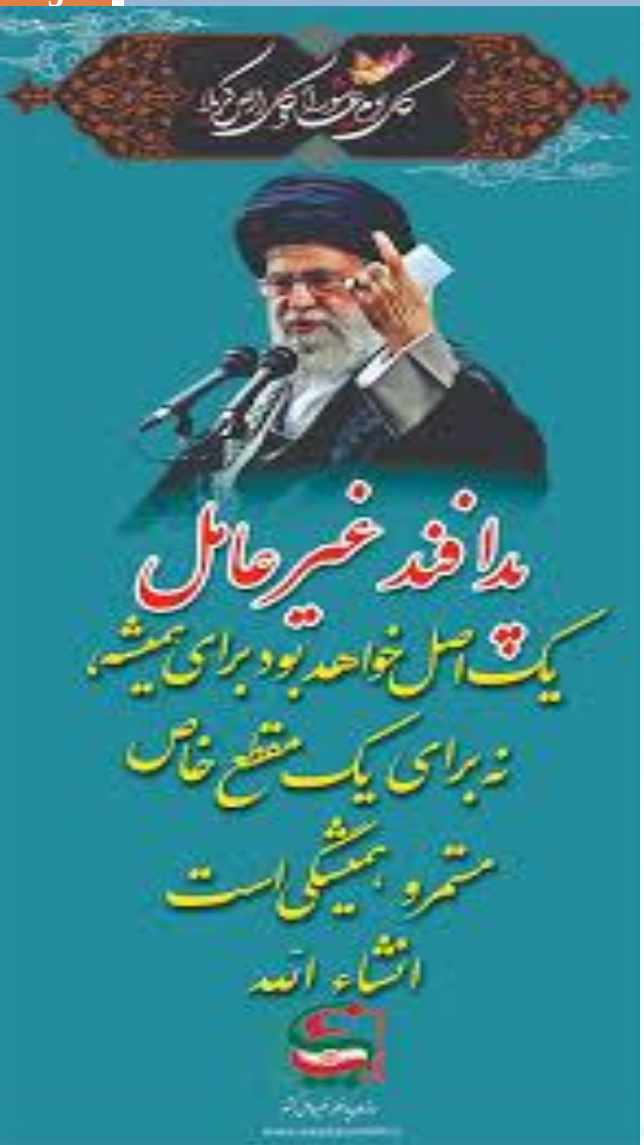
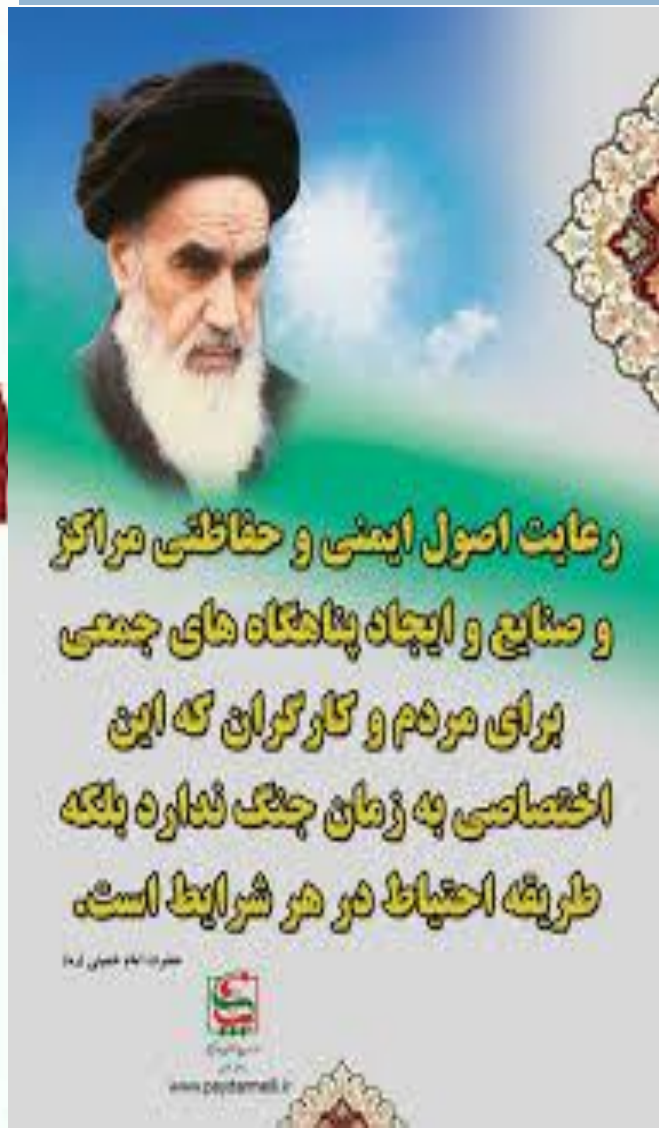
هُوَاللّٰه

هُوَاللّٰه

اصول و مبانی پدافند سایبری

فرمایشات امام ره و مقام معظم رهبری





فهرست مطالب اصول و مبانی پدافند سایبری

- آشنایی با مفهوم سایبر و فضای سایبر
- سناریو های تهدید معیار و دشمن شناسی
- تهدیدات سایبری
- تحلیل پیامد تهدیدات
- تحلیل آسیب پذیری ها
- تحلیل و ارزیابی تهدید ها
- تحلیل مخاطرات و تاب آوری
- مدیریت مخاطرات و تاب آوری
- پدافند سایبری

فهرست منابع و مراجع مورد استفاده

- سند راهبردی پدافند سایبری کشور
- راهنمای تهیه برنامه عملیاتی تداوم کارکرد و بازیابی زیر ساخت ها ، ابلاغیه فرماندهی کل قوا – کمیته دائمی پدافند غیر عامل کشور
- طرح راهبردی حفاظت از زیر ساخت‌های حیاتی کشور ، ابلاغیه فرماندهی کل قوا – کمیته دائمی پدافند غیر عامل کشور،
- کتاب الزامات و ملاحظات پدافند غیر عامل مراکزداده، سند ۱۲۰۱ –نظام فنی و اجرایی پدافند غیر عامل، مهرماه ۱۳۹۹.
- کتاب مباحث تخصصی فنی پدافند سایبری،جلد۳، دکتر محمود خالقی دخت ، دی ۱۳۹۷
- کتاب مباحث تخصصی فنی پدافند سایبری،جلد۴، دکتر محمود خالقی دخت ، دی ۱۳۹۷
- کتاب تهدید سایبری و پدافند سایبری ، مهندس رحمت اله امیرصوفی، مهندس حمید اسکندری،۱۳۹۵
- پروژه امکان سنجی تدوین استراتژی دفاع اطلاعاتی، مهندس رحمت اله امیرصوفی، دکتر حمید شهبازی و مهندس سید محمدرضوی عمرانی، دانشگاه صنعتی مالک اشتر،اسفند ۱۳۸۹
- کتاب اصول و مبانی پدافندسایبری تالیف دکتر غلامرضا جلالی ، دکتر فردرو و مهندس پارسا،۱۳۹۵ استفاده شده است.

فهرست مطالب

- آشنایی با مفهوم فضای سایبر
- ساختار و مؤلفه‌های فضای سایبر
- سرمایه سایبری و سرمایه ملی سایبری
- فضای سایبر ملّی، قلمرو ملی سایبری یا قلمرو کشور در فضای سایبر
- ویژگی‌های فضای سایبر

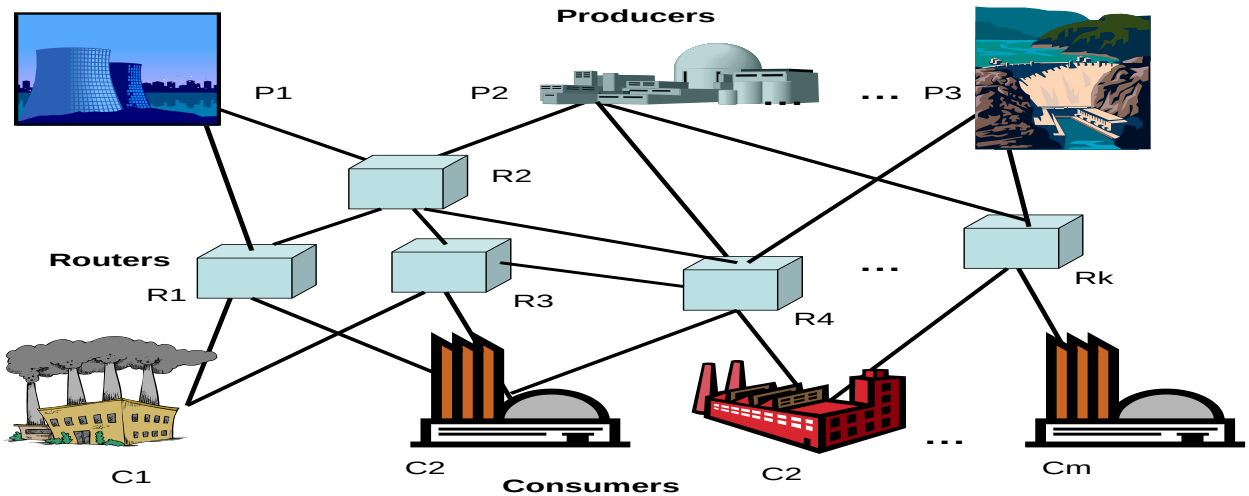
آشنایی با مفهوم فضای سایبر

- فضای سایبر به عنوان بستر ارتباطات و فناوری اطلاعات
- فضای سایبر به عنوان زیرساخت و محرّک توسعه کشور
- فضای سایبر به عنوان فضای کسب‌وکار
- فضای سایبر به عنوان زیست‌بوم سایبری
- فضای سایبر به عنوان زیرساخت حیاتی و سرمایه ملی
- فضای سایبر به عنوان قلمرو حاکمیتی
- فضای سایبر به عنوان مؤلفه‌ی امنیت ملی

آشنایی با مفهوم سایبر

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.



فضای سایبر به عنوان زیست‌بوم سایبری

- هرگونه تهدید فضای سایبر که منجر به تأثیر فاجعه بار بر فضای سایبر به عنوان زیست بومِ اطلاعات است، باید مورد توجه پدافند سایبری قرار گیرد و
- متقابلاً اجرای هرگونه فعالیت مرتبط با پدافند سایبری به منظور تأمین و تداوم امنیت و مصونیّت فضای سایبر،باید باشد .
- لذا رعایت اصول تضمین کننده ی تداوم عملکرد فضای سایبر به عنوان زیست بومِ اطلاعات و تداوم تعاملات فضای سایبر با دنیای واقعی به عنوان زیست بومِ انسان بایستی انجام گیرد.

فضای سایبر به عنوان بستر ارتباطات و فناوری اطلاعات

- واژه فضای سایبر، اولین بار در سال ۱۹۸۴، توسط ویلیام گیبسون در یک رمان علمی‌تخیّلی به نام نورومانسر ، برای اشاره به دنیای مجازی ارتباطات رقومی ابداع شد. دنیایی که در آن، انسانها به جای ارتباط ؟؟ ، با یکدیگر به صورت الکترونیکی و از طریق امواج رادیویی و شبکه های رایانه ای در ارتباط بودند.
- اولین کارکرد مورنظر انسان از فضای سایبر، بستر ارتباطی بود
- با توسعه پردازش و رایانش اطلاعات یا فناوری اطلاعات در کنار موضوع ارتباطات ، کارکرد اصلی فضای سایبر، به موضوع ارتباطات و فناوری اطلاعات تبدیل شد.
- فضای سایبر متشکل ازبعد فنی شامل

سه مؤلفه ی اصلی، شامل شبکه های ارتباطی، سامانه های اطلاعاتی و اطلاعات است

- و در یک تعریف جامع متشکل از پنج مؤلفه ی تجهیزات شبکه ، خدمات شبکه ، خدمات کاربردی ، خدمات محتوایی و محتوا می باشد .

- تولید و عرضه ی محصولات سایبری اعم از سخت افزارها و نرم افزارها،

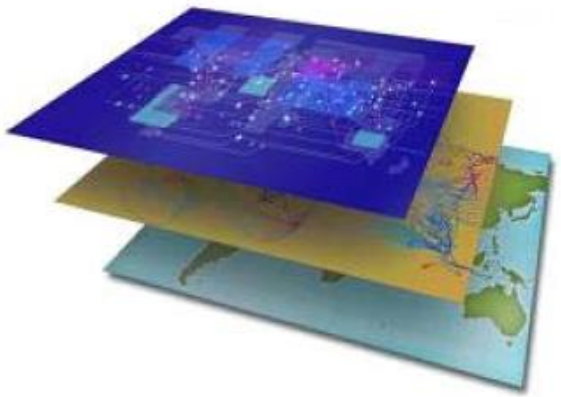
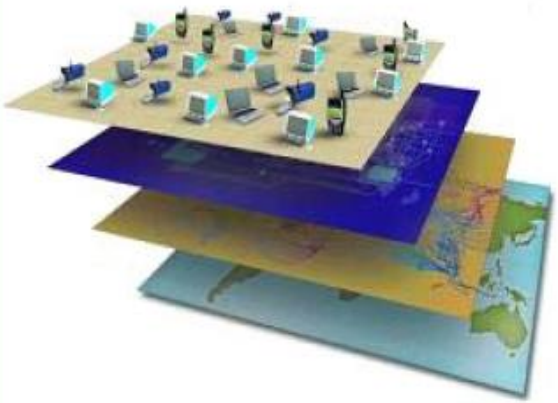
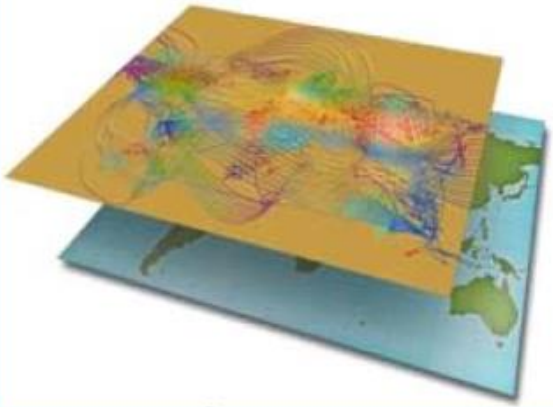
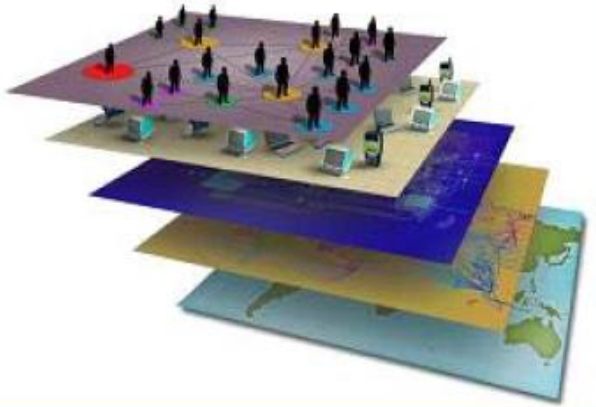
عرضه ی خدمات سایبری از قبیل

- اپراتورهای تلفن ثابت و تلفن همراه، اپراتورهای ارتباطات بی سیم
- عرضه ی خدمات میزبانی (مراکز داده)،
- عرضه ی خدمات رایانش ابری،
- مدیریت فضای سایبر،
- امنیت فضای سایبر و پدافند سایبری اشاره نمود.

فضای سایبر به عنوان زیرساخت و محرّک توسعه کشور

- خدمات الکترونیکی
- پست الکترونیکی(e- mail)
- تجارت الکترونیکی
- آموزش الکترونیکی
- دولت الکترونیکی
- شهروند الکترونیکی
- شهر الکترونیکی

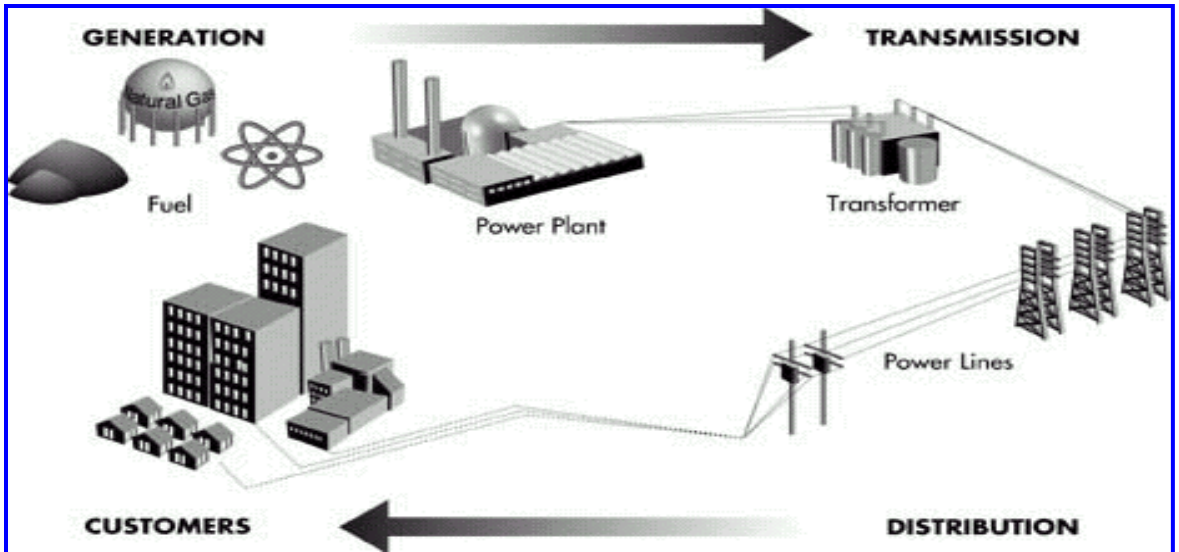
مدل مفهومی، شامل ساختار و مؤلفه های فضای سایبر

Physical Layer	Logical Layer	Social Layer
Geographic Components	Logical Network Components	Persona Components
		
Physical Network Components		Cyber Persona Components
		

سرمایه سایبری

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

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



سرمایه ملی سایبری

سرمایه ملی

به سرمایه‌ای اطلاق می‌گردد که نقش حیاتی یا حساس در امنیت ملی، اقتصاد ملی و سلامت، ایمنی و اطمینان عمومی داشته باشد

طبقه بندی سرمایه های ملی

سرمایه‌های فیزیکی

سرمایه‌های انسانی

سرمایه‌های سایبری

سرمایه‌های ذهنی یا اعتباری

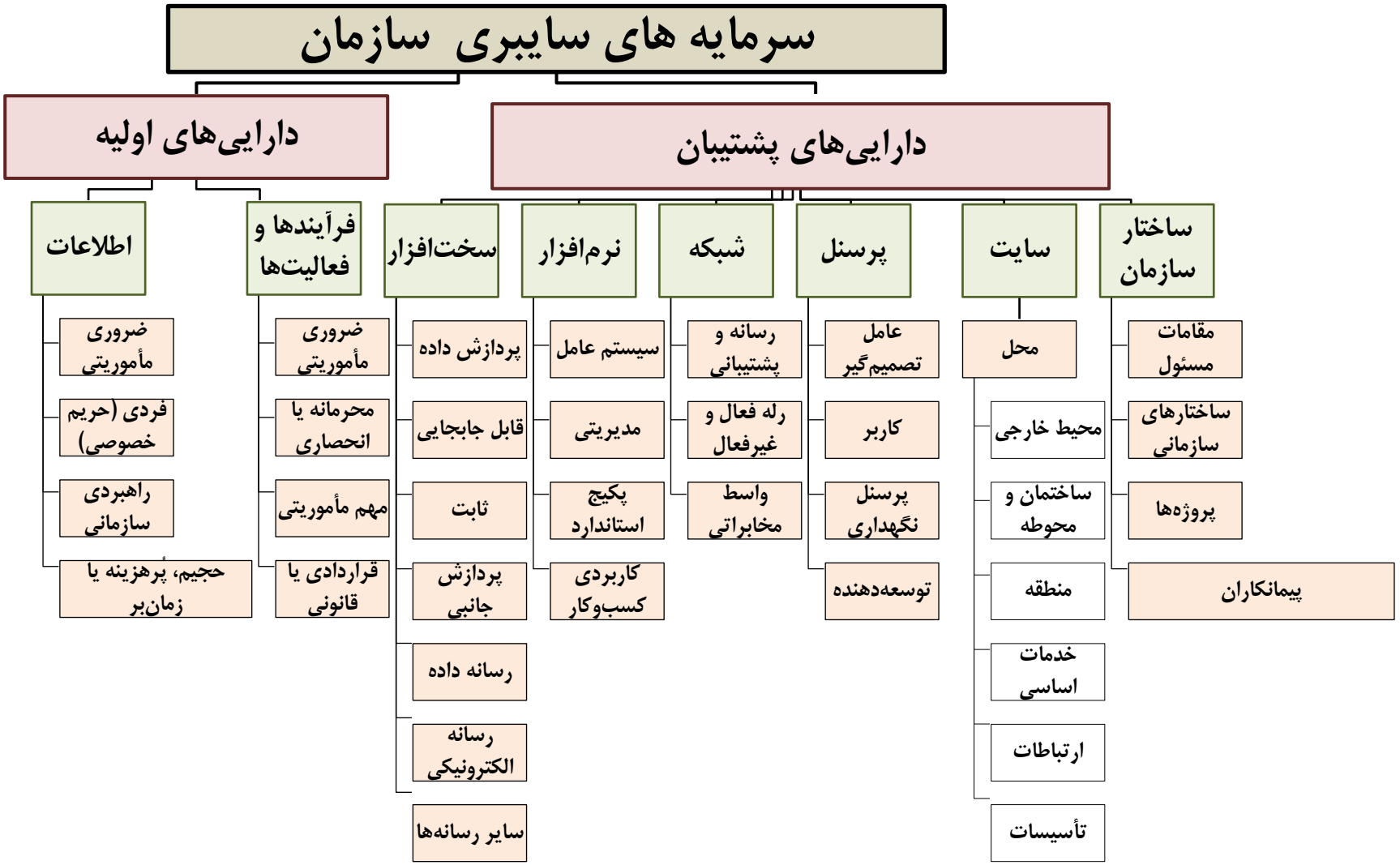
سرمایه ملی سایبری

زیرساخت‌های سایبری حیاتی یا حساس

سامانه‌های سایبری حیاتی یا حساس

اطلاعات سایبری حیاتی یا حساس

نمونه‌های طبقه‌بندی سرمایه‌های سایبری



روش پیشنهادی برای طبقه‌بندی سرمایه‌های سایبری

ماهیت		
دسته اصلی	دسته فرعی	نوع
زیرساخت سایبری	زیرساخت ارتباطی	کابل‌های مسی ، خطوط فیبر نوری
		تجهیزات ارتباط رادیویی / ماهواره‌ای
		تجهیزات مدیریت شبکه (سوئیچ‌ها، مسیریاب‌ها و..)
		تجهیزات امنیت شبکه (I?S، فایروال ، U??، W?F)
	زیرساخت رایانشی	تجهیزات مرکز داده
		تجهیزات خدمات ابری
		سرویس‌دهنده‌ها
		ایستگاه‌های کاری
	زیرساخت نرم‌افزاری	شبکه‌ی نرم‌افزار تعریف (SDN)
		سیستم عامل تجهیزات ارتباطی / رایانشی / سرویس‌دهنده‌ها / میزبان‌ها
	زیرساخت محتوایی	شبکه تحویل محتوا (CDN)
		سامانه‌های ذخیره‌سازی محتوا
		درگاه خدمات اینترنتی
	زیرساخت تشکیلاتی	تشکیلات مدیریت زیرساخت / خدمات / محتوا
		تشکیلات امنیت زیرساخت / خدمات / محتوا

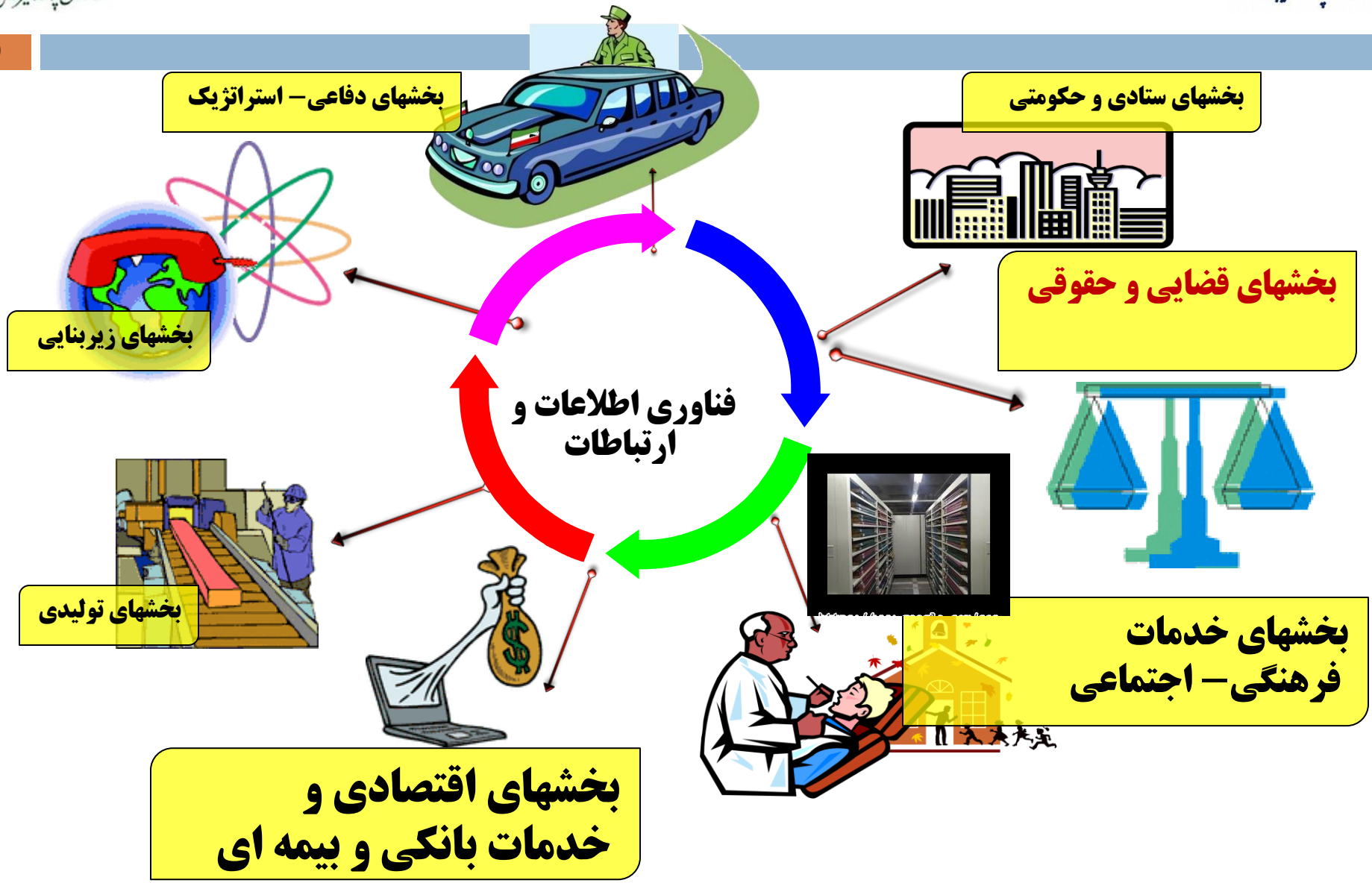
روش پیشنهادی برای طبقه‌بندی سرمایه‌های سایبری

