



استانداری آذربایجان شرقی
اداره کل پدافند غیرعامل

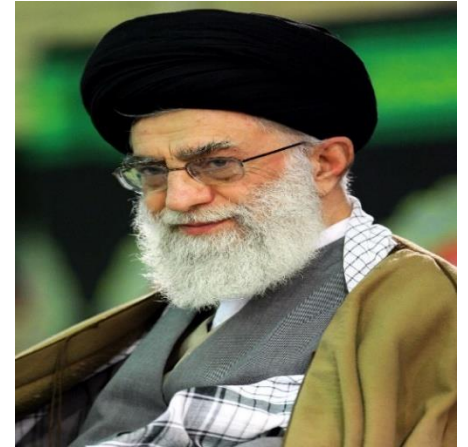
نشریه پدافند غیرعامل
شماره ۳ - مرداد ماه ۱۳۹۴



فرصتی برای تجدید عهد با مردم است

در این شماره خواهید خواند

- ۱..... پدافند غیرعامل یکی از ارکان امنیت ملی است
- ۲..... گزارش عملکرد واحد آموزش پدافند غیرعامل
- ۲..... وظایف کمیته پدافند غیرعامل استان
- ۳..... راکتور اتمی متسامور ارمنستان از دید پدافند غیرعامل
- ۵..... هوشمندی استراتژیک دانش برای مقابله با تهدیدات
- ۶..... برداشت غیرمجاز و سرقت از حساب بانکی
- ۷..... phishing چیست و چگونه در برابر آن از اطلاعات خود محافظت کنیم
- ۹..... پدافند زیستی-دفاع پیش دستانه بیولوژیک
- ۱۰..... مرگ و میر ناشی از مصرف داروهای تبلیغی ماهواره
- ۱۱..... پدافند کالبدی (قسمت دوم)
- ۱۲..... عناوین رویدادهای خبری هفته
- ۱۲..... سایت های مرتبط با پدافند غیرعامل



باید دید دشمن از کجا دارد حمله می کند،
برای یک دفاع خوب هم یک معرفت خوب
لازم است اگرچه برای یک هجوم خوب هم
یک معرفت خوب لازم است.

دبیر مجمع تشخیص مصلحت نظام:

پدافند غیرعامل یکی از ارکان امنیت ملی است

مهم ترین هدف پدافند غیرعامل، تضعیف اراده دشمن و ناامید کردن آن قبل از وقوع جنگ است. علاوه بر این پدافند غیرعامل هم در بازدارندگی و هم در وقوع جنگ ها کاربرد اساسی دارد. اقتدار نظامی یک کشور فقط به موشک ها نیست الان که بزرگترین قدرت موشکی و نظامی منطقه هستیم، آنچه می تواند این موشک ها و توپ ها را کامل کند مسئله پدافند غیرعامل و نبرد اراده هاست.



برای همه نوع تهدیدات باید فرمول پدافند غیرعامل داشته باشیم زیرا پدافند غیرعامل از ارکان اساسی امنیت ملی و استقلال دفاعی و آرامش و توسعه ایران است. اگر پدافند غیرعامل را گسترده کنیم آسیب پذیری کشور کاهش پیدا می کند و مدیریت بحران آسان می شود. باید هزینه تجاوز دشمن را افزایش دهیم و آستانه مقاومت مردمی را بالا ببریم. خسارت زیادی به ایران به دلیل مراعات نکردن پدافند غیرعامل در جنگ تحمیلی وارد شد این در حالیست که پیش از انقلاب مستشاران آمریکایی در ایران بودند اما هیچ گاه دانش پدافند غیرعامل را به ما نمی دادند تا امنیت ملی ایران گروگان آمریکا باشد در چند ماه اخیر هم تمام منطقه جز ایران نا امن بوده و شاهد بودیم که برای برهم زدن ثبات و آرامش کشورمان یک معلم را در سیستان کشتند یا در اصفهان اسیدپاشی کردند و سپس تمام سازمان های آنها بصورت سازماندهی شده و هدفمند آنقدر به این موضوع پرداختند که حدود ۱۰۰۰ نفر را مجبور کردند که در مقابل دادگستری اصفهان تجمع کنند معلوم است که حساب و کتابی در کار است که نشان دادن چهره ناامن از ایران از اهداف دشمنان است.

پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

گزارش عملکرد واحد آموزش پدافند غیرعامل



در راستای تفاهم نامه آموزشی با دستگاه های اجرایی استان در تاریخ ۹۴/۰۵/۰۵ کلاس های آموزش عمومی پدافند غیرعامل در اداره کل شهرک های صنعتی استان در رده مدیران، معاونان و روسای ادارات شرکت شهرک های صنعتی برگزار گردید. همچنین از دهم مرداد ماه سال جاری طبق تفاهم نامه با آموزش و پرورش استان کلاسهای آموزش عمومی پدافند غیرعامل در سطح مدیران مدارس در شهرستان های مرند، آذر شهر، میانه، بناب، سراب، اهر و نواحی پنجگانه تبریز برگزار گردیده است. علاوه بر موارد فوق در ماه جاری پدافند غیرعامل برای شرکت های مهندسين مشاور در حوزه های معماری و شهر سازی، راه و ترابری و سازه و انرژی (آب و برق) کلاس های آموزشی برگزار کرده است.

