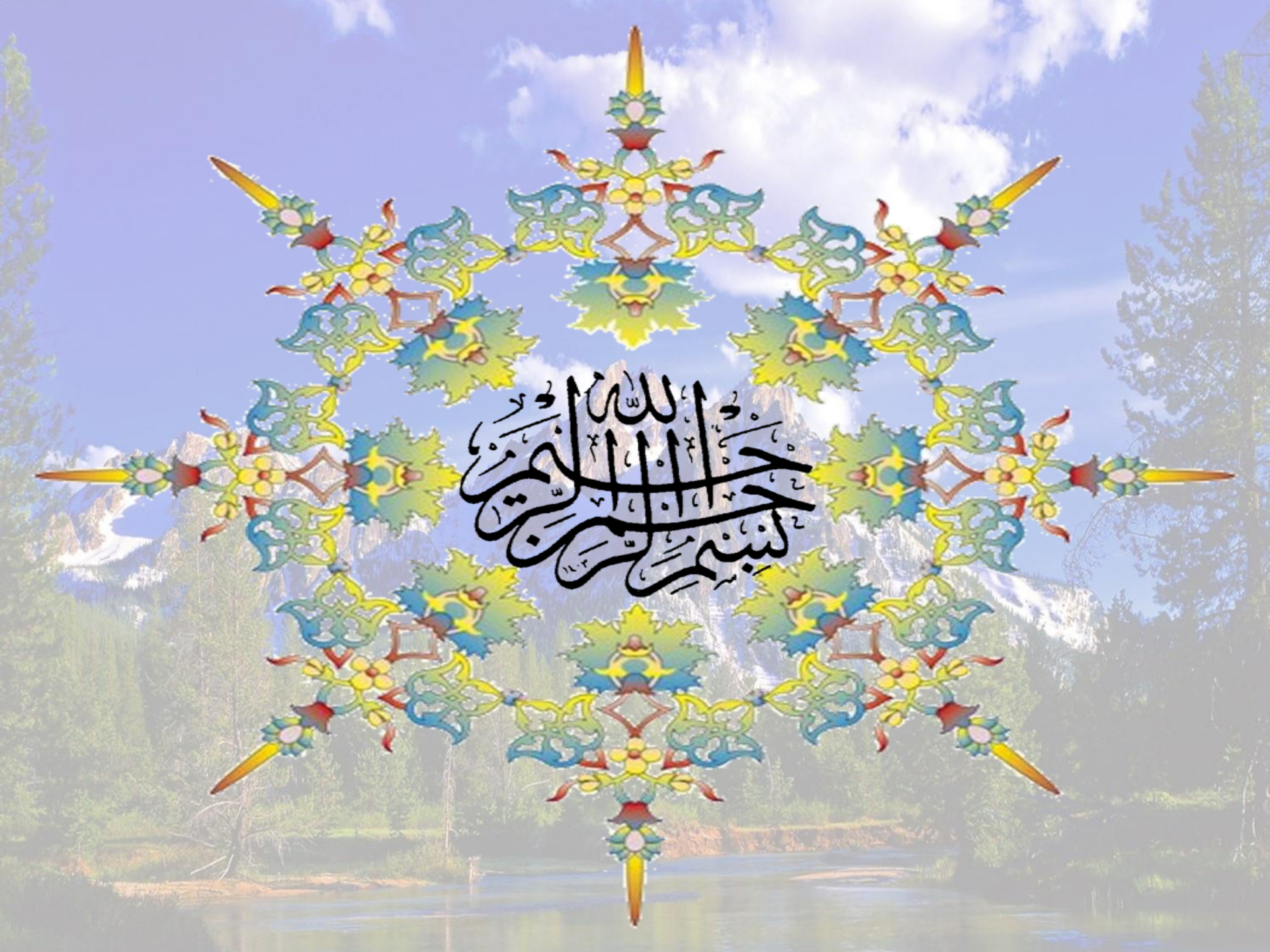

بسم الله الرحمن الرحيم

موضوع ارائه

امنیت و پدافند سایبری
در نظام سلامت کشور

مهندس حمیدرضا کاووسی

کارشناس ارشد مهندسی فناوری اطلاعات،شبکه های کامپیوتری و ارتباطی

نظام سلامت

۱. بهداشت
۲. درمان
۳. دارو
۴. خون
۵. واکسن
۶. تجهیزات پزشکی
۷. خدمات پزشکی

تقاطع نظام سلامت و فضای سایبری (BioCyber)

۱. تولید، نگهداشت و بهره برداری داده های حوزه سلامت جامعه (**داده های حیاتی**)

- اطلاعات پزشکی جامعه (خون،بهداشت،درمان،ژنتیک،بیمه)

❑ تجمیع و نگهداشت داده ها، بانک های اطلاعات حوزه سلامت(**Big Data**)

❑ تحلیل داده ها (داده کاوی – **Data Mining**)

❑ مهندسی اجتماعی (**Social Engineering**)

۲. تولید و بهره برداری از تجهیزات سخت افزاری حوزه سلامت (**مهندسی پزشکی**)

- تامین و بهره برداری از تجهیزات **OT**(کنترل صنعتی): مانند دستگاه های **MRI** و ...
- تامین و بهره برداری از تجهیزات **IT**(فناوری): رایانه ها و شبکه های ارتباطی

تقاطع نظام سلامت و فضای سایبری (BioCyber)

۳. تولید و بهره برداری از نرم افزارهای حوزه سلامت (سیب،ناب،سینا،نسخه الکترونیک،تی تک،بیمه ها و...)

