سازمان پدافند غیرعامل کشور
معاونت امور شهری

دوره مجازی کوتاه‌مدت عمومی پدافند غیرعامل شهری

پدافند سایبری

استاد: مهندس حمیدرضا کاووسی

شماره فصل	موضوع
فصل اول	کلیاتی در مورد اصول و مبانی پدافند **سایبری** (منطبق باسند راهبردی سایبری)
فصل دوم	معرفی و مروری بر ادبیات و کارکردهای فناوری اطلاعات و ارتباطات
فصل سوم	معرفی و مروری بر ادبیات و کارکردهای فضای مجازی(سایبر)
فصل چهارم	امنیت و دفاع در حوزه سایبر
فصل پنجم	مطالعات موردی

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فصل اول

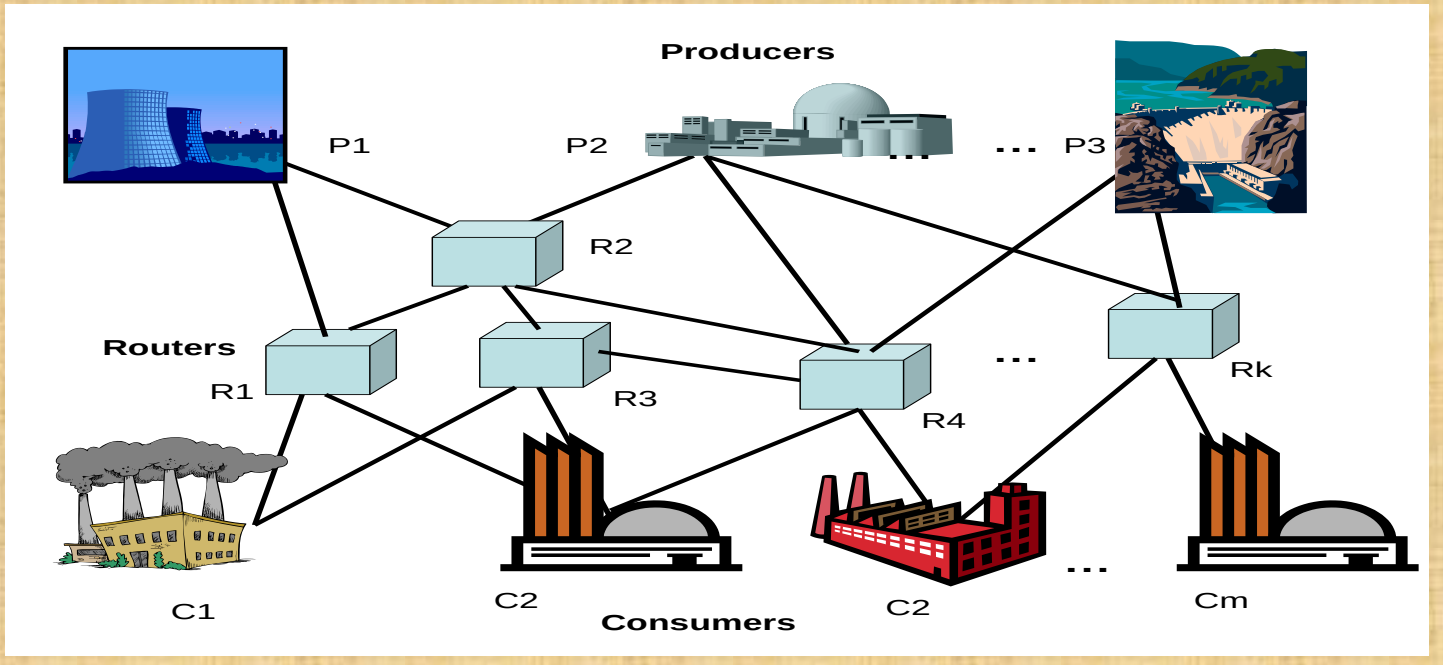
کلیاتی در مورد

اصول و مبانی پدافند سایبری

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تعریف فضای سایبری

شبکه های وابسته به یکدیگر، از زیرساخت های فناوری اطلاعات، شبکه های ارتباطی، سامانه های رایانه ای، پردازنده های تعبیه شده (جاگذاری شده)، کنترل کننده های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور **تولید**، **پردازش**، **ذخیره سازی**، **مبادله**، **بازیابی** و **بهره برداری** از اطلاعات.

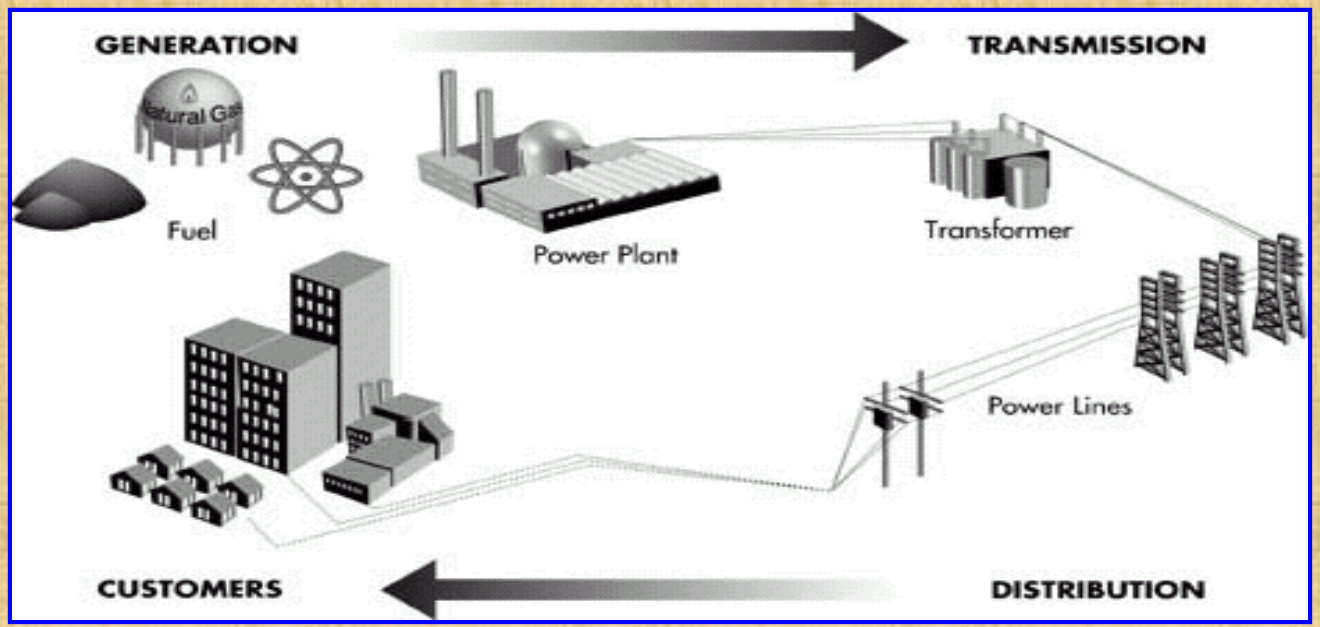


سازمان پدافند غیرعامل کشور
معاونت امور شهری

سرمایه ملی سایبری

بخشی از سرمایه های ملی کشور است که در فضای سایبری قابل حفظ، نگهداری و تهدید می باشد. سرمایه های ملی سایبری را می توان به سرمایه ملی سایبری حیاتی، حساس و مهم طبقه بندی نمود.

سرمایه های ملی فیزیکی که در فضای سایبر قابل مدیریت، کنترل ومحافظت و تهدید باشد هم سرمایه ملی سایبری محسوب می گردد.



سازمان پدافند غیرعامل کشور
معاونت امور شهری

آسیب‌پذیری سایبری

آسیب‌پذیری، به ضعف موجود در داخل یک سرمایه، رویه‌های امنیتی یا کنترل‌های داخلی یا پیاده‌سازی آن سرمایه، که قابلیت بهره‌برداری یا فعال‌شدن توسط یک تهدید خارجی را داشته باشد، اطلاق می‌گردد.

منشاء آسیب‌پذیری‌های سایبری :

- ضعف موجود در فناوری مورد استفاده در سامانه سایبری موردنظر
- ضعف پیاده‌سازی (تولید) سامانه سایبری موردنظر
- ضعف تنظیمات و بهره‌برداری از سامانه سایبری موردنظر

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تهدید سایبری

هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به ماموریت‌ها، وظایف، سامانه های سایبری یا پرسنل دستگاه به واسطه یک سامانه اطلاعاتی، از طریق دسترسی غیرمجاز، تخریب، افشاء، تغییر اطلاعات، ممانعت یا اختلال در ارائه خدمت.

منشاء تهدید سایبری:

- دولت‌ها یا در واقع دولت‌های متخاصم
- مزدوران سایبری یا گروه‌های تحت حمایت پنهان دولت‌ها
- تروریست‌های سایبری
- مجرمین سازمان‌یافته سایبری
- هکرهای دارای انگیزه سیاسی
- هکرها

نمونه تهدیدات سایبری:

- اختلال در شبکه های مخابراتی کشور اعم ازشبکه ثابت و موبایل و ... (شنود، اختلال، انهدام)
- اختلال درشبکه حمل و نقل و ترافیک کشور (مترو، بین شهری، زمینی، هوایی، راه آهن)
- اختلال در شبکه برق کشور(خروج نیروگاه از مدار)
- اختلال در شبکه گاز (انفجار خطوط لوله، پالایشگاه)
- اختلال و سرقت در شبکه بانکی و مالی کشور
- اختلال در شبکه های صدا و سیما
- و ...

