بسم الله الرحمن الرحيم

ضرورت پدافند غیرعامل در حوزه سایبر و ارائه راهکارهای بنیادین

دکتر علوی فر

- ✓ Risk Assessor و سناریست تهدیدات در ۶ پروژه مفهومی پدافند غیر عامل
- ✓ طراحی روش تعمیرات نگهداری ریسک پایه با ملاحظات پدافندی در زمان جنگ به عنوان تز کارشناسی ارشد
- ✓ صاحب طرح (SPA) تجزیه تحلیل بهره وری راهکارهای پدافندی؛ تقدیر شده در دومین جشنواره پایداری ملی
- ✓ سر ممیز ایزو ISMS ۲۷۰۰۱ از Vision

اصطلاحات

- سایبر cyber
- رایانه
- شبکه - نت
- اینترانت
- اینترنت

دلایل موفقیت روز افزون شبکه های سایبری

- سازندگان بدافزارها عمدتا **منفرد و سازمان نایافته** هستند.
- تولید کنندگان برنامه های **امنیتی و ضد بدافزار**، گروهی و سازمان یافته هستند.

پیامدهای نبرد بین کشورها در عصر جدید

- بدون هشدار قبلی است.
- غیر مخرب است و لذا حساسیت اجتماعی و در پی آن بسیج همگانی تولید نمی کند.
- می تواند بسیار موثر و ویرانگر در صنایع زیربنایی عمل نماید.
- هوشمند است و **هدف** خود را تشخیص می دهد.
- قابل تکذیب توسط مهاجم است.

پیامدهای نبرد بین کشورها در عصر جدید

- قادر است مدتها در انتظار مخفی به سربرده و ناگهان از درون سیستم، تهاجم خود را آغاز و بدین ترتیب کاملا غافلگیرانه عمل کند.
- غالبا دو منظوره بوده و علاوه بر تخریب ویژگی جاسوسی و نشر اطلاعات را نیز دارند.
- اعتماد بهره برداری از شیوه های پیشرفته علمی را کاهش داده و به این ترتیب سبب عقب ماندگی از سیر نوآوری های نرم افزاری می شوند.

فرضیه اصلی

- در صورت بروز و تشدید مناقشات بین ایران و کشورهای پیشرفته، امکان تهاجم **دشمن به شبکه و سیستمهای کامپیوتری** افزایش می یابد تا به قطعیت برسد.

زمینه بروز تفکر تهاجم به زیرساخت ها

- خط مشی کشورها و حداقل آمریکاییان بر اساس دکترین حلقه واردن مشتمل بر تهاجم به پنج حلقه قرار گرفته که آخرین آنها نیروی نظامی متخاصم است و لذا تهاجم به زیرساختها در اولویت اول جنگی خواهد بود.

استراتژی تهاجمی دشمن (حلقه های واردن)

حلقه‌ها	عنوان‌ها	مقایسه با اندام انسان	مراکز ثقل
حلقه اول	رهبری ملی	مغز و سامانه عصبی	رهبری سیاسی، مراکز اصلی تصمیم گیری کلان سیاسی و نظامی (وزارت خانه‌ها، قرارگاه‌های عمده فرماندهی، مخابرات راه دور)
حلقه دوم	محصولات کلیدی	سامانه هاضمه و گردش خون	نیروگاه برق، پالایشگاه، صنایع سنگین، مخازن سوخت، صنایع دفاعی، دپوی مهمات، انبارهای عمده مواد غذایی، دارویی و شبکه آب رسانی
حلقه سوم	زیر ساخت‌ها	اندام‌های حرکتی	فرودگاه‌ها، راه آهن، بنادر، جاده‌ها، پل‌ها، اتوبان‌های عمده، شبکه مخابراتی منطقه‌ای و محلی
حلقه چهارم	جمعیت مردمی و اراده ملی	روح و روان و اراده	جمعیت مردمی و افراد نیروهای مسلح که با عملیات روانی دشمن مورد هدف قرار می‌گیرند
حلقه پنجم	نیروهای عملیاتی	سلول‌های دفاعی	سامانه‌های اعلام خبر راداری، مواضع و سایت‌های توپخانه و موشک پدافند هوایی، پایگاه‌های هوایی، پایگاه‌های موشکی زمین به زمین، پایگاه‌های دریایی و شناورها، مراکز تعمیراتی و انبارهای قطعات یدکی، یگان‌های عملیاتی خطوط مقدم، قرارگاه‌های تاکتیکی و ...

