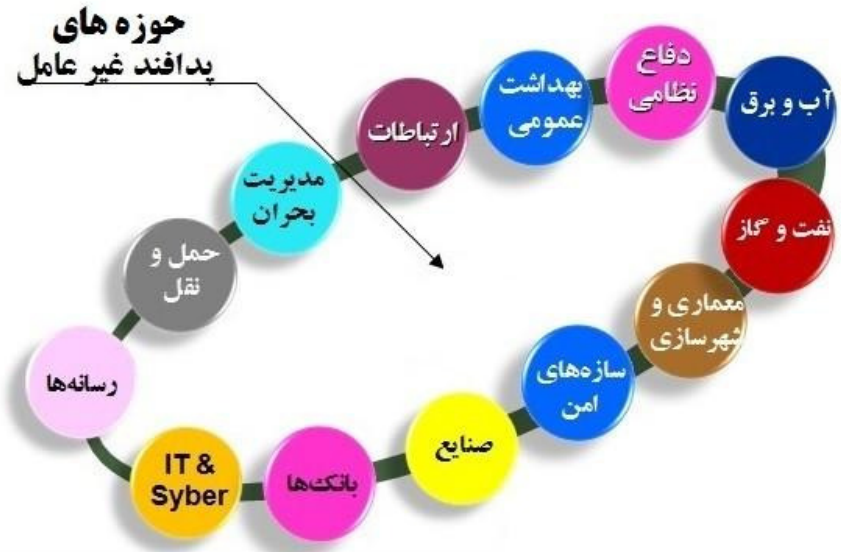
شماره هجدهم – آبان ماه ۱۳۹۷ – تهیه و تنظیم : امور ایمنی ، بهداشت کار و محیط زیست (HSE)

پدافند غیر عامل چیست ؟

پدافند (دفاع) به معنی حفظ جان مردم، تضمین امنیت افراد، صیانت از تمامیت ارضی و حاکمیت ملی در همه‌ی مواقع در برابر هرگونه شرایط، موقعیت و هرگونه تجاوز است. از نظر واژه شناسی، واژه‌ی پدافند از دو جزء "پد" و "آفند" تشکیل شده است.در فرهنگ و ادب پارسی "پاد" یا "پد" پیشوندی است که به معانی "ضد، متضاد، پی و دنبال" است و هرگاه قبل از واژه قرار گیرد، معنای آن را معکوس می‌کند. واژه ی "آفند" نیز به معنای "جنگ، جدال، پیکار و دشمنی" است.(دهخدا،۱۳۷۳).

پدافند به دو شاخه پدافند عامل و پدافند غیرعامل تقسیم می شود، پدافند عامل ، دفاع در مقابل دشمن با به کارگیری سلاح ها، تجهیزات جنگی و تکنیک های رزمی به منظور از کار انداختن ماشین های جنگی دشمن و نابودی آن می باشد. به عبارت دیگر پدافند عامل عبارت است از بکارگیری مستقیم جنگ افزار، به منظور خنثی کردن و یا کاهش اثرات حملات خصمانه ی هوایی، زمینی، دریایی، عملیات نفوذ و خرابکارانه و اقدامات تروریستی دشمن بر روی اهداف مورد نظر.

پدافند غیر عامل به مجموعه اقدامات غیر مسلحانه ای که موجب افزایش بازدارندگی، کاهش آسیب پذیری، تداوم فعالیت های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدها و اقدامات نظامی دشمن می شود. تمهیداتی که در زمان صلح صورت می گیرد و به دنبال محیطی آرام و قابل سکونت در شهرها با آسایش مطلوب می باشد . عمده ترین هدف پدافند غیر عامل، ایمن سازی و کاهش آسیب پذیری زیرساخت های مورد نیاز مردم است که باید با یک برنامه ریزی و طراحی در توسعه پایدار کشور نهادینه شود و برای اصلاح زیرساخت های فعلی راهکارهایی با مهندسی مجدد لازم است.