سازمان پدافند غیرعامل کشور
معاونت امور شهری

مخاطره سایبری

مخاطره سایبری، به احتمال بهره‌برداری یک تهدید سایبری، از یک یا چند آسیب‌پذیری سایبری موجود در یک سرمایه ملی سایبری، به منظور:

- تخریب
- اختلال
- دسترسی غیر مجاز
- افشاء اطلاعات
- تغییر اطلاعات
- ممانعت از ارائه سرویس

سازمان پدافند غیرعامل کشور
معاونت امور شهری

منشاء مخاطره سایبری

منشاء مخاطره سایبری، عبارت است از دو عامل:

- تهدید سایبری موجود علیه سرمایه سایبری
- آسیب‌پذیری سایبری موجود در داخل سرمایه سایبری

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تعریف پدافند سایبری

به مجموعه اقداماتی گفته می شود که موجب بازدارندگی، پیش‌گیری، ممانعت از انجام، تشخیص به موقع، مقابله موثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه های ملی سایبری توسط متخاصمین سایبری، اعم از ارتش سایبری کشورهای متخاصم و یا گروه های تحت حمایت پنهان دولتهای متخاصم می شود.

کلیدواژه‌های پدافند سایبری

- امنیت اطلاعات
- ایمنی سرمایه ها و دارایی ها
- پایداری سیستم در هر شرایط

تغییر مفاهیم در فضای سایبر

تغییر برخی مفاهیم موجود در فضای سایبر در مقایسه با فضای واقعی:

- زمان
- بعد مسافت(فاصله)
- تعداد
- جنس محصول
- نحوه توزیع
- .....

سازمان پدافند غیرعامل کشور
معاونت امور شهری

ایجاد مفاهیم جدید در فضای سایبر

- خدمات الکترونیکی
- پست الکترونیکی(e- mail)
- تجارت الکترونیکی
- آموزش الکترونیکی
- دولت الکترونیکی
- شهروند الکترونیکی
- شهر الکترونیکی
- سرقت الکترونیکی
- جاسوسی الکترونیکی
- تهدیدات الکترونیکی
- سرباز الکترونیکی
- حملات الکترونیکی
- ارتش سایبری
- .....

سازمان پدافند غیرعامل کشور
معاونت امور شهری

ظهور تهدیدات جدید و از جنس فناوری اطلاعات

به موازات افزایش رفاه عمومی، ظهور تهدیدات جدید و از جنس فناوری اطلاعات و در بستر فناوری در حوزه های مختلف:

- **تهدیدات در حوزه فردی**
- **تهدیدات در حوزه اجتماعی، مردمی، زیر ساخت های حیاتی و حساس کشور**
- **تهدیدات در حوزه امنیت ملی**

سازمان پدافند غیرعامل کشور
معاونت امور شهری

دلایل اصلی تغییر ماهیت جنگ ها

- کاهش تلفات انسانی(پیروزی بدون خونریزی)
- کاهش هزینه های جنگی
- کاهش زمان عملیات ها
- اثر بخشی بیشتر
- ابعاد گسترده تر(نظامی، اقتصادی، اجتماعی، سیاسی، مذهبی، صنعتی و....)
- امکان بکارگیری از همه مولفه های قدرت
- ریسک کم
- قدرت زیاد در کنترل احساسات

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فضای سایبر بعد پنجم جنگ یا (فرا بعد)

فضای سایبر

فضا

هوا

زمین

دریا

سازمان پدافند غیرعامل کشور
معاونت امور شهری

جنگ سایبری

- جنگ سایبری، بالاترین سطح و پیچیده ترین نوع از تهاجم سایبری است که علیه منافع ملی سایبری کشورها انجام شده و شدیدترین پیامدها را به همراه خواهد داشت.
- یکی از ویژگی‌های اصلی جنگ سایبری، آن است که این نوع از تهاجم سایبری، حتماً توسط ارتش سایبری کشورها انجام می‌گیرد.

نظام دفاع سایبری کشور، مسئولیت دفاع از سرمایه‌های ملی سایبری، در مقابل ستیز (نزاع) سایبری و بویژه جنگ سایبری را بر عهده دارد.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

شاخص های جنگ سایبری

- منشاء تهاجم سایبری: یک کشور متجاوز سایبری باشد.

  بکارگیری سلاح سایبری به جای ویروس معمولی

  (دارای پیچیدگی، فرمان پذیری و هوشمندی بسیار زیاد)

- سطح تهاجم سایبری و خسارت ناشی از آن: سطح تهدید امنیت ملی
- شدت تهاجم سایبری: بسیار زیاد با اختلال و تخریب فاجعه بار
- پیامد تهاجم سایبری: اختلال گسترده در عملکرد سرمایه‌های ملی سایبری

سازمان پدافند غیرعامل کشور
معاونت امور شهری

پیامد های جنگ سایبری

- براندازی نظام حاکمیتی یا تهدید فاجعه‌بار امنیت ملی
- آغاز همزمان جنگ فیزیکی یا زمینه‌سازی و تسهیل شروع جنگ فیزیکی در آینده نزدیک
- تخریب یا صدمه فاجعه‌بار به وجهه کشور در سطح بین المللی
- تخریب یا صدمه فاجعه‌بار به روابط سیاسی و اقتصادی کشور
- تلفات انسانی یا مخاطره گسترده برای سلامت و ایمنی عمومی (از طریق ایجاد آلودگی هسته ای، شیمیایی یا بیولوژیک)
- هرج ومرج و شورش داخلی
- اختلال گسترده در اداره امور کشور
- تخریب اطمینان عمومی یا باورهای دینی، ملی و قومی
- خسارت شدید به اقتصاد ملی
- تخریب یا اختلال گسترده در عملکرد سرمایه‌های ملی سایبری

سازمان پدافند غیرعامل کشور
معاونت امور شهری

نمونه های حملات سایبری

- از کار انداختن نیروگاه برق در امریکا و قطع برق ۱۰ میلیون نفر در طی یک هفته و مرگ تعدادی از کهنسالان
- انفجار در خط لوله انتقال گاز روسیه به دلیل اعمال تغییرات در نرم افزار مرکزی سیستم اسکادا
- انفجار در خط لوله انتقال بنزین در امریکا به دلیل نفوذ به سیستم اسکادای خط لوله
- حمله سایبری به گرجستان؛ حمله سایبری به وب سایتهای دولتی به ویژه ریاست جمهوری، صدا و سیما و مراکز خدمات دهی عمومی و .... قبل از حمله نظامی

سازمان پدافند غیرعامل کشور
معاونت امور شهری

اقدامات سایبری سایر کشورها

- تشکیل فرماندهی سایبری توسط امریکا با هدف انجام عملیات آفندی و پدافندی در ارتش امریکا و در سطح کلیه نیروهای ارتش
- تشکیل یگان های تخصصی عملیات سایبری در امریکا جهت انجام عملیات تخصصیِ سایبری متشکل از تخصص سایبر و حوزه تخصصی مربوطه (نیروگاه ها، پالایشگاه ها، تاسیسات هسته ای، ارتباطی، بانکی و ....)
- تشکیل یگان های سایبر در اکثر کشورها بویژه : ناتو، انگلیس، ترکیه، رژیم صهیونیستی
- اجرای مانورهای مختلف سایبری در مقاطع مختلف
- انجام حملات سایبری مختلف از قبیل حمله استاکس نت

سازمان پدافند غیرعامل کشور
معاونت امور شهری

قرارگاه پدافند سایبری کشور

از سال ۱۳۹۰ به منظور مقابله با تهدیدات سایبری دشمن و امن سازی زیرساخت های سایبری کشور، قرارگاه پدافند سایبری کشور توسط سازمان پدافند غیر عامل کشور و با هدف راهبری و هدایت دستگاه های اجرایی کشور جهت این امر مهم تشکیل گردید.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

ادامه قرارگاه پدافند سایبری

براساس ابلاغیه قرارگاه پدافند سایبری، کلیه دستگاه های اجرایی کشور، پس از تعیین سطح اهمیت سرمایه های سایبری خود، موظف به امن سازی زیرساخت های حیاتی، حساس و مهم سایبری خود بوده و به منظور آمادگی جهت مقابله با حملات سایبری دشمن، نسبت به ایجاد مراکز پدافند سایبری در سطح وزارتخانه ها، سازمان ها، استان ها و مناطق ویژه اقدام نمایند.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

