استانداری خراسان شمالی
اداره کل پدافند غیرعامل

بسمه تعالی

پدافند غیرعامل، کم هزینه ترین و صلح آمیزترین روش دفاع است.

در دنیای امروز اقدام نظامی مستقیم و استفاده از سلاح ها و جنگ افزارهای نظامی همچون توپ و تانک، هواپیماهای جنگنده، ناوهای جنگی و مواردی از این دست، بر علیه کشوری خاص بسیار پر هزینه و در مواردی غیر ممکن است. از این رو، دشمنان به فکر یافتن راه های نوین کم هزینه و سریعی برای ضربه زدن به کشور یا مجموعه ای افتادند. این مسیرهای جدید بیشتر در حوزه های علمی با تکنولوژی بالا همچون حوزه های سایبری و بیولوژیکی ایجاد شده که با هزینه بسیار اندک، خسارت مالی و حتی در مواردی تلافات انسانی بسیار بالایی ایجاد می کند. به عنوان نمونه در حوزه بیولوژیکی می توان به انتشار یک ویروس کشنده همچون ابولا در یک منطقه اشاره نمود. در این صورت دشمن بدون استفاده از تسلیحات نظامی و کشته شدن نیروهای خودی، تلافات سنگینی به هدف خود وارد می نماید.

برای مقابله با این گونه تهدیدات نوین، نیازمند به دفاعی از جنس همین تهدیدات می باشیم. در همین راستا دو حوزه بسیار مهم و حیاتی در پدافند غیرعامل با عناوین پدافند سایبری و پدافند زیستی ایجاد شده اند که وظیفه هر یک جست و جو و پایش تهدیدات در حوزه تخصصی خود می باشد. در ادامه به بررسی هر یک از این دو حوزه پرداخته خواهد شد.

پدافند سایبری

در کشور ما وظیفه بررسی تهدیدات حوزه سایبری بر عهده ی مجموعه ای از سازمان پدافند غیرعامل کشور با عنوان قرارگاه پدافند سایبری کشور به آدرس الکترونیکی www.papsa.ir می باشد.

تعریف پدافند سایبری:

پدافند سایبری به مجموعه فعالیت هایی که در فضای مجازی به منظور شناسایی و مقابله با حمالات سایبری دشمن صورت می گیرد اطلاق می شود. دشمن با انجام این حملات که بیشتر توسط بدافزارها و ویروس های رایانه ای انجام می پذیرد، قصد ضربه زدن به تاسیسات و زیرساخت های حیاتی و مهم یک کشور (مثل نیروگاه های تولید برق، خطوط حمل و نقل ریلی و هوایی، شبکه های مخابراتی و ...) را دارد تا به این وسیله باعث بروز مشکل در فعالیت های ضروری آن کشور شود. به عنوان نمونه می توان به بدافزار استاکس نت اشاره نمود که تاسیسات هسته ای کشور ما را مورد هدف قرار داد.

جنگ سایبری:

فضای مجازی فضایی است که قوانین خاص خود را دارد. امروزه تهدیدها در حوزه شبکه‌های رایانه‌ای و مخابراتی رو به افزایش است. بخش‌های کلیدی اقتصاد تمامی کشورها، از جمله امکانات دولتی و خصوصی، بانک‌داری و امور مالی، حمل‌ونقل، تولید، پزشکی، آموزش و پرورش، همگی برای انجام عملیات روزانه وابسته به رایانه هستند. فضای مجازی ابزاری برای قدرت و ثروت است. اگر از آن استفاده نکنیم دیگران از آن استفاده خواهند کرد، آن هم بر علیه ما. گاهی به دلیل ناشناخته بودن منبع حمله؛ فضای مجازی به مکانی ایده‌آل برای جنگ تبدیل شده است. برآوردها نشان می‌دهد که دولت آمریکا در یک سال از محل حملات سایبری در جهان، ۱۰۰ میلیون دلار خسارت دیده است.

کشورهایی با فناوری و متخصصان عقب مانده از قافله‌ی جهانی، بازنده‌ی جنگ سایبری هستند. این جنگ می‌تواند اقتصاد را فلج کند، موجب درگیری‌هایی در داخل و خارج کشورها گردد و بهره‌وری نیروی نظامی را کاهش دهد.

هدف از حمله‌ی سایبری، دست‌یابی به اطلاعات سایر کشورها، ایجاد وقفه در تجارت و یا ایجاد خدشه در زیر ساخت‌ها مانند: «آب، برق، حمل‌ونقل و...» به نحوی که هزینه‌های اقتصادی را افزایش دهند. در ۵ سال گذشته میزان حملات سایبری در سطح جهان بسیار افزایش یافته است.

مهم‌ترین مسئله در این بین، این است که حملات سایبری برای مهاجم ارزان تمام شده ولی دفاع در برابر این حملات بسیار گران تمام می‌شود.