وظایف کمیته پدافند غیرعامل استان



۱. تهیه لیست نقاط آسیب پذیر استان در برابر تهدیدات و طبقه بندی آنها
۲. شناسایی و طبقه بندی زیرساختها، مراکز و تاسیسات در سطح استان و شهرستان ها
۳. تهیه برآورد تهدیدات استان
۴. آموزش و فرهنگ سازی و نهادینه سازی موضوع پدافند غیرعامل در سطح استان و دستگاه های اجرایی
۵. تهیه و تدوین طرح های پدافند غیرعامل استان و دستگاههای اجرایی
۶. طرح ریزی، برنامه ریزی و نظارت بر اجرای طرح های پدافند غیرعامل مصوب استانی

۷. اجرای سیاست ها و راهبردهای کلان کمیته دائمی پدافند غیرعامل در استان و شهرستان های تابعه
۸. حفاظت و امنیت طرح های پدافند غیرعامل استانی و پیگیری مصوبات
۹. اطلاع رسانی و مناسب و ایجاد آرامش روانی و روحی برای مردم و مقابله با عملیات روانی دشمن



۱۰. حفاظت و امنیت طرح های پدافند غیرعامل استانی
۱۱. پایش آمادگی دفاعی استان با آموزش، تمرین و رزمایش دوره ای
۱۲. استفاده از ظرفیت ها و قابلیت های بسیج برای مدیریت و کنترل بحران

پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

راکتور اتمی متسامور ارمنستان از دید پدافند غیرعامل

مقدمه

پدافند غیرعامل به مجموعه تدابیر و پیش بینی هایی اطلاق می شود که موجب کاهش احتمال وقوع یا به حداقل رساندن خسارات ناشی از اقدامات خصمانه یا حوادث ناخواسته طبیعی یا غیرطبیعی می شود. پدافند غیرعامل هسته ای مستلزم بکارگیری جنگ افزار نبوده و شامل اقداماتی نظیر رصد و پایش، آشکارسازی، هشداردهی، تشخیص نوع آلودگی پرتویی و آموزش احاد جامعه در خصوص حفاظت پرتویی می باشد. با توجه به تهدیدات بالقوه هسته ای از طرف دشمن و احتمال وقوع حوادث پیش بینی نشده در تاسیسات هسته ای کشورمان یا در تاسیسات اتمی کشورهای همسایه، حفظ آمادگی در پدافند هسته ای از اهمیت زیادی برخوردار می باشد. در این نوشتار به یکی از تهدیدات بالقوه شمالغرب کشورنگاهی اجمالی خواهیم داشت.



دکتر صالح اشرفی

مدیر گروه فیزیک هسته ای دانشگاه تبریز
Ashrafi@tabrizu.ac.ir

راکتور اتمی متسامور کشور ارمنستان

نیروگاه هسته ای ارمنستان یکی از پنج نیروگاه نسل اول فعال در جهان است که در دهه ۱۹۷۰ در سی کیلومتری غرب ایروان، پایتخت ارمنستان و در ۱۰۰ کیلومتری مرزهای شمالغربی کشورمان در شهر متسامور ساخته شد. این نیروگاه با دو راکتور مدل (VVER440) که مختص راکتورهای روسی است کار خود را آغاز کرد و حدود ۴۰ درصد از برق ارمنستان را تولید می کند. مجله National Geographic در تازه ترین مقاله خود نیروگاه متسامور را جزو خطرناکترین نیروگاههای جهان طبقه بندی کرده است. در واقع مشکل اصلی در طراحی این راکتورها فقدان محفظه خارجی (Containment) راکتور می باشد. اتحادیه اروپا به دلیل ایمنی پایین راکتورهای VVER یکی از شرایط پذیرش کشورهای بلغارستان و اسلاواکی در اتحادیه اروپا را تعطیلی راکتورهای VVER خود قرار داده است.



شکل ۱: راکتور اتمی ارمنستان در متسامور

علاوه بر آن، ارمنستان بر روی یکی از دو کمر بند بزرگ زلزله خیز جهان موسوم به کمر بند آلپا (Alpide) قرار دارد و زمین لرزه های بزرگی در آن رخ داده است. این نیروگاه به دنبال زمین لرزه ۶/۷ ریشتری سال ۱۹۸۸ در اسپیتاک تعطیل شد. با این حال ارمنستان علیرغم اعتراضات کشورهای همسایه و مجامع بین المللی به دلیل نیاز شدید به انرژی در سال ۱۹۹۵ مجدداً آن را راه اندازی نمود. موقعیت زلزله خیزی سایت نیروگاه از یک طرف و عمر بالا و ایمنی پایین راکتور از طرف دیگر منطقه شمالغرب کشورمان را در معرض تهدید یک حادثه هسته ای نظیر چرنوبیل قرار داده است.

آثار منطقه ای حادثه هسته ای در نیروگاه ارمنستان

آثار یک حادثه احتمالی در راکتور ارمنستان را می توان با بررسی عواقب انفجار راکتور چرنوبیل تا حدودی برآورد نمود. البته در ارزیابی خطرات باید به موقعیت جغرافیایی و شرایط اقلیمی مانند جهت و سرعت وزش بادهای در منطقه و بارش باران یا برف و غیره نیز توجه نمود زیرا این عوامل طبیعی در انتشار آلودگیهای هسته ای نقش تعیین کننده ای دارند.

پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

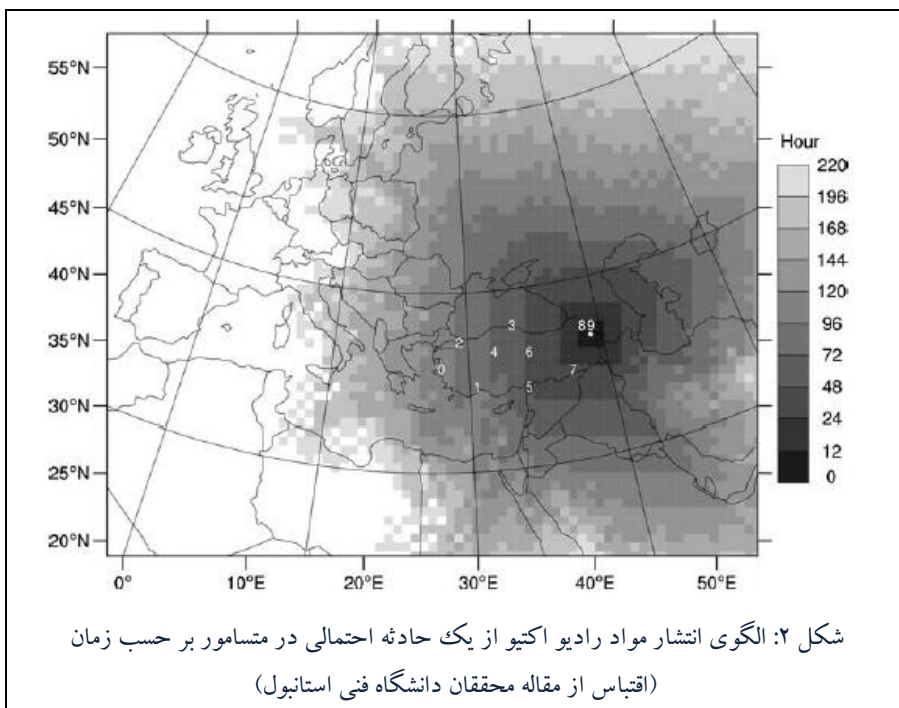
طبق گزارش های معتبر منتشر شده میزان مواد رادیواکتیو آزاد شده در حادثه چرنوبیل ۴۰۰ برابر مواد رادیواکتیو ناشی از بمب اتمی منفجر شده در هیروشیما می باشد. در انفجار چرنوبیل بیش از ۱۰۰ عنصر رادیواکتیو وارد منطقه شدند. البته اکثر این عناصر نیمه عمر کوتاهی داشتند و خیلی زود پرتو زایی خود را از دست دادند. ید، استرانسیوم و سزیوم خطرناک ترین عناصری بودند که آزاد شدند و به ترتیب نیمه عمری برابر با ۸ روز، ۲۹ سال و ۳۰ سال داشتند. به همین دلیل ایزوتوپ های استرانسیوم و سزیوم هنوز در منطقه اروپای شرقی موجود هستند. همانطور که ید باعث سرطان تیروئید می شود، استرانسیوم هم لوسمی یا سرطان خون ایجاد می کند. سزیوم هم عنصری بود که بیشتر از همه عناصر پراکنده شد و بیشتر از همه آنها هم در طبیعت باقی می ماند. این عنصر بقیه اعضای بدن را تحت تأثیر قرار می دهد و کار کبد و طحال را مختل می کند. تعداد زیادی از نوزدان منطقه چرنوبیل دچار معلولیت های بسیار وخیمی هستند. وسعت منطقه ای که در بلاروس، روسیه و اوکراین در اثر حادثه اتمی آلوده شد در حدود ۱۵۰ هزار کیلومتر مربع می باشد. این منطقه مساحتی به شعاع ۵۰۰ کیلومتر در شمال نیروگاه را تشکیل می دهد.

پدافند غیرعامل برای کاهش خسارات یک حادثه احتمالی

عناصر رادیواکتیو آزاد شده در یک حادثه هسته ای به کمک جریان باد و آب های سطحی و زیر زمینی به فواصل دورتری از محل حادثه می رسند. در سال ۲۰۰۸، محققان دانشگاه فنی استانبول - با استفاده از داده های جریان های هوا در یک دوره ۳۰ ساله - سرعت انتشار مواد رادیواکتیو در صورت بروز حادثه در راکتور متسامور را شبیه سازی و محاسبه نموده اند. نتایج تحقیقات آنها نشان می دهد که در صورت بروز یک حادثه هسته ای در متسامور عناصر رادیواکتیو در عرض کمتر از ۱۲ ساعت وارد کشورمان شده و در کمتر از ۲۴ ساعت به شهر پر

جمعیت تبریز می رسند. در شکل (۲) الگوی انتشار مواد پرتو زا در همسایگی راکتور متسامور بر حسب زمان نشان داده شده است.

با توجه به تهدید بالقوه هسته ای منطقه شمالغرب، به عنوان نخستین اقدام پدافندی بایستی جهت اندازه گیری سیستماتیک غلظت رادیو ایزوتوپ های حاصل از شکافت هسته ای پایگاههای پایش پرتوی در نقاط مختلف منطقه تاسیس و راه اندازی شوند. در این راستا لازم است پتانسیل های تخصصی و سخت افزاری دانشگاههای منطقه شناسایی و برای اقدامات پدافندی بسیج و سامان دهی شوند. این پایگاهها تحت نظارت فنی سازمان انرژی اتمی ایران نه تنهایی تواند هر گونه افزایش غلظت رادیوایزوتوپها را اعلام



کنند بلکه در صورت بروز حوادث غیر مترقبه در تاسیسات هسته ای کشور نیز می توانند به عنوان پایگاههای معین وارد عمل شوند. اقدام پدافندی بعدی آموزش نیروهای امدادی مردمی یا نظامی جهت مقابله با حوادث هسته ای می باشد. نهایتاً آموزش عمومی برای آحاد جامعه می تواند در کاهش خسارات محتمله بسیار موثر باشد.