وضعیت بد افزارهای سایبری در سال ۲۰۱۴

- هوشمند تر
- مرموز تر
- پنهان تر

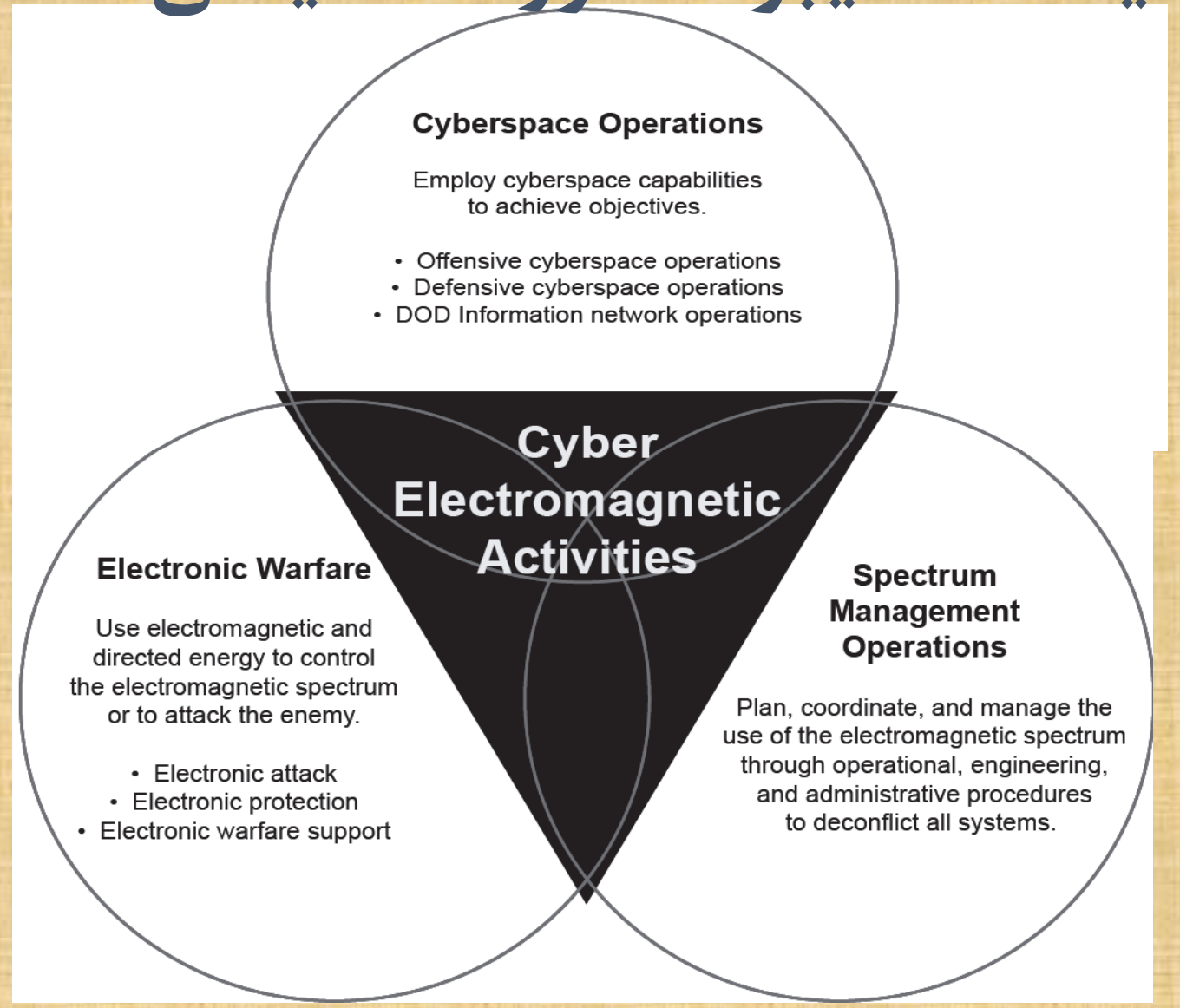
سازمان پدافند غیرعامل کشور
معاونت امور شهری

تهدیدات سایبر الکترومغناطیسی

- یکپارچگی و همزمانی فعالیت های سایبری و الکترومغناطیسی مفهوم جدیدی به نام سایبرالکترومغناطیس بوجود آورده است.
- اقدامات سایبر الکترومغناطیسی، به منظور ضبط، حفظ و بهره برداری از برتری های موجود علیه دشمنان و حریفان در فضای سایبری و طیف الکترومغناطیسی و به طور همزمان، جلوگیری و مانع تراشی در برابر بهره برداری دشمن از همان امکانات و حفاظت از سامانه فرماندهی صورت می گیرد.
- این اقدامات شامل: عملیات فضای سایبری، جنگ الکترونیک و عملیات مدیریت طیف می باشد.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تهدیدات سایبر الکترومغناطیسی



سازمان پدافند غیرعامل کشور
معاونت امور شهری

کارکردهای اصلی پدافند سایبری

- کاهش آسیب پذیری زیرساختهای سایبری
- افزایش پایداری و تولید قدرت در حوزه سایبری
- تداوم فعالیتهای ضروری سایبری کشور
- ارتقاء پایداری ملی زیرساختهای سایبری کشور
- گسترش تولید داخلی و بومی سازی سامانه های مبتنی بر حوزه سایبر
- تسهیل مدیریت بحران در زیرساختهای سایبری کشور

سازمان پدافند غیرعامل کشور
معاونت امور شهری

سطوح پدافند سایبری

- مصون سازی زیرساخت های حیاتی سایبری
- امن و پایدار سازی زیرساخت های حساس سایبری
- ایمن سازی و کاهش آسیب پذیری زیرساخت های مهم سایبری

سازمان پدافند غیرعامل کشور
معاونت امور شهری

ویژگی های پدافند سایبری کشور

قدرت بازدارندگی موثر در برابر تهدیدات سایبری دشمن مبتنی برنظام پدافند سایبری:

هوشمندانه	انحصاری	ابتکاری	عمیق
لایه به لایه	بومی	پیشگیرانه	شبکه ای
چابک و منعطف		گسترش یافته و سلسله مراتبی	

سازمان پدافند غیرعامل کشور
معاونت امور شهری

دفاع لایه به لایه

۱. سیاست های فرماندهی، دفاعی و اداره (دستورالعمل ها)
۲. دفاع فیزیکی(دوربین های مداربسته مبتنی برIP- روشهای شناسایی بیومتریک)
۳. دفاع پیرامونی و مرزبانی(UTM-Firewall-Honeypot)
۴. دفاع در شبکه (Router-Switch L2/L3-HSM)
۵. دفاع در سطح داده و محتوا (Data Encryption-Recovery Data)
۶. دفاع در سطح سیستم عامل(CPU/Proccesor-Virtualization-Industrial Computer)
۷. دفاع در نقاط پایانی(ضدبدافزارها- سامانه های تشخیص نفوذ)
۸. دفاع در سطح برنامه های کاربردی (دیتابیس- WAF -DB Monitoring/Scanning)

سازمان پدافند غیرعامل کشور
معاونت امور شهری

متدولوژی پدافند سایبری

گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری:

۱- شناسایی دارایی ها، مراکز و شبکه های سایبری و متکی به سایبر

۲- تعیین سطح اهمیت مراکز و شبکه های سایبری و متکی به سایبر به سطوح حیاتی، حساس و مهم

۳- تعیین تهدیدات سایبری مراکز و شبکه های تعیین سطح شده

۴- شناسایی آسیب پذیری های سایبری مراکز و شبکه های تعیین سطح شده

۵- تعیین مخاطرات سایبری در صورت اعمال تهدیدات بر آسیب پذیری ها

سازمان پدافند غیرعامل کشور
معاونت امور شهری

متدولوژی پدافند سایبری

۶- محاسبه ریسک و تعیین ریسک قابل قبول

۷- ارائه راهکارهای پدافندی به منظور کاهش آسیب پذیری ها و مقابله با تهدیدات سایبری

۸- ارائه راهکارهای مقابله با حملات سایبری (تشکیل تیم cert و ...)

۹- ارائه طرح تداوم خدمات و فعالیت های ضروری در صورت بروز بحران سایبر ی

۱۰- پیاده سازی و اجرای راهکارهای ارائه شده

۱۱- نظارت، ارزیابی و کنترل اقدامات

۱۲- برگزاری رزمایش های سایبری

سازمان پدافند غیرعامل کشور
معاونت امور شهری

متدولوژی پدافند سایبری

۱۳- رصد و پایش تهدیدات و آسیب پذیری ها و تعیین تهدیدات و آسیب پذیری های جدید

۱۴- تعیین پیامدهای تهدیدات و آسیب پذیری های جدید

۱۵- به روز رسانی راه کارهای پدافندی با توجه به تهدیدات و آسیب پذیری های جدید

۱۶- برگزاری آموزش های ارتقاء توانمندی های سایبری

دستورات اجرایی حوزه پدافند سایبری

۱. سامانه ها و شبکه های فناوری اطلاعات و ارتباطات سطح بندی شود.

۲. دسترسی های فیزیکی و الکترونیکی به نقاط حساس سایت ها و شبکه ها و مراکز حیاتی، حساس و مهم کنترل شود.

۳. برنامه مدیریت بحران دفاع سایبری تهیه و تدوین شود.

۴. برای مقابله با تهدیدات سایبری، مانورهای عملیاتی در بخش فناوری اطلاعات و ارتباطات طراحی و اجرا شود.

دستورات اجرایی حوزه پدافند سایبری

۵. سازه های ویژه برای مراکز داده، اتاق سرور و اتاق کنترل و نظارت در مراکز حیاتی و حساس تامین شود.

۶. بخشهای حیاتی، حساس و مهم متناسب با اهمیت آن در برابر تهدیدات الکترومغناطیسی حفاظت گردد.

۷. از تجهیزات امنیتی بومی حوزه سایبری استفاده شود.

۸. درخرید تجهیزات و خدمات فناوری اطلاعات خارجی بر وجود قابلیت بومی سازی آن تاکید شود.

دستورات اجرایی حوزه پدافند سایبری

۹. از رمز کننده های سخت افزاری و نرم افزاری بومی و ساخت داخل استفاده گردد.

۱۰. برنامه ارتقاء امنیت برای نرم افزارهای سیستمی پایه در حوزه کارگزار(Server) و در حوزه کارخواه (Client) تهیه و تدوین شود.

۱۱. امنیت سرویس های تحت وب، سرویس دهندگان شبکه و همچنین سرویس کارگزار نامه امن(e-mail) ارتقاء یابد.

۱۲. اتصال تمامی نقاط شبکه یا کاربر منفصل در لایه های حیاتی و حساس از اینترنت قطع کامل ودر صورت ضرورت ارتباط با اینترنت، از نقاط جداگانه فاقد طبقه بندی استفاده گردد.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

دستورات اجرایی حوزه پدافند سایبری

۱۳. از خطوط ارتباطی فیبر نوری استفاده حداکثری و از خطوط زمینی رادیوئی استفاده حداقلی شود و ارتباطات ماهواره ای در شبکه های حیاتی و حساس حذف گردد.

۱۴. از ظرفیت میزبانی بانکهای اطلاعاتی در داخل کشور استفاده گردد.

۱۵. نسخه پشتیبان از محتوی و اطلاعات موجود در شبکه در بازه های زمانی برنامه ریزی شده تهیه شود.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

دستورات اجرایی حوزه پدافند سایبری

۱۶. جهت نگهداری، ذخیره سازی، بازیابی و پشتیبانی اطلاعات موجود در شبکه، برنامه امن سازی تدوین شود.