ماهیت		
دسته اصلی	دسته فرعی	نوع
خدمات سایبری	خدمات ارتباطی	خدمت ارتباطی بدون پروتکل / ارتباطی مبتنی بر پروتکل IP
		شبکه خصوصی مجازی
		خدمت ابری IaaS
	خدمات رایانشی	خدمات میزبانی در مرکز داده
		خدمات ابری PaaS
		خدمات اشتراک‌گذاری اطلاعات
	خدمات نرم‌افزاری پایه	خدمات نام دامنه / پیام‌رسانی / مرور وب / پست الکترونیکی
		خدمات جویش اینترنتی / پرداخت اینترنتی / ابری SaaS
	خدمات محتوایی	خدمت تأمین و تحویل محتوای متنی / صوتی / ؟ زنده
		خدمت تأمین و تحویل محتوای ؟/؟/ ویدیوئی مبتنی بر تقاضا
		پایگاه داده متنی / صوتی /تصویری /ویدیوئی
	پرسنل سایبری	پرسنل مدیریت زیرساخت/ خدمات/ محتوا
		پرسنل امنیت زیرساخت/ خدمات/ محتوا
		کاربران خدمات ارتباطی / رایانشی /نرم‌افزاری / محتوایی

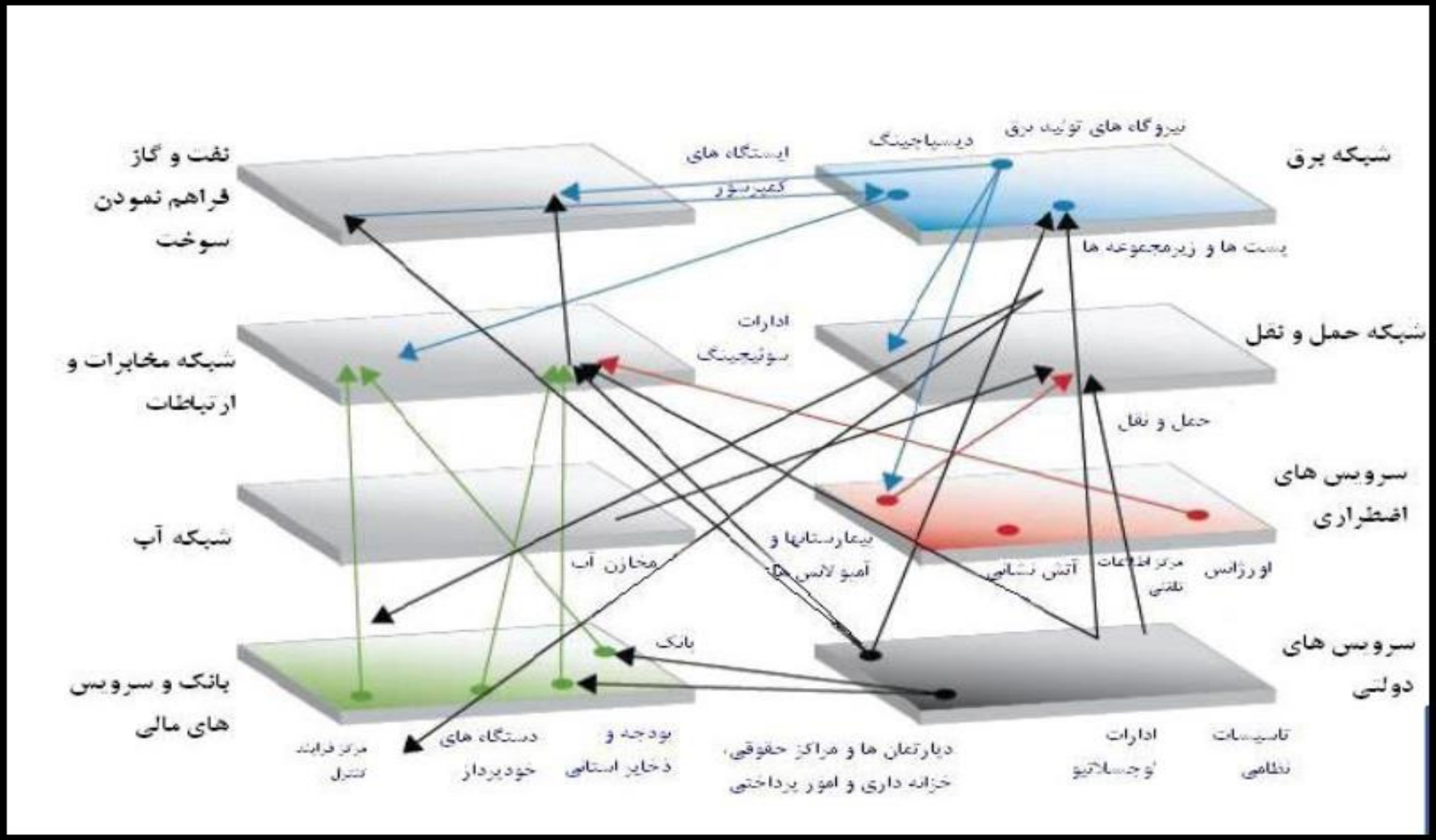
توصیه‌های ضروری در مدیریت صحیح سرمایه‌های سایبری

- تهیه لیست کامل و دسته‌بندی شده‌ای از کلیه سرمایه‌های سایبری سازمان،
- برای هر یک از سرمایه‌های سایبری موجود در لیست، ارزش اقتصادی تقریبی، شامل هزینه‌ی خرید، تست، نصب، راه‌اندازی و ورود اطلاعات را محاسبه و درج نمائید.
- طبقه‌بندی ۵ سطحی ارزش اقتصادی سرمایه‌های سایبری سازمان
- طبقه‌بندی ۵ سطحی میزان حساسیت یا اهمیت آن سرمایه سایبری در ارتباط با اجرای مأموریت‌های سازمان
- بازنگری و به‌روزرسانی اطلاعات لیست تهیه شده از سرمایه‌های سایبری سازمان
- لیست تکمیل‌شده‌ی سرمایه‌های سایبری، حاوی اطلاعات ارزشمندی است و حتماً باید جزء اسناد طبقه‌بندی شده محسوب گردد.

نفوذ فناوری اطلاعات در کلیه عرصه‌ها و وابستگی متقابل زیرساخت ها



وابستگی متقابل زیرساخت ها



فضای سایبر از منظر تهدیدات نوین

- سرقت الکترونیکی
- جاسوسی الکترونیکی
- تهدیدات الکترونیکی
- سرباز الکترونیکی
- حملات الکترونیکی
- ارتش سایبری
- .....

معماری فنی اینترنت اشیاء

IoT

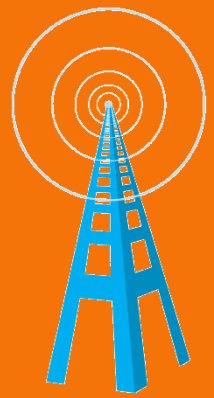
اینترنت افراد
(شبکه ها و
رسانه های
اجتماعی)

اینترنت سرویس
(وب نسل ۲
و امکان تولید محتوا
توسط کاربران)

اینترنت محتوا
(وب نسل ۱
بر روی بستر
اینترنت سنتی)

قبل از اینترنت
(ارتباطات
انسان به انسان)

شبکه مخابراتی
ارتباطی



بستر ابری

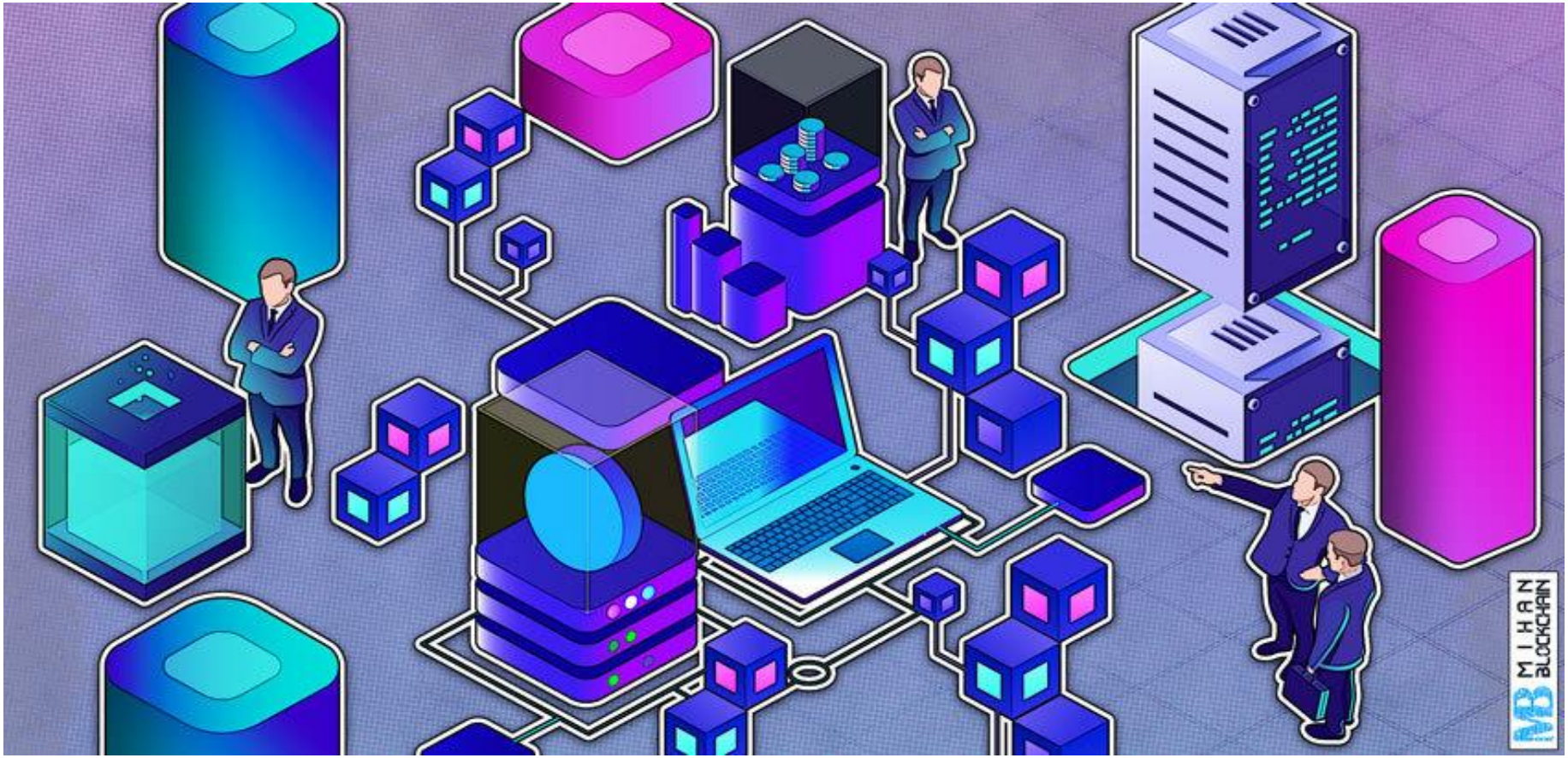
برنامه های
کاربردی

سخت افزار

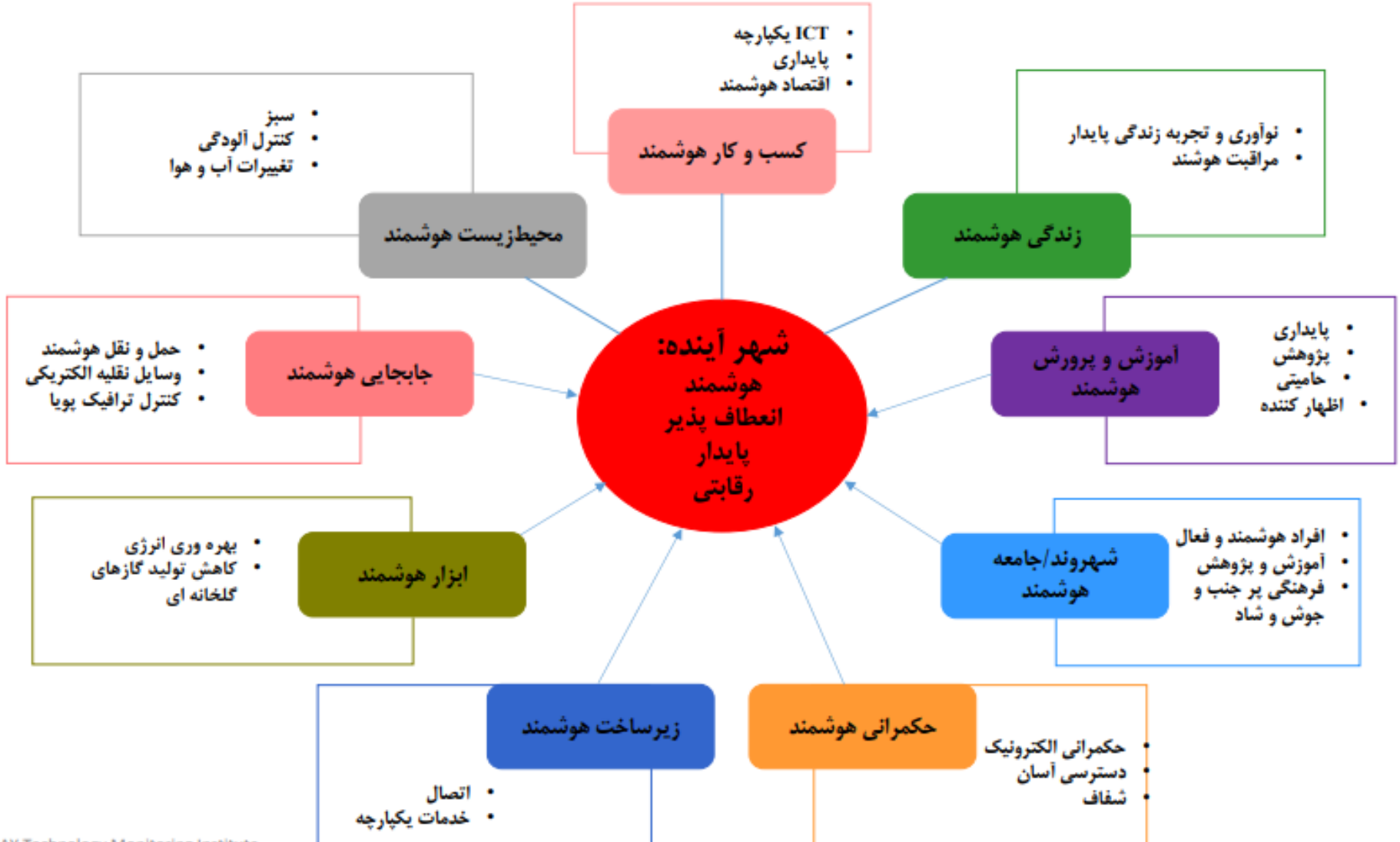
کاربردهای اینترنت اشیاء

اینترنت اشیاء می تواند از نقش شایانی در حوزه هایی همچون سلامت الکترونیک، شهر هوشمند، خانه هوشمند، امنیت شهری، خدمات خودرویی، مدیریت هوشمند انرژی از جمله برق، تدارکات هوشمند، مانیتورینگ محیطی و... برخوردار باشد

فناوری بلاک چین و رمز ارز دیجیتال



شهر هوشمند


شهر آینده:
هوشمند
انعطاف پذیر
پایدار
رقابتی
کسب و کار هوشمند
ICT یکپارچه
پایداری
اقتصاد هوشمند
زندگی هوشمند
نوآوری و تجربه زندگی پایدار
مراقبت هوشمند
آموزش و پرورش هوشمند
پایداری
پژوهش
حامیتی
اظهار کننده
شهروند/جامعه هوشمند
افراد هوشمند و فعال
آموزش و پژوهش
فرهنگی پر جنب و جوش و شاد
حکمرانی هوشمند
حکمرانی الکترونیک
دسترسی آسان
شفاف
زیرساخت هوشمند
اتصال
خدمات یکپارچه
ابزار هوشمند
بهره وری انرژی
کاهش تولید گازهای گلخانه ای
جابجایی هوشمند
حمل و نقل هوشمند
وسایل نقلیه الکتریکی
کنترل ترافیک پویا
محیطزیست هوشمند
سبز
کنترل آلودگی
تغییرات آب و هوا

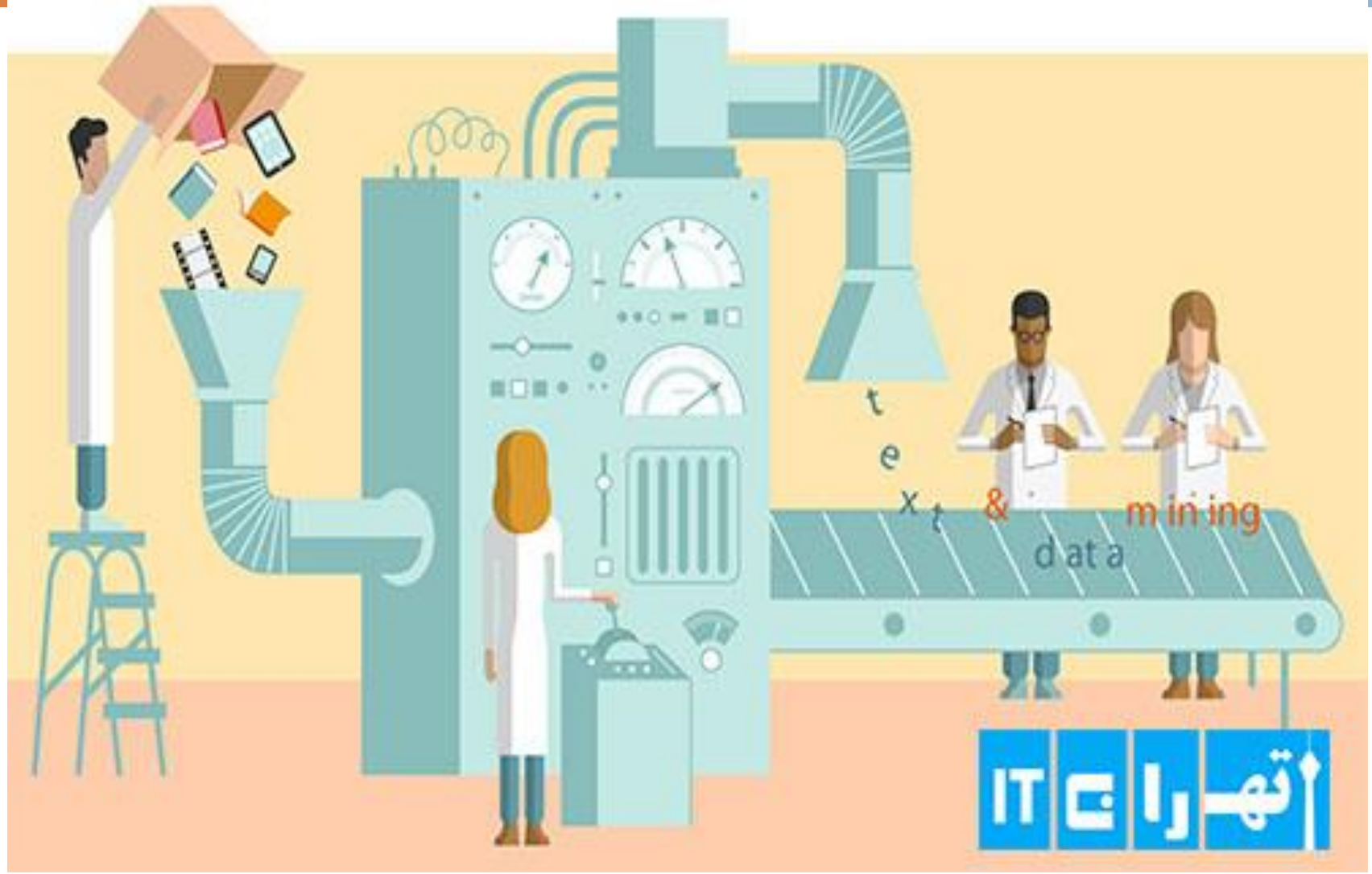
شهر هوشمند

خروجی های شهر پایدار هوشمند

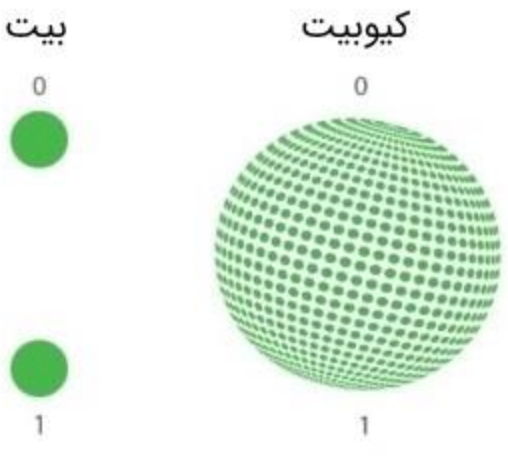
زیرساخت شهری	خدمات شهری	اقتصاد پایدار
مرتفع ساختن چالشهای اصلی شهر از جمله ترافیک و آلودگی هوا	شفاف سازی (فرایندها و سازمانهای شیشه ای)	درآمدهای پایدار
مدیریت پایدار منابع (آب ، انرژی ، پسماند و ...)	کاهش بوروکراسی	ظرفیت سازی
تاب آوری و مقاوم سازی	بالا بردن کیفیت زندگی – افزایش سطح رضایتمندی	کاهش هزینه های کلان شهری
کاهش اختلال در سیستم های شهری	مشارکت حداکثری- شهروندمحوری	ایجاد اشتغال پایدار

ساختمان هوشمند

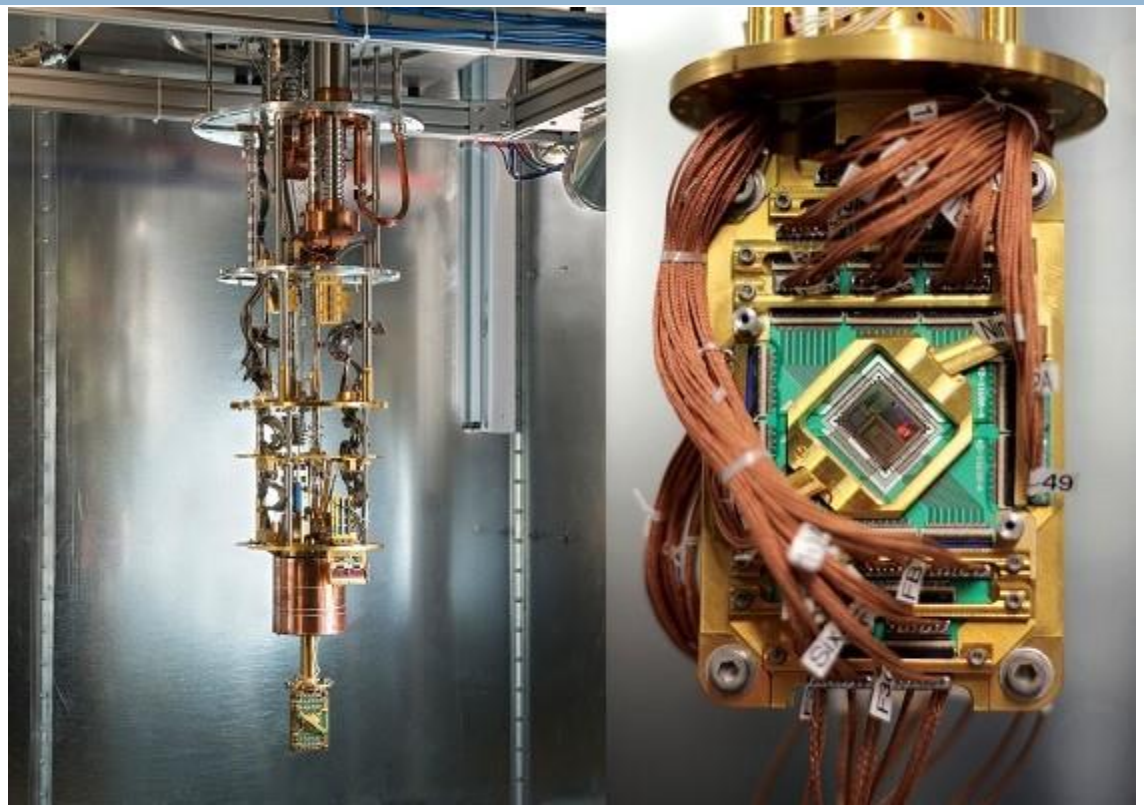
هوش مصنوعی و سیستم خبره
داده کاوی data mining



پردازش کوانتومی



یک کیوبیت برخلاف بیت که تنها در یکی از دو حالت 0 و یا 1 است، می‌تواند هر حالتی بین این دو مقدار را داشته باشد.