پدافند غیرعامل که در منابع لاتین ، معادل دقیق آن Passive Defense است ، مجموعه اقداماتی است که مستلزم به کارگیری جنگ افزار و تسلیحات نبوده و با اجرای آن می‌توان از وارد شدن خسارات مالی به تجهیزات و تأسیسات حیاتی، حساس و مهم نظامی، غیرنظامی و تلفات انسانی جلوگیری نموده و یا میزان خسارات و تلفات ناشی از حملات و بمباران های هوایی موشکی دشمن را به حداقل ممکن کاهش داد. به عبارت دیگر پدافند غیرعامل عبارت است از به کارگیری هرگونه ابزار ، شرایط و موقعیت‌ها به طوری که بدون نیاز به عامل انسانی از طریق مقاوم سازی ، ایمن سازی ، استتار ، اختفا و فریب دشمن با حملات نظامی ، تروریستی ، نفوذ و خرابکاری صنعتی و حملات سایبری دشمن مقابله می کند.

در آیین نامه ی اجرایی بند ۱۱ تبصره ۱۲۱ قانون برنامه چهارم توسعه، پدافند غیرعامل اینچنین تعریف شده است: مجموعه اقدامات غیر مسلحانه ای که موجب کاهش آسیب پذیری نیروی انسانی، ساختمان ها، تأسیسات، تجهیزات و شریان های کشور در مقابل عملیات خصمانه و مخرب دشمن و مخاطرات ناشی از سوانح طبیعی می‌گردد. همانطور که از این تعریف بر می آید، پدافند غیرعامل با تأکید بر دفاع پیشگیرانه و محافظت از غیرنظامیان تعبیر شده است که در آن از یک سو محافظت از غیر نظامیان در شرایط جنگ، شورش های داخلی، تحریم و ... (باعامل انسانی) معرفی شده است و از سوی دیگر در معنایی عام و گسترده تر بر محافظت از شهروندان در برابر آثار بلایا طبیعی دلالت دارد که موجب کاهش آسیب پذیری نیروی انسانی، ساختمان ها، تاسیسات، تجهیزات، اسناد و شهرهای کشور در مقابل بحران های خشکسالی، سیل، زلزله، رانش، لغزش، طوفان و ... (با عامل طبیعی) می گردد.

جنگ سایبری ....

برخی حوزه‌ی مجازی را پنجمین حوزه از نبرد می‌دانند. تحلیل‌گران نظامی، حوزه‌ی مجازی را به عنوان یک دامنه‌ی جدید در حوزه‌ی جنگ به رسمیت شناخته‌اند که اهمیت آن در حال حاضر در حال فزونی گرفتن از سایر حوزه‌هاست. وجود نداشتن قوانین بین‌المللی باعث شده که هر کشوری به خود اجازه دهد تا برضد کشور دیگر وارد جنگ مجازی شود . امروزه تهدیدها در قالب شبکه‌های رایانه‌ای و مخابراتی رو به افزایش است. بخش‌های کلیدی اقتصاد تمامی کشورها در حال حاضر، از جمله امکانات دولتی و خصوصی، بانک‌داری و امور مالی، حمل و نقل، تولید، پزشکی، آموزش و پرورش و دولت، همگی برای انجام عملیات روزانه وابسته به رایانه هستند. جنگ مجازی اشاره به درگیری‌ها در فضای مجازی با اهداف سیاسی و ایدئولوژیک دارد. این مفهوم به جنگ اطلاعاتی اشاره دارد، درست به

HSE News
خبر نامه علمی- آموزشی ایمنی ، بهداشت کار و محیط زیست
شرکت مدیریت تولید برق بعثت
ویژه نامه هفته پدافند غیر عامل
شماره هجدهم – آبان ماه ۱۳۹۷ – تهیه و تنظیم : امور ایمنی ، بهداشت کار و محیط زیست (HSE)