۱۷. طراحی و اجرای آموزش امنیت و قابلیت های دفاعی در حوزه سایبری برای کاربران و مدیران دستگاه در برنامه پیش بینی گردد.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

اهم راه کارهای مقابله با تهدیدات سایبری در کشور

۱- اجرای پروژه های متکی به سایبر براساس اصول و ضوابط پدافند سایبری و از مرحله مطالعه، امکان سنجی، طراحی، تامین کالا، اجرا(نصب و راه اندازی)، نگهداری و بهره برداری

۲- ایجاد شبکه ملی اطلاعات کشور (اینترانت ملی) مستقل از اینترنت

۳- اتخاذ و بکارگیری تدابیر امنیتی مربوط به تجهیزات و شبکه های مرتبط و متصل به فضای سایبر

۴- ایجاد مراکز داده متعدد بومی در داخل کشور و انتقال سایتها بر روی آنها

سازمان پدافند غیرعامل کشور
معاونت امور شهری

ادامه اهم راهکارهای اصلی

۵- داشتن سیستم عامل ملی (بومی)

۶- داشتن سیستم موتور جستجو ملی

۷- ایجاد تیم های امداد و نجات رایانه ای موسوم به CERT جهت مقابله با حملات سایبری

۸- داشتن تجهیزات شبکه ای بومی

۹-استفاده از فیبر نوری به عنوان بستر ارتباطی

۱۰- استفاده از توپولوژی مناسب ارتباطی و حتی الامکان از توپولوژی Full Mesh

۱۱- استفاده از سیستم ها و سایت های Redundant

۱۲- تهیه نسخه های پشتیبان از اطلاعات موجود

سازمان پدافند غیرعامل کشور
معاونت امور شهری

ادامه راه کارهای اصلی

۱۳- بکارگیری اصول پدافند غیرعامل برای تاسیسات فیزیکی در کلیه مراحل از طراحی تا بهره برداری از قبیل : مکان یابی ، پراکندگی ، مقاوم سازی و ...

۱۴- ایجاد مراکز امنیت شبکه (SOC)

۱۵- ایجاد لایه های دفاعی سایبری در پروژه ها و طرح های سایبری یا متکی به سایبر

۱۶- تهیه دستورالعمل های امنیتی و پدافندی

۱۷- آموزش مداوم و مستمر کلیه کارکنان مرتبط

۱۸- برگزاری رزمایش های دوره ای پدافند سایبری

۱۹-رصد و پایش دائمی تهدیدات سایبری و ارائه راه کارهای پدافندی مربوطه

۲۰- ایجاد مراکز پدافند سایبری در سطوح مختلف اعم از ملی، دستگاهی، استانی به منظور مقابله با حملات سایبری

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فصل دوم

معرفی و مروری بر ادبیات و

کارکردهای فناوری اطلاعات و ارتباطات

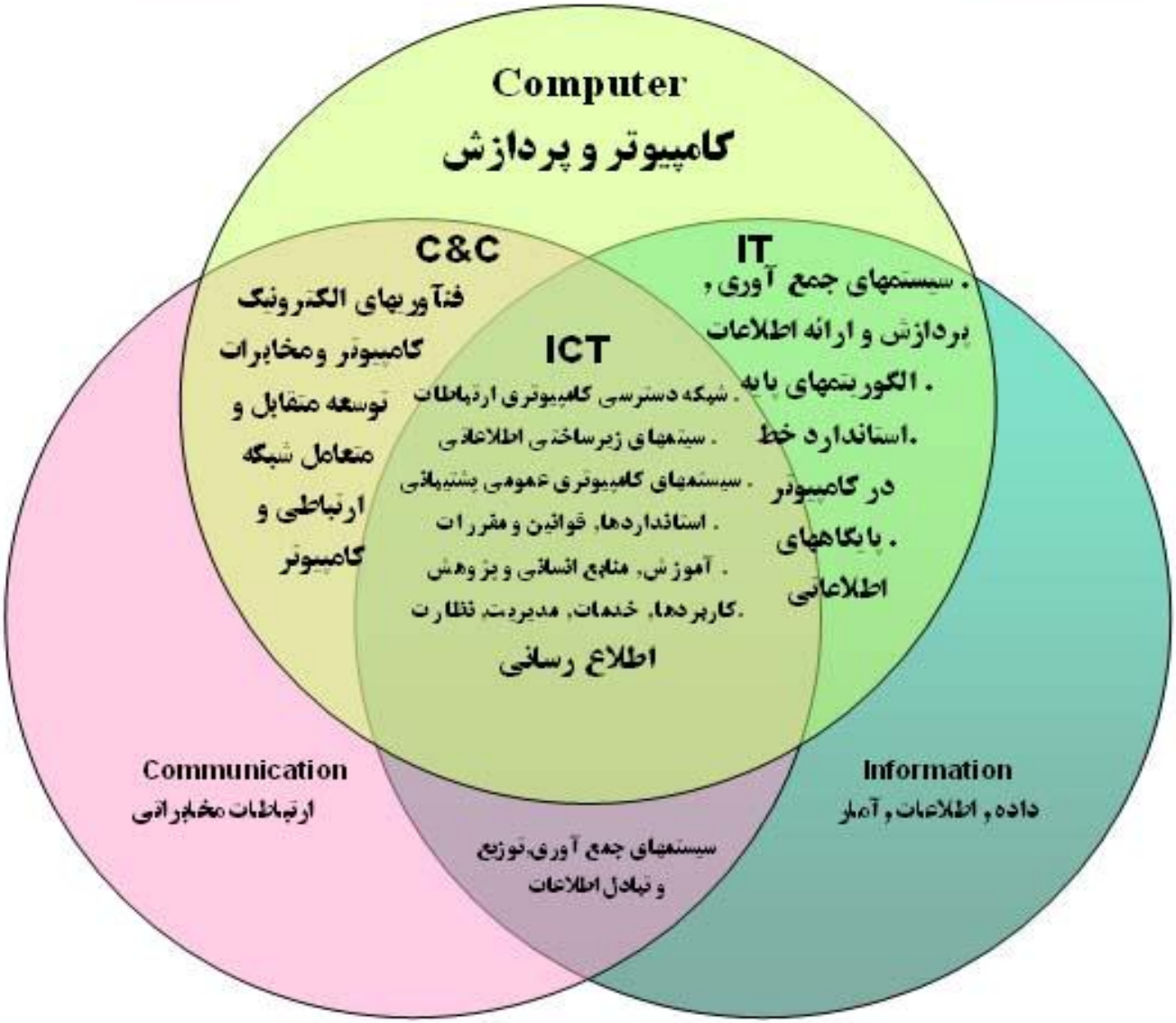
سازمان پدافند غیرعامل کشور
معاونت امور شهری

فناوری اطلاعات و ارتباطات؟!

فرصت یا تهدید ؟!

راهکار(ها)؟!

فن آوری اطلاعات و ارتباطات



ICT : Information and Communication Technology

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فناوری اطلاعات و ارتباطات - ICT

دانش

- ✓**تولید**
- ✓**جمع آوری**
- ✓**ذخیره سازی**
- ✓**تحلیل و پردازش**
- ✓**انتقال**
- ✓**وبهره برداری بهینه**

از اطلاعات(شامل صوت و تصویر و دیتا) **را** **ICT** **گویند.**

سازمان پدافند غیرعامل کشور
معاونت امور شهری

لایه های تشکیل دهنده شبکه

- لایه پسیو شبکه یا لایه فیزیکی (Cabling)
- لایه اکتیو شبکه(Firewall-Sw-Router-...)
- لایه ذخیره سازها(Server-Storage-...)
- لایه نرم افزارها و سامانه ها(OS-Software-...)
- لایه انتقال(ارتباطات)
- لایه بهره برداری(کاربر)

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فناوری اطلاعات و ارتباطات - ICT

دانش

مدیریت صحیح منابع و اطلاعات

(مدیریت دارایی ها)

خدمات فناوری اطلاعات و ارتباطات

- آموزش همگانی
- بهداشت و درمان
- مدیریت سازمانی
- توسعه اقتصادی(تولید ثروت)
- خدمات شهری (اجتماعی و فرهنگی)
- و....

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فناوری اطلاعات و توسعه اقتصادی(تولید ثروت)

توسعه فناوری اطلاعات
بمنظور تولید ثروت

- تبدیل علم به فناوری
- تولید ثروت
- کاهش هزینه
- بهبود کیفیت

سازمان پدافند غیرعامل کشور
معاونت امور شهری

برترین شرکت‌های تجاری(برند) جهان از نظر بیشترین میزان سرمایه

http://www.millwardbrown.com/brandz/

	Category	Brand	Brand value 2013 $M
1	Technology		185,071
2	Technology	Google	113,669
3	Technology	IBM	112,536
4	Fast Food		90,256
5	Soft Drinks	Coca-Cola	78,415
6	Telecoms	at&t	75,507
7	Technology	Microsoft	69,814
8	Tobacco	Marlboro	69,383
9	Credit Card	VISA	56,060
10	Telecoms		55,368

سازمان پدافند غیرعامل کشور
معاونت امور شهری

مهارت نظامی

مهار کردن دشمن بدون رویارویی فیزیکی !