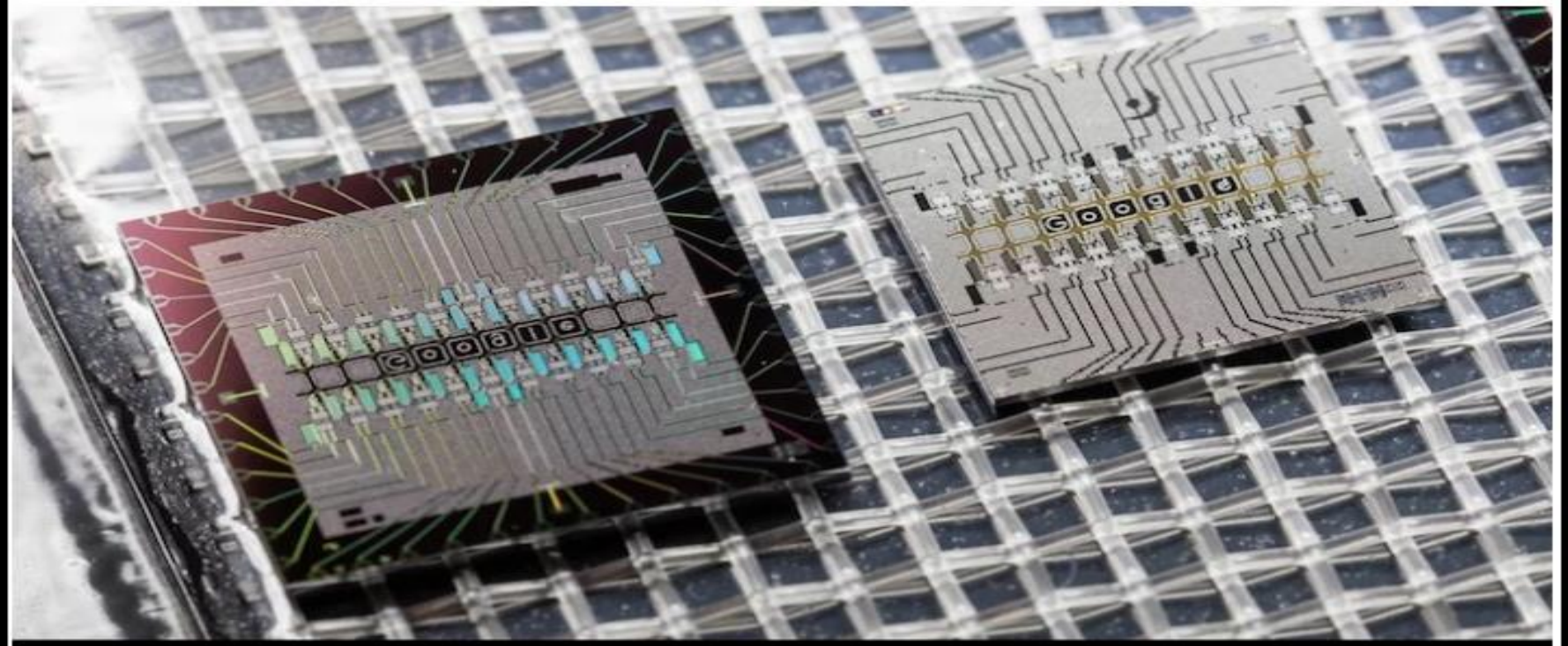


نمایی از تراشه ۲۰۴۸ کیوبیتی کامپیوتر کوانتومی Q ۲۰۰۰ ساخت شرکت کانادایی D-Waveبر اساس فیزیک ابررسانا. این تراشه در دمایی ۰.۰۱۵ کلوین بالای صفر مطلق کار می‌کند.

کامپیوتر کوانتومی گوگل

این یک کامپیوتر کوانتومی است که از پردازنده ۵۴ کیو بیتی Sycamore گوگل بهره می گیرد و گوگل از آن برای نشان دادن برتری کوانتومی خود استفاده کرد. مخزن استوانه ای بزرگی که می بینید برای سرد کردن کامپیوتر به کار می رود تا انرژی خارجی مزاحمتی را برای کیوبیت های فوق حساس ایجاد نکنند.

کامپیوتر کوانتومی گوگل



گوگل چیپ های رایانش کوانتومی خود را با کمک دو قطعه ای می سازد که به یکدیگر متصل شده اند. در ست چپ اینترفیس کنترلی قرار دارد که برای برقراری ارتباط کامپیوتر با جهان خارج به کار می رود و در سمت راست المان چین قرار داده شده که کیوبیت های پردازش کننده دیتا را در دل خود دارد. اگر از نزدیک به این سازه نگاه کنید کلمه گوگل را مشاهده می کنید که از نقاط ریز ایریدیوم ساخته شده و از بخش میانی قابل مشاهده است.

ویژگی‌های فضای سایبر

- گمنامی ناشی از هویت سایبری و تعارض آنها با اِستنادپذیری
- مرز سایبری، بی‌مرزی در فضای سایبر و تعارض آن با اِستنادپذیری
- بی نظمی ،عدم تقارن و عدم قطعیت برگرفته از ویژگی‌های ذاتی فضای سایبر
- قابلیت فضای سایبر در ایجاد پیامد جنبشی (فیزیکی و اجتماعی)
- توانایی فضای سایبر در تأثیرگذاری بر اداره امور کشور
- توانایی فضای سایبر در تأثیرگذاری بر مؤلفه‌های حاکمیت و اقتدار ملّی

خود آزمایی

۱- فناوری نوین مورد استفاده در فضای سایبر عبارت است از:

الف) بلاکچین ب) اینترنت اشیا (IOT)

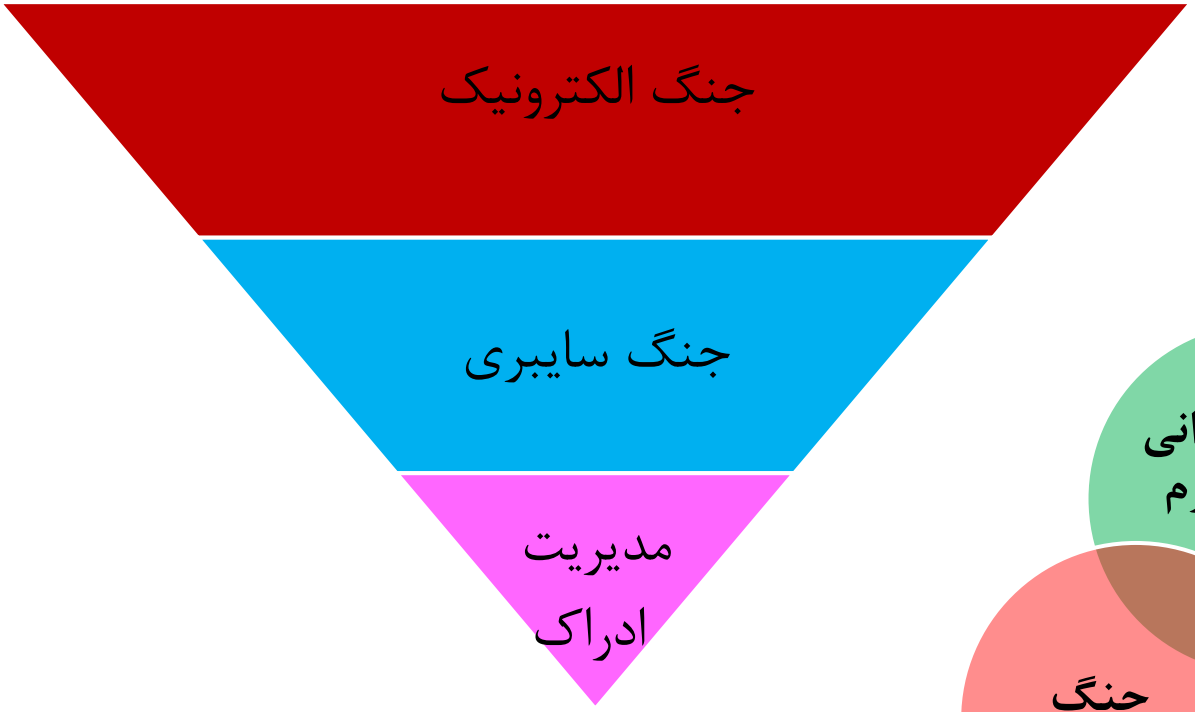
ج) پردازش کوانتومی د) همه موارد

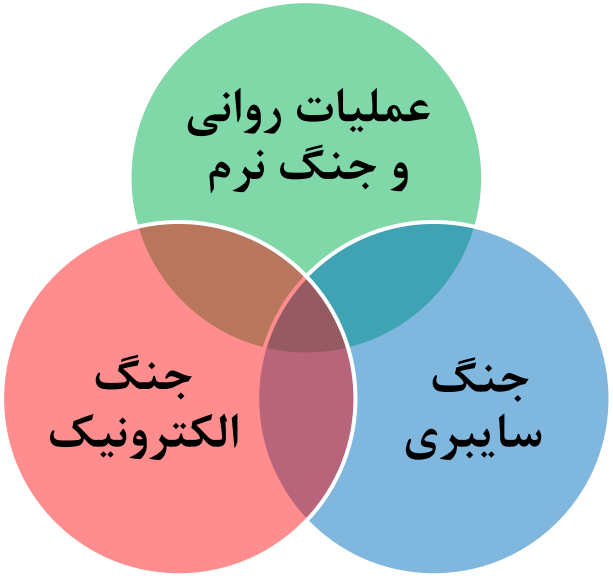
۲- فناوری (های) مورد استفاده در ارزهای دیجیتالی مثل بیت کوین عبارت است از:

الف) بلاکچین ب) اینترنت اشیا

ج) پردازش کوانتومی د) هیچکدام

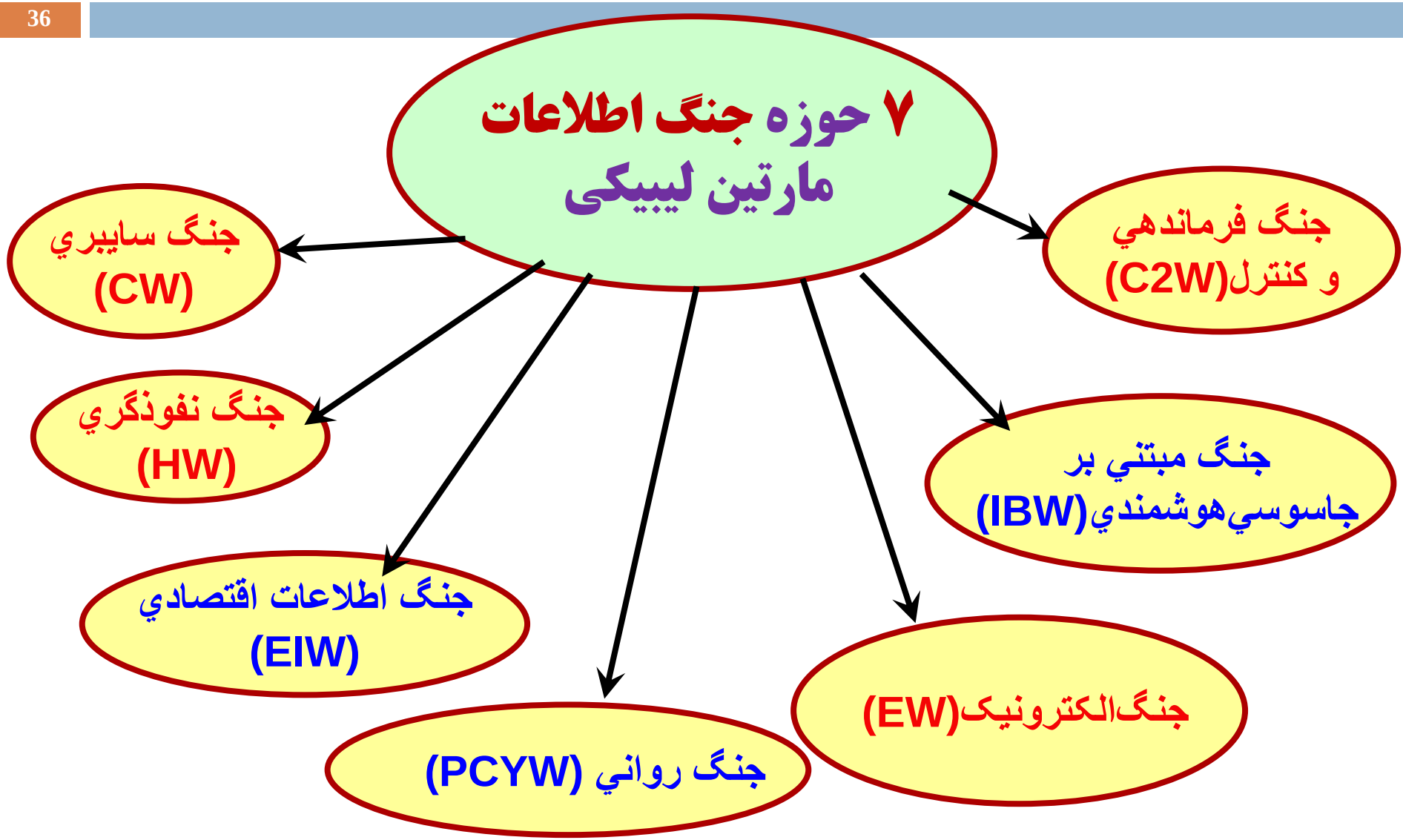
سناریو های تهدید معیار و دشمن شناسی





مدل لایه ای جنگ اطلاعات بومی شده

جنگ اطلاعات

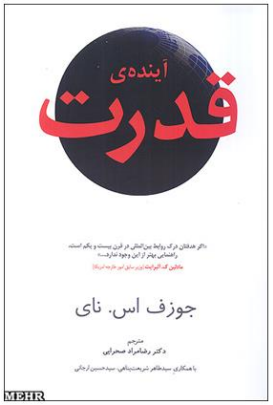

۷ حوزه جنگ اطلاعات
مارتین لیبیکی
جنگ سایبري (CW)
جنگ فرماندهي و کنترل(C2W)
جنگ نفوذگري (HW)
جنگ مبتني بر جاسوسي‌هوشمندي(IBW)
جنگ اطلاعات اقتصادي (EIW)
جنگ‌الکترونیک(EW)
جنگ رواني (PCYW)

طبقه بندی جنگ اطلاعات توسط مارتین لیبیکی

1. جنگ فرماندهی و کنترل که هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن، است.
2. جنگ برپایه اطلاعات که متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم هائی است که برای برتری بر فضای نبرد در جستجوی دانش کافی هستند.
3. جنگ الکترونیک تکنیک‌های رادیوئی، الکترونیک، یا رمزنگاری.
4. جنگ روانی که در آن از اطلاعات برای تغییر ذهنیت و طرزفکر دوستان، بی طرف‌ها، و دشمنان استفاده می‌شود.
5. جنگ هکرها که در آن به سیستم‌های رایانه‌ای حمله می‌شود.
6. جنگ اطلاعاتی اقتصادی ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی.
7. جنگ سایبری ترکیبی از همه موارد شش گانه بالا.

تئوری قدرت نرم

جوزف ساموئل نای مبتکر تئوری قدرت نرم و استاد دانشگاه هاروارد در کتاب آینده ی قدرت، پس از تفکیک فضای سایبر به دو لایه زیرساخت فیزیکی و مجازی (اطلاعات)، با اشاره به جنبه اقتصادی تهدید در فضای سایبر، تأکید دارد که "لایه اطلاعاتی فضای سایبر، از بازده فزاینده نسبت به مقیاس برخوردار بوده و عرصه و حوزه سیاسی آن به گونه ای است که کنترل قانونی را مشکل می سازد، لذا بهتر است از حوزه اطلاعاتی که هزینه ها در آن پائین است، تهدید را علیه لایه فیزیکی که منابع آن کمیاب و گران هستند، اعمال نمود".



تکنیک های علوم شناختی در جنگ های اطلاعاتی

آبشار، بیابان ، کویر

اعتراض ذهنی،

اجتماع ارتباطی

و دهها

تکنیک دیگر...

محبوبِ مشغول

واقعیت مجهول

تکنیک های علوم شناختی در جنگ های اطلاعاتی

تکنیک " اعتراض ذهنی، اجتماع ارتباطی

- در حوزه علوم شناختی مهمترین رکن، نزد رسانه این است که باید بتواند ذهن های افراد جامعه هدف را به گونه ای معترض بکند، که این ذهن های معترض در فضای رسانه های اینتراکتیو یا سوپراینتراکتیو در فضای مجازی یا فضای اجتماعی خودشان و اجتماع شان براساس نقطه مشترک یا متصل شان، یعنی آن اعتراض ذهنی قرار دهند.
- اعتراض های مثل زاینده رود در اصفهان ، اعتراض معلمان به عدم رتبه بندی فرهنگیان ، اعتراض بازنشستگان به عدم دائمی شدن طرح همسان سازی و....

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 پدافنـــدی در استفاده از فناوری

تغییر ماهیت جنگ ها

تغییر ماهیت جنگ ها

از حالت سخت و نظامی

به حالت نرم و سایبری و شبکه ای (چند جانبه)

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

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

فضای سایبر بعد پنجم جنگ یا (فرا بعد)

جنگ سایبری و نفوذ های هد فمند

هجوم سایبری

تخریب، انهدام، بهره‌بـرداری از اطلاعـات دشـمن، جلـ
اطلاعات دشمن توسط وی و یا تأثیرگذاری بر آگاهی‌های

پدافند سایبری

حفاظت از زیرساخت‌های اطلاعاتی خودی در مقابل تهاجمات دشمن از طریق ایجاد و بکارگیری الزامات پدافند غیر عامـل در فضای سایبر و سیستم‌های اطلاعاتی

تهدیدات سایبری

منشاء– بازیگران

نیروی سایبری کشورها

مزدوران سایبری تحت حمایت کشورها

سرویس های امنیتی کشورها

تروریست های سایبری

مجرمین سایبری سازمان یافته

هکرهای دارای انگیزه سیاسی

جاسوسان صنعتی، اقتصادی

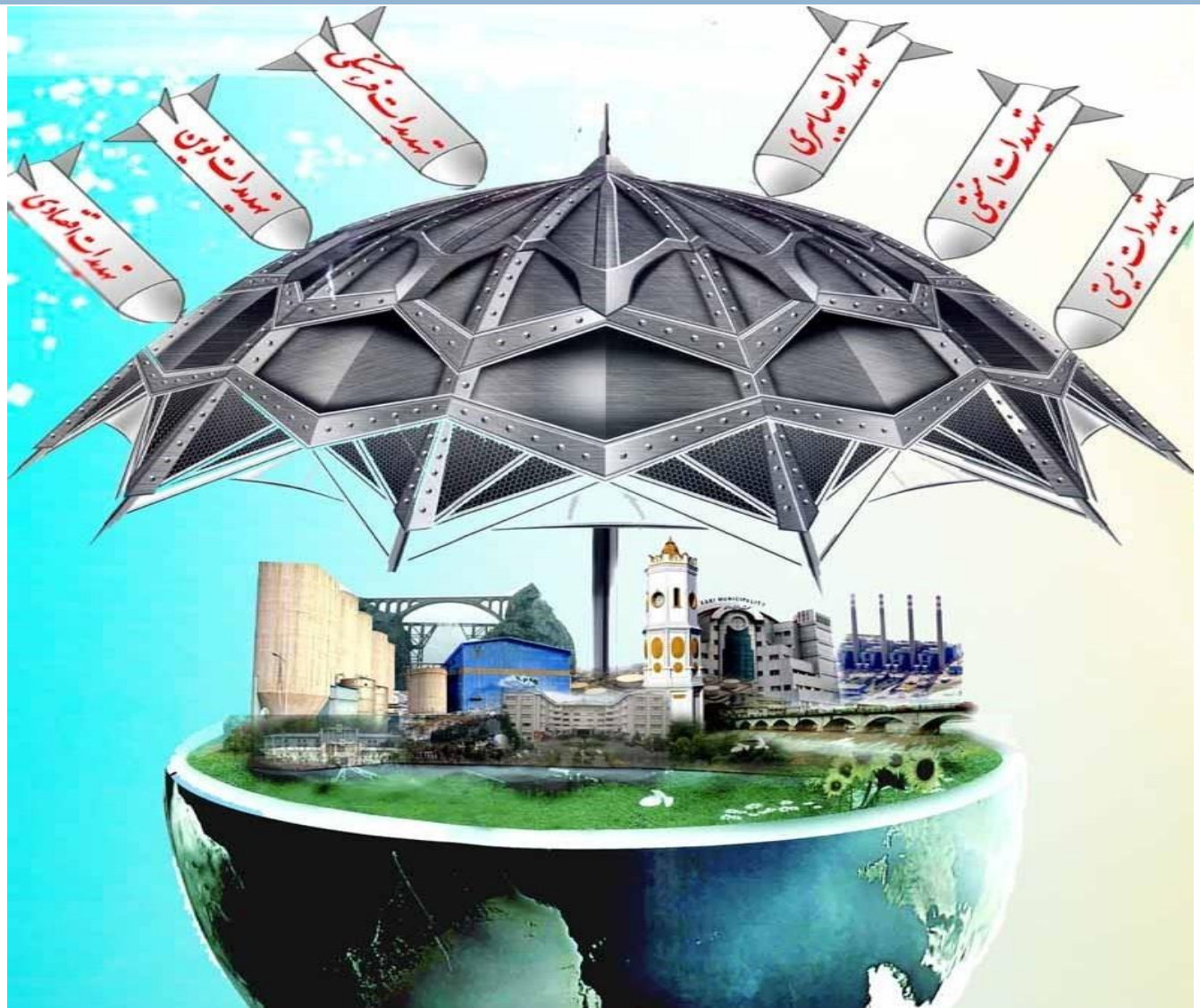
هکرها

خودی ها

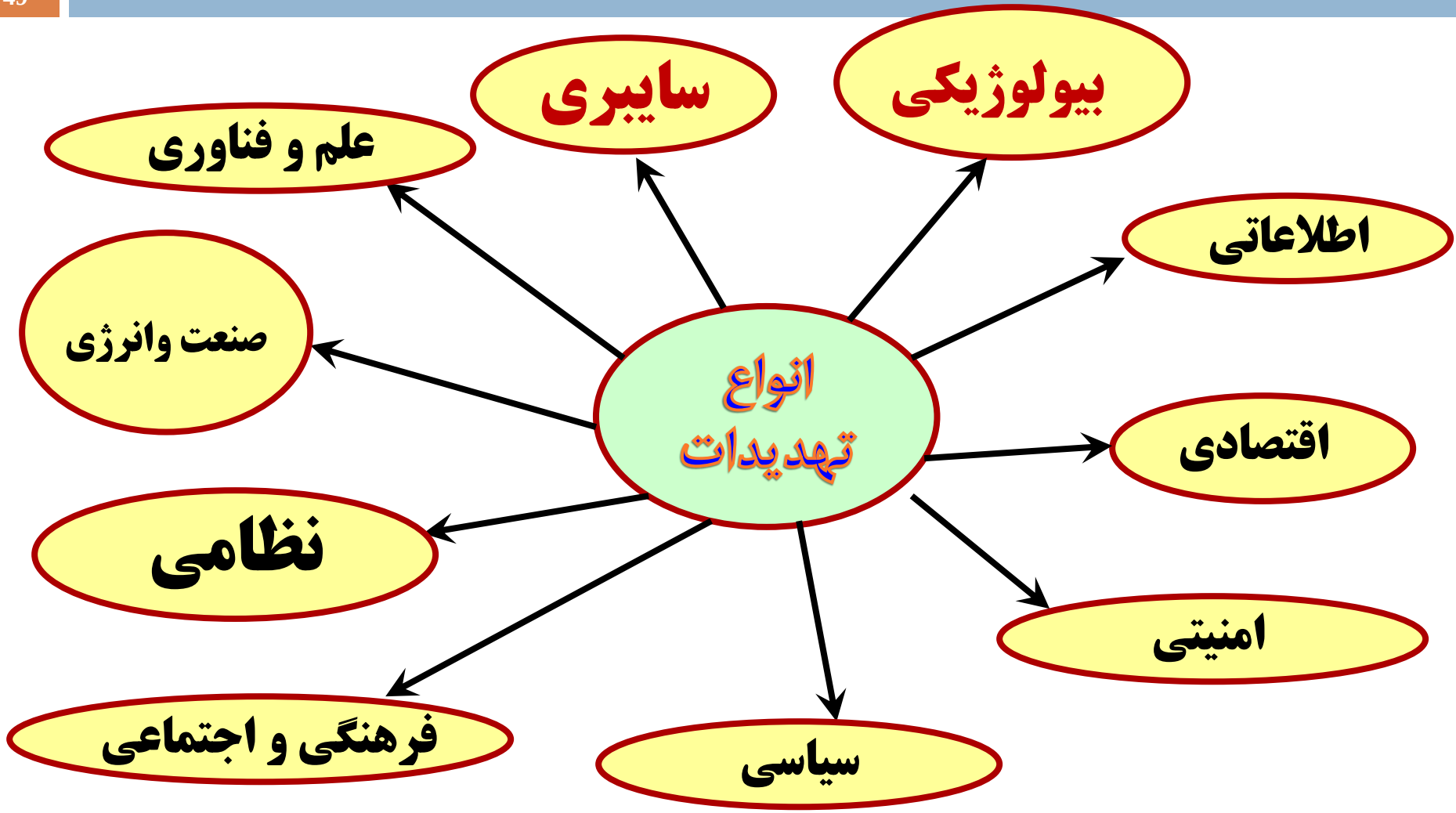
نوع

- جنگ، مخاصمه یا تجاوز سایبری
- نزاع سایبری
- جاسوسی سایبری
- تروریسم سایبری
- جرم سایبری
- حمله سایبری منتهی به حوادث سایبری