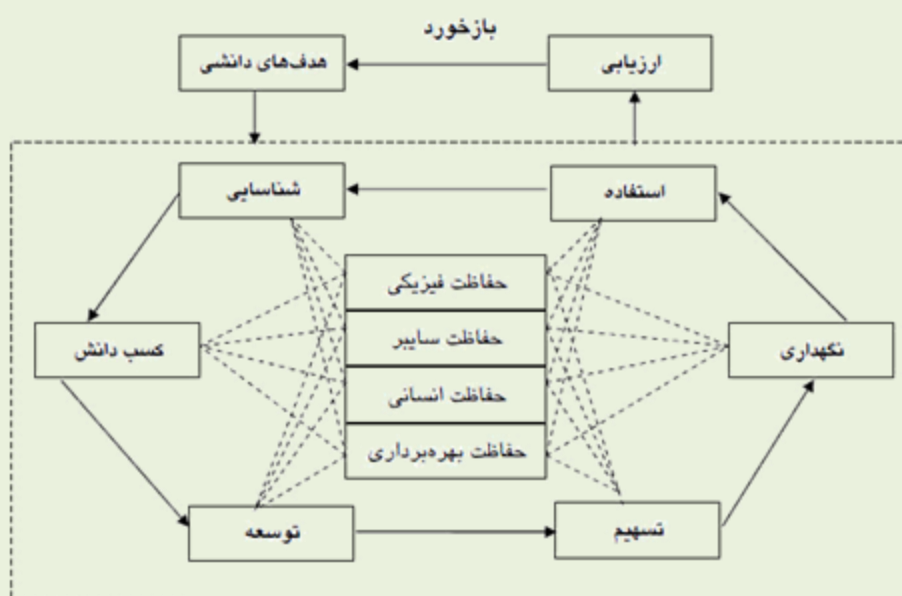
پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

هوشمندی استراتژیک دانش برای مقابله با تهدیدات

یکی از تهدیدات بالقوه در سطح استراتژیک، غافلگیری استراتژیک است. یکی از راهکارهای پدافند غیرعاملی برای این تهدید، دستیابی به یک ضریب هوشمندی مناسب در سطح استراتژیک است. به عبارت دیگر، هوشمندی استراتژیک موجب پیشگیری از غافلگیری استراتژیک خواهد شد. هوشمندی استراتژیک حاصل به اشتراک گذاری نظام مند دانش در اتاق های فکر و اندیشکده ها با تأکید بر قابلیت محوری است.

توجه به چند نکته درباره هوشمندی استراتژیک با تأکید بر قابلیت های پدافندی ضروری به نظر می رسد: هوشمندی استراتژیک ایده آل، یک هوشمندی حاصل از یکپارچگی مؤلفه های آینده نگاری، چشم انداز سازی، تفکر سیستمی، انگیزه بخشی، مشارکت و مدیریت دانش است، یکی از جدی ترین تهدیدات در تحقق هوشمندی استراتژیک وجود شکاف مأموریتی و فناوریانه بین این مؤلفه ها و همچنین عدم وجود ادبیات مشترک بین پردازنده های دانش است، بهترین گزینه برای



پوشش شکاف های بین این مؤلفه ها و یکپارچه سازی آنها استفاده از دانش است، استفاده از دانش برای یکپارچه سازی این مؤلفه ها علاوه بر یکپارچگی و چابکی، انعطاف پذیری را نیز برای سازمان به ارمغان خواهد آورد.

بنابر تعیری می توان گفت: هوشمندی استراتژیک ذاتاً دارای ماهیتی از جنس پدافند غیرعامل است. زیرا هوشمندی استراتژیک اساساً به دنبال آماده شدن برای آینده با تأکید بر قابلیت سازی و قابلیت محوری است و آمادگی یکی از اصول پدافند غیرعامل است. بنابراین از آنجایی که سناریوها به عنوان بستری برای خلق قابلیت ها و استراتژی های گوناگون هستند که هر کدام می توانند متناسب با شرایط و اقتضائات مختلف پدید آیند.

نتیجه پردازش نظام مند دانش استراتژیک در سازمان ها، هوشمندی استراتژیک است. به هوشمندی استراتژیک می توان با رویکردهای متعددی نگریست. یکی از این رویکردها، رویکرد پدافند غیرعامل است. بخش قابل توجهی از هوشمندی استراتژیک با رویکرد پدافند غیرعامل را قابلیت محوری با رویکرد پدافند غیرعامل تشکیل می دهد. هوشمندی و هوشیاری در مقابل سیگنال های ضعیف تغییر، توان بقا و تعامل را برای سازمان های مدرن افزایش می دهد. بنابراین برای رسیدن به یک ضریب هوشمندی قابل قبول باید بین گذشته، حال و آینده هم افزایی های نظام مند شکل داده شود تا برآندهایی قدرت را برای سازمان به ارمغان آورده شوند. مقوله هوشمندی استراتژیک به دنبال دستیابی به یک ضریب هوشمندی قابل قبول با توجه به شرایط زمانی، مکانی و وضعیتی سازمان است.

مدل پیشنهادی پدافند غیرعامل مبتنی بر مدیریت دانش

هدف اصلی این مدل، ایجاد قابلیت های مدیریت دانش سازمانی برای تسهیل خلق، تبادل، اشتراک، طبقه بندی، نگهداری و به کارگیری دانش برای پدافند غیرعامل است. و این مدل در حوزه های حفاظت فیزیکی، سایبری، انسانی و بهره برداری ارایه شده است:

پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

مدیریت دانش در موفقیت پدافند غیرعامل از طریق ایجاد استراتژی های دانش نقش مهمی ایفا می کند. در این زمینه طی بررسی های به عمل آمده در مورد روش های استفاده از پدافند غیرعامل و مدل های علمی مدیریت دانش، مدلی ترکیبی پدافند غیرعامل مبتنی بر مدیریت دانش با توجه به شرایط سازمان های ایرانی ارایه شد که با تعریف پروژه ای در این زمینه و به کارگیری مدل یادشده از طریق ایجاد و استقرار سیستم مربوط می توان از اتلاف هزینه، زمان، دوباره کاری و اثرات آسیب ها جلوگیری کرده و به حفظ دانش و تجارب متخصصان سازمان - به خصوص در صنعت برق - آب - گاز و . با تعیین سطح امنیتی مناسب اقدام کرد.