جرائم سایبری:

هرگونه دخل و تصرف غیرمجاز از طریق ورود یا خروج، ضبط و ذخیره، پردازش و کنترل داده ها و نرم افزارهای رایانه ای و ایجاد یا وارد کردن انواع ویروس های رایانه ای و امثال آن جرم محسوب می شود.

چند نمونه از تهدیدهای ناشی از جنگ سایبری:

۱- جاسوسی و نقض امنیت ملی:

جاسوسی سایبری به عملی اشاره دارد که با استفاده از روش‌های بهره‌برداری غیر قانونی از اینترنت، نرم‌افزار و رایانه ها، اسراری (حساس، اختصاصی و یا اطلاعات طبقه‌بندی شده) از افراد، رقبا، گروه‌ها، دولت‌ها و دشمنان، برای بهره برداری های نظامی، سیاسی و یا اقتصادی جمع آوری می نماید.

۲- خراب‌کاری:

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

۳- شبکه‌ی برق:

شبکه‌های انتقال برق به دلیل وابستگی به فضای مجازی و اینترنت از مهم‌ترین هدف‌ها در جنگ سایبری محسوب می‌شوند. در سال ۲۰۰۹ میلادی دولت امریکا بیان داشت که دولت‌های چین و روسیه قصد داشتند تا با نفوذ نرم‌افزاری در شبکه‌های برق در این کشور در آن اختلال ایجاد کنند. از سوی دیگر و در نقطه‌ی مقابل نیز حملات نظامی به شبکه‌های انتقال برق برای از کار انداختن اینترنت از موارد مورد توجه در جنگ سایبری است.

نمونه‌هایی از جنگ های سایبری:

- در سال ۲۰۰۶ میلادی در جریان جنگ ۳۳ روزه حزب‌الله و اسراییل، دولت صهیونیستی اعلام کرد که مورد حملات سایبری سازمان یافته از طرف کشورهای خاورمیانه و روسیه قرار گرفته است.

- در سال ۲۰۰۷ میلادی این بار کشور «استونی» بود که خبر از حمله‌ی سایبری به خود داد. هدف این حمله گویا رسانه‌ها، بانک‌ها و وزارتخانه‌های کشور استونی بودند که از سوی سروری در روسیه مورد حمله قرار گرفتند.

- در سال ۲۰۰۷ میلادی سایت انتخابات کشور «قزاقستان» در جریان یک حمله‌ی سایبری از کار افتاد.

- در سال ۲۰۰۸ میلادی سایت‌های کشورهای روسیه، گرجستان و آذربایجان در جریان درگیری‌ها در اوستیای جنوبی مورد حمله‌ی هکرها قرار گرفتند.

- در سال ۲۰۰۹ میلادی حملات گسترده‌ای به بخش‌های دولتی، رسانه‌ای و مالی دو کشور امریکا و کره جنوبی صورت پذیرفت. در حالی که همه به راه‌اندازی حمله از سوی کره شمالی نظر داشتند یک تحقیق نشان داد که با کمال تعجب حمله از یک سرور ناشناخته در انگلستان بوده است.

- در ماه می ۲۰۱۰ میلادی در پاسخ به حمله‌ی سایبری هند، سایت سازمان موشکی هند، بنیاد ملی علوم هند، دفتر چندین حزب و ... مورد حمله‌ی هکرهای پاکستانی قرار گرفتند.

- در سپتامبر ۲۰۱۰ میلادی تأسیسات اتمی کشورمان توسط ویروس استاکس نت مورد هجوم قرار گرفت. این ویروس یکی از پیشرفته‌ترین ویروس‌های رایانه‌ای بوده و برگ جدیدی را در مبارزه‌های سایبری گشود.

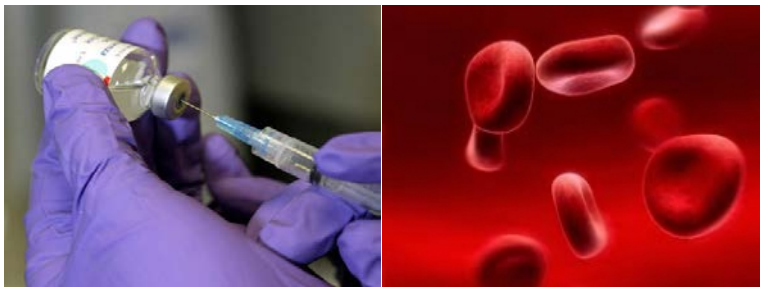
- در سال۲۰۱۰ میلادی دوباره دولت انگلیس اعلام کرد که در هر ماه، هدف بیش از ۱۰۰۰ حمله‌ی سایبری قرار می‌گیرد.

- در ژوئیه‌ی ۲۰۱۱ میلادی سایت شرکت ارتباطاتی (SK) کره جنوبی هک شده و اطلاعات شماره تلفن، پست‌های الکترونیک و آدرس منزل ۳۵ میلیون نفر دزدیده شد.