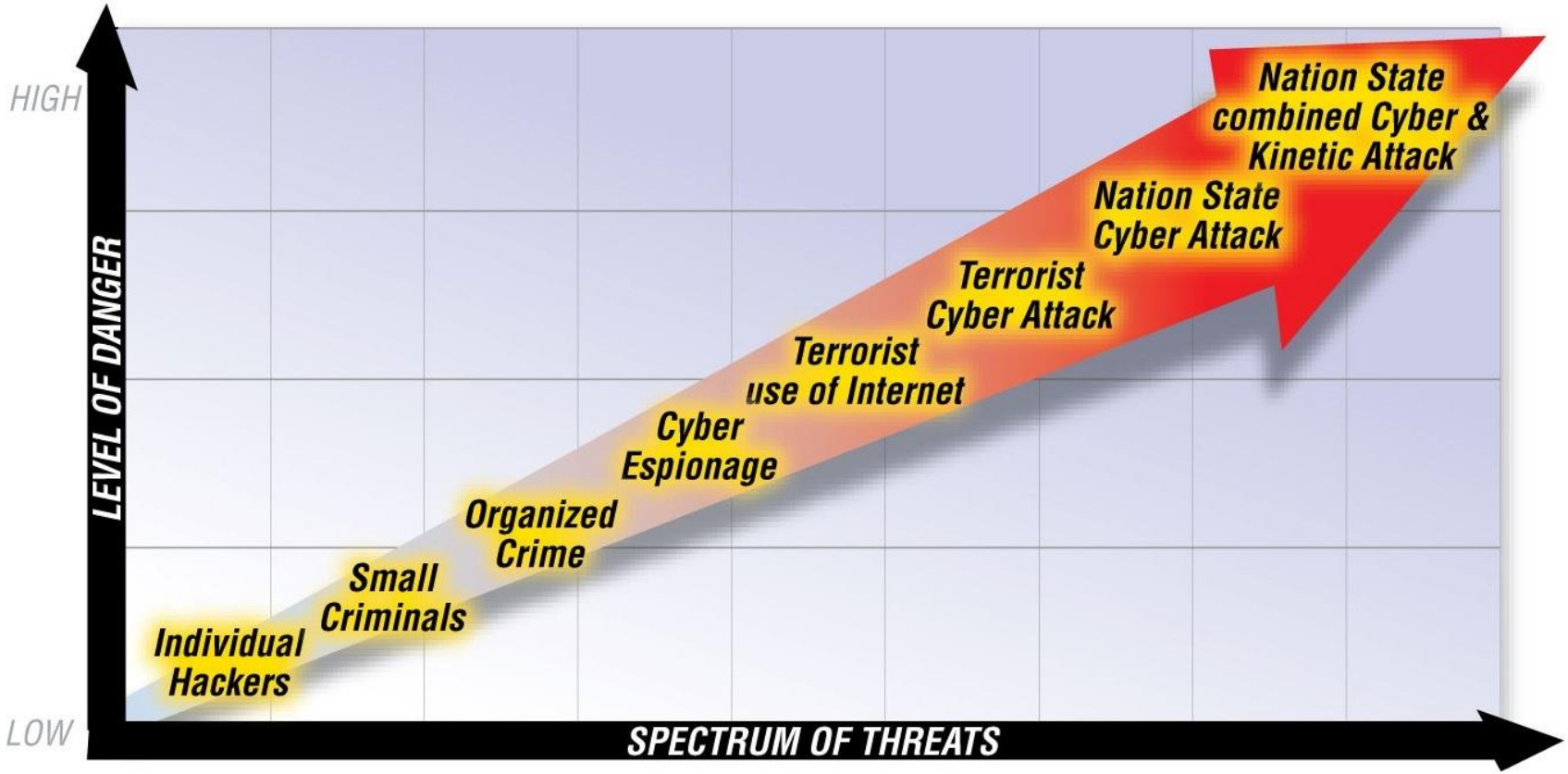
سناریوهای تهدید در حوزه پدافند غیر عامل



سناریو انواع تهدیدات



طیف کلی تهدیدات سایبری و سطوح رو به افزایش خطر



طبقه بندی تهدیدات سایبری

از منظر منشاء یا عامل تهدید

تهدیدات با منشاء انسانی (مهاجم سایبری یا متجاوز سایبری)
تهدیدات با منشاء ماشینی (سازه مخرب سایبری، بدافزار یا سلاح سایبری)
تهدیدات با منشاء طبیعی (زلزله، سیل، طوفان، رعد و ...)
تهدیدات با منشاء صنعتی (تشعشع حرارتی یا الکترومغناطیسی و ...)
تهدیدات با منشاء خرابی

از منظر نیت منشاءتهدید

تهدیدات عمدی
تهدیدات تصادفی
تهدیدات محیطی

منشاء تهدید سایبری

منشاء انسانی

دولت‌های متخاصم
مزدوران سایبری (گروه‌های تحت حمایت پنهان دول متخاصم)
جاسوسان سایبری
تروریست‌های سایبری
مجرمین سازمان‌یافته سایبری
هکرهای دارای انگیزه سیاسی
...

منشاء ماشینی

سلاح‌های سایبری
بدافزارها (جاسوس‌افزارها، ویروس‌ها، کرم‌ها، هرزنامه‌ها و ...)
سازه‌های مخرّب
...

جدول ابزارها و سلاح های مورد استفاده در جنگ سایبری

	ابزار تهدید	نوع اقدام	هدف
۱	بد افزارهای پیشرفته (APT)	آلوده کردن سیستم ها و از کار انداختن آنها	اختلال و یا از کار انداختن مراکز داده یا سرورهای مراکز حیاتی و حساس
۲	اسب های تروا	انتشار از طریق ایمیل، محل های اشتراک فایل	ثبت کلیدهای فشرده شدن صفحه کلید، مشاهده صفحه نمایش کاربر
۳	عدم دسترسی به سرویس	قطع دسترسی به وب سایت توسط شرکت ارائه کننده خدمات میزبانی	عدم دسترسی به سرویس
۴	دروازه پشتی (حفره نفوذ مخفی)	قرار دادن یک حفره نفوذ مخفی در تجهیزات تولیدی توسط تولید کننده	ورود به شبکه در زمان دلخواه و به‌صورت مخفیانه
۵	نرم افزارهای جاسوسی	در پوشش نرم افزارهای کاربردی مانند دیکشنری بابیلون	سرقت اطلاعات رایانه ها و شبکه های کاربران
۶	نرم افزارهای تبلیغاتی اینترنتی	قرار گرفتن در رایانه حریف و اصرار بر حداقل یک بار استفاده از آنها	سرقت هویت کاربران و کلمه عبور آنها
۷	شبکه های "بات نت"	در اختیار گرفتن غیرقانونی سرورها و کامپیوترهای سازمان ها و مردم	مشارکت غیرارادی در حملات سایبری به عنوان سرباز الکترونیکی
۸	حملات DOS	بالا بردن کاذب ترافیک ارتباطی دسترسی به سایت	از کار انداختن سرورها و جلوگیری از ارائه خدمات به مردم
۹	حمله (هک و نفوذ)	ورود غیرقانونی به شبکه ها از طریق پورت های آسیب پذیر	اختلال و یا جلوگیری از ارائه خدمات

خود آزمایی

۱- برا ی کنترل دسترسی افراد مجاز به یک شبکه و تجهیزات آن نظیر سرویس های اطلاعاتی و دیتا سنتر یک سازمان حیاتی یا حساس ، چه استراتژی امنیتی مورد استفاده قرار می گیرد.

الف) دفاع در عمق　　ب) ضعیفترین حلقه

ج) حداقل امتیاز　　د) ۵ حلقه واردن

۲- بالا بردن کاذب ترافیک ارتباطی دسترسی به سایت با هدف از کار انداختن سرورها و کامپیوترهای سازمان ها که باعث جلوگیری از ارائه خدمات به مردم می شود، را چه حمله ای گویند.

الف) انسداد و قطع خدمات (DOS)　　ب) بات نت

ج) حمله مهندسی اجتماعی　　د) الف و ج

برخی نمونه ها و مصادیق حملات 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)

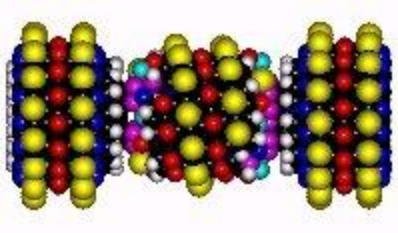
- اختلال در شبکه نفت ، گاز و سوخت کشور

(انفجار خطوط لوله، پالایشگاه ، حمله سایبری به سامانه ها)

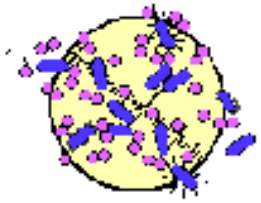
- اختلال و سرقت در شبکه بانکی و مالی کشور
- اختلال در شبکه های صدا و سیما
- و ...

سلاح سایبری وویژگی های آن
سلاحهای سخت افزاری

- بمب تراشه ای (Chipping Bomb)



- نانو ماشین ها (Nano Machines)
- میکروب های خورنده سیلیکن (Microbes)



سلاح سایبری وویژگی های آن
سلاحهای نرم افزاری

۱ – حملات نرم‌افزاری

۱ – ویروس‌ها و کرم‌ها

۲ – کدهای تغییر دهنده تنظیمات امنیتی رایانه(Adware)

۳ – درب‌های‌پشتی(Backdoor)

۴ – اسب‌های‌تروآ(Trojan Horses)

۵ – جاسوس‌افزارها (Spyware)

۶ – آسیب‌پذیری‌نرم‌افزار Software Exploitation،

۷ – سرریز بافر(Buffer Over Flow)

۸ – شنود اطلاعات (Man in the Middel OR Sniffing)

۹ – از کار انداختن سرویس(Denial of Service) و . . . .

مهندسی اجتماعی یا Social Engineering

تکنیک های رایج در حملات مهندسی اجتماعی از نوع آنلاین

فیشینگ
Phishing

نیزه ای فیشینگ
(هدفدار)

اسمیشینگ

ویشینگ یا
فیشینگ تلفنی

فارمینگ

پنجره پاپ آپ
PopUp Window

تکنیک های رایج در حملات مهندسی اجتماعی از نوع فیزیکی

طعمه

Bating

چیزی برای چیزی

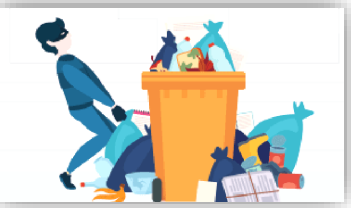
S4S

بهانه

PRETEXTING

زباله گردی

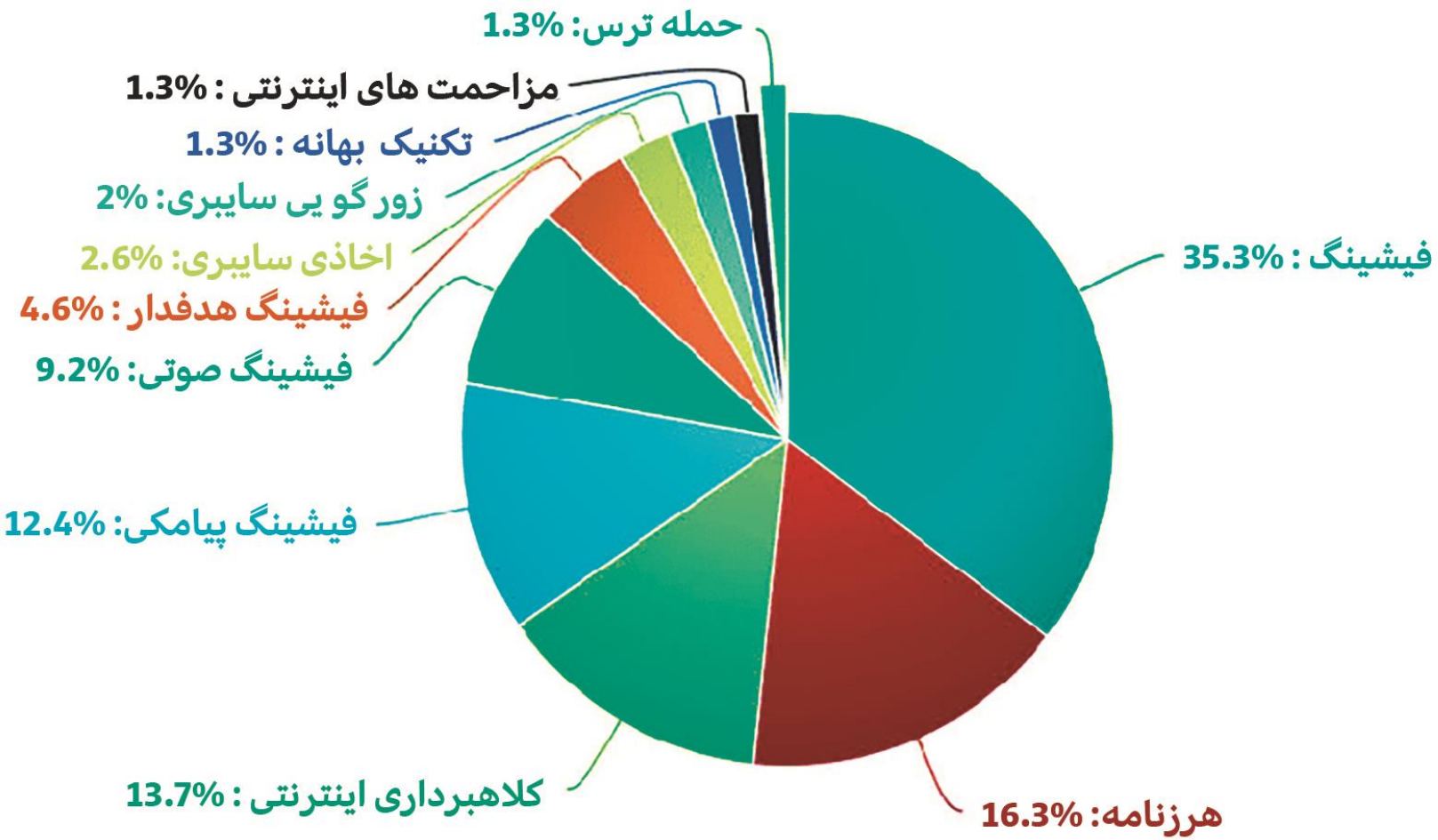
Dumpster Diving



از پشت شانه کسی نگاه کردن

shoulder surfing

مروری بر آمارهای منتشرشده
حملات مهندسی اجتماعی



https://www.researchgate.net/figure/Different-social-engineering-techniques-used-for-cyber-attacks-threats-during-the_fig5_348165214

خود آزمایی

۳– ..... توانایی استخراج اطلاعات محرمانه یک سیستم رایانه‌ای با فریب، کسب اعتماد و تهدید افراد مجاز در آن سیستم می‌باشد .

الف) نفوذگری
ب) مهندسی اجتماعی
ج) تخلیه اطلاعاتی
د) هیچکدام

۴– در تکنیک مهندسی اجتماعی .....، مهاجم از اطلاعات روی صفحه مانیتور کامپیوتر قربانی سوء استفاده می کند.

الف) E-mail attachments
ب) جمع آوری اطلاعات به صورت online
ج) جستجو در زباله ها یا آشغال گردی
د) از پشت شانه کسی نگاه کردن

۵– در تکنیک مهندسی اجتماعی .....، مهاجم ، هدفش سوء استفاده از فرد خاصی در سازمان می باشد.

الف) فیشینگ
ب) فیشینگ نیزه ای
ج) فارمینگ
د) هیچکدام

نمونه های حملات و جنگ های سایبری در دنیا

- در ژوئن ۲۰۱۰ تأسیسات هسته‌ای ایران در نطنز توسط یک بدافزار به نام «استاکس‌نت» مورد حمله سایبری واقع شد.[۷] طبق گزارش‌ها، استاکس‌نت که با مشارکت آمریکا و اسرائیل طراحی شده بود، نزدیک به ۱،۰۰۰ سانتریفیوژ تأسیسات اتمی ایران را نابود کرد. ایران به راه حلی برای مقابله با این ویروس دست یافت که این باعث بهتر شدن وضعیت دفاع سایبری این کشور و پیشرفت آن شد.
- پخش شدن کرم در میان سخت افزارهای قابل جا به جایی از قبیل حافظه های USBو یا درایورهای CDکمک می کند.

وابستگی متقابل زیرساخت ها و استراتژی ۵ حلقه واردن

قرارگاه پدافند سایبری کشور

سازمان پدافند غیرعامل کشور

حلقه ها	عناوین	مقایسه با اندام انسان	مراکز ثقل
حلقه ۱	رهبری ملی	مغز و سیستم عصبی	رهبری سیاسی، مراکز مخابراتی، تجهیزات صدا و سیما، سیستم ارتباطات مایکروویو و ماهواره‌ای، تجهیزات مخابراتی و الکترونیکی مقرهای فرماندهی و قرارگاه‌ها، سیستم‌های فرماندهی و کنترل و ...
حلقهٔ ۲	محصولات کلیدی	سیستم هاضمه و گردش خون	مراکز کنترل نیروگاه‌های برق، صنایع سنگین، پالایشگاه‌ها، صنایع تولید تجهیزات نظامی، کامپیوترهای کنترل پردازش و تولید محصولات، تجهیزات بانک‌های اطلاعاتی و مالی و ...
حلقهٔ ۳	زیر ساخت ها	اندام های حرکتی (دست و پا)	تجهیزات هدایت و ناوبری دریایی و بنادر، مراکز علائم و کنترل راه‌آهن، مترو، فرودگاه‌ها و هواپیماهای مستقر در آنها و **مراکز کنترل رایانه‌ای سیستم‌های حمل و نقل جاده‌ای و**
حلقهٔ ٤	جمعیت مردمی و اراده ملی	روح و روان و اراده	جمعیت مردم و افراد نیروهای مسلح، گیرنده‌های صدا و سیما، رادیو، تلویزیون و کامپیوترهای خانگی، تلفن‌های ثابت، همراه و ...
حلقهٔ ۵	نیروهای عملیاتی	سلول های دفاعی	تجهیزات الکترونیکی، ارتباطی و رایانه‌ای در مراکز فرماندهی و کنترل مناطق عملیاتی، تجهیزات و سیستم‌های هواپیماهای مستقر در پایگاه‌های شکاری، تجهیزات رادارها، موشک‌ها و مراکز پست فرماندهی در سیستم‌های پدافند هوایی کشور و ...

جدول ابزارها و سلاح های مورد استفاده در جنگ سایبری

	ابزار تهدید	نوع اقدام	هدف
۱	بد افزارهای پیشرفته (APT)	آلوده کردن سیستم ها و از کار انداختن آنها	اختلال و یا از کار انداختن مراکز داده یا سرورهای مراکز حیاتی و حساس
۲	اسب های تروا	انتشار از طریق ایمیل، محل های اشتراک فایل	ثبت کلیدهای فشرده شدن صفحه کلید، مشاهده صفحه نمایش کاربر
۳	عدم دسترسی به سرویس	قطع دسترسی به وب سایت توسط شرکت ارائه کننده خدمات میزبانی	عدم دسترسی به سرویس
۴	دروازه پشتی (حفره نفوذ مخفی)	قرار دادن یک حفره نفوذ مخفی در تجهیزات تولیدی توسط تولید کننده	ورود به شبکه در زمان دلخواه و به‌صورت مخفیانه
۵	نرم افزارهای جاسوسی	در پوشش نرم افزارهای کاربردی مانند دیکشنری بابیلون	سرقت اطلاعات رایانه ها و شبکه های کاربران
۶	نرم افزارهای تبلیغاتی اینترنتی	قرار گرفتن در رایانه حریف و اصرار بر حداقل یک بار استفاده از آنها	سرقت هویت کاربران و کلمه عبور آنها
۷	شبکه های "بات نت"	در اختیار گرفتن غیرقانونی سرورها و کامپیوترهای سازمان ها و مردم	مشارکت غیرارادی در حملات سایبری به عنوان سرباز الکترونیکی
۸	حملات DOS	بالا بردن کاذب ترافیک ارتباطی دسترسی به سایت	از کار انداختن سرورها و جلوگیری از ارائه خدمات به مردم
۹	حمله (هک و نفوذ)	ورود غیرقانونی به شبکه ها از طریق پورت های آسیب پذیر	اختلال و یا جلوگیری از ارائه خدمات

خود آزمایی

۶- مراکز ثقل یک کشور در چه استراتژی مورد بررسی قرار می گیرد.

الف) دفاع در عمق ب) ضعیفترین حلقه

ج) حداقل امتیاز د) ۵ حلقه واردن

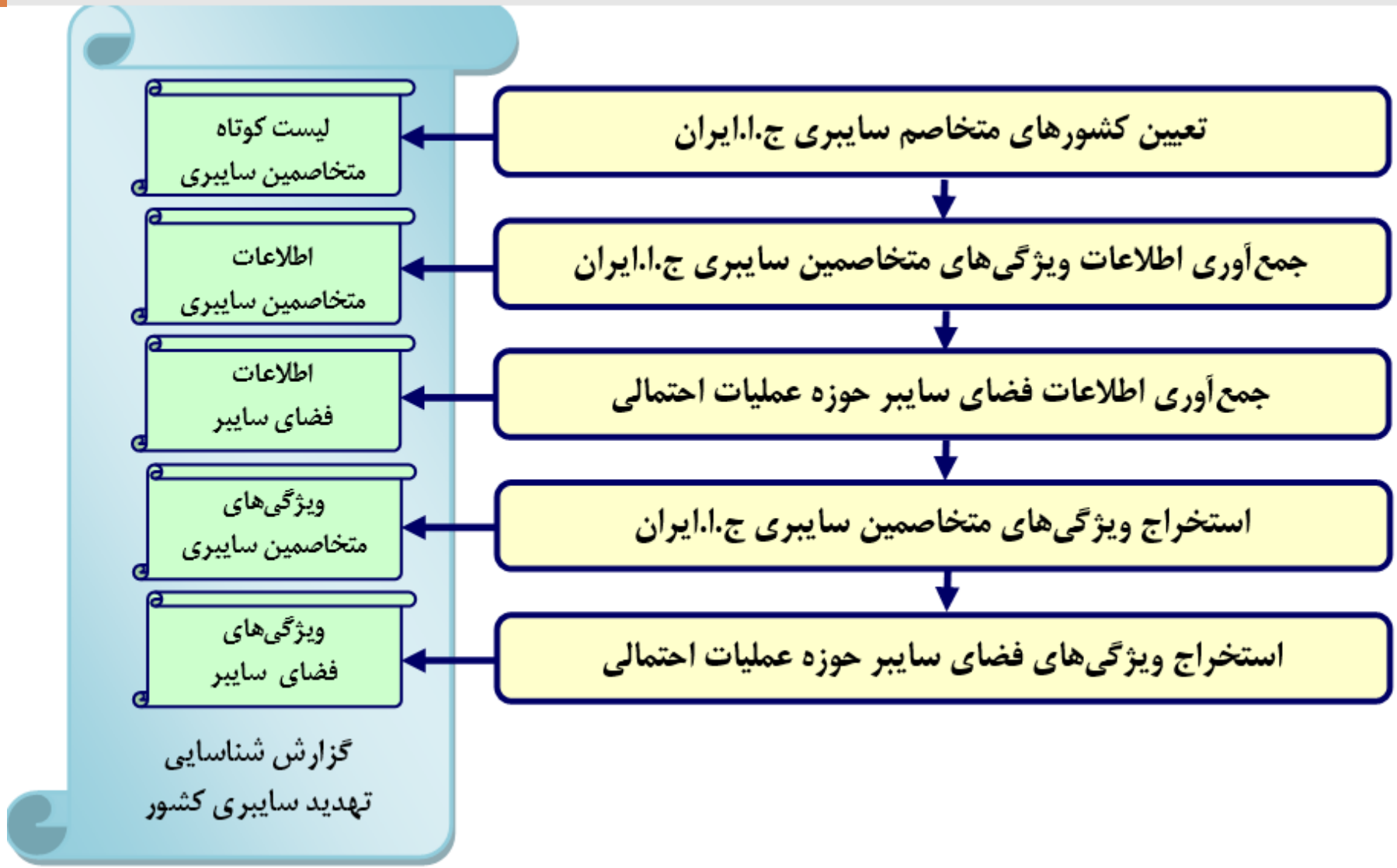
۷- در اختیار گرفتن غیرقانونی سرورها و کامپیوترهای سازمان ها و مردم را چه حمله ای گویند.