منبع: کتاب نقشه علم و فناوری از دکتر الوانی - تهیه و تنظیم: شمسعلی محمودیان (کارشناس پدافند غیرعامل استانداری)

برداشت غیرمجاز و سرقت از حساب بانکی

برداشت های غیرمجاز پیش از این توسط روش هایی مانند جعل چک های بانکی انجام می شد اما امروزه نیمی از جرائم سایبری مربوط به برداشت غیرمجاز از حساب بانکی افراد است که از روش های مختلفی مانند سرقت از طریق عابربانک، از طریق دستگاه کارت خوان و در نهایت از طریق اینترنت انجام می شود.



انواع روش های سرقت از عابربانک

۱- اسکیمر: در این روش مجرم به کمک یک اسکیمر که روی ورودی کارت دستگاه قرار می دهد، اطلاعات کارت را می خواند و توسط دوربین کوچکی که بالای دستگاه خودپرداز نصب کرده است رمز فرد را سرقت می کند و سپس اقدام به کپی کردن کارت وی می کند. در بعضی موارد حتی دوربین هم برای خواندن رمز فرد استفاده نمی شود. در عوض از یک کیبورد جعلی روی کیبورد اصلی استفاده می شود که ترتیب فشردن کلیدها را ذخیره می کند. برای جلوگیری از این نوع کلاهبردای و تخلف، یک قطعه پلاستیک در دریچه ورود کارت دستگاه های خودپرداز قرار داده می شود.



۲- چسب مایع: در جای کارت دستگاه خودپرداز چسب مایع ریخته می شود.
۳- تعویض کارت و خالی کردن حساب: فرد سارق در صف می ایستد و پیشنهاد کمک به افراد را می دهد و به محض دریافت کارت در یک لحظه آن را با کارت دیگری تعویض می کند.

۴- سرقت در ساعت های مرده: این نوع سرقت مربوط به ساعات غیر اداری که بانک تعطیل است می باشد و فرد پس از گیر کردن کارت ناچار است تا روز اداری صبر کند.

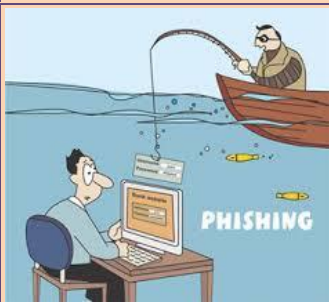
۵- نصب دستگاه عابربانک تقلبی: کلاهبرداران از روی دستگاه های کارتخوان شبیه سازی و آن را در محل های مخصوصی نصب می کنند.

پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

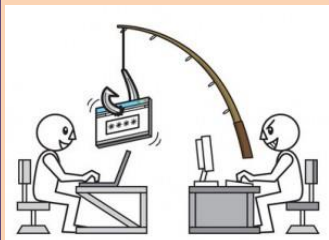
- ۶- انتقال کارت به کارت : در این حالت فرد به بهانه برداشتن مبلغ مربوط به آن روز از شخص دیگری می خواهد که برایش از حساب خود پول برداشت کند و سپس به صورت تقلبی پول را به حساب شخص واریز می کند.
- برای جلوگیری از سرقت پول از طریق عابر بانک توصیه های زیر را به خاطر داشته باشید:**
 - ۱- نباید به افراد ناشناس (تماس های تلفنی از افراد ناشناس)، اعتماد کرده و اطلاعات خود را به آنها دهید.
 - ۲- هیچ مرکز خصوصی و دولتی ، جوایز با مبلغ بالا را غیر حضوری و همچنین بدون طی مراحل رسمی به برندگان پرداخت نمی کند.
 - ۳- اهدای هیچ جایزه ای از طریق عابر بانک و در هیچ کجای دنیا انجام نمی شود.
- تهیه و تنظیم: لیدا رسول اهری (کارشناس آموزش و پژوهش پدافند غیرعامل استانداری)

phishing چیست و چگونه در برابر آن از اطلاعات خود محافظت کنیم



Fishing (ماهیگیری) یک سرگرمی بسیار جذاب است اما وقتی حرف اول آن تغییر کرده و به Phishing تبدیل می گردد چندان خوشایند نیست.

تلاش برای بدست آوردن اطلاعاتی مانند نام کاربری، گذرواژه، اطلاعات حساب بانکی و... از طریق جعل یک وب سایت، آدرس ایمیل و... Phishing نام دارد. phishing در واقع نوعی از فریب است که برای دزدیدن هویت شما طراحی شده است. در یک حيله از نوع phishing، یک فرد آسیب رسان سعی می کند تا اطلاعات شخصی شما را -با متقاعد کردن شما به دادن این اطلاعات تحت ادعاهای دروغین- بدست آورد. ماهیت و یا بهتر بگوئیم رمز موفقیت این نوع از حملات بر قدرت جلب اعتماد مردم استوار است.



مهاجمان به منظور فریب کاربران از روشهای متعددی استفاده می نمایند:

دستکاری پیوند: در این تکنیک برای گمراه کردن کاربر از اسامی معتبری در آدرس استفاده می شود مانند

استفاده از زیردامنه آشنای gmail در www.gmail.phisher.com، که در واقع کاربر را به سایت phisher هدایت می کند.

جعل وب گاه: جعل وب سایت های پرداخت الکترونیک یا هر وب سایت دیگر. مثلاً شکل زیر نمونه جعلی وب سایت بانک ملت را نشان می دهد که کاملاً شبیه آن ساخته شده است و کاربر با وارد کردن اطلاعات کارت خود، عملاً حساب بانکی خود را در اختیار Phisher قرار می دهد.



وب سایت جعلی



وب سایت اصلی

پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

فیشینگ تلفنی: پیامهایی که ظاهراً از طرف بانک فرستاده شده و از کاربر می خواهد تا مثلاً به دلیل وجود ایراد در حسابشان، شماره خاصی را شماره گیری کنند، بعد از گرفتن شماره از کاربر خواسته می شود تا شماره حساب و پین (PIN) خود را وارد کند.