حوزه شمول پدافند غیرعامل با توجه به حلقه های واردن

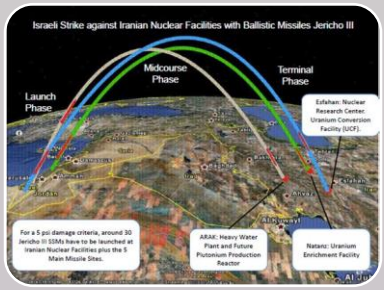
- تأسیسات زیربنائی کشور مانند نیروگاه ها، پالایشگاه های نفت و گاز، تأسیسات انبار نفت و گاز کشور، کارخانجات حیاتی و حساس و منحصر به فرد مانند ذوب فلزات، فولاد، آلومینیوم سازی، خودرو سازی،
- حوزه های جمعیتی کشور، بیمارستان ها، پناهگاه های دسته جمعی؛
- سیستم های ارتباطی و مخابراتی ملی و منطقه ای؛
- حوزه های مالی و پولی و سیستم بانکداری کشور؛
- تاسیسات آب و فاضلاب شهرها،
- تأسیسات مواصلاتی مانند راه ها، پل ها و تونل ها؛

پدافند غیرعامل چیست؟

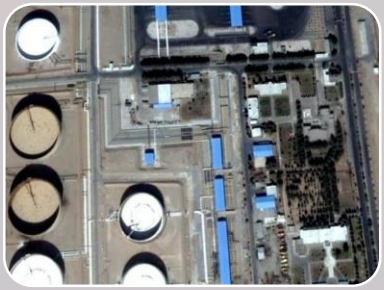
- افزایش بازدارندگی
- کاهش آسیب پذیری
- تداوم خدمت رسانی
- تسهیل در مدیریت بحران
- ارتقای پایداری ملی

تهدید

نرم: بر موضوع تهاجم فرهنگی و اطلاعاتی، حملات سایبری و تهاجم‌های کامپیوتری و هکرها تمرکز دارد و تمرکز آن بر تهدید نرم‌افزاری است.



نیمه سخت: بیشتر روی تهدیدات امنیتی تمرکز دارد.



سخت: تمرکز مباحث روی اقدامات سخت افزاری نظامی بیشتر است.

اهداف تهدید

- از بین بردن زیر ساخت‌های دفاعی و صنعتی کشور
- از بین بردن میل دفاعی کشور در مقابل دشمن
- فلج کردن کشور هدف با تهاجم به زیر ساخت‌های ارتباطی، مردمی، صنعتی، برق، آب و ...
- جلوگیری از عکس‌العلمل به موقع و مناسب
- انهدام تجهیزات مهم و حیاتی دفاعی و صنعتی

اهداف تهدید

- از بین بردن سیستم فرماندهی کنترل و تفکر و مدیریت کشور در بکارگیری توان خودی
- تحمیل بار مضاعف اداره مردم بر دولت با از بین بردن زیرساخت‌های حیاتی (مثل برق، آب، گاز، ارتباط صدا و سیما)
- ایجاد زمینه‌ها و شرایط مناسب برای تهاجم زمینی یا فلج کردن کشور
- کاهش آستانه مقاومت و تحمل ملی