الف) انسداد و قطع خدمات (DOS) ب) بات نت

ج) انسداد و قطع خدمات توزیع شده(DDOS) د) الف و ج

تحلیل پیامد تهدیدات

اقدام‌های مرحله‌ی رصد و پایش تهدید سایبری

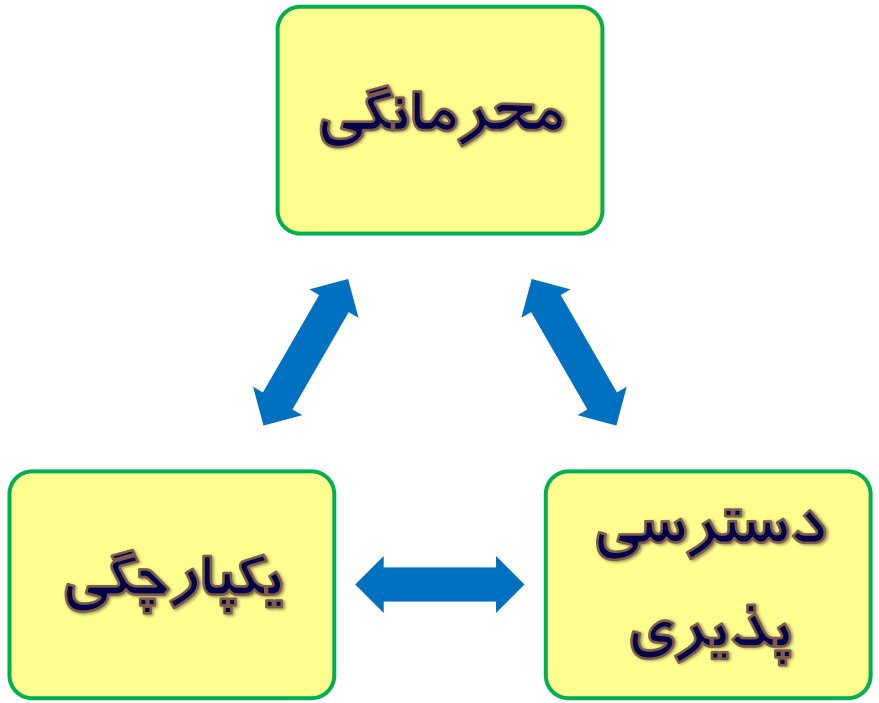


مدلسازی تهدیدات سایبری مبتنی بر تکنیک STRIDE

Type of Threat	Examples
Spoofing	•Forging Email Message •Replaying Authentication
Tampering	•Altering data during transmission •Changing data in database
Repudiation	•Delete critical data and deny it •Purchase product and deny it
Information disclosure	•Expose information in error messages •Expose code on web site
Denial of Service	•Flood web service with invalid request •Flood network with SYN
Elevation of Privilege	•Obtain Administrator privileges •Use assembly in GAC to create acct in .Net

سه مفهوم مهم امنیت سایبری

- محرمانگی (Confidentiality)
- یکپارچگی (Integrity)
- دسترسی پذیری (Availability)



طبقه بندی تهدیدات سایبری

از منظر پیامد تهدید

- تهدیدات منجر به فریب و جعل S
- تهدیدات منجر به تغییر داده های ارسالی یا بروز اختلالT
- تهدیدات منجر به تخریب (حذف داده های حیاتی R
- تهدیدات منجر به افشاء اطلاعاتID
- تهدیدات منجربه قطع خدماتDOS)
- تهدیدات منجر به دسترسي غیرمجازE

شدت تهدید سایبری

شدت خیلی کم : تهدید سایبری تحت کنترل

شدت کم : تهدید سایبری حادثه آفرین

شدت متوسط : تهدید سایبری مخلّ امنیت

شدت زیاد : تهدید سایبری بحران‌زا

شدت خیلی زیاد :تهدید سایبری فاجعه‌بار

عدد وسطوح هشدار سایبری

شدت پیامد / احتمال وقوع	خیلی غیرمحتمل	غیرمحتمل	ممکن	محتمل	قریب‌الوقوع
خیلی کم (تحت کنترل)	۰	۱	۲	۳	٤
کم (حادثه آفرین)	۱	۲	۳	٤	٥
متوسط (مخلّ امنیت)	۲	۳	٤	٥	٦
زیاد (بحران‌زا)	۳	٤	٥	٦	۷
خیلی زیاد (فاجعه‌بار)	٤	٥	٦	۷	۸

۰ و ۱ و ۲ = وضعیت سفید = تحت کنترل سایبری

۳ و ۴ و ۵ = وضعیت زرد = تهدید سایبری

۶ و ۷ = وضعیت نارنجی = بحران سایبری

۸ = وضعیت قرمز = جنگ سایبری

تحلیل پیامد تهدیدات سایبری بر سازمان

تاثیر امتیازات	ماموریت	اهداف عملیاتی	اهداف مالی	تعهدات
تعاریف	ضروری	ضروری	اختیاری	ضروری
۱= ناچیز	افشای بخشنامه های داخلی باعث بروز مشکل ناچیز و قابل تحمل در فرآیندهای معمولی درون سازمان می‌شود.	اختلال در سامانه های اطلاعاتی و وقفه در برخی از سیستمهای امنیتی سازمان باعث بروز مشکل ناچیز و قابل تحمل درسازمان می‌شود.	اختیاری	تغییر، جعل و یا حذف اطلاعات مربوط به برخی از سامانه های اطلاعاتی و سیستمهای امنیتی سازمان موجب خدشه ناچیز و قابل تحمل در انجام برخی از تعهدات سازمان می شود.
۲= قابل قبول	افشای بخشنامه های داخلی محرمانه، اطلاعات پرسنلی کارمندان، مشخصات شبکه داخلی باعث بروز مشکل در فرآیندهای درون سازمان می‌شود لیکن قابل کنترل می باشد.	اختلال در سامانه های اطلاعاتی و وقفه در برخی از سیستمهای امنیتی سازمان باعث بروز مشکل کمی و تاثیر منفی جزیی در اهداف عملیاتی سازمان می‌شود.	اختیاری	تغییر، جعل و یا حذف اطلاعات مربوط به برخی از سامانه های اطلاعاتی و سیستمهای امنیتی سازمان موجب خدشه جزیی در انجام برخی از تعهدات سازمان می شود.
۳= غیرقابل قبول و مخل امنیت	افشای مشخصات سامانه های اطلاعاتی ، مشخصات سیستمهای امنیتی باعث اخلال در امنیت و بروز مشکل در ماموریتهای کسب و کاری سازمان می‌شود.	قطعی سامانه های اطلاعاتی و وقفه در سیستمهای امنیتی سازمان باعث اخلال در امنیت و بروز مشکل و عدم تحقق برخی از اهداف عملیاتی سازمان می‌شود.	اختیاری	تغییر، جعل و یا حذف اطلاعات مربوط به به برخی از سامانه های اطلاعاتی و سیستمهای امنیتی سازمان سازمان موجب خدشه در انجام برخی از تعهدات سازمان می شود.
۴= زیاد (بحران زا)	افشای بخشنامه های خیلی محرمانه، اطلاعات مرکز داده موجب بروز مشکل در ماموریتهای اساسی سازمان می‌شود.	وقفه در اکثر زیرساخت ها و سرویس کلیدی سازمان و عدم دسترسی به برخی اطلاعات خیلی محرمانه سازمان نظیر اطلاعات مرکز داده باعث اختلال جدی و عدم تحقق اهداف عملیاتی سازمان می شود.	اختیاری	تغییر، جعل و یا حذف اطلاعات مربوط به برخی از زیرساخت ها و سرویس کلیدی سازمان موجب صدمه به اعتبار و حسن شهرت و خدشه جدی در انجام تعهدات سازمان می شود.
۵= فاجعه‌بار	افشای اطلاعات فوق محرمانه سازمان مرتبط با حاکمیت و یا سازمان بالا دستی باعث اختلال جدی در ماموریت کلان سازمان می شود.	وقفه در کل زیرساخت ها و سرویس کلیدی سازمان و عدم دسترسی به اطلاعات فوق محرمانه سازمان مرتبط با حاکمیت و یا سازمان بالا دستی باعث اختلال جدی و عدم تحقق اهداف کلان سازمان می شود.	اختیاری	تغییر، جعل و یا حذف اطلاعات مربوط به زیرساخت ها و سرویس کلیدی سازمان موجب صدمه به اعتبار و حسن شهرت و خدشه جدی و فاجعه بار در انجام تعهدات سازمان می شود.

کارگاه آموزشی عدد و سطح هشدار سایبری

کارگاه آموزشی مبتنی بر سناریو نویسی				I + P = S
شماره سناریو	سناریو حمله سایبری	عدد هشدار سایبری از ۰ تا ۸	احتمال وقوع حمله از ۰ تا ۴	شدت پیامد حمله از ۰ تا ۴
۱	سامانه اتوماسیون اداری سازمان			
۲	پورتال سازمان			
۳	سامانه مدیریت هوشمند			
۴	شبکه داخلی یا اینترانت سازمان			

خود آزمایی

۳– راههای مقابله با تهدیدات سایبری نظیر ویروس های رایانه ای و نفوذگر ها عبارتنداز:

الف)تعریف سیاست امنیتی مناسب ب)استفاده کاربران از آنتی ویروس به روز

ج)تهیه بایگانی ازاطلاعات بطوردائم ومستمر د)همه موارد

۴– حملات فعال (Active) سایبری عبارتند از :

الف) نظارت پنهانی بر تبادل اطلاعات در شبکه (Sniffer) ب) بات نت

ج) قطع خدمات (DOS) د) ب و ج

۵– کدامیک از مواردزیرازعلائم وجودویروس دریک رایانه می باشد.

الف)کم شدن سرعت رایانه بیش ازحدمعمول ب)اتفاقات عجیب درصفحه نمایش

ج)کاهش چشمگیرسرعت نصب برنامه د)همه موارد

ویژگی های مشترک حملات ارتش های سایبری

- حملات همگی هدفمند بودند.
- حملات با شناسایی قبلی از هدف طراحی شده بودند.

این شناسایی شامل اطلاعات سیستمها به ویژه آسیب پـــذیریهای امنیتی بود.

- روش انتشار به گونه ای است که عدم اتصال به اینترنـــت هم راهکار مفیدی نبوده است.
- حملات با دانش فنی بالا و خیلی پیچیده طراحـــی شـــده بودند.
- همگی از آسیب پذیری های جدید و ناشـــناخته (0-day) بهره می بردند.

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.

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

(شبکه های مخابراتی ، نیروگاه ها، پالایشگاه ها، تاسیسات هسته ای، بانکی و ....)

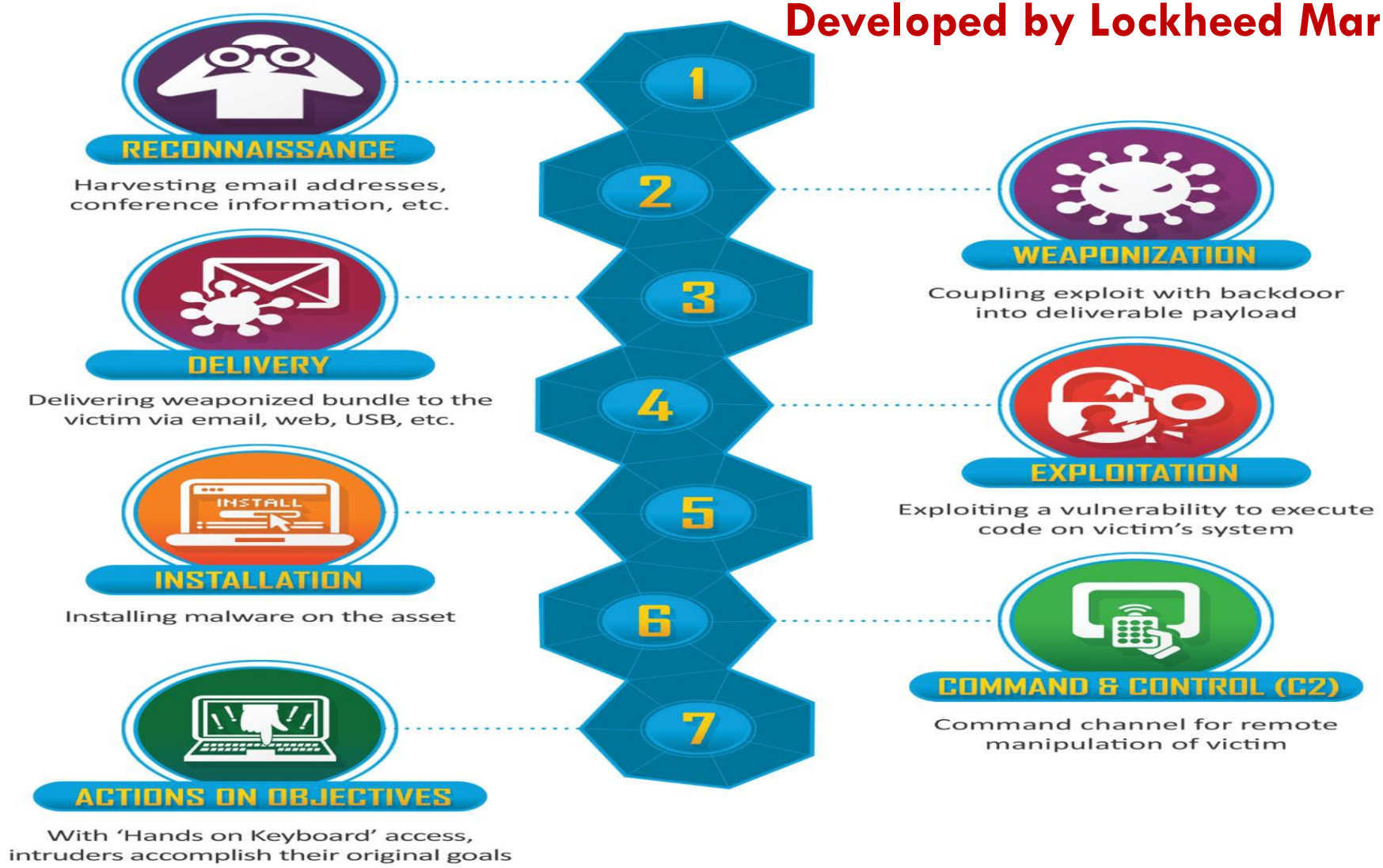
تشکیل یگان های سایبر در اکثر کشورها بویژه : ناتو، انگلیس، ترکیـــه، رژیم صهیونیستی

اجرای مانورهای مختلف سایبری در مقاطع مختلف

انجام حملات سایبری مختلف از قبیل حمله استاکس نت

Cyber Kill Chain

Developed by Lockheed Martin



تحلیل آسیب‌پذیری ها

- تعریف آسیب‌پذیری سایبری
- انواع آسیب‌پذیری سایبری
- روش‌های شناسایی آسیب‌پذیری سایبری
- آشنایی با نمونه‌هایی از پویش‌گرهای آسیب‌پذیری سایبری
- توصیه‌های ضروری به‌منظور پیش‌گیری از ایجاد آسیب پذیری
- متدولوژی احصای آسیب پذیری ها
- مروری بر آسیب پذیری های احصاء شده
- توصیه‌های ضروری به‌منظور پیش‌گیری /کاهش آسیب‌پذیری

تعریف آسیب پذیری سایبری

- **آسیب‌پذیری**، ضعفی است که در یک سرمایه سایبری یا مکانیزم های امنیتی آن سرمایه وجود دارد و می‌تواند توسط یک یا چند تهدید، مورد بهره‌برداری قرار گیرد.
- انواع آسیب پذیری، از نظر زمان ایجاد
- انواع آسیب پذیری، از نظر پیامد

انواع آسیب پذیری، از نظر وضعیت کشف و استفاده

- آسیب‌پذیری سایبری، از نظر وضعیت کشف، به دو دسته‌ی شناخته شده (کشف شده) و ناشناخته (کشف نشده) تفکیک می‌شود.
- چرخه‌ی حیات یا مدل تعالی یک آسیب‌پذیری، از شش مرحله‌ی «ایجاد توسط منشأ»، «کشف»، «بهره‌برداری توسط مهاجم»، «افشاء وجود یا بهره‌برداری»، «عرضه‌ی وصله توسط سازنده» و «رفع / وصله‌زنی توسط استفاده‌کننده» تشکیل می‌شود.

شش مرحله چرخه حیات آسیب پذیری در هشت وضعیت زمانی

روش های شناسایی آسیب پذیری سایبری

برای شناسایی آسیب پذیری سایبری، چهار روش اصلی، به شرح ذیل، وجود دارد :

- مراجع آگاهی رسانی و پایگاه های داده آسیب پذیری این مراجع
- پویش آسیب پذیری برای کشف آسیب پذیری های ؟
- تست نفوذبرای کشف آسیب پذیری های ؟
- ارزیابی عملکرد، ارزیابی امنیتی و ارزیابی پدافندی مبتنی بر تحلیل شکاف شناسایی ضعیفترین حلقه ها در ۳ حوزه فرایندی و سیستمی، منابع انسانی و فناورانه طبق روشگان PPT

نمونه هایی از پویش گرهای آسیب پذیری سایبری

❖ پویش گر آسیب پذیری Nessus

این پویش گر، قادر به شناسایی آسیب پذیری موجود در محدوده ی گسترده ای از انواع سیستم عامل های مختلف، پایگاه های داده، نرم افزارهای کاربردی، تجهیزات مورد استفاده در زیرساخت ابری و تجهیزات شبکه های مجازی و فیزیکی می باشد .

❖ پویش گر آسیب پذیری OpenVAS

یک پویش گر متن باز است که علاوه بر پویش و شناسایی آسیب پذیری، یک ابزار ارزیابی امنیتی و مدیریت آسیب پذیری نیز محسوب می شود

❖ پویش گر آسیب پذیری Retina CS

یک پویش گر متن باز و برخوردار از کنسول مبتنی بر وب است که علاوه بر پویش و شناسایی آسیب پذیری، یک ابزار بسیار ساده و متمرکز برای مدیریت آسیب پذیری نیز محسوب می شود.

نمونه هایی از پویش گرهای آسیب پذیری سایبری

❖ پویش گر آسیب پذیری MBSA

این ابزار، از طریق پویش به روزرسانی¬های انجام شده و Service Packهای نصب شده، اقدام به شناسایی پیکربندی نادرست، فقدان به روزرسانی و فقدان نصب وصله های امنیتی می نماید. این ابزار در خاتمه ی پویش، اقدام به ارائه ی راه حل مناسب برای رفع آسیب پذیری های شناسایی شده نیز می نماید.

❖ پویش گر آسیب پذیری Nexpose

یک ابزار پویش متن باز آسیب پذیری است. این ابزار، علاوه بر پویش آسیب پذیری، اقدام به انجام تعداد زیادی بررسی در شبکه می¬کند، مثلاً در صورت اتصال هر وسیله ی جدید به شبکه، این ابزار، اقدام به پویش خودکار آسیب پذیری های موجود در آن وسیله نموده و آنها را گزارش می نماید.

❖ پویش گر آسیب پذیری Tripwire IP360

این محصول، آسیب پذیری ها، پیکربندی ها، کاربردها، میزبان ها، ایستگاه های کاری و ... را در محدوده ی گسترده ای از شبکه ها، شناسایی می کند و بر اساس استانداردهای باز، اقدام به مدیریت مخاطره می نماید.

نمونه هایی از پویش گرهای آسیب پذیری سایبری

acunetix

برخی از قابلیت‌های پویشگر Acunetix

- بررسی روش‌های گوناگون SQL Injection و XSSکه جزو پرمخاطره‌ترین حملات علیه کاربردهای وب هستند
- بررسی آسیب پذیری‌های مشخص شده در ده گروه OWASP و امکان گزارش گیری انطباقی با OWASP Top 10
- اجرای جستجوهای Google hacking database
- شناسایی نوع وب‌سرور و زبان استفاده شده
- پویش پورت‌ها و بررسی امنیتی برنامه‌های وب در حال اجرا بر روی آنها
- پیمایش همزمان صفحات وب با توجه به معماریMulti-thread
- امکان تعریف CAPTCHA و عبور از آن با توجه به تنظیمات انجام شده
- قابلیت زمانبندی به منظور اجرای خودکار برای انجام پویش‌های دوره‌ای
- گزارش‌دهی جامع و ارائه گزارش‌های انطباقی با استانداردهایی از قبیل OWASP Top 10وPCI-DSS

توصیه‌های ضروری به‌منظور پیش‌گیری /کاهش آسیب‌پذیری

- محصولات و خدمات سایبری را از تولیدکننده یا عرضه‌کننده‌ی معتبر و دارای گواهی از مراجع ذی‌صلاح قانونی خریداری نمائید.
- در انتخاب محصولات سایبری، امنیت سایبری و پدافند سایبری، یک ویژگی کلیدی را ابتدا مورد توجه قرار دهید. که محصول موردنظر، حتماً دارای گواهی اعتبار عملکردی و امنیتی از مراجع ذی‌صلاح قانونی باشد.
- در انتخاب محصولات و خدمات سایبری، به هشدارهای مراجع آگاهی‌رسانی امنیت و پدافند سایبری، به ویژه پایگاه اطلاع‌رسانی پدافند سایبری کشور و مرکز ماهر وزارت ارتباطات و فناوری اطلاعات، توجه نمائید.
- به‌صورت مداوم و دوره‌ای، به پایگاه‌های داده آسیب‌پذیری داخلی و خارجی معتبر، مراجعه و از آخرین اخبار آسیب‌پذیری‌های مرتبط با محصولات و خدمات سایبری مورد استفاده در سازمان خود، مطلع شوید .
- وصله‌های امنیتی ارائه شده توسط سازندگان محصولات یا عرضه‌کنندگان خدمات سایبری مورد استفاده در سازمان خود را در اسرع وقت و به‌صورت دقیق، بر اساس راهنمای ارائه شده توسط سازنده، نصب نموده و مورد بهره‌برداری قرار دهید.

توصیه‌های ضروری به‌منظور پیش‌گیری /کاهش آسیب‌پذیری

- راهکارهای ارائه شده برای رفع یا کاهش آسیب‌پذیری توسط پایگاه اطلاع رسانی پدافند سایبری کشور یا مرکز ماهر وزارت ارتباطات و فناوری اطلاعات را مورد توجه و بهره‌برداری قرار دهید.
- به‌صورت مداوم و دوره‌ای، اقدام به پویش امنیتی کلیه بخش‌های شبکه ارتباطی و کلیه سامانه‌های اطلاعاتی سازمان خود، با بهره‌گیری از پویش گرهای آسیب‌پذیری مورد تائید مرکز پدافند سایبری کشور نمائید.
- به‌منظور کشف آسیب‌پذیری‌های ناشناخته، به‌صورت مداوم و دوره‌ای، بخش‌های کلیدی شبکه و سامانه‌های اطلاعاتی کلیدی سازمان خود را مورد تست نفوذ قرار دهید. برای این امر، حتماً از تیم‌های خبره و مورد تائید مرکز پدافند سایبری کشور، استفاده نمائید .

متدولوژی احصای آسیب پذیری ها

ردیف	نوع آسیب پذیری	آسیب پذیری درحوزه IT و کنترل صنعتی
۱	سازمان	ضعف در ارتباط با نهادهای حاکمیتی و تخصصی امنیت سایبری
۲	سازمان	ضعف درطبقه‌بندی اطلاعات و روال گردش اطلاعات طبقه‌بندی شده و کنترل مستندات
۳	سازمان	ضعف در کنترل تغییرات
۴	سازمان	ضعف در مدیریت حوادث امنیت اطلاعات
۵	سازمان	ضعف در مدیریت دارایی‌ها
۶	سازمان	ضعف در مدیریت دسترسی
۷	سازمان	ضعف در ملاحظات امنیتی برای ارتباط با تأمین‌کنندگان
۸	سازمان	عدم درج الزامات امنیتی در قراردادها و مقررات
۹	سازمان	نبود یا عدم کفایت خط مشی میز پاک صفحهٔ پاک
۱۰	سازمان	ضعف یاعدم ارزیابی مخاطرات امنیتی در فعالیتهای IT

متدولوژی احصای آسیب پذیریها

ردیف	نوع آسیب پذیری	آسیب پذیری درحوزه IT و کنترل صنعتی
۱	نرم افزار	ضعف در اعمال کنترل های مناسب بر کدهای منبع
۲	نرم افزار	ضعف در بروز رسانی نسخه ها و وصله های جدید
۳	نرم افزار	ضعف در ثبت و مدیریت لاگ ها
۴	نرم افزار	ضعف در اعمال محدویت نصب نرم‌افزار
۵	نرم افزار	ضعف در کنترل کارآمد تغییرات مرتبط با نرم افزار
۶	نرم افزار	عدم استفاده از Captcha
۷	نرم افزار	عدم تعیین لیست نرم افزاری مجاز
۸	نرم افزار	عدم خروج قطعی از نرم افزار در هنگام ترک ایستگاه کاری
۹	نرم افزار	فقدان یا ضعف در رسیدگی به آسیب پذیری های فنی

متدولوژی احصای آسیب پذیریها

ردیف	نوع آسیب پذیری	آسیب پذیری درحوزه IT و کنترل صنعتی
۱	سخت افزار	آسیب پذیری درمقابل تغییرات دما
۲	سخت افزار	ضعف در کنترل تغییرات ولتاژ و شبکه برق ناپایدار
۳	سخت افزار	ضعف در امحاء
۴	سخت افزار	ضعف در آماده سازی تجهیزات جایگزین
۵	سخت افزار	ضعف در سیستم اعلام و اطفاء حریق
۶	سخت افزار	ضعف در فعالیتهای تعمیر و نگهداری سخت افزار
۷	سخت افزار	ضعف در کنترل استفاده از تجهیزات سیار
۸	سخت افزار	ضعف در کنترل تشعشعات الکترومغناطیسی و شوکهای الکترونیکی
۹	سخت افزار	عدم کفایت وجود دوربین های مدار بسته
۱۰	سخت افزار	لوله کشی نامناسب آب و فاضلاب

متدولوژی احصای آسیب پذیریها

ردیف	نوع آسیب پذیری	آسیب پذیری درحوزه IT و کنترل صنعتی
۱	شبکه	ارتباط بدون محافظت به شبکه عمومی
۲	شبکه	ضعف در سیستم های مخابراتی
۳	شبکه	ضعف در مدیریت ترافیک شبکه
۴	شبکه	ضعف در مدیریت حسابهای کاربری
۵	شبکه	ضعف در مقابله با بدافزارها
۶	شبکه	ضعف ساختاری در معماری شبکه
۷	شبکه	باز بودن پورت های بلا استفاده
۸	شبکه	ضعف در تفکیک شبکه ها
۹	شبکه	عدم رمزنگاری پیام های ارسالی یا دریافتی
۱۰	شبکه	کابل کشی یا اتصالات و ارتباطات ضعیف

متدولوژی احصای آسیب پذیریها

ردیف	نوع آسیب پذیری	آسیب پذیری درحوزه IT و کنترل صنعتی
۱	منابع انسانی	ضعف در روش های استخدام
۲	منابع انسانی	ضعف درآموزش امنیت اطلاعات
۳	منابع انسانی	ضعف در استفاده صحیح و مناسب از دارایی های اطلاعاتی سازمان
۴	منابع انسانی	ضعف در آگاهی امنیتی
۵	منابع انسانی	ضعف در تعریف و استفاده از کلمه عبور
۶	منابع انسانی	ضعف در رویه های ورود امن به سیستم
۷	منابع انسانی	ضعف در سازوکار پایش امنیت اطلاعات
۸	منابع انسانی	ضعف در همراهی و مراقبت ورود افراد به مناطق امن
۹	منابع انسانی	عدم کفایت الزامات امنیت اطلاعات در قرارداد کارمندان
۱۰	منابع انسانی	عدم کفایت خط مشی های لازم برای کاربرد صحیح رسانه های مخابراتی و پیام

متدولوژی احصای آسیب پذیریها

ردیف	نوع آسیب پذیری	آسیب پذیری درحوزه IT و کنترل صنعتی
۱	مکان و سایت	ضعف در حفاظت فیزیکی از ساختمان، درها و پنجره ها
۲	مکان و سایت	ضعف در کنترل میزان عوامل محیطی از جمله رطوبت، غبار وآلودگی
۳	مکان و سایت	ضعف در کنترل های دسترسی فیزیکی برای ساختمان ها و اتاق ها
۴	مکان و سایت	واقع شدن در ناحیه ای آسیب پذیر نسبت به آتشفشان و یا مواد قابل اشتعال
۵	مکان و سایت	واقع شدن در ناحیه ای آسیب پذیر نسبت به پدیده های جوی ومحیطی (تغییرات نور، دماو ارتفاع)
۶	مکان و سایت	واقع شدن در ناحیه ای آسیب پذیر نسبت به زلزله
۷	مکان و سایت	واقع شدن در ناحیه ای آسیب پذیر نسبت به سیل و یا آسیب های مربوط نشت آب

مروری بر آسیب پذیری های احصاء شده

شبکه

- خطوط ارتباطی محافظت نشده
- ترافیک محافظت نشده
- انتقال کلمه رمز ناامن
- طرح امنیت ناقص
- کابل کشی نامناسب

نرم‌افزار

- حفره‌های شناسایی نشده در نرم‌افزار
- پشتیبان‌گیری نامناسب
- عدم مدیریت مناسب سطوح دسترسی
- فقدان مستندات راهنما
- عدم تست کافی هنگام پذیرش

سخت‌افزار

- خرابی تجهیزات
- جانمایی نامناسب
- تعمیرات ناامن
- حساسیت به نوسانات ولتاژ
- حساسیت به رطوبت و گرد و غبار

کارکنان | پیمانکاران | سایت سازمان | اسناد کاغذی | و ...