مانند جنگی واقعی است که البته در مورد انگیزه‌های این جنگ و جنگ واقعی اختلاف نظر وجود دارد. تعریف دقیق جنگ مجازی به "اقدام‌های انجام شده توسط دولت یک کشور و سایر افراد به منظور نفوذ در رایانه‌ها و شبکه‌های سایر کشورها جهت اقدام‌های تخریب و آسیب اشاره دارد که این روش از راه روش‌های الکترونیکی صورت می‌گیرد "

هدف از حمله‌ی سایبری، دست‌یابی به اطلاعات سایر کشورها، ایجاد وقفه در تجارت و یا ایجاد خدشه در زیر ساخت‌ها مانند شبکه های آب، برق، سوخت ، حمل و نقل ، ارتباطات و ... است به نحوی که هزینه‌های اقتصادی را افزایش دهند. نقطه‌ی شروع برای جنگ مجازی را جنگ «بالکان» می‌دانند که نیروهای متخاصم سعی در نفوذ به اطلاعات یکدیگر داشته‌اند. امروزه رشد شبکه‌های رایانه‌ای بسیار سریع‌تر از رشد نرم‌افزارهای امنیتی مرتبط به آن‌هاست.

انواع تهدید های مختلف ناشی از جنگ سایبر :

۱- جاسوسی و نقض امنیت ملی: جاسوسی سایبر به عملی اشاره دارد که به منظور به دست آوردن اسرار (حساس، اختصاصی و یا اطلاعات طبقه‌بندی شده) از افراد، رقبا، گروه‌ها و دولت‌ها برای استفاده‌ی نظامی، سیاسی یا اقتصادی با استفاده از روش‌های بهره‌برداری غیر قانونی در اینترنت، شبکه، نرم‌افزار و یا رایانه صورت می گیرد.

۲- خراب‌کاری : فعالیت‌های نظامی که با استفاده از ماهواره و رایانه برای اختلال در تجهیزات دشمن صورت می‌پذیرد، خراب‌کاری نام دارد. زیرساخت‌های آب، برق ، سوخت، ارتباطات و حمل‌ونقل ممکن است در جنگ مجازی در معرض خطر باشند. سایر تهدیدها می‌تواند شامل سرقت اطلاعات کارت‌های اعتباری، اختلال در برنامه‌ی قطارها و یا حتی بازار سهام باشد.

انگیزه‌های جنگ سایبر :

۱- مقاصد نظامی : درست مانند جنگ واقعی است اما این جنگ در سایه‌ی فضای مجازی صورت می‌پذیرد. در اینجا به یک مرکز فرماندهی جنگ سایبر نیاز است و نیازمند سلاح‌های مجازی و دفاعی هستیم تا جلوی حمله بگیریم و ما نیز قادر به حمله‌ی متقابل باشیم.

۲- اهداف غیر نظامی : این امر عبارت از اختلال در سرویس دهنده‌ی وب، سیستم‌های اطلاعات سازمانی، سیستم‌های سرور، لینک‌های ارتباطی، تجهیزات شبکه و رایانه‌های رومیزی و لپ‌تاپ‌های خانگی و امور تجاری است که گاهاً برای کسب انگیزه‌های تجاری رقابتی و یا مالی صورت می‌پذیرد و گاهی نیز خراب‌کاری به دلیل صرفاً سرگرمی است.

۳- اهداف شخصی : باید باور کرد که بیش از ۹۰درصد حملات سایبر برای اهداف شخصی صورت می‌گیرد. بسیاری از حملات برای جلب توجه رسانه‌ها انجام می‌شود. شرکت McAfee می‌گوید، روزانه با میلیون‌ها جنبه از این نوع حملات سایبر توسط نرم‌افزارهای امنیتی‌اش روبه‌رو می‌شود.