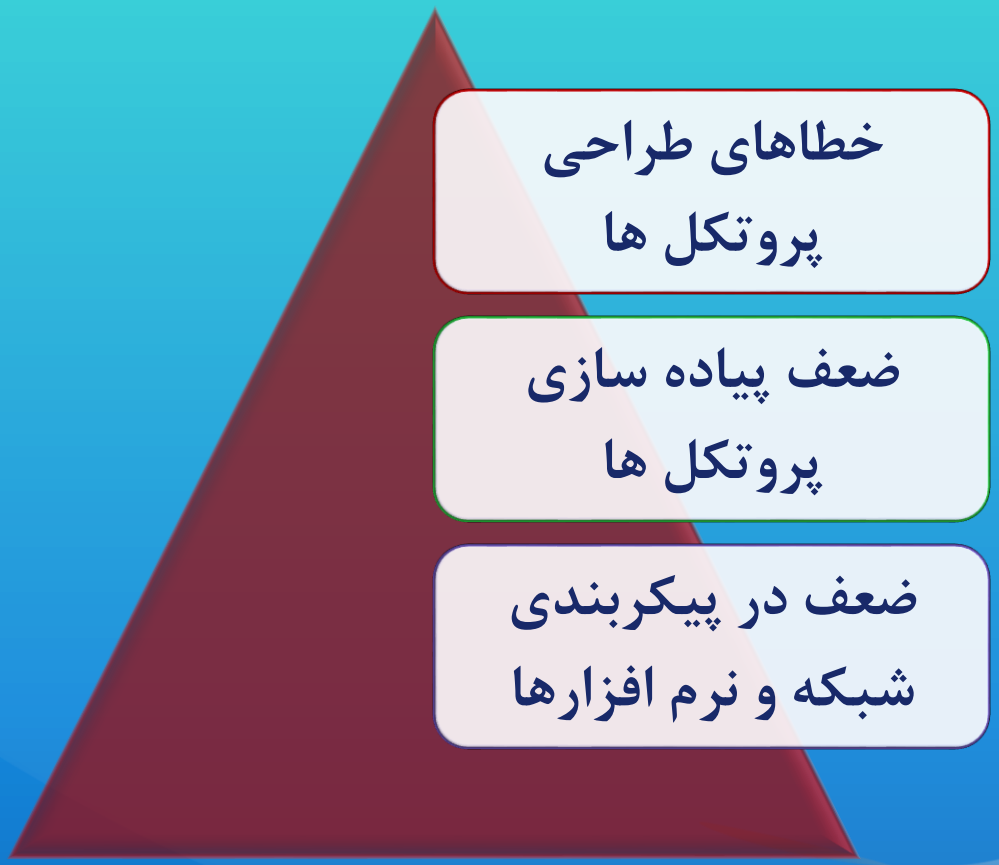
اهداف کلان درپدافند غیرعامل

- دستیابی به توان پایش ، شناسایی وکشف نقاط ضعف وآسیب پذیری ها درفناوری اطلاعات و ارتباطات
- دستیابی به توان پیشگیری ومقابله با تهدیدات دیجیتالی وکاهش آسیب پذیری ها در درفناوری اطلاعات و ارتباطات
- نیل به توان بازدارندگی وپدافندی درحوزه سایبری
- آگاهی رسانی وآموزش پدافند غیرعامل به مدیران وکارشناسا ن درفناوری اطلاعات و ارتباطات دستگاه های اجرایی کشور

امنیت فناوری اطلاعات از دیدگاه پدافند غیرعامل

- دستیابی به توان پایش ، شناسایی وکشف نقاط ضعف وآسیب پذیری ها درفناوری اطلاعات و ارتباطات
- دستیابی به توان پیشگیری ومقابله با تهدیدات دیجیتالی وکاهش آسیب پذیری ها در درفناوری اطلاعات و ارتباطات
- نیل به توان بازدارندگی وپدافندی درحوزه سایبری
- آگاهی رسانی وآموزش پدافند غیرعامل به مدیران وکارشناسا ن درفناوری اطلاعات و ارتباطات دستگاه های اجرایی کشور

آسیب‌پذیری‌ها



تهدیدات جنگ سایبری

- ویروسهای کامپیوتری (Computer Viruses)
- کرم (Worm)
- اسب تروا (Trojan Horse)
- بمب های منطقی (Logic Bombs)
- درهای پشت قلعه ای (Trap Doors)

راههای انتشار بدافزارها

- External Network
- Guest Client
- Executable File
- Documents Macro
- Email
- Removable Disk

راهبردهای کلان پدافند غیرعامل در حوزه سایبر

- حفاظت فیزیکی و محیطی (لایه فیزیکی)
- حفاظت زیرساخت (لایه زیرساخت اطلاعاتی)
- حفاظت نرم افزار (لایه زیرساخت اطلاعاتی)
- حفاظت سخت افزاروسکو ها (لایه زیرساخت اطلاعاتی)
- حفاظت تجهیزات (لایه زیرساخت اطلاعاتی)
- حفاظت اطلاعات و اسناد محرمانه (لایه زیرساخت اطلاعاتی)
- حفاظت سیگنال وجنگ الکترونیک (لایه زیرساخت اطلاعاتی)
- حفاظت منابع انسانی(لایه ادراکی)

طرح های حفاظتی

- **طرح حفاظت فیزیکی و محیطی**
- تهیه الزامات حفاظت پیرامونی
- ارزیابی ریسک آسیب پذیری ناشی از خرابی تجهیزات و.....
- اتخاذکنترل‌های‌مناسب‌جهت‌جلوگیری‌از:دزدی، آتش، انفجار، غبار، ارتعاش، امواج‌الکترومغناطیس و...
- نصب تمامی تجهیزات در یک اتاق قفل شده امن با دسترسی محدود برای افرادمجاز

طرح های حفاظتی

- **طرح حفاظت از زیر ساخت های حیاتی**
- حفاظت از خطوط اصلی که برای مهاجم غیرقابل دسترس باشد.
- تدوین روالهای کنترل تغییرات
- تهیه قراردادهاوپروتکل های ارتباطی امن
- اجراء تست نفوذ به طور متناوب

طرح های حفاظتی

- **طرح حفاظت از تجهیزات**
- **طرح حفاظت از سخت افزار و سکوها**
  - مانیتور کردن ثبت رخدادها بطورمنظم به منظور کشف فعالیتهای مشکوک
  - انجام عملیات پشتیبان گیری و بازیابی در فواصل زمانی معینی

طرح های حفاظتی

- **طرح حفاظت از سیگنال و جنگ الکترونیک**
- **طرح حفاظت از اسناد و اطلاعات محرمانه**
- برقراری مجازاتهایی به منظور پیشگیری ازرفتارهای متناقض
- شناسایی و معرفی ابزارها وتکنیک هایی برای پشتیبانی از ارسال امن اطلاعات

طرح های حفاظتی

- **طرح حفاظت از منابع انسانی**
- **طرح بازیابی در خصوص رخداد ها و تهدیدات سایبری**
- تشکیل تیمهای CERT به منظور واکنش سریع به رخدادها
- تهیه طرح های واکنشی در مواقع بحران سایبری
- توانمند سازی در جهت شناسایی راه های نفوذ پذیری به فضای سایبری