مروری بر آسیب پذیری های احصاء شده

شبکه

- خطوط ارتباطی محافظت نشده
- ترافیک محافظت نشده
- انتقال کلمه رمز ناامن
- طرح امنیت ناقص
- کابل کشی نامناسب

نرم‌افزار

- حفره‌های شناسایی نشده در نرم‌افزار
- پشتیبان‌گیری نامناسب
- عدم مدیریت مناسب سطوح دسترسی
- فقدان مستندات راهنما
- عدم تست کافی هنگام پذیرش

سخت‌افزار

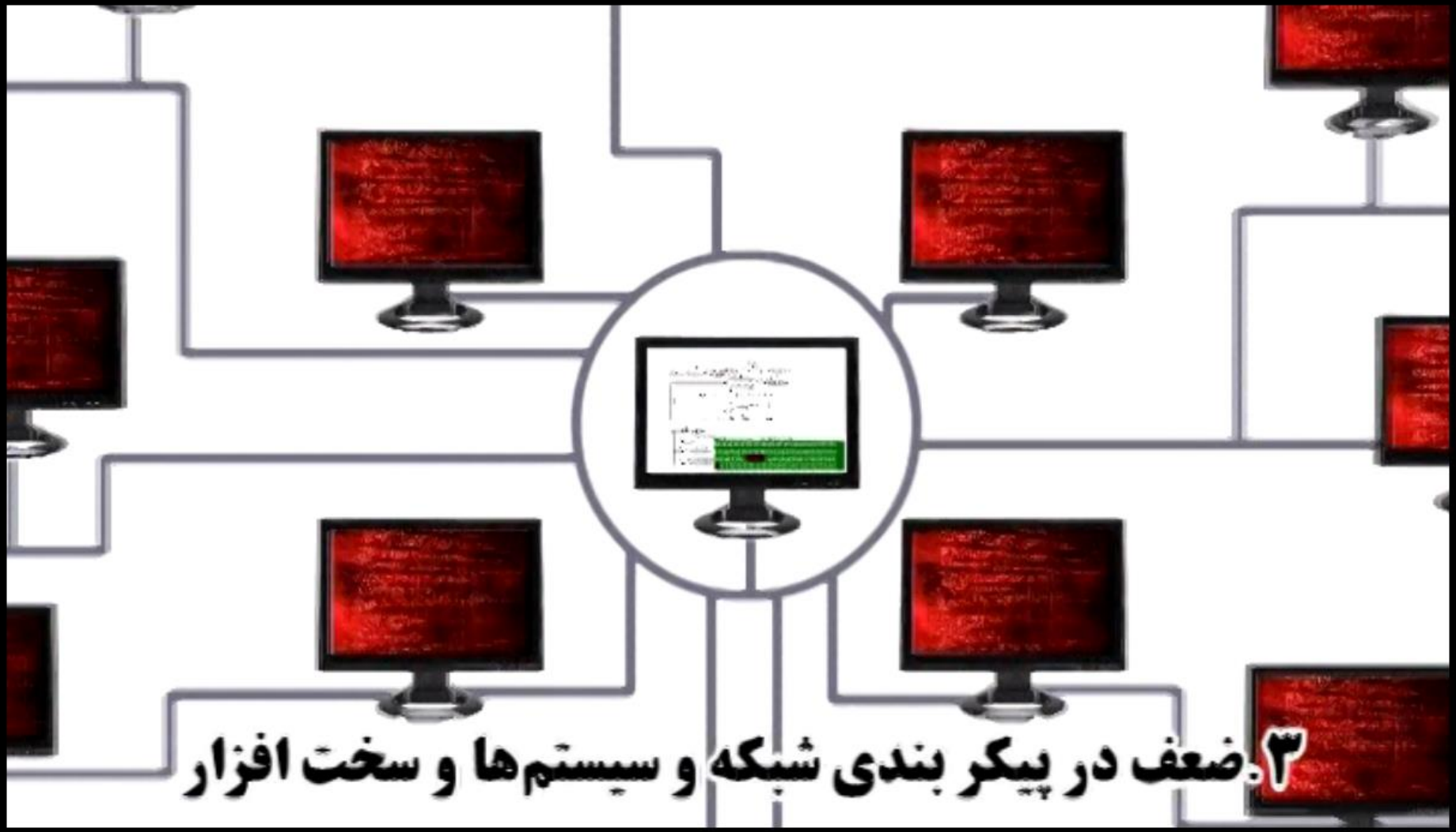
- خرابی تجهیزات
- جانمایی نامناسب
- تعمیرات ناامن
- حساسیت به نوسانات ولتاژ
- حساسیت به رطوبت و گرد و غبار

کارکنان | پیمانکاران | سایت سازمان | اسناد کاغذی | و ...

مروری بر آسیب پذیری های احصاء شده

مروری بر آسیب پذیری های احصاء شده

مروری بر آسیب پذیری های احصاء شده



تحلیل و ارزیابی تهدید ها

VERIS (the Vocabulary for Event Recording and Incident Sharing)

تعداد حوادث	۸۸۹۳	از	۷/۲۹/۲۰۲۱
دسته دارایی	مجموع تعداد تهدید / صنعت	درصد	شاخص
سازمانی	۴۴۵۸	۵۰٪	۳
برنامه های کاربردی	۱۲۵۳	۱۴٪	۱
داده	۴۴۵۸	۵۰٪	۳
تجهیزات	۷۹۸	۹٪	۱
شبکه	۶۲	۱٪	۱
کاربران	۴۴۵۸	۵۰٪	۳
ناشناخته	۸۶۳	۱۰٪	۱

تحلیل و ارزیابی تهدید ها

VERIS Community Database (VCDB)

جستجوی فهرست VCDB	عدد بلوغ	شاخص VCDB	نمره تهدید مورد انتظار
۵۱	۵	۱	۱
۵۲	۵	۲	۱
۵۳	۵	۳	۱
۵۴	۵	۴	۲
۵۵	۵	۵	۲
۴۱	۴	۱	۱
۴۲	۴	۲	۲
۴۳	۴	۳	۲
۴۴	۴	۴	۳
۴۵	۴	۵	۳
۳۱	۳	۱	۱
۳۲	۳	۲	۲
۳۳	۳	۳	۳
۳۴	۳	۴	۴
۳۵	۳	۵	۵
۲۱	۲	۱	۳
۲۲	۲	۲	۳
۲۳	۲	۳	۴
۲۴	۲	۴	۴
۲۵	۲	۵	۵
۱۱	۱	۱	۴
۱۲	۱	۲	۴
۱۳	۱	۳	۵
۱۴	۱	۴	۵
۱۵	۱	۵	۵

لیستی از تهدیدات و منابع تهدید رایج

نوع	تهدید	منبع
آسیب فیزیکی	آتش‌سوزی	عمدی– اتفاقی– محیطی
	خرابی آب	عمدی– اتفاقی– محیطی
	آلودگی	عمدی– اتفاقی– محیطی
	سانحه اصلی	عمدی– اتفاقی– محیطی
	آسیب به تجهیزات و یا رسانه	عمدی– اتفاقی– محیطی
	آلودگی، خوردگی و انجماد	عمدی– اتفاقی– محیطی
رویدادهای طبیعی	پدیده اقلیمی	محیطی
	پدیده زلزله	محیطی
	پدیده آتش‌فشان	محیطی
	سیل	محیطی
ازدست‌رفتن خدمات ضروری	خرابی تهویه هوا یا سامانه تامین آب	عمدی – اتفاقی
	خرابی منبع نیرو	عمدی – اتفاقی – محیطی
	خرابی تجهیزات ارتباطی راه دور	عمدی – اتفاقی – محیطی
اختلال بر اساس تشعشع	تشعشات الکترومغناطیسی	عمدی – اتفاقی – محیطی
	تشعشع حرارتی	عمدی – اتفاقی – محیطی
	پالس‌های الکترومغناطیسی	عمدی – اتفاقی – محیطی
به خطر افتادن عملکردها	اشکال در استفاده	اتفاقی
	سوءاستفاده از حقوق	عمدی– اتفاقی
	تخطی از حقوق	عمدی
	انکار اقدامات	عمدی
	نقض در دسترس‌بودن پرسنل	عمدی– اتفاقی – محیطی
به خطر افتادن عملکردها	اشکال در استفاده	اتفاقی
	سوءاستفاده از حقوق	عمدی– اتفاقی

نوع	تهدید	منبع
به خطر افتادن اطلاعات	پذیرش قطع تداخل سیگنال‌ها	عمدی
	جاسوسی از راه دور	عمدی
	شنود	عمدی
	سرقت اسناد	عمدی
	سرقت تجهیزات	عمدی
	بازیابی رسانه بازیافتی یا رهاشده	عمدی
	افشاء	عمدی – اتفاقی
	بازیابی داده از منابع نامعتبر	عمدی– اتفاقی
	تحریف سخت‌افزار	عمدی
	تحریف نرم‌افزار	عمدی– اتفاقی
	شناسایی موقعیت	عمدی
شکست فنی	خرابی تجهیزاتی	اتفاقی
	اشکال تجهیزات	اتفاقی
	اشباع سامانه اطلاعات	عمدی– اتفاقی
	نقص نرم افزار	اتفاقی
	نقض نگهداری اطلاعات سامانه	عمدی– اتفاقی
اقدامات غیرمجاز	استفاده غیرمجاز از تجهیزات	عمدی
	رونوشت جعلی از نرم‌افزار	عمدی
	استفاده از نرم‌افزارهای تقلبی و یا رونوشت‌شده	عمدی– اتفاقی
	خرابی داده‌ها	عمدی
	پردازش غیرقانونی داده‌ها	عمدی

تحلیل مخاطرات و تاب آوری

مخاطره

محرّک

آسیب پذیری

تهدید

سه عنصر تشکیل دهنده ریسک های امنیتی

مراحل ارزیابی مخاطرات امنیتی

۱.شناسایی **مخاطرات** وتعیین **مالکان** مخاطره

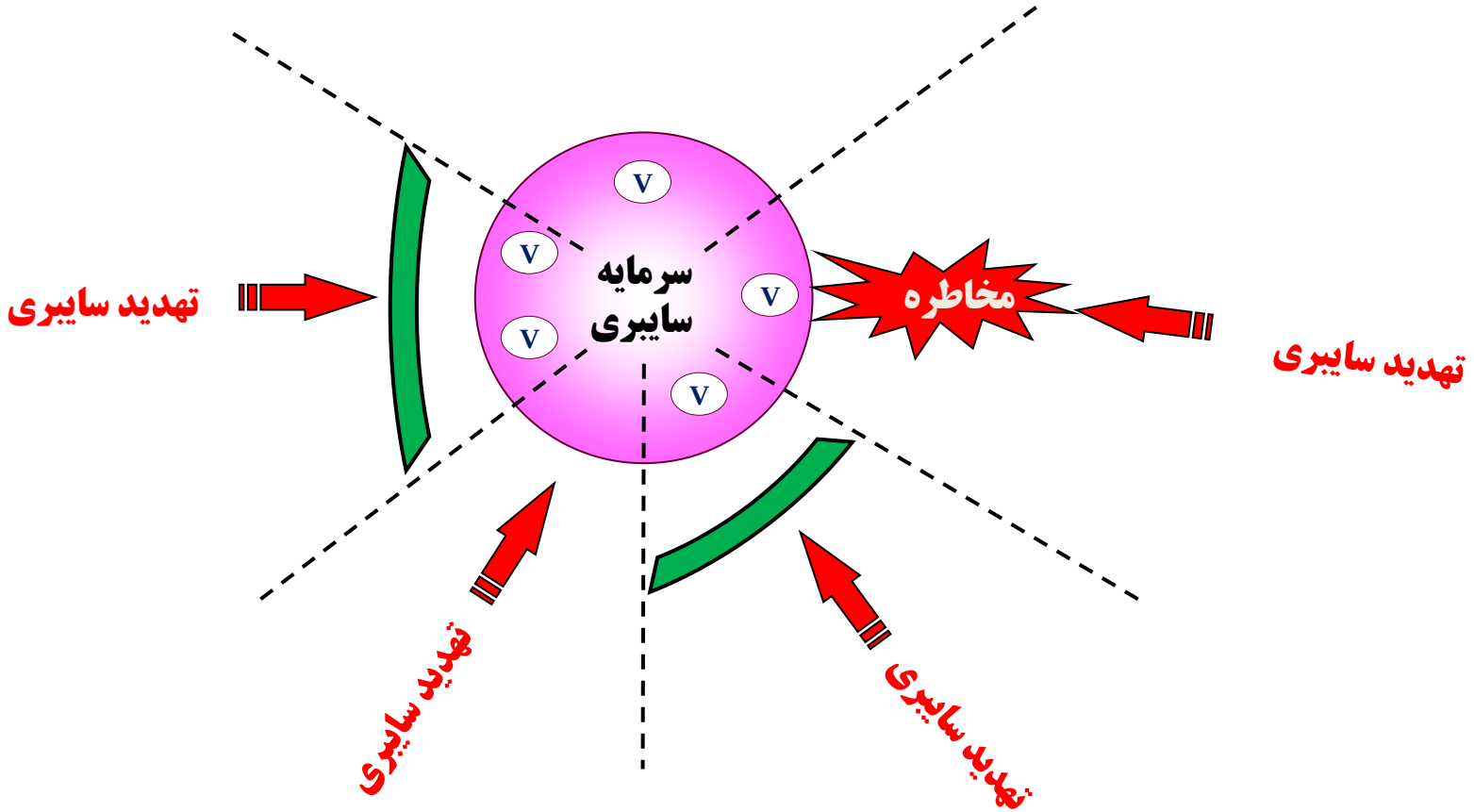
- شناسایی **دارایی‌های** اطلاعاتی موجود در دامنه
- شناسایی **تهدیدات** علیه دارایی‌ها و توانمندی‌ها
- شناسایی **آسیب‌پذیری‌های** متناظر با دارایی ها

۲.تحلیل مخاطرات

۳.ارزشیابی مخاطرات

سازمان باید مخاطرات امنیتی را ارزیابی کند.

مدیریت مخاطرات و تاب آوری



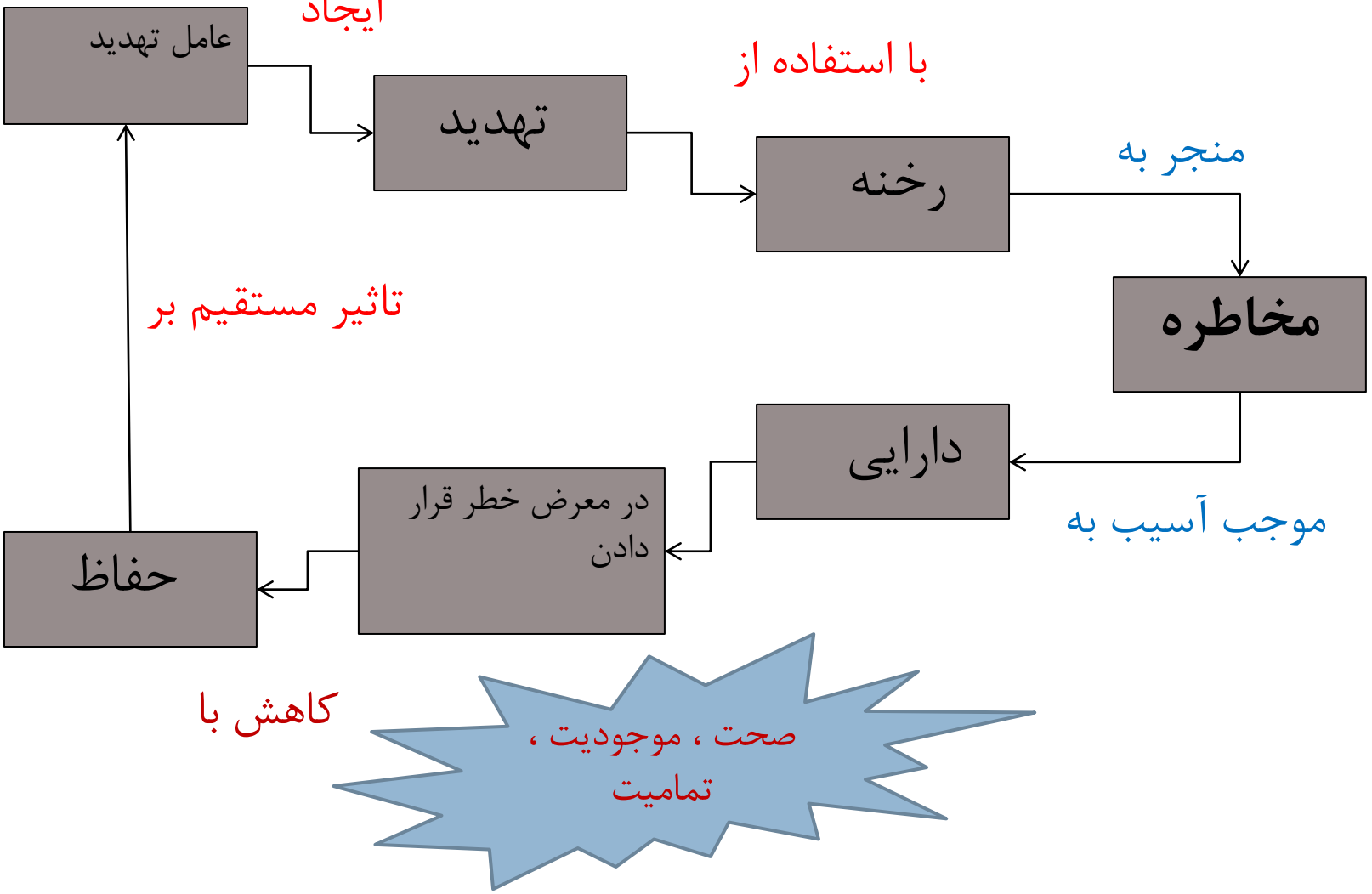
مدیریت مخاطره چیست؟

مدیریت مخاطره، فرایند شناسایی و ارزیابی مخاطرات، کاهش آن به سطح قابل قبول و اجرای ساز و کار مناسبی که مخاطره را در سطح مطلوب نگه دارد.

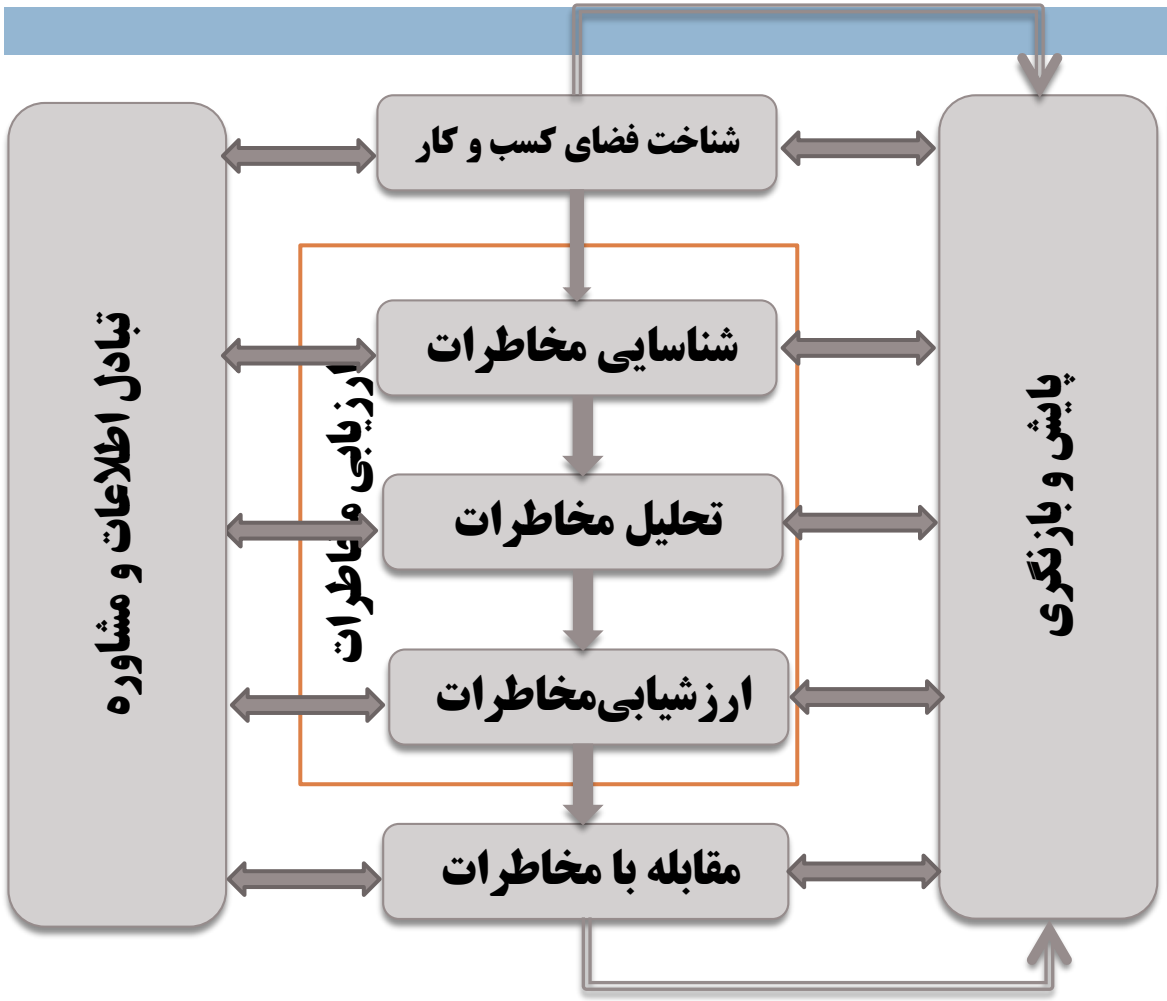
مدیریت مخاطرات، فعالیت‌های هماهنگ شده برای هدایت و کنترل یک سازمان با توجه به مخاطرات آن.

مدیریت مخاطرات، فرایند شناسایی مخاطرات و انجام گام‌هایی برای کاهش آن‌ها تا سطح قابل قبول است.

روند مدیریت مخاطرات



فرایند مدیریت مخاطرات سایبری



- انتخاب متدلوژی ارزیابی مخاطرات
- شناسایی مخاطرات
- شناسایی مالکان مخاطره
- شناسایی دارایی‌ها
- شناسایی تهدیدات
- شناسایی آسیب‌پذیری‌ها
- تحلیل مخاطرات
- شناسایی پیامدها
- ارزیابی احتمال رخداد مخاطرات
- تعیین سطح مخاطرات
- ارزیابی مخاطرات
- اولویت‌بندی مخاطرات
- تدوین طرح برطرف‌سازی
- اجرای RTP
- پایش اثربخشی

مدل مدیریت ریسکRAMCAP

- برای اولین بار؛ وزارت امنیت داخلی ایالات متحده الگوریتم آن را در هفت مرحله مدیریت ریسک و بحران تنظیم نمود.
- این متدولوژی که بر اساس مدیریت ریسک تنظیم شده بود، توسط سازمان پدافند غیر عامل ایران مورد ارزیابی قرار گرفت از ۷ گام به هفده گام افزایش یافت و به سازمان ها ابلاغ گردید. بر اساس این متدولوژی همه سازمان ها و وزارت خانه ها ملزم به اجرای آن می باشند.