جنگ در فضای مجازی تا حد زیادی به ضعف سیستم دفاعی مورد حمله قرار گرفته بستگی دارد. این جنگ ابهام‌هایی همچنین در مورد شخص حمله کننده دارد که به واقع چه کسی حمله را آغاز می‌کند. مشکل بزرگ این است که شبکه‌ها به هم متصل هستند. اگر یک رایانه‌ی خانگی در یک کشور سیستم دفاعی ضعیفی داشته باشد، ممکن است از راه این رایانه بتوان به سایر رایانه‌های آن کشور هم دسترسی پیدا کرد. امروزه میزان استفاده از رایانه‌های شخصی با سرعت زیادی در حال پیشرفت است. در جنگ واقعی همه چیز قابل پیش‌بینی است. میزان خسارتی که یک بمب می‌تواند وارد کند و خسارت‌های احتمالی مالی و جانی، اما در جنگ مجازی هیچ خسارتی قابل پیش‌بینی نیست.

شاید اولین سازمان بین‌المللی سازمان همکاری‌های شانگ‌های باشد که جنگ مجازی را به عنوان عامل مخرب برای اخلاق، معنویت و فرهنگ از سوی مهاجمان تعریف کرده است. در سپتامبر ۲۰۱۱میلادی کشورهای عضو پیشنهاد تدوین شاخص‌های بین‌المللی برای یک سند جامع امنیت اطلاعاتی را به دبیر کل سازمان ملل ارائه دادند. این طرح از سوی کشورهای غربی

HSE News
خبر نامه علمی- آموزشی ایمنی ، بهداشت کار و محیط زیست
شرکت مدیریت تولید برق بعثت
ویژه نامه هفته پدافند غیر عامل
شماره هجدهم – آبان ماه ۱۳۹۷ – تهیه و تنظیم : امور ایمنی ، بهداشت کار و محیط زیست (HSE)

حمایت نگردید. رویکرد کشورهای غربی بیشتر بر جنبه‌های اقتصادی متمرکز بود.

پدافند زیستی ....

پدافند زیستی عبارت است از : مجموعه ای از اقدامات شامل رصد و پایش، آشکارسازی، هشداردهی، تشخیص، تصمیم و عملیات، کنترل، حفاظت و پیشگیری، امداد و نجات، درمان، بازیابی و باز توانی منابع، محدود سازی و رفع آلودگی در برابر تهدیدات زیستی که موجب حفاظت از سرمایه های ملی در برابر تهدیدات زیستی و کاهش آثار و عواقب ناشی از آنها می گردد.
تهدید زیستی ، هر نشانه یا رویداد یا اتفاق زیستی است که به صورت طبیعی و غیر طبیعی منجر به تضعیف و نابودی سرمایه های انسانی یا اقتصادی کشور از طریق تخریب و نابودی محصولات کشاورزی (گیاهان، دام و حیوانات) محیط زیست و منابع طبیعی بگردد و ثبات و امنیت جامعه را به خطر می اندازد. بر خلاف حملات شیمیایی و انفجاری، تشخیص یک حمله بیولوژیک به دلیل فقدان بو و رنگ و مشخصه های فیزیکی دیگر، بسیار سخت است و در صورت عدم آشنایی و احتمال تهدید زیستی، ممکن است تا چند روز و حتی هفته به طول انجامد و فاجعه ای رخ دهد و اکثرا پس از بروز علائم بیماری، احتمال وقوع حمله زیستی حدس زده می شود و این بسیار دیر است.

علایم زیر می تواند در شناخت وقوع حمله زیستی 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.
- افزایش ناگهانی میزان حشرات و ناقلین.
- ابتلا به طور غیر مستقیم به بیماری هایی که اغلب در حالت طبیعی از طریق ناقل منتقل می شوند.
- همه گیری های متعدد و هم زمان از بیماری های عفونی مختف.
- مشاهده همه گیری بیماری های گوارشی پس از مصرف آب و غذا از یک منشاء مشترک .

تفاوت‌های تهدیدات زیستی نسبت به شیمیایی و هسته‌ای

۱- تسلیحات بیولوژیک نسبتاً آسان ساخته می‌شوند. توانایی تولید عوامل بیولوژیک در مقیاس آزمایشگاهی برای مقاصد تروریستی کفایت می‌کند و برای مقاصد نظامی، تولید مقیاس بزرگ لازم است که به راحتی از امکانات و تجهیزات دارای کاربرد دو جانبه بدست می‌آید. اکثر کشورهای صنعتی، تجهیزات و موادی برای تولید، تخلیص، کنترل کیفیت و پایداری عوامل بیولوژیک و پخش و انتشار آن را دارند. دستیابی به عوامل بیولوژیک جنگی نیز نسبتاً آسان است .