اهداف مهاجمان در حملات phishing:

- اطلاعات بانکی نظیر کارت های اعتباری و اینترنت بانک
- اطلاعات مربوط به رمز عبور حساب های ایمیل و شبکه های اجتماعی

چگونه می توانیم یک کلاهبرداری فیشینگ را شناسایی کنیم؟

نکته اول: دریافت ایمیل از بانک تان یا هر موسسه و سازمانی با این مضمون که "به علت

فعالیت های غیرمجاز، حساب شما در حال بسته شدن است، جهت جلوگیری از تعلیق، حساب خود را بازبینی و تایید کنید." اگر چنین ایمیلی دریافت کردید، نباید به آن اهمیت دهید. همچنین ممکن است ایمیلی دریافت کنید که در آن نوشته شده باشد "شما در قرعه کشی برنده ریال شده اید و برای واریز این پول، اطلاعات حساب خود را وارد کنید" که نباید به هیچ وجه آن را باور کنید. در مقابل این گونه ایمیل ها، هوشمندانه عمل کنید.

نکته دوم: اینکه ایمیل های فیشینگ، شخص خاصی را مورد خطاب قرار نمی دهد و در اغلب موارد برای حجم زیادی از کاربران که بصورت تصادفی انتخاب می شوند ارسال می شود. احتمالاً در ابتدای ایمیل ها عباراتی نظیر "مشترک گرامی" را ببینید. آنها معمولاً اسم شما را خطاب قرار نمی دهند بنابراین اگر چیزی شبیه اینها دیدید احتمال دهید در دام این شیوه از کلاهبرداری اینترنتی افتاده اید.



نکته سوم: درباره URL فیشینگ است. این امکان وجود دارد به وب سایتی هدایت شوید که کاملاً شبیه سایت اصلی باشد، ولی باید بدانید ممکن است به سایت فیشینگ رفته باشید. همواره به URL نگاه کنید تا متوجه شوید آیا در وب سایت اصلی هستید یا در یک وب سایت فیشینگ.

برای جلوگیری از فیشینگ همیشه نکات زیر را رعایت کنیم:

۱- به آدرس وب سایت همیشه موقع کار کردن توجه کنیم که وب سایت اصلی باشد.

۲- بررسی کنید تا مطمئن شوید که وب سایت از رمزنگاری استفاده می کند.

۳- بطور منظم اعلامیه های کارت اعتباری و بانک تان را مرور کنید.

۴- هرگز به تقاضاهایی که از طریق ایمیل یا پنجره های pop-up اطلاعات شخصی شما را می خواهند، پاسخ ندهید. اگر شک دارید، با موسسه ای که مدعی ارسال ایمیل یا پنجره pop-up است، تماس بگیرید.

در پایان یادآور می شود همیشه سوء استفاده های مشکوک از اطلاعات شخصیتان را به مراکز مربوطه از جمله پلیس فتا گزارش نمایید. **تهیه و تنظیم: حمید غفارلو (کارشناس ارشد حفاظت و امنیت پدافند غیر عامل)**

منابع:

<http://www.srco.ir/Articles/TipsView.asp?ID=445>
<http://www.ircert.com/articles/Phishing.htm>

پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

پدافند زیستی - دفاع پیش دستانه بیولوژیک



تهدیدات بیولوژیک به عنوان یکی از تهدیدات فزاینده در دهه گذشته به شدت مورد توجه مسئولین دولتهای مختلف قرار گرفته و نگرانی در باره توسعه آن و توجه گروه های تروریستی به دستیابی عوامل بیولوژیک و استفاده از آنها برای توسعه نا آرامی ها شده است.

تهدیدات بیولوژیک یا استفاده از عوامل بیولوژیک کشنده و ناتوان کننده در جنگ ها (جنگ میکروبی، جنگ بیولوژیک) و یا بیوتروریسم بعنوان یکی از تهدیدات جدید و نوظهوری است که متأسفانه بر اساس شواهد موجود در حال گسترش است. واقعه پخش

گسترده پاکت های سیاه زخم بلافاصله پس از حادثه ۱۱ سپتامبر در امریکا نشان داد که بیوتروریسم می تواند چقدر هراس انگیز و سبب بی ثباتی یک جامعه گردد. دولتمردان امریکا پیرو همین موضوع بیوتروریسم و تهدیدات بیولوژیک را بعنوان یکی از اصلی ترین تهدیدات بر علیه امریکا معرفی نمودند و پیرو آن بودجه های کلان جهت توسعه برنامه های دفاعی در مقابل تهدیدات بیولوژیک اختصاص یافت که بر اساس آمر تا سال ۲۰۱۳ امریکا بالغ بر ۶۰ میلیارد دلار صرف تجهیز آزمایشگاه ها و یگان های خود جهت توسعه سیستم های هشدار، تشخیص سریع پیشگیری و درمان تهدیدات بیولوژیک نموده است.



به همین دلیل تهدیدات بیولوژیک بعنوان یکی از تهدیدات فزاینده در دهه گذشته به شدت مورد توجه مسئولین دولتهای مختلف قرار گرفته و نگرانی در باره توسعه آن و توجه گروه های تروریستی به دستیابی عوامل بیولوژیک و استفاده از آنها برای توسعه نا آرامی ها شده است. بحث های بسیار مختلفی در مورد راهکارهای مقابله با تهدیدات بیولوژیک شده است و پیشنهاداتی شامل هشدار سریع، تشخیص آزمایشگاهی، پیشگیری، درمان و رفع آلودگی در کتب و مقالات متعددی ارائه شده است.