انواع روش های مدل یافته

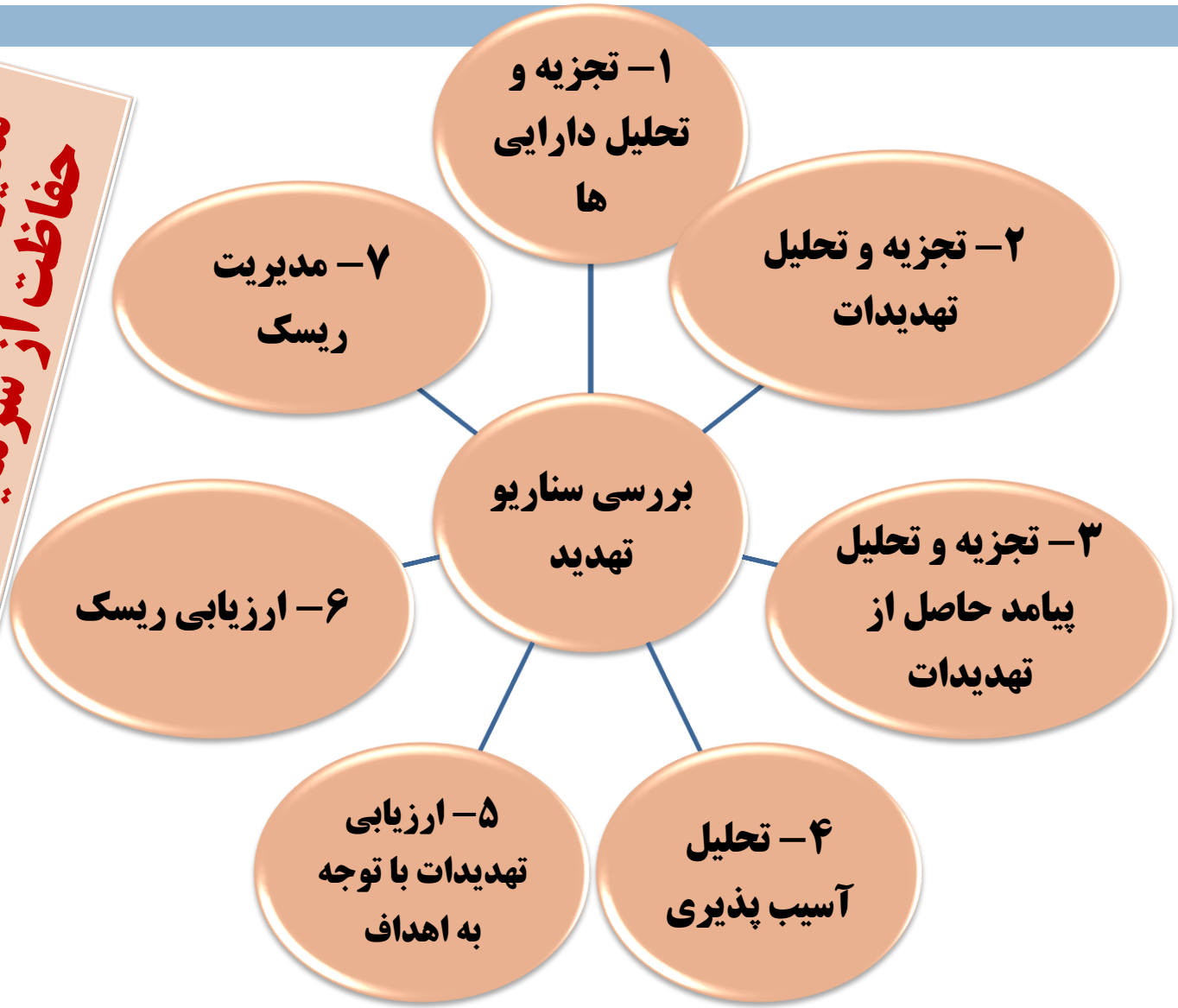
❖ مدل مدیریت ریسک RAMCAP

Risk Analysis & Management For Critical Asset Protection

❖الگوی مطالعات تهدید شناسی به روش مثلث ATV (دارایی، تهدید، آسیب)

هفت گام اصلی RAMCAP

مدیریت و تحلیل ریسک برای حفاظت از سرمایه های کلیدی



مدیریت مخاطرات زیرساخت ها و سرویس های کلیدی

گام اول
شناسایی قلمرو سازمان و تعیین چارچو ب RMF

گام دوم:
شناسایی سرمایه های سایبری

گام سوم:
بررسی تهدیدات متصور

گام چهارم:
بررسی آسیب پذیری ها و پیامد ها بر دارایی

گام پنجم:
شناسایی مخاطرات و بررسی وابستگی های متقابل

گام ششم:
تحلیل مخاطرات سایبری

گام هفتم:
طرح کاهش مخاطرات RRP

گام هشتم:
تصویب و ابلاغ برنامه VRP

مدیریت مخاطرات سایبری

تعیین دامنه برآورد

- ✓ دامنه برآورد تعیین می‌کند که چه چیزهایی باید در برآورد لحاظ شوند.
- ✓ در تعیین دامنه برآورد، بررسی سه مورد ضروری است:
  - قابلیت اجرایی سازمان
  - چارچوب زمانی مؤثر
  - معماری سازمانی

مدیریت مخاطرات زیرساخت ها و سرویس ها مبتنی بر CIS RAM V08

- **مدیریت و ارزیابی مخاطرات سایبری سازمان و سناریوهای مرتبط مبتنی بر وابستگی های متقابل و بر اساس روشگان بهینه CIS-RAM نسخه ۸ و گروه پیاده سازی ۳ که مدیریت مخاطرات آن کنترل محور بوده و شامل ۱۸ حوزه کنترلی و ۱۵۳ کنترل به شرح ذیل می باشد.**

جدول معیارهای ۴ گانه امتیاز دهی بلوغ

امتیازات بلوغ ۴ معیار از ۵	خط مشی تعریف شده	کنترل پیاده‌سازی شده	کنترل خودکار	کنترل گزارش شده	امتیازات بلوغ هر کنترل امنیت سایبری
1	بدون خط مشی	پیاده‌سازی نشده	غیر خودکار (به صورت دستی)	گزارش نشده	1
2	خط مشی غیر رسمی	برخی از خط مشی پیاده‌سازی شده	بخش های از خط مشی خودکار شده	بخش های از خط مشی گزارش شده	2
3	خط مشی تا حدی نوشته شده	در برخی سیستم ها پیاده‌سازی شده	خودکار در برخی از سیستم ها	گزارش شده در برخی از سیستم ها	3
4	خط مشی مکتوب	در اکثر سیستم ها پیاده‌سازی شده	خودکار در اکثر سیستم ها	گزارش شده در اکثر سیستم ها	4
5	خط مشی کتبی تصویب شده	در تمام سیستم ها پیاده‌سازی شده	خودکار در تمام سیستم ها	گزارش شده در تمام سیستم ها	5
ناشناخته – بدون امتیاز	تعریف نشده	تعریف نشده	تعریف نشده	تعریف نشده	ناشناخته – بدون امتیاز
نامعلوم – N/A	کاربرد نا پذیر	کاربرد نا پذیر	کاربرد نا پذیر	کاربرد نا پذیر	نامعلوم – N/A

مدیریت مخاطرات سایبری

قابلیت اجرایی

- ✓ قابلیت اجرایی تعیین‌کننده توان و ظرفیت همه‌جانبه سازمان برای اعمال روند مدیریت مخاطرات در حوزه فناوری اطلاعات است.
- ✓ با شناسایی محدودیت‌های اثرگذار در تعیین دامنه برآورد، می‌توان به تشخیص قابلیت اجرایی برآورد، کمک کرد . برخی از محدودیت‌ها عبارت‌اند از :

- فرآیندهای قبل
- فنی
- مالی
- زیست محیطی
- زمانی
- راهکاری
- سازمانی (عملیاتی، منابع انسانی، توسعه، روابط خارجی)

مدیریت مخاطرات سایبری

تعیین منابع اطلاعات

- ✓ لزوم استفاده از منابع اطلاعاتی معتبر داخلی و خارجی جهت تعیین تهدیدات، آسیب پذیری‌ها و پیامدهای ناشی از آن‌ها

منابع داخلی:

- گزارش‌های برآورد مخاطرات
- گزارش‌های رخدادهای امنیتی
- بایگانی وقایع امنیتی ثبت‌شده
- بایگانی مشکلات و نتایج بازرسی-های قبل

منابع خارجی:

- مرکز ماهر و مراکز آپای کشور
- شرکای سازمان
- مراکز تحلیل و اشتراک اطلاعات
- سازمان‌های غیردولتی تحقیقاتی

آشنایی با یک روش فراگیر ارزیابی مخاطرات امنیتی

برآورد

- ✓ برآورد مخاطرات، فرآیند تعیین مخاطرات امنیت اطلاعات و تخمین ارزش و اولویت بندی است.
- ✓ برآورد مخاطرات مستلزم تحلیل دقیق تهدیدات و آسیب‌پذیری‌ها برای تعیین اینکه چه شرایطی یا وقایعی و با چه احتمال وقوعی، مستعد اثر نامطلوب هستند، می-باشد.
- ✓ برآورد مخاطرات شامل ۱۰ فاز می‌باشد که عبارتند از:

لیستی از آسیب پذیری ها و تهدیدات رایج

نوع	آسیب پذیری	تهدید
سخت‌افزار	تعمیر و نگهداری ناقص رسانه‌های ذخیره-سازی اطلاعات	نقص در سیستم اطلاعات قابل نگهداری
	نقص طرح جایگزینی تناوبی	تخریب تجهیزات و رسانه‌ها
	حساسیت به گرد و خاک و رطوبت	خوردگی تجهیزات و رسانه‌ها
	حساسیت به امواج الکترومغناطیسی	اختلال در تجهیزات الکترونیکی و مخابراتی
	نقص تنظیمات کنترل تغییرات	خطا در استفاده
	حساسیت به تغییرات ولتاژ	از دست‌دادن منبع تغذیه
	حساسیت به تغییرات دما	اثر سوء بر تجهیزات شبکه نظیر سوئیچ ها
	رسانه‌های ذخیره‌سازی محافظت نشده	سرقت از رسانه‌ها و یا اسناد
	نقص مراقبت در دسترس	سرقت از رسانه‌ها و یا اسناد

لیستی از آسیب پذیری ها و تهدیدات رایج

نوع	آسیب پذیری	تهدید
نرم‌افزار	نقص یا تست ناکافی نرم‌افزار	سوءاستفاده از حقوق
	نقص شناخته شده در نرم‌افزار	سوءاستفاده از حقوق
	خارج نشدن از حساب کاربری در حین خارج شدن از پشت ایستگاه کاری	سوءاستفاده از حقوق
	دفع یا استفاده مجدد از رسانه‌های ذخیره‌سازی بدون پاک سازی مناسب	سوءاستفاده از حقوق
	نقص در ممیزی	سوءاستفاده از حقوق
	دادن مجوزهای دسترسی اشتباه	سوءاستفاده از حقوق
	توزیع نرم‌افزار به صورت گسترده	تحریف در داده ها
	استفاده از برنامه‌های کاربردی برای داده‌های نادرست در زمان نامناسب	تحریف در داده ها
	واسط کاربری پیچیده	خطا در استفاده
	رمز عبورهای محافظت نشده	تقلب

نوع	آسیب پذیری	تهدید
نرم‌افزار	نقص سازوکار شناسایی و تصدیق (مانند تصدیق کاربران)	تقلب
	مدیریت رمز عبور ضعیف	تقلب
	خدمات غیر لازم فعال شده	پردازش غیرقانونی
	نرم‌افزارهای جدید تکامل نیافته	نقص نرم‌افزار
	مشخصه‌های ناکامل و ناواضح برای توسعه-دهندگان	نقص نرم‌افزار
	نقص در کنترل تغییرات موثر	نقص نرم‌افزار
	دانلود و استفاده از نرم افزارها به صورت کنترل‌نشده	مداخله و سوءاستفاده در نرم-افزار
	نقص در پشتیبان‌گیری مناسب	مداخله و سوءاستفاده در نرم-افزار
	نقص در حفاظت فیزیکی ساختمان، درب‌ها و پنجره ها	سرقت رسانه‌ها و اسناد
	عدم ایجاد گزارش‌های مدیریتی	استفاده غیرمجاز از تجهیزات

لیستی از آسیب پذیری ها و تهدیدات رایج

نوع	آسیب پذیری	تهدید
شبکه	نقص در مدارک و مستندات ارسال و دریافت پیام	انکار اعمال
	خطوط ارتباطی محافظت-نشده	استراق سمع
	عبور و مرور محسوس محافظت‌نشده	استراق سمع
	کابل‌کشی ضعیف	معیوب بودن تجهیزات ارتباطی
	نقص در شناسایی و تصدیق فرستنده و گیرنده	تقلب
	ساختار شبکه ناامن	جاسوسی از راه دور
	انتقال رمزهای عبور	جاسوسی از راه دور
	مدیریت شبکه نامناسب	اشباع سیستم اطلاعاتی
	اتصالات شبکه عمومی محافظت نشده	استفاده از تجهیزات بدون تصدیق

نوع	آسیب پذیری	تهدید
کارکنان	غیبت کارکنان	عدم دسترس-پذیری کارکنان
	فرآیند نامناسب استخدام	تخریب تجهیزات و رسانه‌ها
	آموزش ناکافی امنیتی	خطا در استفاده
	استفاده نادرست از سخت-افزار و نرم‌افزار	خطا در استفاده
	نقص در هشدارهای امنیتی	خطا در استفاده
	نقص در نظارت و پایش سازوکارها	پردازش غیرقانونی
	نقص در سیاست‌های استفاده مناسب از رسانه-های ارتباطی و پیام‌رسان	استفاده تصدیق نشده از تجهیزات

لیستی از آسیب پذیری ها و تهدیدات رایج

نوع	آسیب پذیری	تهدید
سایت سازمان	نقص یا بی دقتی در استفاده از کنترل‌های دسترسی فیزیکی به ساختمان و اتاق ها	تخریب تجهیزات یا محیط
	ناپایداری توان شبکه	نقص توان تغذیه
	نقص در پشتیبانی فیزیکی برای ساختمان و درب‌ها و پنجره‌ها	سرقت تجهیزات
	نقص در رویه‌های رسمی برای دسترسی ثبت‌شده و ثبت‌نشده	سوءاستفاده از حقوق
	نقص در رویه‌های بازبینی دسترسی صحیح (نظارت)	سوءاستفاده از حقوق
	نقص در نارسایی تدارکات متعهدشده (درخصوص امنیت) به مشتریان و/یا شخص سوم	سوءاستفاده از حقوق
	نقص در رویه‌هایی برای پایش از وسایل تحویل اطلاعات	سوءاستفاده از حقوق
	نقص در بازرسی‌های قانونی (نظارت)	سوءاستفاده از حقوق
	نقص در رویه‌های شناسایی مخاطره و ممیزی	سوءاستفاده از حقوق
	نقص در گزارش‌های ثبت شده اشتباه در مدیریت و ثبت وقایع	سوءاستفاده از حقوق
	سرویس نامناسب نگهداری از پاسخ ها	نقض قوانین نگهداری سیستم اطلاعات
	نقص یا نارسایی در سطوح سرویس قراردادی	نقض قوانین نگهداری سیستم اطلاعات
	نقص در روش رسمی برای مستندسازی کنترل ISMS	تحریف داده
	نقص در روش رسمی برای نظارت بر ثبت ISMS	تحریف داده
	نقص در روش علمی برای اجازه دسترسی عمومی اطلاعات	داده به‌واسطه منابع غیرقابل-اعتماد
	نقص در تخصیص وظایف امنیت اطلاعات ویژه	عدم پذیرش کارها

نوع	آسیب پذیری	تهدید
سایت سازمان	نقص در سیاست استفاده از ایمیل	خرابی تجهیزات
	نقص در رویه‌هایی برای ورود نرم‌افزار به سیستم های عملیاتی	خطا در استفاده
	نقص در بایگانی در متولی و فهرست کارمندان	خطا در استفاده
	نقص در رویه‌هایی برای بررسی طبقه‌بندی اطلاعات	خطا در استفاده
	نقص در ضمانت امنیت اطلاعات در شرح کارها	خطا در استفاده
	نقص یا نارسایی قوانین تعهدشده (درخصوص امنیت اطلاعات) به کارمندان	تهیه‌کردن غیرقانونی داده‌ها
	نقص در سیاست‌های رایانه‌های قابل‌حمل	سرقت تجهیزات
	نقص در کنترل‌های غیرمنطقی دارایی‌ها	سرقت تجهیزات
	نقص یا نارسایی در خط‌مشی میز پاک و صفحه پاک	سرقت تجهیزات
	نقص در اجازه تهیه کردن اطلاعات تجهیزات	سرقت محیط و مستندات
	نقص در سازوکارهای پایش برای شکاف‌های امنیتی	سرقت محیط و مستندات
	نقص در بازبینی‌های مدیریتی قانونمند	استفاده غیرمجاز از محیط
	نقص در رویه‌هایی برای عیوب گزارش‌های امنیتی	استفاده غیرمجاز از محیط
	نقص در رویه هایی برای فراهم آوردن مطلوبیت‌ها به‌وسیله افکار صحیح	استفاده از نرم‌افزارهای کپی یا جعلی

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 ازارتش سایبری کشورهای متخاصم، گروه های تحت حمایت پنهان دولتهای متخاصم، جاسوسان سایبری، تروریسم‌های سایبری می شود.

پدافند سایبری

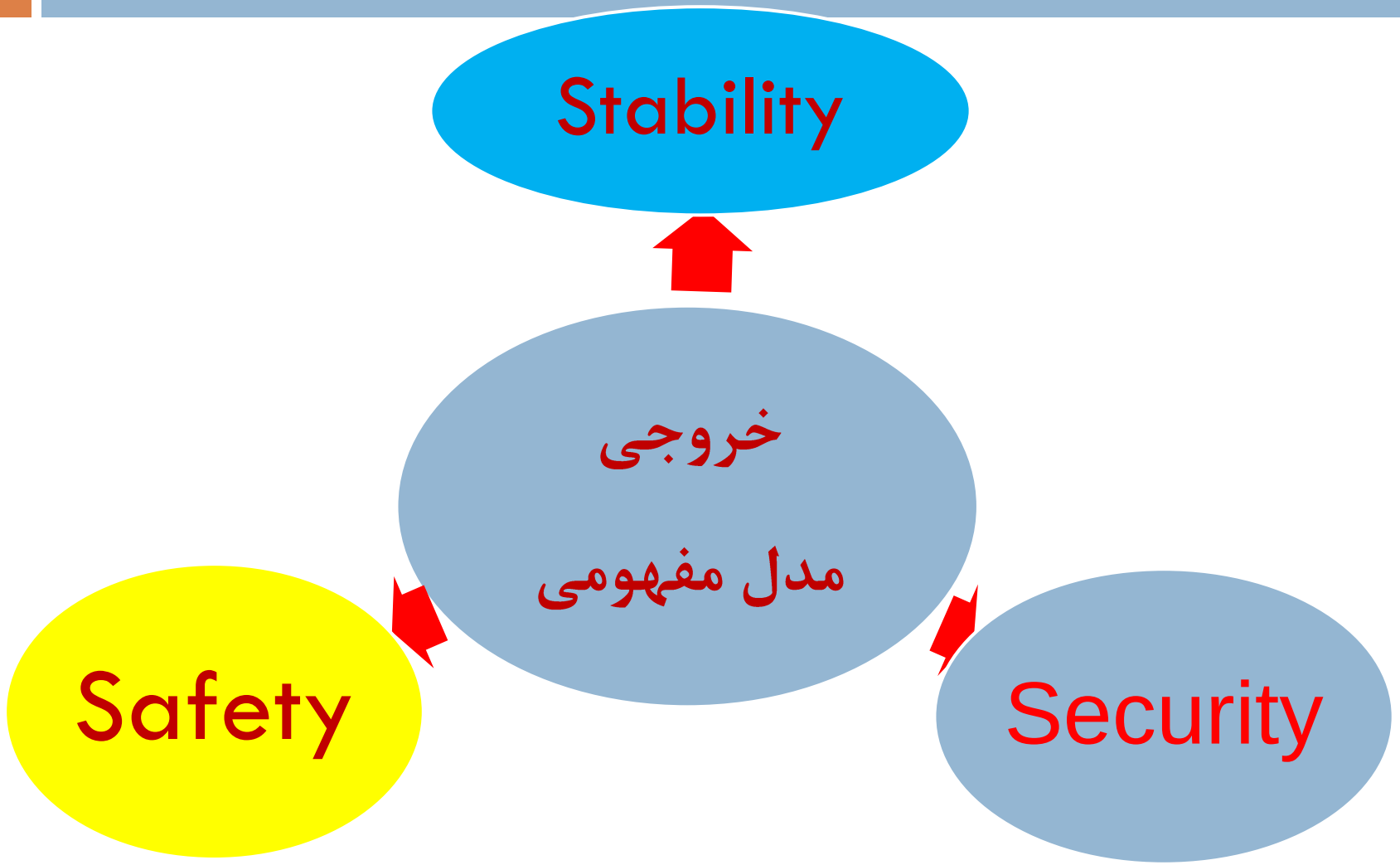
حفاظت از زیرساخت‌های اطلاعاتی خودی با تمرکز برهدف های ۳ گانه کاهش آسیب پذیری ها ، تداوم فعالیت های ضروری و ارتقا پایداری در مقابل تهاجمات دشمن از طریق ایجاد و بکارگیری الزامات پدافند غیر عامل در فضای سایبر و سیستم‌های اطلاعاتی

استراتژی دفاع همه جانبه

(در هنگام نبرد مجال پرداختن به همه جهات ، قوتها ، ضعفها ، برنامه‌ها و در حقیقت ترسیم استراتژی دفاع همه جانبه ، نبوده است . ولی در شرایط عادی باید با سعه صدر و به دور از حب و بغض‌ها به این مسائل پرداخت و از همه اندوخته‌ها ، تجربه‌ها ، استعدادها طرحهااستفاده نمود).

امام خمینی (ره) صحیفه نور ۲۸ فروردین ۱۳۶۸

تفاوت امنیت سایبری با پدافند سایبری



راهبردهای امنیت سایبری

راهبرد حداقل رده دسترسی (Least Privilage)

یک راهبرد امنیتی مبتنی بر مفهوم فراهم کردن حداقل محاسن و مزایا است در این راهبرد امکان حملات محدود می‌شود زیرا اگرچه هکر به درون اجزاء سیستم رخنه می‌کند لیکن یک حداقل امکاناتی را دسترسی پیدا می‌کند.

راهبرد دفاع در عمق(Defense in depth)

راهبردی است جهت مصونیت و افزایش تاب آوری سازمان از تهدیدات موجود و همچنین تهدیدات و جنگ سایبری احتمالی که در آن سیستم با استفاده از یک مکانیزم امنیتی چند لایه، ایمن ، مصون و پایدار می‌گردد. تمرکز دفاع در عمق، روی ایمن نمودن و افزایش تاب آوری لینکهای شبکه، انتقال، کاربرد و لایه‌های شبکه می‌باشد تا آن را در مقابل حملات زنجیره کشتار سایبری و نفوذهای هدفمند غیر قابل نفوذ و غیر شکننده بنماید، در این راهبرد، انواع مختلف فناوری‌ها و مکانیزم‌ها بکار گرفته می‌شود تا از ورود و نفوذ هکرهای خارج از سیستم جلوگیری شود.

راهبردهای امنیت سایبری

راهبرد گلوگاهی(Chock Point)

یک راهبرد جهت برقراری یک گلوگاه عمدی بین شبکه محلی و اینترنت می‌باشد.

راهبرد ضعیفترین حلقه(Weakest Link)

در این راهبرد سیستم به منظور شناسایی شکاف‌های امنیتی و آسیب‌پذیری‌های صنعت در ۳ حوزه ضعیف‌ترین حلقه‌های منابع انسانی در برابر حملات مهندسی اجتماعی، آسیب‌پذیری‌های فرایندی و سیستمی و آسیب پذیری‌های فناورانه. مورد تحلیل شکاف کامل در سه حوزه (فرایندی ، منابع انسانی و فناورانه) قرار گرفته و نقاط ضعف آن نمایان می‌گردد

راهبرد موضع ایمن از خرابی(Fail – Safe Stance)

الف) موضع جلوگیری پیش‌فرض:
در این وضعیت، مدل امنیتی دسترسی به سیستم را به استثنای کاربران مجاز غدغن می‌کند.
ب) موضع دسترسی پیش فرض:
در این وضعیت، مدل امنیتی دسترسی به سیستم را به استثنای کاربران منع شده مجاز فرض می‌نماید.

اصول حاکم بر حوزه پدافند سایبری کشور

WWW.PAPSA.IR

بازدارندگی در فضای سایبری متکی به سه عنصر اساسی است:

- قدرت تحمل و حفظ تداوم کارکرد در برابر حملات دشمن(قدرت دفاعی سایبری)
- قدرت پشیمان‌کنندگی دشمن بر اثر بهم‌خوردن تعادل هزینه و فایده در ارزیابی حمله سایبری
- قدرت پاسخ به تهدید و حملات دشمن در فضای سایبری

اصول حاکم بر حوزه پدافند سایبری کشور

@PAPSANEWS

سازمان پدافند غیرعامل کشور

قرارگاه پدافند سایبری کشور

نظام های مقابله با تهدیدات فضای سایبر

ردیف	عنوان نظام	اهداف
۱	نظام پدافند غیرعامل	تأمین ایمنی و پایداری
۲	نظام امنیت فضای تبادل اطلاعات (افتا)	تأمین امنیت و مقابله با حوادث سایبری
۳	نظام پدافند سایبری	تأمین مصونیّت و تضمین تداوم آن (آمادگی پدافندی)
۴	نظام دفاع همه جانبه سایبری	قدرت پاسخ همه‌جانبه به حملات دشمن در فضای سایبر
۵	نظام مقابله با جرایم سایبری	مقابله با جرم سایبری
۶	نظام مقابله با جاسوسی و تروریسم سایبری	مقابله با جاسوسی و تروریسم سایبری

تشکیل 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.

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.

تجربیات قرارگاه پدافند سایبری کشور در پدافندلایه به لایه سایبری (دفاع در عمق)

پدافند جامع در حوزه سایبری باید در لایه های مختلف ۸ گانه زیر تعریف گردد:

1. **خط مشی ها، روش های اجرایی و دستورالعمل ها و کنترل های امنیتی**
2. **پدافند فیزیکی (دوربین های مدار بسته،روش های بیومتریک و حفاظ های ایمنی)**
3. **پدافند پیرامونی (کوزه عسل – دیوار آتش و مدیریت تهدید یکپارچه)**
4. **پدافند درشبکه (ماژول امنیتی سخت افزاری ، سویچ لایه ۲ و ۳ – روتر)**
5. **پدافند در سطح داده و محتوا (بازیابی داده – رمزنگاری داده)**
6. **پدافند در سطح سیستم عامل (مجازی سازی)**
7. **پدافند در نقاط پایانی(آنتی ویروس– IDS)**
8. **پدافند در سطح برنامه های کاربردی (WAF –DB)**

چشم اندازپدافند سایبری کشور

(۱) برخوردار از نظام جامع پدافند سایبری هوشمندانه، انحصاری، ابتکاری، عمیق، لایه به لایه، بومی، پیشگیرانه، شبکه ای، گسترش یافته و سلسله مراتبی ، چابک و منعطف در سطح ملی، منطقه ای و استانی

(۲) برخوردار از نظام مدیریت کنترل جامع و هوشمند با قابلیت رصد،پایش،تشخیص،هشدارو مدیریت و کنترل بهنگام صحنه عملیات پدافند سایبری

(۳) مصونیت در زیر ساخت های حیاتی ، استحکام و پایداری درزیر ساخت های حساس و امنیت و ایمنی در زیر ساخت های مهم

(۴) برخوردار از سرمایه های انسانی آموزش دیده، مومن، متعهد، متخصص، کارآمد، بصیر، امین و رازدار و دارای روحیه بسیجی

(5)نظام دیپلماسی پدافند سایبری فعال ...