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تغییر ماهیت جنگ ها

از جنگ در فضای سخت و نظامی

به جنگ در فضای فناوری

دلایل اصلی تغییر ماهیت جنگ ها

- کاهش تلفات انسانی(پیروزی بدون خونریزی)
- کاهش هزینه های جنگی
- کاهش زمان عملیات ها
- اثر بخشی بیشتر
- ابعاد گسترده تر(نظامی، اقتصادی، اجتماعی، سیاسی، مذهبی، صنعتی و....)
- امکان بکارگیری از همه مولفه های قدرت
- ریسک کم
- قدرت زیاد در کنترل احساسات

سازمان پدافند غیرعامل کشور
معاونت امور شهری

مقایسه اقتصادی در انواع سلاح ها

هزینه یک فروند بمب افکن Stealth: $1.5 to $2 billion

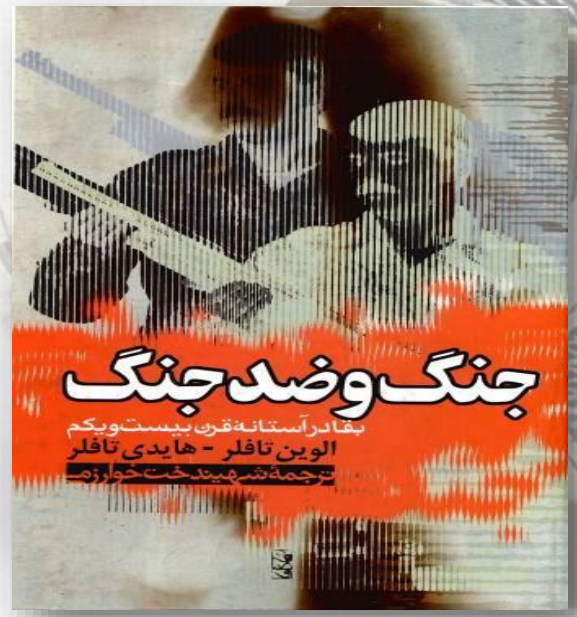
هزینه یک فروند جنگنده Stealth: $80 to $120 million

هزینه یک فروند موشک Cruise: $1 to $2 million

هزینه یک سلاح سایبری: $400 to $50,000

تغییر در شیوه رزم :شیوه جنگ متناسب با شیوه تولید ثروت !

- آلوین تافلر در سال ۱۹۹۳ و در کتاب « جنگ و ضد جنگ» می گوید :



شیوه جنگ در هر کشوری متناسب با شیوه تولید ثروت در آن جامعه است و همان عواملی که باعث دگرگونی اقتصاد کشورها می شوند منشا دگرگونی های نظامی و جنگ نیز می باشند. زمانی که کشورها صنعتی شدند ، نیروهای نظامی رو به تولید ماشین آلات و تجهیزات صنعتی /نظامی و تسلیحات و جنگ افزارهای ماشینی کردند.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فناوری اطلاعات و مدیریت خدمات شهری

- تأمین نیازهای اطّلاعاتی شهروندان، بازرگانان و توریست‌ها از طریق شبکه‌های اینترنتی
- هوشمندسازی کنترل حمل و نقل و ترافیک
- دیدار و گردهمایی‌های مجازی با مدیران شهری
- تفریحات و سرگرمی‌ها و آموزش مجازی
- خدمات مهارت‌آموزی و کارآفرینی مجازی
- ارائه نظام خدماتی مطلوب

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فناوری اطلاعات و مدیریت خدمات شهری

- کاهش فساد اداری از طریق شفاف‌سازی فرایندها.
- کاهش آلودگی هوا با کاهش ترافیک شهری.
- یکپارچه‌سازی سیستم‌های مدیریّتی و عملیاتی شهرداری و سازمان‌های مرتبط.
- صرفه‌جویی در زمان و هزینه.
- ارتباط بهتر با سازمان‌ها و ارگان‌های مختلف شهری.
- دسترسی ۲۴ ساعته به خدمات شهری.
- بهره‌گیری از خدمات اینترنتی با کیفیّت و سرعت بالا

ظهور تهدیدات جدید و از جنس فناوری اطلاعات

به موازات افزایش رفاه عمومی ناشی از قابلیت های فناوری اطلاعات، ظهور تهدیدات جدید و از جنس فناوری اطلاعات و در بستر فناوری در حوزه های مختلف:

- **تهدیدات در حوزه فردی**
- **تهدیدات در حوزه اجتماعی و مردمی**
- **تهدیدات در حوزه شرکت ها و سازمان ها**
- **تهدیدات در حوزه زیر ساخت های اصلی و حیاتی و حساس کشور**
- **تهدیدات در حوزه امنیت ملی**

سازمان پدافند غیرعامل کشور
معاونت امور شهری

مقایسه متوسط سرعت ارتباط با اینترنت (شبکه جهانی)

- کره جنوبی با میانگین سرعت اتصال ۲۲.۵ Mbpsدر مقام اول
- هنگ کنگ۱۷Mbps
- ژاپن۱۶.۵Mbps
- سوئد،سوئیس و هلند با رنج ۱۵Mbps
- لتونی ۱۴.۵Mbps
- ایرلند ۱۴.۱Mbps
- جمهوری چک۱۳.۳Mbps
- فنلاند ۱۳.۱Mbps
- ایالات متحده با میانگین سرعت اتصال۱۲Mbps

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تحول ، یک ضرورت است نه یک انتخاب !

PETER DRUCKER

- سازمانهای موفق امروز آنهایی هستند که به استقبال تغییر می روند . سازمانهایی که هنوز در مقابل تغییر مقاومت می کنند در واقع با قاعده بازی در این عصر آشنا نیستند

.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فصل سوم

معرفی و مروری بر ادبیات و

کارکردهای فضای مجازی(سایبر)

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فضای سایبر (فضای مجازی)

ظهور فضای سایبر به موازات فضای واقعی و فیزیکی

ولی با ویژگی های خاص متکی برفناوری اطلاعات

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تغییر مفاهیم در فضای سایبر

تغییر برخی مفاهیم موجود در فضای سایبر در مقایسه با فضای واقعی:

* زمان
* بعد مسافت(فاصله)
* تعداد
* جنس محصول
* نحوه توزیع
* .....

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تعریف فضای سایبری

اجماع نظر واحدی در زمینه تعریف مفهوم فضای سایبری وجود ندارد و در دنیا با تعاریف بی شماری از این اصطلاح مواجه هستیم.

توماس وینگفیلد در کتاب قانون امنیت ملی در فضای سایبر ، تعریف ساده ای ارائه می کند :

فضای سایبر یک مکان فیزیکی نیست ، به لحاظ بعد فیزیکی یا طیف زمانی هم قابل سنجش نیست . فضای سایبر اشاره به محیطی دارد که از ترکیب و یکی شدن شبکه های کامپیوتری ، سیستم های اطلاعاتی و زیر ساخت های ارتباط از راه دور ایجاد شده که از آن به عنوان شبکه گسترده جهانی یاد می شود.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تعریف فضای سایبری

مرکز پژوهش های کنگره آمریکا نیز در سال ۲۰۰۱ فضای سایبر را این گونه تعریف نمود:

« کلیه ارتباطات موجودات بشری از طریق کامپیوترها و فناوری های ارتباط از راه دور بدون

توجه به جغرافیای فیزیکی »مرکز استراتژی نظامی ملی آمریکا هم فضای سایبر را این گونه

تعریف می کند :

« حوزه ای با ویژگی استفاده از کامپیوترها و دیگر تجهیزات الکترونیک برای ذخیره

سازی،تغییر و تبادل داده ها از طریق سیستم های شبکه ای و زیر ساخت های فیزیکی مربوط

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تعریف فضای سایبری

شبکه های وابسته به یکدیگر، از زیرساخت های فناوری اطلاعات، شبکه های ارتباطی، سامانه های رایانه ای، پردازنده های تعبیه شده ، کنترل کننده های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به منظور تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره برداری از اطلاعات.

این فضا، ممکن است در ارتباط مستقیم و مداوم با سامانه های فناوری اطلاعات و شبکه های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به محیط پیرامونی، در آن تعبیه شده باشد.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تبدیل سرمایه های فیزیکی به سرمایه های سایبری(مجازی)

- زمانی که سرمایه های فیزیکی تبدیل به سرمایه های سایبری گردید، این سرمایه ها می تواند حیاتی، حساس، مهم و فاقد اهمیت باشد، در این صورت بحث آفند و پدافند و امنیت ملی و دفاع از آن ها مطرح می شود.لذا سرمایه های سایبری می تواند منافع ملی و منافع حیاتی را نیز شکل داه و تعریف نماید.

سرمایه سایبری

- در ابتدای کار فضای سایبری یک شبکه داخلی تعریف می شد، ولی بعد از آن که توسعه پیدا کرد و حوزه مختلفی را در بر گرفت و مفهومی به نام سرمایه‌های سایبری کنار سرمایه های فیزیکی، انسانی و معنوی تولید شد، در واقع تعریف فضای سایبری تا اندازه ای متفاوت شد.
- برای مثال ماهیت فیزیکی پول و طلا به ماهیت سایبری و اعتبار در فضای سایبری تبدیل شده، زمانی که مدیریت، کنترل و مراقبت و حفاظت و دفاع از آن در فضای سایبر شکل می‌گیرد، می‌شود ماهیت سایبری یعنی برای دفاع از نظام پولی هم باید حفاظت فیزیکی و امنیتی کرد و هم حفاظت سایبری در واقع سرمایه های فیزیکی در حال تبدیل به سرمایه سایبری است.

سرمایه ملی سایبری(سرمایه فضای مجازی)

بخشی از سرمایه های ملی کشور است که در فضای سایبری قابل حفظ، نگهداری و تهدید می باشد.

سرمایه های ملی سایبری را می توان به سرمایه ملی سایبری حیاتی، حساس و مهم طبقه بندی نمود.

سرمایه های ملی فیزیکی که در فضای سایبر قابل مدیریت، کنترل ومحافظت و تهدید باشد هم سرمایه ملی سایبری محسوب می گردد.