دانشمندان کشورهای مختلف تلاش های گسترده ای را برای توسعه روش های اطلاع سریع و عاجل از یک حمله بیولوژیک و بیوتروریستی بعنوان اصلی ترین راهکار پیشگیری از توسعه عوامل بیولوژیک بین مردم انجام داده و می دهند. با همه این تلاش ها شیوع انواع همه گیری های نوظهور مانند سارس، انفلوانزاهای مختلف، کورونا ویروس های جدید و اخیرا شیوع ابولا در افریقا و بروز مواردی در امریکا و اروپا مجددا توجه همگان را به این تهدید معطوف

پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

نموده است. کشف اطلاعاتی از گروه خطرناک داعش در مورد تهیه، تولید و بکارگیری از عوامکل بیولوژیک هشدارها در توجه به این مورد را افزایش داده است. جوامع اطلاعاتی و امنیتی کشورها تلاش مجددی را برای بازنگری روش های پیشگیری از اشاعه این سلاح های خطرناک شروع کرده اند.

کنوانسیون خلع سلاح بیولوژیک بعنوان یک راهکار بین المللی قصد دارد از اشاعه سلاح های بیولوژیک و بیوتروریسم جلوگیری نماید ولیکن در طول ۳۰ سال گذشته از فعالیت این معاهده و برگزاری ده ها جلسه و بحث و مذاکره به نظر می رسد به دلیل فقدان یک دستور العمل اجرایی نتوانسته است اقدامی جدی را در این مورد انجام دهد به همین دلیل کشورها خود مشغول به کار شده و هر کدام در مسیر توسعه اقدامات کاهش دهنده تهدیدات بیولوژیک فعالیت می کنند.

منبع: <http://paydarymelli.ir/fa/news/10742>

مرگ و میر ناشی از مصرف داروهای تبلیغی ماهواره



معاون غذا و دارو دانشگاه علوم پزشکی کرمانشاه گفت: مردم فریب تبلیغات شبکه های ماهواره ای را نخورند، چراکه موارد متعددی از آسیب های جدی و مرگ و میر ناشی از مصرف این قبیل داروها مشاهده شده است.

قباد محمدی اظهار کرد: در حال حاضر در کشور، داروهای قاچاق و غیرمجاز مخاطرات زیادی را ایجاد کرده اند.

معاون غذا و دارو دانشگاه علوم پزشکی کرمانشاه با اشاره به تولید و توزیع قاچاق و زیرزمینی برخی داروها، گفت: از جمله این داروها می توان به داروهای غیرمجازی اشاره کرد که از طریق شبکه های ماهواره ای تبلیغ می شوند.

داروخانه ها تنها مراکز مجاز فروش دارو هستند

به گفته وی، تبلیغ دارو ممنوع است و داروخانه ها تنها مراکز مجاز فروش دارو هستند و در این رابطه تجویز پزشک برای مصرف دارو الزامی است. محمدی ادامه داد: مردم فریب تبلیغات شبکه های ماهواره ای را نخورند، چراکه موارد متعددی از آسیب های جدی و مرگ و میر ناشی از مصرف این قبیل داروها مشاهده شده است.



این مسئول بیان کرد: طبق آخرین مطالعات انجام شده بر روی داروهای تبلیغی ماهواره

همچون پودرهای تقویتی و مکمل ها، این مواد حاوی مواد شیمیایی غیرمجاز بوده که از ۳۰ سال گذشته تاکنون فروش آن ها به دلیل داشتن عوارض جانبی در بازار ممنوع اعلام شده است. وی در بخش دیگری از سخنانش به مباحثی پیرامون نظارت بر مواد لبنی اشاره کرد و گفت: معاونت غذا و دارو دانشگاه علوم پزشکی کرمانشاه نظارت کامل بر تهیه و بسته بندی شیر و لبنیات در کارخانه های استان دارد. معاون غذا و دارو دانشگاه علوم پزشکی کرمانشاه ادامه داد: شیری که در فروشگاه ها به عنوان لبنیات سنتی عرضه می شود، مورد تایید دانشگاه علوم پزشکی نیست و مسئولیت آن با عرضه کنندگان این فروشگاه ها است.

معاون غذا و دارو دانشگاه علوم پزشکی کرمانشاه تعداد کارخانه فرآورده های گوشتی را ۱۳ واحد عنوان کرد و افزود: کیفیت کارخانه های استان وضعیت مناسب تری نسبت به سایر نقاط کشور دارد.

منبع: <http://paydarymelli.ir/fa/news/10742>

پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

پدافند کالبدی (قسمت دوم)

در قسمت قبل، مفهوم پدافند کالبدی و انواع تهدیدات توضیح داده شد. بیان شد که پدافند کالبدی شاخه ای از پدافند غیرعامل است که خصوصا در مورد زیرساخت ها، مراکز جمعی شهری، مجتمع های مسکونی و سازه های مختلف از دید معماری، شهرسازی و مهندسی عمران می پردازد. در این قسمت تلاش بر آن است تا مروری بر برجسته ترین تهدیدات انسان ساز و تروریستی محتمل بر سازه ها داشته باشیم. لازم به ذکر است که در جنگ نرم هدف دشمن حذف فعالیت هاست و نه از بین بردن سازه و کالبد های بی اهمیت. بر این اساس همواره سعی بر آن است که زیرساخت ها و کالبد کشور با توجه به میزان اهمیت آنها از اصول پدافند غیرعامل بهره مند شوند.