(6)صنعت بومی پدافند سایبری روزآمد و پاسخگو به تهدید

سند راهبردی پدافند سایبری

(۷) برخوردار از استانداردها، نظامات و الگو های پدافند سایبری بومی و روزآمد و امن

(۹) توانمند در مدیریت بحران سایبری و تضمین تداوم خدمات رسانی ضروری به مردم

(۱۰) برخوردار از جامعه ای آگاه و آموزش دیده ، سازماندهی شده، بصیر و آماده در برابر انواع تهدیدات و حملات سایبری

(۱۲) نظام تولید ،حفظ و ارتقاء آمادگی های پدافند سایبری در برابر تهدیدات

ارزیابی عوامل محیطی داخلی پدافند سایبری کشور – قوت ها

[۱]توجه جدی و حمایت های مؤثر مسئولین عالی نظام به فضای سایبری، ظرفیت ها و مخاطرات آن

[۲]درک نسبی مسئولین از تبعات تهدیدات و حملات سایبری قبلی دشمن به زیرساخت‌های کشور

[۳]وجود ساختار پدافند غیرعامل سایبری برای دفاع از فضای سایبری کشور

[۴]وجود ظرفیت‌های مناسب در اسناد بالادستی و حمایتی

سند راهبردی پدافند سایبری

[۵]وجود سند افتا و ابلاغیات دولت در این حوزه

[۶]وجود قوانین جزایی مربوط به جرایم رایانه ای

[۷]وجود تجربیات مفید از تهدیدات فضای سایبر درسازمان‌های نظامی، دولتی و خصوصی

[۸]شکل گیری نسبی ساختارهای مصوب در عرصه امنیت سایبری کشور

ارزیابی عوامل محیطی داخلی پدافند سایبری کشور – قوت ها

سند راهبردی پدافند سایبری

[۹]وجود ظرفیت‌های علمی، پژوهشی و صنعتی حوزه سایبری و افتا در بخش‌های دولتی و خصوصی کشور

[۱۰]وجود رشته‌های دفاع سایبری در دانشگاه‌های کشور

[۱۱]برخورداری نسبی از نیروی انسانی متعهد و متخصص در حوزه سایبری

[۱۲]توانایی نسبی طراحی، تولید بومی و مهندسی معکوس نرم افزارها و سخت‌افزارهای پدافند سایبری

[۱۳]توانایی طراحی و تولید الگوریتم‌های رمزنگاری بومی

[۱۴]توانایی کشف و تحلیل آسیب پذیری های شناخته شده و ناشناخته در زیرساخت های سایبری کشور

[۱۵]توانایی نسبی مقابله و پاسخگویی به تهدیدات سایبری

[۱۶]وجود ظرفیت های ارتباطی پشتیبان برای پدافند سایبری از سرمایه های کشور

ارزیابی عوامل محیطی داخلی پدافند سایبری کشور– ضعف ها

[۱] تنوع دیدگاه¬های فرهیختگان نسبت به تهدیدات فضای سایبری

[۲] کم توجهی به استفاده از ظرفیت های بخش خصوصی در حوزه سایبری

[۳] کمبود رشته ها، دروس و پایان نامه های دانشگاهی در حوزه تهدیدات سایبری

سند راهبردی پدافند سایبری

[۴] کُندی رشد صنعت پدافند سایبری

[۵] بهره برداری از تجهیزات غیر بومی در حوزه سایبری

[۶] پایین بودن سرعت رشد تجهیزات سخت افزاری و نرم افزاری بومی در فضای سایبری کشور

[۷] کندی سرعت رشد دانش، فناوری، استانداردها و محصولات بومی حوزه سایبری

[۸] قطع نشدن وابستگی به دانش، فناوری ها و استانداردهای غیربومی در حوزه سایبری

سند راهبردی پدافند سایبری

[۹] کمبود آزمایشگاه‌های مرجع سایبری

[۱۰] فقدان نظام جامع حقوقی و قانونی در حوزه سایبری به منظور دفاع از منافع ملی در مجامع بین المللی

سند راهبردی پدافند سایبری

[۱] انگیزه دشمن برای تسلط بر فضای سایبری

[۲] وجود راهبردهای تهاجمی دشمن در فضای سایبری

[۳] وجود سازمان رزم سایبری در کشورهای متخاصم

[۴] ساختارمند شدن تهدیدات استکبار جهانی بر علیه ج.ا.ا. در فضای سایبری

[۵]مخاطرات ناشی از بکارگیری بدافزارها و سلاح‌های سایبری توسط حریف

[۶] تأثیرات شبکه‌های اجتماعی و فناوری‌های نوظهور دشمن در تضعیف امنیت ملی

[۷] وجود شبکه ها و گروه های جاسوسی و نفوذی وابسته به دشمن در فضـــای سایبری

سند راهبردی پدافند سایبری

[۸] توافقات و تفاهمات کشورهای متخاصم علیه ج.ا.ا

[۹] فقدان حقوق بین‌المللی عادلانه در حوزه دفاع سایبری

[۱۰] بهره گیری دشمن از بلاتکلیفی قلمرو سایبری کشور

[۱۱] تقدم راهبردهای جنگ سایبری نسبت به جنگ فیزیکی

[۱] امکان استفاده از ویژگی بی مرزی و گستردگی جهانی فضای سایبری در امر پدافند سایبری

[۲] اتکای شدید دشمن به زیر ساخت‌های اطلاعاتی،ارتباطی و پردازشی و سرویس‌های عمومی

[۳] فعال شدن ظرفیت‌های دفاع سایبری به واسطه وجود تحریم ها و تهدیدات

[۴] امکان بهره گیری از دانش و فناوری‌های نو ظهور

[۵] امکان ارتقاء سطح همکاری‌های بین‌المللی و منطقه‌ای در زمینه پدافند سایبری

[۶] رقابت کشورها، دولت‌ها و شرکت‌های چند ملیتی صاحب دانش و فناوری

[۷] امکان همکاری‌های بین‌المللی در زمینه حقوق بین‌الملل و پیمان‌های همکاری و دفاعی سایبری همسو(اسلامی، نم، منطقه و ...)

سند راهبردی پدافند سایبری

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 روز آمد پدافند سایبری

خود آزمایی

٦- کدام گزینه به این فرمایش امام خمینی (ره) : در هنگام نبرد مجال پرداختن به همه جهات ، قوتها، ضعفها، برنامه ها و در حقیقت ترسیم استراتژی دفاع همه جانبه نبوده است . ولی در شرایط عادی باید با سعه صدر و به دور از حب و بغضها به این مسائل پرداخت و از همه اندوخته‌ها ،تجربه‌ها، استعدادها و طرحها استفاده نمود . اشاره دارد.

الف) ISMS ب) SWOT ج) PEST

د) هیچکدام

۷- برای ارزیابی عوامل محیطی پدافند سایبری داخلی و خارجی تاثیرگذار بر یک سازمان، کدام یک از گزینه های زیر اثربخش تر و منطقی تر است.

الف)-CIA ب)- SMART

ج)- SWOT د)- RAMCAP

مأموریت‌های پدافند سایبری

1. رصد، پایش، شناسایی و خنثی‌سازی تهدید سایبری
2. استخراج و رفع آسیب‌پذیری سایبری
3. تجزیه و تحلیل تهدید و آسیب‌پذیری و پیش‌بینی مخاطرات سایبری
4. دفاع قانونی و ثبت ادله
5. مدیریت صحنه‌ی جنگ سایبری
6. بازیابی و ریشه‌کنی پیامدهای جنگ سایبری
7. امن‌سازی و ارتقاء آمادگی پدافند سایبری
8. ارتقاء قدرت پاسخ به تهدید سایبری
9. تجربه‌اندوزی و بهره‌گیری از تجارب ارزشمند دفاع سایبری

مأموریت‌های پدافند سایبری

زمان	قبل از جنگ سایبری				آستانه جنگ سایبری	حین جنگ سایبری	پس از جنگ سایبری		
موضوع	سرمایه سایبری	تهدید سایبری	آسیب‌پذیری سایبری	مخاطره سایبری	جنگ سایبری قریب‌الوقوع	جنگ سایبری	پیامد جنگ سایبری	امنیت و آمادگی سایبری	قدرت و بازدارندگی سایبری
رویکرد دفاع	پیش‌گیرانه	پیش‌گیرانه	پیش‌گیرانه	پیش‌گیرانه	پیش‌دستانه و قانونی	واکنش‌گرایانه و بازدارنده و قانونی	منفعلانه وواکنش گرایانه و بازدارنده	پیش-گیرانه	بازدارنده
	پیش‌بینانه	پیش‌بینانه			پیش‌بینانه	پیش‌بینانه		پیش‌بینانه	
مأموریت		۱–رصد و پایش تهدید سایبری	۲– استخراج آسیب-پذیری سایبری	۳–تجزیه و تحلیل تهدید و آسیب-پذیری و پیش‌بینی مخاطرات سایبری	رصد و پایش تهدید سایبری استخراج آسیب-پذیری سایبری تجزیه و تحلیل شواهد و قرادن و پیش‌بینی جنگ سایبری ۴–ثبت ادلّه دفاع قانونی	۵–مدیریت صحنه جنگ سایبری تجزیه و تحلیل جنگ سایبری و پیش‌بینی پیامدهای احتمالی آن ثبت ادلّه دفاع قانونی	۶– بازیابی و ریشه‌کنی پیامدهای جنگ سایبری	۷–امن‌سازی و ارتقاء آمادگی پدافند سایبری ۸–تولید قدرت پاسخ به تهدید سایبری احقاق حقوق کشور (دفاع قانونی) ۹–تجربه‌اندوزی و بهره‌گیری از تجارب ارزشمند دفاع سایبری	

مصون سازی و حفاظت زیرساخت های حیاتی و حساس سایبری CCIP

- معماری واستقرار پدافند سایبری در مراکز حیاتی وحساس کشور
- استفاده از سیستم ها و سایت های جایگزین
- داشتن نسخه پشتیبان از اطلاعات موجود
- به کارگیری اصول عام پدافند غیرعامل برای تأسیسات فیزیکی در کلیه مراحل از طراحی تا بهره برداری از قبیل: مکان یابی، پراکندگی، مقاوم سازی و ...
- به کارگیری اصول پدافند غیرعامل سایبری برای فضای مجازی و متناسب با تهدیدات از قبیل فریب سایبری، اختفاء سایبری و ...
- مدیریت بحران سایبری و تهیه دستورالعمل های امنیتی و پدافندی
- آموزش مداوم و مستمر کلیه پرسنل مرتبط
- برگزاری مانورهای دوره ای پدافند غیرعاملی در فضای سایبر

موارد عملیاتی مرتبط با مدیریت تداوم کسب‌وکار در پدافند سایبری

- برنامه‌ریزی و کنترل عملیاتی
- تحلیل اثر کسب و کاری
- ارزیابی ریسک
- طرح ریزی تداوم کسب‌وکار
- ایجاد و پیاده‌سازی رویه‌های تداوم کسب‌وکار
- تمرین و رزمایش پدافند سایبری

خود آزمایی

۸– برگزاری مانورهای سایبری در یک سازمان حیاتی و حساس:

الف)– اختیاری است و سازمان موظف به برگزاری آن نیست.

ب)– طبق فرایند مدیریت تداوم کسب و کار در پدافند سایبری یک الزام است.

ج)– اختیاری است ولی اجرای آن نشان دهنده سطح بلوغ بالای سازمان است.

د)– پدافند سایبری به این موضوع نپرداخته است.

معماری پدافند سایبری مبتنی بر مدل 5WH

برخی ازراهبردهای ۲۱ گانه پدافند سایبری کشور

- طراحی ، پیاده سازی و راهبری نظام جامع بومی پدافند سایبری
- طراحی ، پیاده سازی و راهبری طرح ها و برنامه های پدافندسایبری
- ارتقاء کمی و کیفی منابع انسانی حوزه پدافند سایبری
- طراحی ، پیاده سازی و راهبری نظام دیپلماسی پدافند سایبری
- مدیریت بر مصون سازی،واکنش به موقع و ارتقاء پایداری ؟ دربرابر ؟
- تقویت صنعت بومی و توسعه خدمات و محصولات روز آمد پدافند سایبری
- استفاده هوشمندانه (توجه به OT در فناوری ها) از سامانه ها و فناوری در زیر ساخت ها

با هدف ایجادقدرت بازدارندگی موثر در برابر تهدیدات سایبری دشمن:

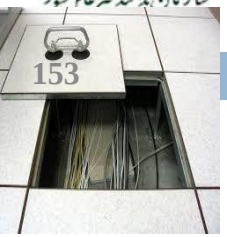
هوشمندانه	انحصاری	ابتکاری	عمیق
لایه به لایه	بومی	پیشگیرانه	شبکه ای
چابک و منعطف		گسترش یافته و سلسله مراتبی	

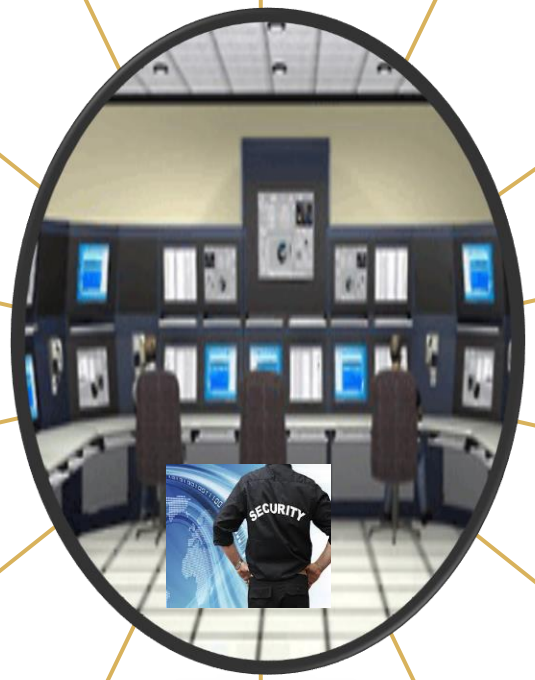
طرح راهبردی حفاظت از زیرساخت‌های کشور

با توجه به لزوم ارتقاء امنیت و پایداری زیرساخت ها و شریان های حیاتی کشور با تهیه طرح های جامع عملیاتی پدافندی در جهت مصون سازی، افزایش آمادگی، ارتقاء تاب آوری و امن سازی اضطراری ـ EOP ـ با رویکرد زیست بوم، متمرکز بر اقدامات اساسی زیر:

- **تهیه و پیاده سازی طرح پاسخ اضطراری به حوادث و تهدیدات زیرساختی ـ ERP**
- **تهیه و پیاده سازی طرح تضمین و تسهیل تداوم کارکردهای اساسی ـ BCP**
- **تهیه و پیاده سازی طرح بازیابی و برگشت پذیری زیرساختی و سیستمی ـ DRP**
- **تهیه و پیاده سازی طرح امن سازی و مصون سازی و تاب آوری ـ ISP**
- **تهیه و پیاده سازی طرح کاهش آسیب پذیری ـ VRP**
- **تهیه و پیاده سازی طرح بهینه سازی وابستگی و وابستگی های متقابل ـ OIP**
- **تهیه و پیاده سازی طرح های ارزیابی و ارتقاء آمادگی های زیرساختی ـ PPP**

Emergency opration plan
Emergency response plan
Business continuity plan
Disaster recovery plan
Immunius&security plan
Vulnerability reduction plan
Optimizing interdependency plan
Preparedness promotly plan





دسترسی بیومتریک و سنسور خروج

رک مقاوم در برابر زلزله

دوربین مدار بسته

کابل کشی امن

زمین و شیلد مناسب

ژنراتور و UPS

کنترلر HVAC

سیستم اعلان و اطفای حریق

پایش عملیات سرورها

افسر امنیتی مستقر در سایت

هشدار نفوذ غریبه‌ها

سنسور حرکتی

کف، سقف و دیوارهای مناسب

درب ضد حریق و محکم

استقرار فرایندهای پدافند سایبری
مدیریت مخاطرات سایبری

دارایی	تهدید	آسیب پذیری
اعتبار و شهرت	مختل شدن عملکرد سرویس های حیاتی	عدم نظارت کامل برعملکرد پیمانکاران عدم وجود فایروال کارآمد و هک شدن سایت کامپیوتری عدم آگاهی پرسنل عدم صلاحیت پرسنل فنی

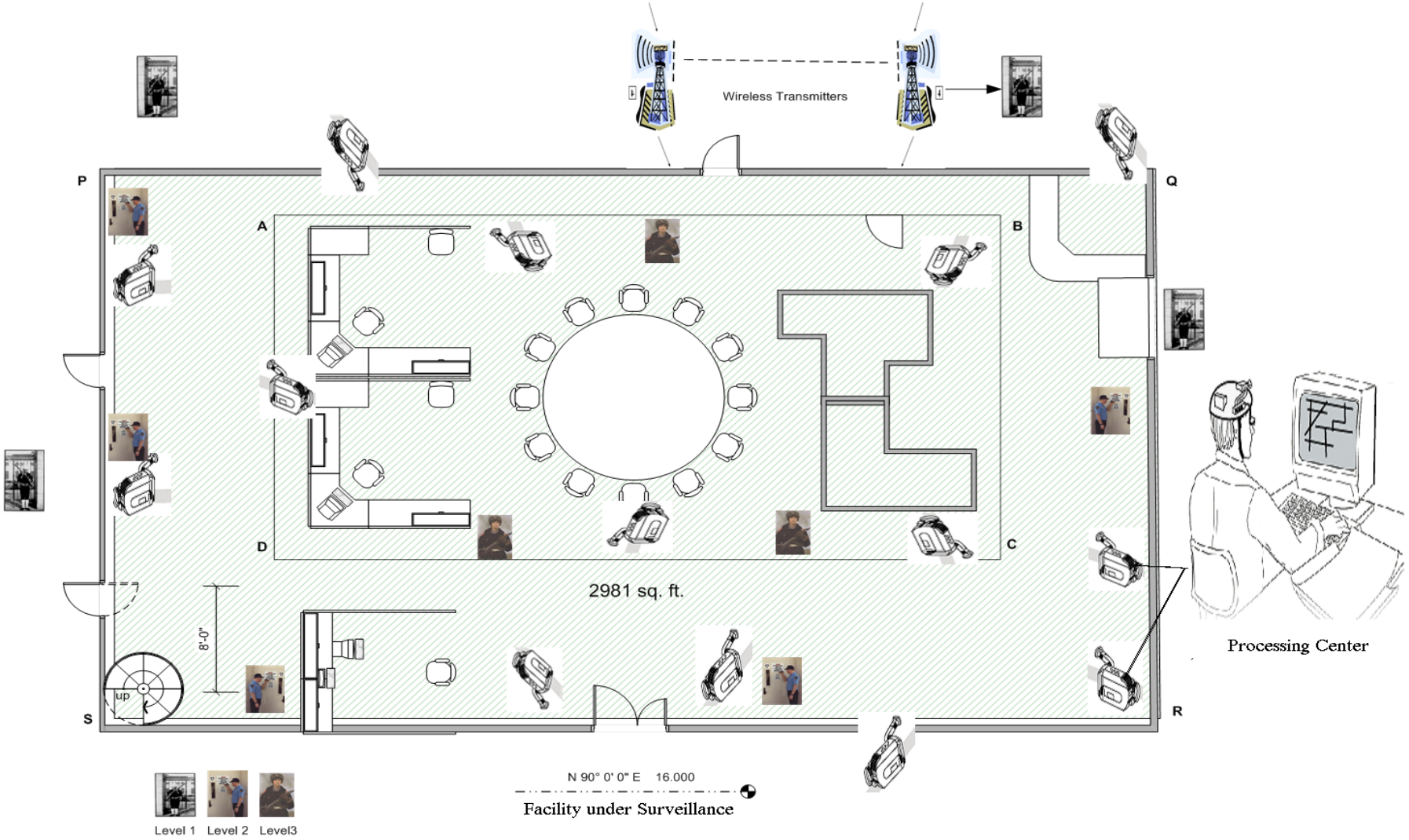
محرمانگی
صحت
دسترس پذیری

انتساب ATV

خود آزمایی

	الف– ضعف در آگاهی امنیتی	ب– تغییرات عمدی یا سهوی پیمانکار در خدمات	ج– عدم کفایت وجود دوربین های مدار بسته	د– ضعف در کنترل های دسترسی فیزیکی برای ساختمان ها و اتاق ها
	ه– ضعف امنیتی در معماری شبکه	و– ضعف در پیکربندی	ز– افشای عمدی اطلاعات طبقه بندی شده	ح– اقدام به تخریب اطلاعات
سوال	دارایی	آسیب پذیری	تهدید	C-I-A پیامد
۹	کارکنان سازمان	؟	مهندسی اجتماعی	
۱۰	Service Antivirus	ضعف در الزامات قرارداد با تامین کنندگان	؟	
۱۱	سرور فیزیکی	؟؟	دستکاری عمدی در سخت‌افزار (سوئیچ، رایانه، سرور و غیره)	
۱۲	router	؟؟	دستکاری عمدی در ارتباطات شبکه	
۱۳	اطلاعات BCP مربوط به کلیه پسورد های سیستمی	ضعف در اجرای روال کار با اطلاعات طبقه بندی شده	؟؟	

نظارت و مانیتورینگ هوشمند
شبکه‌های مراکز حیاتی



خود آزمایی

۱۴- بر خی راهبردهای نظام پدافند سایبری کشور عبارتند از :

الف) مصون سازی زیست بوم سایبری و الزام و همراه سازی سازمان‌های متولی زیرساخت‌های حیاتی وحساس کشوردرایجاد واستفاده از محصولات امن داخلی

ب) تولید و مدیریت دانش و فناوری پدافندسایبری متناسب با تهدیدات نوین

ج) کاهش آسیب پذیری، پایدارسازی، مصون سازی، ارتقاءتوان بازدارندگی زیرساخت‌های حیاتی وحساس کشوردربرابرتهدیدات وحملات سایبری

د) همه موارد

۱۵- از کدامیک از ادوات ذیل برای پایش و کنترل رطوبت و دما در دیتا سنتر یا اتاق سرور استفاده می شود.

الف) سنسور دود

ب) HVAC

ج) UPS

د) همه موارد

سنجش و ارزشیابی بلوغ سازمانی طرح تداوم کسب‌وکار

TOP ARE ?

ابزار/ فناورانه: سازمان بایدفناوری ها و ابزارهای لازم برای ایجاد،پیاده‌سازی، نگهداری و بهبود مستمر چارچوب BCM را تعیین و تامین نماید.

اهداف: اطمینان از اینکه BCM به نتایج و اهداف مورد انتظار خود دست می‌یابد

آگاهی‌بخشی: افرادی که زیر نظر سازمان، فعالیت می‌کنند باید بسته به موقعیت خود، نسبت به طرح تداوم کسب‌وکار سازمان، آگاهی لازم را داشته باشند.

نقش ها و مسؤولیت ها:
سازمان باید نقش ها و مسؤولیت های امنیتی برای ارتباطات درونی و بیرونی مرتبط با BCM را تعیین نماید.

شایستگی: سازمان باید شایستگی‌ها و قابلیت‌های لازم برای افرادی که در ارتباط با تداوم کسب‌وکار فعالیت می‌کنند را تعیین نماید و اطمینان یابد که این افراد، آموزش و تجربه مناسب را دارند.

خط مشی و روش اجرایی :
اطلاعات و سوابقی که از سوی سازمان برای اثربخشی چارچوب BCM، ضروری شمرده می‌شوند باید مبتنی بر روش اجرایی ثبت گردند.

طرح بازیابی فاجعهDRP

فاجعه، رویدادی ناگهانی و برنامه‌ریزی نشده است که به وارد آمدن آسیب یا زیان جدی بر سازمان منجر می‌گردد. فاجعه باعث می‌شود تا سازمان برای مدت زمانی نتواند کارکردهای تجاری حیاتی را فراهم آورد.

با افزایش استفاده از فناوری اطلاعات به عنوان توانمندسازی **کسب و کاری** در سازمان‌ها، **آمادگی** برای مدیریت هر اختلال یا فاجعه‌ای که باعث **قطعی سیستم‌ها یا خدمات سازمان** می‌شود بیش از پیش اهمیت یافته است.

یک **برنامه بازیابی از فاجعه (DRP)** بیان می‌کند که در صورت وقوع فاجعه‌ای احتمالی، سازمان چگونه با آن روبه‌رو می‌شود، اثرات آن را به حداقل می‌رساند و عملیات اصلی خود را در سریع‌ترین زمان ممکن به حالت عادی باز می‌گرداند.

مراحل برنامه‌ریزی برای بازیابی از فاجعه (DRP)

۱. شناسایی و تحلیل ریسک‌ها یا تهدیدها

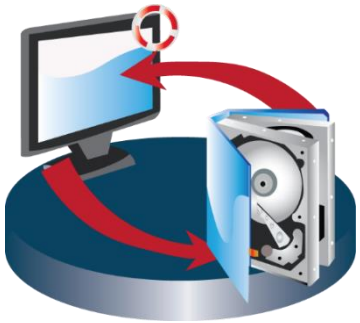
۲. طبقه‌بندی ریسک‌ها بر اساس وزن‌های نسبی

۳. ایجاد ارزیابی ریسک

۴. تعیین اثرات فاجعه

۵. ارزیابی سازوکارهای بازیابی از فاجعه

۶. تشکیل گروه بازیابی از فاجعه



خود آزمایی

۱۶- حفاظت از زیرساخت‌های اطلاعاتی خودی با تمرکز برهدف های ۳ گانه کاهش آسیب پذیری ها ، تداوم فعالیت های ضروری و ارتقا پایداری در مقابل تهاجمات دشمن در فضای سایبر و سیستم‌های اطلاعاتی..... می باشد.

الف) ISMS ب) پدافند سایبری ج) RAMCAP د) هیچکدام

۱۷- طرحی که بیان می‌کند در صورت وقوع فاجعه‌ای احتمالی، سازمان چگونه با آن روبه‌رو می‌شود، اثرات آن را به حداقل می‌رساند و با انجام اقدامات احیاء و بازیابی خود را در سریع‌ترین زمان ممکن به حالت عادی باز می‌گرداند.

الف) BCP ب) DRP

ج) RTP د) همه موارد

متدولوژی تاب آوری و بازدارندگی سایبری