سرمایه ملی سایبری

- یک زیرساخت حیاتی (یا حساس) کشور، یک سامانه حیاتی (یا کلیدی) سایبری و یا اطلاعات حیاتی (یا کلیدی) متعلق به کشور و برخوردار از شرایط ذیل :
- دارای سطح اهمیت حیاتی یا حساس
- دارای کارکرد ملی (فرا استانی)
- برخوردار از اداره متمرکز (اداره زیرساخت، از مرکز کشور انجام می‌گیرد)
- برخوردار از حوزه عملکرد تخصصی
- برخوردار از قابلیت تاثیرگذاری بر امنیت ملی، اقتصاد ملی، سلامت و ایمنی عمومی، اطمینان عمومی و باورهای دینی و ملی

سازمان پدافند غیرعامل کشور
معاونت امور شهری

سطح تهدیدات سایبری

- تهدیدات سایبری، قادر به تاثیرگذاری بر سرمایه های ملی سایبری، در سطوح فراملی، ملی، دستگاهی، استانی، منطقه حیاتی و حساس و زیرساختی می‌باشند.

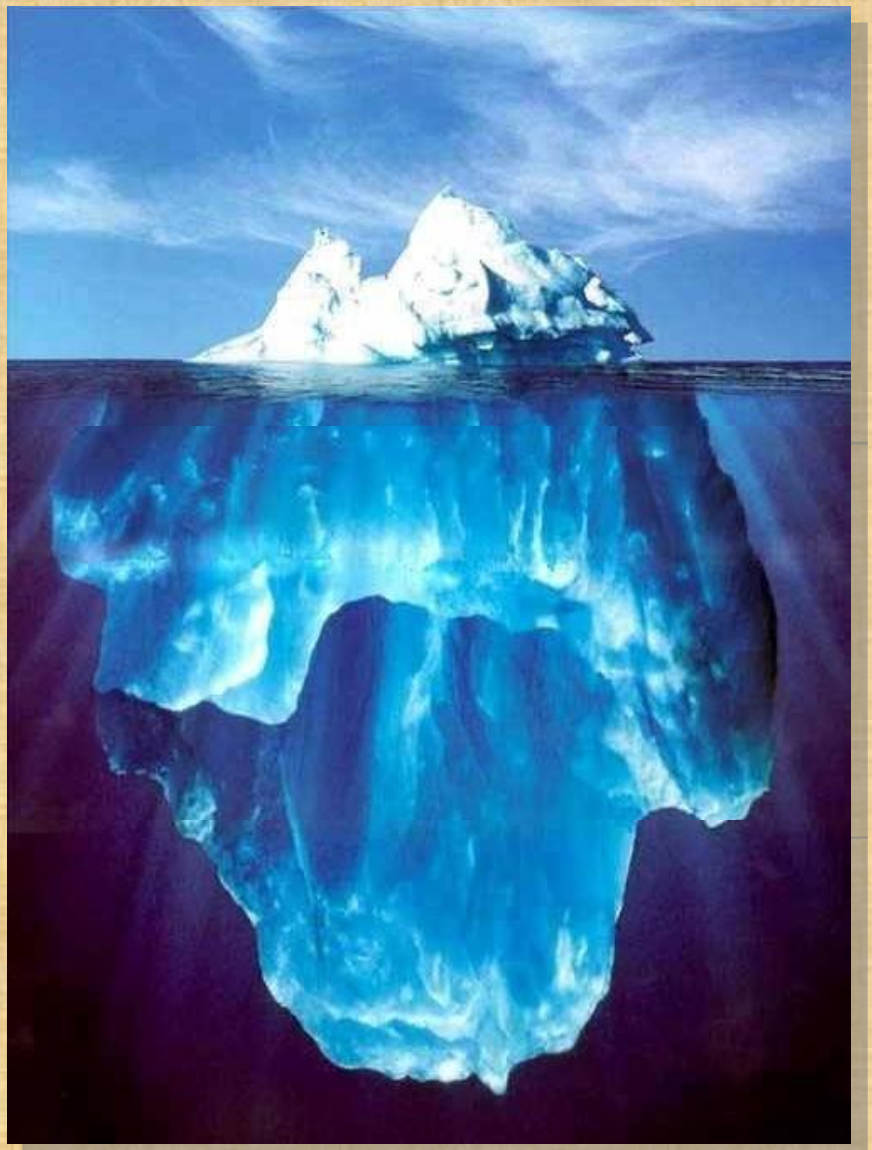
سازمان پدافند غیرعامل کشور
معاونت امور شهری

کوه یخی مخاطرات امنیتی در فضای سایبر

حوزه مخاطره تحت پوشش بازار تجاری امنیت

حوزه مخاطره تحت پوشش سرویس های عمومی امنیت

عمق واقعی مخاطرات فضای سایبر



سازمان پدافند غیرعامل کشور
معاونت امور شهری

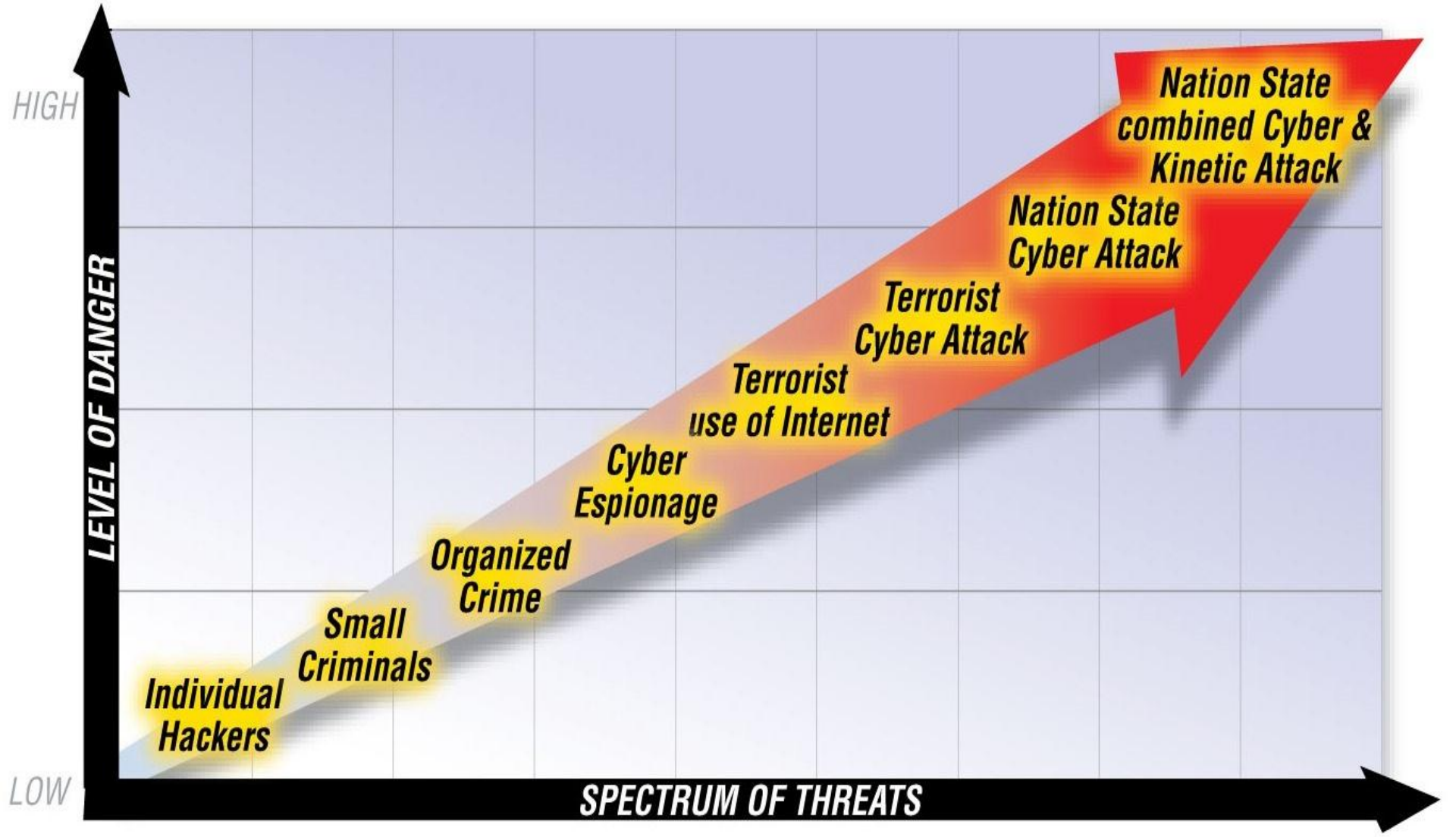
برخی از عمده ترین تهدیدات سایبری(مجازی)

انقلاب اطلاعات در دهه اخیر و رشد فناوری اطلاعات و ارتباطات در عرصه های مختلف جوامع بشری و ظهور فضای سایبر(مجازی) به موازات فضای واقعی و فیزیکی ولی با ویژگی های خاص متکی برفناوری اطلاعات (به عنوان بخشی از سرمایه ملی کشورها) به عنوان بعد پنجم جنگ.

- اختلال در شبکه های ارتباطی و مخابراتی(در سطح ملی – منطقه ای)
- اختلال در شبکه های ریلی ، حمل و نقل و ترافیک
- اختلال در شبکه های آب ، فاضلاب ،برق ،گاز،سوخت(در سطح ملی – منطقه ای)
- اختلال در شبکه پولی ،مالی و بانکی(در سطح ملی – منطقه ای)
- و ....