۲- کشف و سنجش عوامل بیولوژیک به آسانی مقدور نیست. برای شناسایی دقیق عامل بیولوژیک به تجهیزات و امکانات پیشرفته نیاز است و شناسایی دقیق عامل، مدتی طول می‌کشد در حالیکه کشف و سنجش در تسلیحات شیمیایی و هسته‌ای به راحتی با وسایل و دستگاه های آشکار ساز قابل دسترسی و به سرعت انجام می‌شود.

۳- عوامل بیولوژیک به سرعت وسعت و گسترش می یابند و کنترل یا پیشگیری از گسترش دامنه بیماری بسیار مشکل است. معمولا برای انتشار عوامل بیولوژیک از بستر هوا استفاده می‌کنند. بعضی از عوامل بیولوژیک قابلیت انتقال از فردی به فرد دیگر را دارند. بعضی از عوامل نیز دارای ناقل یا میزبان ذخیره هستند در نتیجه برخی از عوامل بیولوژیک می‌توانند به وسیله مسافران یا مهاجران، پرنده‌ها و حیوانات مهاجر، حشرات یا حیوانات ناقل و ذخیره از منطقه‌ای به منطقه دیگر حمل شوند و موجب گسترش بیماری شوند. این نوع پخش و گسترش در تسلیحات شیمیایی و هسته‌ای وجود ندارد.

۴- مداومت اثر عوامل بیولوژیک در منطقه زیاد است. بیشتر عوامل شیمیایی مدت زیادی در منطقه پخش شده باقی نمی‌مانند اما عوامل بیولوژیک که موجودات زنده و فعالی هستند می‌توانند در محیط زندگی کنند و یا باعث ایجاد بیماری شوند و در چرخه انتقال بیماری قرار بگیرند.

۵- مزیت دیگر تسلیحات بیولوژیک این است که بسیار ارزان تهیه می‌شوند و از نظر اقتصادی هزینه زیادی را صرف نمی‌کنند. در مورد تسلیحات شیمیایی و بویژه هسته‌ای نیاز به وجود تاسیسات و اقدامات زیر بنایی است.

۶- عوامل بیولوژیک هیچگونه آسیبی به تجهیزات، مراکز صنعتی، کارخانه ها و سایر تاسیسات نداشته و دارای این مزیت است که مهاجم

HSE News
خبر نامه علمی- آموزشی ایمنی ، بهداشت کار و محیط زیست
شرکت مدیریت تولید برق بعثت
ویژه نامه هفته پدافند غیر عامل
شماره هجدهم – آبان ماه ۱۳۹۷ – تهیه و تنظیم : امور ایمنی ، بهداشت کار و محیط زیست (HSE)

بعدها قادر به استفاده از این مراکز خواهد بود. به عبارت دیگر تسلیحات بیولوژیک و تا حدی سلاح های شیمیایی خسارت چندانی به موارد غیر زنده وارد نمی‌کنند. تسلیحات اتمی دارای قدرت تخریب و سرعت عمل بالایی هستند و در عرض چند ثانیه تا کیلومترها را تخریب می‌کنند و تا مدت ها غیر قابل استفاده خواهد بود.

بیوتروریسم چیست؟

بر اساس تعریف پلیس بین الملل درسال ۲۰۰۷ بیوتروریسم عبارت است از منتشر کردن عوامل بیولوژیکی یا سمی با هدف کشتن یا آسیب رساندن به انسان‌ها، حیوانات و گیاهان با قصد و نیت قبلی و به منظور وحشت‌آفرینی، تهدید و وادار ساختن یک دولت یا گروهی از مردم به انجام عملی یا برآورده کردن خواسته‌ای سیاسی یا اجتماعی .