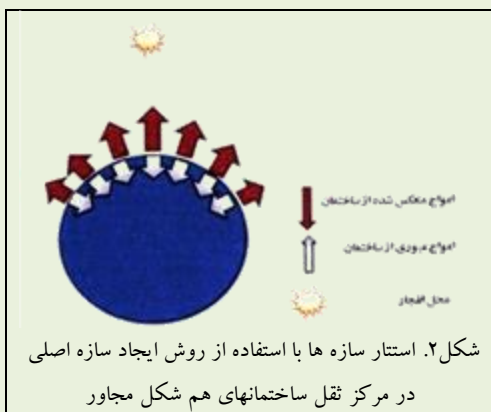
تهدید برجسته کالبدی: تمرکز بر روی نودها- جنگ مهندسی شده (نقطه زنی)



شکل ۱. استتار سازه ها با استفاده از روش همگون سازی با محیط

نودها (گره): در واقع گره های زیر ساختی هستند که در ساختار یک کشور وجود دارند، به نحوی به یکدیگر وابسته هستند. وقتی میزان وابستگی بالا برود گره تولید می شود، در واقع تمرکز بر روی گره ها رویکرد دشمن است، یعنی هر چه در نظام معماری مهندسی کشور گره و نود تولید کنیم این گره و نود در لیست اهداف دشمن قرار می گیرد و هر چه این گره بزرگتر باشد در اولویت بیشتر توجه دشمن قرار می گیرد. لذا ابتدا بایستی تهدیدات وارد و محتمل بر این گره ها بصورت کامل شناسایی و رفع شود. پراکندگی، استتار، اختفا و عدم تمرکز در ساخت زیر ساخت های اساسی به عنوان اصلی ترین روشهای رفع این

تهدید می توانند در نظر گرفته شوند. شکل ۱ و ۲ چند نمونه از استتار ساختمان های مهم را نشان می دهد که به روشهای مختلف صورت می گیرد. همانطور که در این شکل ها دیده می شود میتوان برای استتار ساختمانها از روشهای مختلف مانند همگون سازی با محیط یا ایجاد سازه مهم در مرکز ثقل ساختمانهای مشابه و به فرم پلان دایره ای استفاده کرد. روشهای دیگری مانند استفاده از نماهای اکسیژن دار یا سبز نیز وجود دارد که استفاده از آنها نیز علاوه بر صرفه جویی در مصرف انرژی، کاهش آلاینده گی هوا میتواند باعث استتار ساختمانهای مهم نیز بشود.



شکل ۲. استتار سازه ها با استفاده از روش ایجاد سازه اصلی در مرکز ثقل ساختمانهای هم شکل مجاور

یکی دیگر از روشهای کاهش آسیب پذیری سازه ها و کالبد کشور (که در واقع از اهداف پدافند غیرعامل است) رعایت اصل پراکندگی است. بر اساس این اصل سازه های مهم به جای اینکه در چند طبقه و در یک موقعیت متمرکز شوند بهتر است در مکانهای مختلف و با ارتفاع کم ساخته شوند تا میزان آسیب پذیری آنها کاهش یابد. برای نمونه ساختمان وزارت کشور، استانداری ها بایستی به جای تمرکز در یک موقعیت خاص، در نقاط مختلف شهر پراکنده شوند. روشهای فوق و رعایت اصول بیان شده تا حد زیادی می توانند زیرساخت ها و سازه ها را در مقابل جنگ هدفمند و مهندسی شده محافظت کنند. عدم طراحی دقیق و رعایت این

اصول باعث به وجود آمدن مشکلات اساسی در مواقع بحران خواهد شد و دشمن از این نقاط ضعف نهایت استفاده را خواهد برد. بطور مثال به نقل از رییس سازمان پدافند غیرعامل کشور در جنگ اسرائیل علیه لبنان، فاضلاب روستایی هدف تجاوز اسرائیلی ها قرار گرفت که باعث به وجود آمدن مشکلات عدیده شده و پایداری منطقه را به مخاطره انداخت. در قسمت بعد در مورد رعایت اصول پدافند غیرعامل از دید مستحکم سازی مانند پناهگاه و فضای امن بحث خواهد شد.

پدافند غیرعامل، مصونیت سازی با عزم ملی

پدافند غیرعامل

عناوین رویدادهای خبری هفته



شناسایی کلاهبرداران سایت
های تبلیغ و فروش داروهای
غیرمجاز در اردبیل

<http://www.cyberpolice.ir/news/48551>



تذکر وزارت بهداشت به
۱۰ درصد بیمارستانها برای بی
خطر سازی زباله های عفونی

<http://paydarymelli.ir/fa/news/16118>

رئیس پلیس فضای تولید و تبادل اطلاعات استان مازندران، از
شناسایی سارقان اینترنتی ۸۵۰ میلیونی در شهرستان بابلسر خبر
داد.

<http://www.cyberpolice.ir/news/48441>

۶۴۷ فقره کلاهبرداری با فروش پنل اینترنتی جعلی

<http://www.cyberpolice.ir/news/48651>

موضع اعضای کمیسیون بر جام درباره توافق هسته ای؛ فردو برای
پدافند غیرعامل تأسیس شده است

<http://paydarymelli.ir/fa/news/16369>

جایجایی مخازن انبار نفت یاسوج ضروری است
معاون تهدیدات تخصصی اداره کل پدافند غیرعامل استانداری کهگیلویه و
بویراحمد در مانور ایمنی و اطفای حریق که در محل انبار شرکت پخش
فراورده های نفتی برگزار گردید بر ضرورت اتخاذ تمهیدات لازم بمنظور
جایجایی مخازن انبار نفت یاسوج اجتناب ناپذیر دانست.

<http://paydarymelli.ir/fa/news/16210/>

سایت های مرتبط با پدافند غیرعامل

http://www.paydarymelli.ir/	وب سایت پایداری ملی
http://www.pdrc.ir	مرکز مطالعات پدافند غیرعامل
http://padafand.eaz.gov.ir/	پورتال پدافند غیرعامل استانداری آذربایجان شرقی
http://ostan-as.gov.ir/?PageID=42	استانداری آذربایجان شرقی - دفتر پدافند غیرعامل
http://www.cyberpolice.ir/	پلیس فتا



صاحب امتیاز: اداره کل پدافند غیرعامل استانداری آذربایجان شرقی

مدیر مسئول: سردار جهانسری

سر دبیر: محمد بامدادی

دبیر تحریریه: رامین زارعی

شماره تماس: ۰۴۱-۳۳۳۳۶۲۰۹