سازمان پدافند غیرعامل کشور
معاونت امور شهری

طیف کلی تهدیدات سایبری و سطوح رو به افزایش خطر



سازمان پدافند غیرعامل کشور
معاونت امور شهری

برخی آسیب های متصور در حوزه سایبر (فضای مجازی)

- عدم داشتن مراکز میزبانی داده (Hosting) در داخل کشور
- عدم داشتن نرم افزارهای پایه و نرم افزارهای عمومی کاربردی اداری
- عدم توجه به الزامات پدافند غیر عامل در طرح های فناوری اطلاعات و ارتباطات
- عدم رعایت الزامات و استانداردهای امنیتی در طرح های فناوری اطلاعات و ارتباطات کشور

سازمان پدافند غیرعامل کشور
معاونت امور شهری

برخی آسیب های متصور در حوزه سایبر (فضای مجازی)

- عدم وجود محصولات بومی در خصوص امنیت فضای سایبری
- استفاده بخش عمده ایی از زیر ساختهای ارتباطی حیاتی کشور از سیستمها و تجهیزات غیر بومی در زمینه ارتباطات و شبکه
- عدم وجود نرم افزار بومی برای تجهیزات ارتباطی مورد استفاده در شبکه های اصلی ارتباطی
- اتصال شبکه های داخلی سازمان ها به اینترنت

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فصل چهارم

امنیت . دفاع و پدافند

در حوزه سایبری

سازمان پدافند غیرعامل کشور
معاونت امور شهری

پدافند سایبری

- بهره گیری از کلیه امکانات غیرمسلحانه سایبری و غیرسایبری کشور، به منظور ایجاد بازدارندگی، پیش‌گیری، ممانعت از انجام، تشخیص به موقع، مقابله موثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه های ملی سایبری جمهوری اسلامی ایران، توسط متخاصمین سایبری، اعم از نیروی سایبری کشورهای متخاصم و گروه های تحت حمایت پنهان دولت های متخاصم، به نحوی که امکان تهاجم سایبری را از کلیه متخاصمین، سلب نماید.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

کارکردهای اصلی پدافند سایبری

- کاهش آسیب پذیری و ایمن سازی زیرساختهای سایبری
- افزایش پایداری و تولید قدرت در حوزه سایبری
- تداوم فعالیتهای ضروری سایبری کشور
- ارتقاء پایداری ملی زیرساختهای سایبری کشور
- گسترش تولید داخلی و بومی سازی سامانه های مبتنی بر حوزه سایبر
- تسهیل مدیریت بحران در زیرساختهای سایبری کشور

سازمان پدافند غیرعامل کشور
معاونت امور شهری

جنگ سایبری

- جنگ سایبری، بالاترین سطح و پیچیده ترین نوع از تهاجم سایبری است که علیه منافع ملی سایبری کشورها انجام شده و شدیدترین پیامدها را به همراه خواهد داشت.
- یکی از ویژگی‌های اصلی جنگ سایبری، آن است که این نوع از تهاجم سایبری، حتماً توسط ارتش سایبری کشورها انجام می‌گیرد.

نظام دفاع سایبری کشور، مسئولیت دفاع از سرمایه‌های ملی سایبری، در مقابل ستیز (نزاع) سایبری و بویژه جنگ سایبری را بر عهده دارد.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

شاخص های جنگ سایبری

- **منشاء تهاجم سایبری:** یک کشور متجاوز سایبری باشد.

  بکارگیری سلاح سایبری به جای ویروس معمولی

  (دارای پیچیدگی، فرمان پذیری و هوشمندی بسیار زیاد)

- **سطح تهاجم سایبری و خسارت ناشی از آن:** سطح تهدید امنیت ملی

- **شدت تهاجم سایبری:** بسیار زیاد با اختلال و تخریب فاجعه بار
- **پیامد تهاجم سایبری:** اختلال گسترده در عملکرد سرمایه‌های ملی سایبری

برخی ویژگی های جنگ سایبری

- عدم مواجهه با دشمن در جنگ سایبری .....حضور دشمن ناپیدا و مخفی است.
- دشمن در مرزها نیست ..... در عمق استراتژیک حریف وارد می شود.
- نبرد سایبری هوش محور است ..... به تبع آن *انسان پایه* است.
- در جنگ سایبری هدف تصرف سرزمین نیست ..... هدف اختلال، سرقت، جاسوسی، تخریب است.
- از جنگ های سایبری بعنوان جنگ سوم جهانی یاد می شود.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

زمینه سازان جنگ سایبری

- اتکاء زیاد به فناوری غیر بومی
- اعتماد به ابزار و تجهیزات غیر خودی
- وابسته شدن زیرساختهای حیاتی به فناوری آسیب پذیر
- وابسته شدن خدمات حیاتی به بستر اینترنت
- عدم رعایت ملاحظات و توصیه های امنیتی و پدافندی در استفاده از فناوری

نمونه تهدیدات سایبری:

- اختلال در شبکه های مخابراتی کشور اعم ازشبکه ثابت و موبایل و ... (شنود، اختلال، انهدام)
- اختلال درشبکه حمل و نقل و ترافیک کشور (مترو، بین شهری، زمینی، هوایی، راه آهن)
- اختلال در شبکه برق کشور(خروج نیروگاه از مدار)
- اختلال در شبکه گاز (انفجار خطوط لوله، پالایشگاه)
- اختلال و سرقت در شبکه بانکی و مالی کشور
- اختلال در شبکه های صدا و سیما
- و ...

سازمان پدافند غیرعامل کشور
معاونت امور شهری

پیامد های جنگ سایبری

- براندازی نظام حاکمیتی یا تهدید فاجعه‌بار امنیت ملی
- آغاز همزمان جنگ فیزیکی یا زمینه‌سازی و تسهیل شروع جنگ فیزیکی در آینده نزدیک
- تخریب یا صدمه فاجعه‌بار به وجهه کشور در سطح بین المللی
- تخریب یا صدمه فاجعه‌بار به روابط سیاسی و اقتصادی کشور
- تلفات انسانی یا مخاطره گسترده برای سلامت و ایمنی عمومی (از طریق ایجاد آلودگی هسته ای، شیمیایی یا بیولوژیک)
- هرج ومرج و شورش داخلی
- اختلال گسترده در اداره امور کشور
- تخریب (یا صدمه گسترده به) اطمینان عمومی یا باورهای دینی، ملی و قومی
- خسارت شدید به (یا اختلال گسترده در) اقتصاد ملی
- تخریب یا اختلال گسترده در عملکرد سرمایه‌های ملی سایبری

آمریکا و فضای سایبری

- قرارگاه سایبری آمریکا در زمان تأسیس دارای ۱۰۰۰ نفر نیروی متخصص و بودجه‌ای بالغ بر **۱۲۰ میلیون دلار** برای سال ۲۰۱۰ بود.
- بودجه این سازمان در سال ۲۰۱۱، **۱۵۹ میلیون دلار** برآورد گردید.
- بودجه این سازمان در سال ۲۰۱۲، **۳/۲ میلیارد دلار** برآورد گردید.
- بودجه این سازمان در سال ۲۰۱۳، **۷۶۹میلیون دلار** برآورد گردید.
- بودجه این سازمان در سال ۲۰۱۴، **۶/۴ میلیارد دلار** برآورد گردید.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

اقدامات سایبری سایر کشورها

- تشکیل فرماندهی سایبری توسط امریکا با هدف انجام عملیات آفندی و پدافندی در ارتش امریکا و در سطح کلیه نیروهای ارتش
- تشکیل یگان های تخصصی عملیات سایبری در امریکا جهت انجام عملیات تخصصیِ سایبری متشکل از تخصص سایبر و حوزه تخصصی مربوطه (نیروگاه ها، پالایشگاه ها، تاسیسات هسته ای، ارتباطی، بانکی و ....)
- تشکیل یگان های سایبر در اکثر کشورها بویژه : ناتو، انگلیس، ترکیه، رژیم صهیونیستی
- اجرای مانورهای مختلف سایبری در مقاطع مختلف
- انجام حملات سایبری مختلف از قبیل حمله استاکس نت

سازمان پدافند غیرعامل کشور
معاونت امور شهری

قرارگاه پدافند سایبری کشور

از سال ۱۳۹۰ به منظور مقابله با تهدیدات سایبری دشمن و امن سازی زیرساخت های سایبری کشور، قرارگاه پدافند سایبری کشور توسط سازمان پدافند غیر عامل کشور و با هدف راهبری و هدایت دستگاه های اجرایی کشور جهت این امر مهم تشکیل گردید.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

ادامه قرارگاه پدافند سایبری

براساس ابلاغیه قرارگاه پدافند سایبری، کلیه دستگاه های اجرایی کشور، پس از تعیین سطح اهمیت سرمایه های سایبری خود، موظف به امن سازی زیرساخت های حیاتی، حساس و مهم سایبری خود بوده و به منظور آمادگی جهت مقابله با حملات سایبری دشمن، نسبت به ایجاد مراکز پدافند سایبری در سطح وزارتخانه ها، سازمان ها، استان ها و مناطق ویژه اقدام نمایند.

سازمان پدافند غیرعامل کشور
معاونت امور شهری

تهدیدات سایبر الکترومغناطیسی

- یکپارچگی و همزمانی فعالیت های سایبری و الکترومغناطیسی مفهوم جدیدی به نام سایبرالکترومغناطیس بوجود آورده است.
- اقدامات سایبر الکترومغناطیسی، به منظور ضبط، حفظ و بهره برداری از برتری های موجود علیه دشمنان و حریفان در فضای سایبری و طیف الکترومغناطیسی و به طور همزمان، جلوگیری و مانع تراشی در برابر بهره برداری دشمن از همان امکانات و حفاظت از سامانه فرماندهی صورت می گیرد.
- این اقدامات شامل: عملیات فضای سایبری، جنگ الکترونیک و عملیات مدیریت طیف می باشد.

سناریو (۱): شناسایی به منظور تهاجم سایبری با حمایت دولتها با هدف جمع آوری اطلاعات برای برنامه ریزی تهاجم های سایبری بعدی

در این سناریو، تهاجم سایبری، وسیله ای است برای دستیابی به اطلاعات مستند و معتبر در خصوص یک موضوع مشخص. اطلاعاتی که از طریق جاسوسی سایبری بدست می آید، در مراحل بعدی، برای برنامه ریزی و انجام تهاجم سایبری یا تهاجم فیزیکی، مورد استفاده قرار خواهد گرفت.