- در اکتبر ۲۰۱۱ میلادی دولت آمریکا پذیرفت که کنترل هواپیمای جاسوسی RQ- 170 خود را در یک حمله‌ی سایبری از سوی ایران از دست داده است.

- در سال ۲۰۱۲ میلادی بیان شد که هند اطلاعات کمیسیون دوجانبه‌ی اقتصادی بین چین و آمریکا را هک کرده است. گویا اطلاعات هک شده شامل تبادلات پست‌های الکترونیک بین اعضای کمیسیون دوجانبه بوده است.

پدافند زیستی



در کشور ما وظیفه بررسی تهدیدات حوزه زیستی بر عهده ی مجموعه ای از سازمان پدافند غیرعامل کشور با عنوان قرارگاه پدافند زیستی کشور (شفا) به آدرس الکترونیکی www.bdiran.ir/farsi می باشد.

تعریف پدافند زیستی:

پدافند زیستی به مجموعه فعالیت های گفته می شود که به موجب مقابله با تهدیدات زیستی (همچون انتشار ویروس در یک منطقه، آلودگی آب آشامیدنی، انتشار بیماری های واگیر دامی یا نباتی و ...)، سبب حفاظت از سرمایه های ملی و انسانی و کاهش آثار و عواقب ناشی از آنها، می شود.

اقداماتی که قرارگاه پدافند زیستی در برابر تهدیدهای زیستی انجام می دهد، عبارتند از:

- رصد و پایش
- آشکار سازی و هشدار دهی
- تشخیص
- تصمیم و عملیات
- کنترل
- حفاظت و پیشگیری
- امداد و نجات
- درمان، بازیابی و بازتوانی منابع
- محدودسازی و رفع آلودگی

حوزه تهدیدات زیستی:

بستر تهدیدات زیستی از نظر تأثیر پذیری بر شش حوزه زیستی مهم تقسیم می شود. هر یک از این حوزه ها به عنوان سرمایه ملی قلمداد می شود و تهدید هر یک از این حوزه ها ممکن است خطرات و آسیب های جدی و جبران ناپذیری را بر کشور وارد سازد. این حوزه ها در شکل زیر آورده شده است.

جنگ زیستی:

استفاده آشکار یا پنهان از تسلیحات زیستی علیه منابع انسانی و یا زیرساخت های اقتصادی که توسط یک کشور متخاصم و با هدف وارد نمودن ضربه نظامی، از بین بردن مقاومت، تحمیل خسارات اقتصادی و خدشه دار نمودن امنیت ملی کشور انجام می گیرد را جنگ زیستی می گویند.

تهدید زیستی:

هر رویداد یا حادثه طبیعی یا غیر طبیعی که با استفاده از عوامل زیستی باعث تضعیف و نابودی سرمایه‌های انسانی و یا سرمایه‌های ملی زیستی کشور گردد، تهدید زیستی محسوب می‌شود. برای نمونه می توان به عامل سیاه زخم، طاعون، وبا، برخی بیماری های خونی، ویروس ابولا و ... اشاره نمود.

تروریسم زیستی:

استفاده عمدی و سوء از عوامل زیستی (باکتری‌ها، ویروس‌ها، قارچ‌ها و کتورها) و فراورده‌های آنها (توکسین‌ها، ژن‌ها، پریون‌ها، هورمون‌ها و موارد مشابه) برای آسیب زدن، تخریب و از بین بردن سرمایه‌های انسانی و منابع ملی (دام، نباتات، محیط زیست، منابع طبیعی، آب آشامیدانی، مواد تجهیزات و ابنیه) و در نهایت ایجاد رعب و وحشت برای بدست آوردن موفقیت‌های سیاسی و اجتماعی را تروریسم زیستی گویند.

منشا تهدیدات زیستی:

تهدیدات حوزه زیستی از یکی از راه های زیر تولید می شوند.

۱) ***حوادث محیطی و بیماری‌های طبیعی:*** به حوادثی که بدون دخالت انسان در اثر انتشار طبیعی عوامل زیستی ایجاد و به اپیدمی های فراگیر مبدل می گردد اطلاق می‌گردد.

۲) ***فعالیت های تروریستی:*** بکارگیری و استفاده از عوامل زیستی علیه منابع انسانی و زیرساخت‌های اقتصادی توسط اشخاص، گروه‌ها یا دولت‌ها که با هدف ایجاد وحشت و برهم زدن ثبات و امنیت اجتماعی انجام می‌گیرد.

۳) ***فعالیت های دشمن:*** استفاده آشکار یا پنهان از تسلیحات زیستی علیه منابع انسانی و یا زیرساخت‌های اقتصادی که توسط یک کشور متخاصم و با هدف وارد نمودن ضربه نظامی، از بین بردن مقاومت، تحمیل خسارات اقتصادی و خدشه‌دار نمودن امنیت ملی کشور انجام می‌گیرد.