سلاح‌های میکروبی، چه در عرصه جنگی و چه در عرصه تروریستی، وسیله‌ای بسیار مطلوب برای دشمنان شده است. توان تولید بالا، نگهداری راحت، قابلیت انتشار، قابلیت مصون‌سازی نیروی خودی، قابلیت تکثیر برای عوامل میکروبی زنده، دشواری بسیار در ردیابی فرد یا افراد متخاصم، گستردگی عمل‌کرد از انسان تا دام و محصولات کشاورزی و بسیار محسنات دیگر، موجب شده تشکل‌های تروریستی به این فن‌آوری جدید بشدت کشش یابند بدون آن‌که بتوان گناهی را متوجه آن‌ها نمود.

سلاح‌های میکروبی به خصوص در عرصه تروریسم دولتی و علیه ساختارهای صنعتی کشاورزی در سالیان اخیر بسیار به کار رفته است. اگرچه کشور هدف هرگز نتوانسته ادعا خود را علیه دشمنش به اثبات برساند. اروپا شیوع جنون گاوی را متوجه سازمان‌های جاسوسی امریکا و استرالیا می‌داند که با هدف ضربه اقتصادی به صادرات گوشت اروپا انجام شده. چین در شیوع سارس امریکا را مقصر می‌داند که باعث شد چین در آستانه شکوفایی اقتصادی، سال‌ها از گردونه رقابت تولید ارزان قیمت به واسطه تعطیلی کارخانه‌هایش عقب بیفتد. کره شمالی شیوع وبا در پیونگ یانگ را در اواخر دهه ۸۰ نتیجه فعالیت جاسوس‌های امریکایی می‌داند که با هدف مجبور کردن این کشور به پذیرش شرایط دول اروپایی امریکایی، برای قطع آزمایشات هسته‌یی انجام شده است .

وظایف پدافند زیستی

- سیاست‌گذاری، برنامه‌ریزی، راهبری، نظارت، فرماندهی و مدیریت یکپارچه دستگاه های اجرایی کشور و نیروهای مسلح در برابر تهدیدات زیستی .
- استفاده از توانمندی های موجود و ارتقاء ظرفیت و توانمندی های تخصصی در محورهای پایش، آشکارسازی، هشدار، تشخیص، کنترل، حفاظت، پیشگیری، درمان، بازیابی منابع، محدودسازی و رفع آلودگی های زیستی و نیز صیانت از منافع ملی، ارتقاء آگاهی و آرامش بخشی روانی به جامعه در مواجهه با تهدیدات زیستی .
- افزایش توانمندی اجرای عملیات و مدیریت صحنه بحران های زیستی در حوزه های مرتبط .
- آموزش مدیران اصلی، میانی، رده های تخصصی و نیروهای بخش های مختلف نظام سلامت یک کشور جهت آشنایی با اصول پدافند غیرعامل، تهدیدشناسی، شناخت آسیب پذیری و روش های ایمنی فردی و جمعی، نقش مهمی در فرهنگ سازی ملی و اجرایی شدن برنامه های ارتقای ایمنی و پایداری ملی دارد. این آموزش باید مستمر و همراه با اجرای مانورهای دوره ای در سطوح مختلف باشد. توسعه این آموزش به دانشجویان و دانش آموختگان رشته های مختلف پزشکی و پیراپزشکی می تواند در تربیت نسل آینده مدیران و کارکنان نظام سلامت، نقش مهمی ایفا نماید. در این برنامه، با تربیت متخصصین فوریت های پزشکی آشنا به موضوعات پدافند غیرعامل در بحران های طبیعی می توان آن ها را آماده خدمت رسانی در این شرایط نمود. در پایان مجددا تاکید می شود که تنها راه مقابله با تهدیداتی از قبیل تهدیدات زیستی، اهمیت دادن به اصل آموزش و فرهنگ سازی در حوزه پدافند غیرعامل و سپس انجام اقدامات اجرایی مناسب در این حوزه می باشد.