سناریو (۲) : یورش سایبری با هدف بسترسازی برای هرج ومرج و شورش مردمی

در این سناریو، تهاجم سایبری با هدف تخریب یا ایجاد اختلال گسترده در زیرساختهای حیاتی کشور هدف، ایجاد اختلال در اداره امور کشور و بسترسازی برای شورش مردمی از داخل کشور هدف، انجام می گیرد.

تمرکز اصلی تهاجم های مبتنی بر این سناریو، زیرساخت های حیاتی کشور هدف خواهد بود.

زیرساختهای اقتصادی و بانکی، انرژی (بویژه در فصل سرما)، برق و ارتباطات، از جمله اهداف مهم تهاجم های مبتنی بر این سناریو محسوب می گردند.

سناریو (۳) : یورش (تهاجم) سایبری با هدف از کار اندازی تجهیزات و تسهیل تهاجم فیزیکی

در این سناریو، هدف از انجام تهاجم سایبری، انهدام، ایجاد اختلال و از کار انداختن زیرساختهای حیاتی یا سامانه های خاص (از قبیل سامانه های پدافند هوایی یا موشکی) کشور هدف، به قصد کاهش توان پاسخ به حملات آن کشور می باشد تا از این طریق، بتوان انجام تهاجم فیزیکی به کشور هدف را تسهیل نمود.

بر اساس این سناریو، تهاجم سایبری، مقدمه تهاجم فیزیکی است و لذا هدف این سناریو، کاهش توان دفاع فیزیکی و بویژه بازدارندگی دفاعی کشورها است.

سناریو (۴) : یورش (تهاجم) سایبری به عنوان مکمّل تهاجم فیزیکی

در این سناریو، تهاجم سایبری، تقریباً همزمان و یا کمی زودتر از تهاجم فیزیکی انجام می گیرد و هدف آن نیز مختل نمودن سامانه های راهبردی کشور هدف است که در جنگ فیزیکی قابل استفاده خواهند بود.

با عنایت به همزمانی تهاجم سایبری و تهاجم فیزیکی، کشور مهاجم، عمدتاً عملیات تهاجم سایبری را توام با فریب انجام نداده و تهاجم سایبری، مستقیماً از آدرس های IP کشور مهاجم صورت خواهد گرفت.

از سوی دیگر، شدت این نوع از تهاجم های سایبری، از سه سناریو قبلی، بالاتر خواهد بود. از سوی دیگر، بخشی از این نوع تهاجم های سایبری، متوجه توان تهاجم و دفاع فیزیکی کشور هدف تهاجم خواهد بود.

بر این اساس، بخشی از تهاجم سایبری، مصروف شناسایی آسیب پذیریهای حیاتی سرمایه های هدف تهاجم خواهد شد.

سناریو (۵) : یورش (تهاجم) سایبری با هدف تخریب یا اختلال گسترده به عنوان هدف نهایی جنگ سایبری

در این سناریو، هدف نهایی، باید توسط تهاجم سایبری محقق گردد و هیچ عامل فیزیکی (از جمله مردم کشور هدف یا نیروی نظامی کشور مهاجم سایبری) در تحقق این اهداف، نقشی نخواهد داشت.

تهاجم های سایبری مبتنی بر این سناریو، قاعدتاً کلیه شرایط ایجاد هشدار سطح (۱) که در بخش قبل، به عنوان شرایط وقوع جنگ سایبری مطرح نمودیم را خواهند داشت.

عرصه های عمده جنگ سایبری

- زیرساخت های حیاتی وحساس کشور
  - هسته ای
  - برق
  - آب
  - گاز
  - نفت
  - صنعت
- زیر ساخت های دفاعی و امنیتی
- زیر ساخت های بانکی و مالی و پولی کشور
- زیر ساخت های ارتباطی و رسانه ای کشور
- زیر ساخت های خدمات مردمی
- زیر ساخت های درمان و بهداشت و سلامت کشور

شاخص های تهدید در حوزه دفاع سایبری

- تهدید کننده یک دولت یا گروه وابسته به دولت متخاصم باشد.
- تهدید علیه امنیت ملی کشور باشد
- تهدید علیه زیر ساخت های حیاتی وحساس کشور باشد
- حوزه تاثیر تهدید در مقیاس ملی و یا منطقه ای باشد
- پیامد های تهدید به تلفات وخسارت عمده اقتصادی بیانجامد
- تهدید برعلیه یک حوزه عمده وتاثیر گذار باشد
- پیش درآمد یک تهاجم نظامی باشد

سازمان پدافند غیرعامل کشور
معاونت امور شهری

راهبردهای نظام پدافند سایبری کشور

- مصون سازی زیرساخت های حیاتی و حساس کشور در مقابل تهدیدات و حملات سایبری
- ایجاد و توسعه نظام های مورد نیاز پدافند سایبری
- ارتقاء کمی و کیفی منابع انسانی حوزه پدافند سایبری
- ارتقاء سطح آگاهی، دانش و مهارتهای بومی و فرهنگ سازی در حوزه پدافند سایبری
- تقویت صنعت بومی و توسعه خدمات و محصولات روزآمد پدافند سایبری


چرخه
پدافند
سایبری
رصد، پایش و تشخیص تهدید
استخراج آسیب پذیری
تجزیه و تحلیل ریسک
مدیریت دفاعی صحنه
بازیابی اطلاعات
ایمن سازی و پایدارسازی
مصون سازی سایبری
ارتقاء آمادگی پدافند سایبری
تولید قدرت پاسخ گویی به تهدید
به روزسازی تهدیدات و مقایسه با وضع موجود
به روزسازی اقدامات پدافند سایبری

سازمان پدافند غیرعامل کشور
معاونت امور شهری

جهت‌گیری کلان پدافند سایبری

- حذف و یا کاهش آسیب پذیری تأسیسات و تجهیزات حیاتی، حساس و مهم و نیز زیرساخت های ارتباطات و فن آوری اطلاعات در مقابل تهدیدات دفاعی و امنیتی
- پایدارسازی ارتباطات بین‌المللی، ملی، منطقه ای و محلی
- پایدارسازی فعالیت شبکه‌های ارتباطی و الکترونیکی برای استمرار جریان اطلاع رسانی عمومی
- پاسداری از آرامش و امنیت روانی جامعه از طریق حفظ بستر ارتباطات مردم (مخابرات) و ظرفیت فعال اطلاع رسانی (صدا و سیما)
- ایجاد یأس در دشمن در تحقق اهداف خصمانه خود

سازمان پدافند غیرعامل کشور
معاونت امور شهری

فصل پنجم

مطالعات موردی

سازمان پدافند غیرعامل کشور
معاونت امور شهری

وضعیت بد افزارها

- هوشمند تر
- مرموز تر
- پنهان تر

نفوذ سایبری در گوشی های هوشمند و تبلت ها

مراقبت:
- صوت
- دوربین
- ثبت تماس ها
- مکان
- پیامک
- شنود

جعل هویت:
- تغییر مسیر پیامک
- ارسال پیامک های ایمیل
- ارسال به رسانه های اجتماعی

مالی:
- ارسال پیامک های مرتبط با پرداخت
- سرقت اطلاعات تصدیق هویت تعاملات مالی
- اخاذی از طریق بد افزارهای خاص (Ransomware)
- آنتی ویروس جعلی
- برقراری مکالمات پرهزینه

سرقت اطلاعات:
- جزئیات حساب بانکی
- فهرست مخاطبان
- اطلاعات ثبت تماس ها
- شماره تلفن
- سرقت اطلاعات ار طریق آسیب پذیری برنامه ها
- سرقت شماره بین المللی شناسایی موبایل (IMEI)
- سرقت کلمات عبور
- سرقت اطلاعات شخصی
- سرقت اطلاعات بیومتریک اثر انگشت

نفوذ:
- در سیستم عامل
- دربهای پشتی

فعالیت های بات نتی:
- راه اندازی حملات DDOS
- کلاه برداری مالی از طریق کلیک کردن مکرر
- ارسال پیامک های مرتبط با پرداخت

سازمان پدافند غیرعامل کشور
معاونت امور شهری

شبکه های اجتماعی مبتنی بر موبایل

وایبر(Viber)

- توسط یک شخص آمریکایی-اسرائیلی به نام Talmon Marcoطراحی شده است.
- کاربران وایبر در حدود ۶۰۸ میلیون
- **پشت پرده نرم افزار:**
  - دسترسی به اطلاعات مکانی کاربر
  - دسترسی به اطلاعات دفترچه تلفن،شامل نام و تلفن ،اطلاعات تماس ها
  - خواندن پیامک ها،حتی اگر توسط وایبر ارسال نشده باشد.
- ویرایش وخواندن اطلاعات آشنایان، تغییر یا حذف محتویات کارت حافظه
- ضبط صدا، گرفتن عکس ،دسترسی به برنامه‌های در حال اجرا

سازمان پدافند غیرعامل کشور
معاونت امور شهری

شبکه های اجتماعی مبتنی بر موبایل

واتس آپ (Whatsapp)

- توسط یک شخص آمریکایی و دیگری اکراینی که هر دو از کارمندان Yahoo بوده اند در سال ۲۰۰۹طراحی شده است .

- **پشت پرده نرم افزار:**
  - ذخیره اطلاعات شخصی در سرورهای خود
  - اطلاعاتی را بر روی سرورهای خود همچون لیست مخاطبین که کاربر واتس آپ نیستند را نگهداری میکنند.
  - نگهداری پیامک ها در سرور برای مدت ۳۰روز
  - مکالمات را روی وب سایت های دیگر بعنوان بک آپ قرار می دهد.