۴. شبکه ها و زیرساخت های ارتباطی حوزه سلامت (مراکز داده،اتاق های تجهیزات،لینک های ارتباطی)

۵. توسعه کاربرد اینترنت اشیا در نظام سلامت (IOMT): انواع سنسورها،ایمپلنت ها

۶. توسعه هوش مصنوعی در نظام سلامت: تحلیل داده،تشخیص،درمان،تصویربرداری،ربات، صنایع دارو و...

۷. سایر : نیروی انسانی متخصص (سایبری)، ساختار مدیریت BIOCYBER

اهداف کلان

دست یابی به:

۱. **مصون سازی** زیرساخت های سایبری و وابسته به سایبر نظام سلامت در برابر تهدیدات سایبری.

۲. **کاهش آسیب پذیری** های زیرساخت های سایبری و وابسته به سایبر نظام سلامت.

۳. **ارتقا سطح آمادگی ها** در زیرساخت های سایبری و وابسته به سایبر نظام سلامت.

۴. **حفظ و تضمین تداوم** کارکردهای اساسی زیرساخت های سایبری و وابسته به سایبر نظام سلامت.

کلیدواژگان (Key Words)

۱. زیرساخت(Infrastructure) / نظام سلامت(Health)

۲. دارایی‌های سایبری(Asset)

۳. تهدیدات سایبری(Threat)

۴. آسیب‌پذیری سایبری(Vulnerability)

۵. پیامدهای سایبری(Consequence)

۶. ریسک‌ها/مخاطرات سایبری(Risk)

۷. هشدار(اعلام وضعیت)سایبری(Alert)

برخی مستندات داخلی

۱. نظام جامع عملیاتی پدافند غیر عامل کشور
۲. نظام آمادگی و رزمایش دستگاه های اجرایی در برابر تهدیدات
۳. طرح راهبردی حفاظت از زیرساخت های کشور
۴. نظام فنی و تخصصی حفاظت از زیرساخت های کشور
۵. سند راهبردی پدافند سایبری کشور
۶. دستورالعمل عملیاتی پدافند سایبری زیرساخت های صنعتی کشور
۷. سند راهبردی پدافند غیر عامل شهری
۸. کتاب مرجع آموزش عرضی و کوتاه‌مدت مباحث تخصصی پیشرفته پدافندسایبری
۹. سایر کتب و مستندات راهبردی، فنی و تخصصی حوزه سایبری

برخی مستندات خارجی

1. **PPD 21 *(Presidential Policy Directive 21)***
2. **NIPP (*National Infrastructure Protection Plan)***
3. **Cybersecurity and Infrastructure Security Agency (CISA)**
4. **DHS LEXICON**
5. **FEMA Series (452 - …)**
6. **etc**

1. **https://www.cisa.gov/**
2. **https://www.dhs.gov/**
3. **https://www.fema.gov/**

گام های اجرایی(۱)در حصول به اهداف: انجام مطالعات پدافند سایبری

۱. مهندسی(شناسایی، ارزیابی و تحلیل کمی و کیفی) دارایی‌های سایبری

۲. مهندسی(شناسایی، ارزیابی و تحلیل کمی و کیفی) تهدیدات سایبری

۳. مهندسی(شناسایی، ارزیابی و تحلیل کمی و کیفی) آسیب‌پذیری‌های سایبری

۴. مهندسی(شناسایی، ارزیابی و تحلیل کمی و کیفی) پیامدهای سایبری

۵. مهندسی و مدیریت ریسک‌های سایبری

روش اقدام

۱. چک لیست های ارزیابی

۲. مصاحبه های کارشناسی، عمیق

۳. تدوین جداول و ماتریس های تقاطعی (دارایی،تهدید،آسیب پذیری،پیامد)

۴. روش ها و سامانه های کاربردی (CARVER،MSHARPP،RAMCP،جوشن،....)

مدیریت ریسک

(Risk Management)

تخمین ریسک

Risk Identification

- شناسایی ریسک
- ارزیابی ریسک
- تحلیل و کمی سازی ریسک

کنترل ریسک

Risk Control

- حذف ریسک
- کاهش ریسک
- انتقال ریسک
- پذیرش ریسک

گام های اجرایی(۲)در حصول به اهداف: انجام مطالعات پدافند سایبری

خروجی اقدامات

۱. تدوین راهبردها،برنامه ها و اقدامات امنیت و پدافند سایبری

۲. پیاده سازی برنامه ها و اقدامات تدوین شده

۳. بازخورد گیری و اصلاح برنامه ها و اقدامات


طرح های شش گانه پدافند سایبری
پاسخ به شرایط اضطراری سایبری (CERP)
امن سازی اضطراری سایبری
مصون سازی سایبری
طرح تداوم فعالیت های ضروری زیرساخت (BCP)
طرح بازیابی از حوادث و حملات سایبری (DRP)
طرح رزمایش سایبری

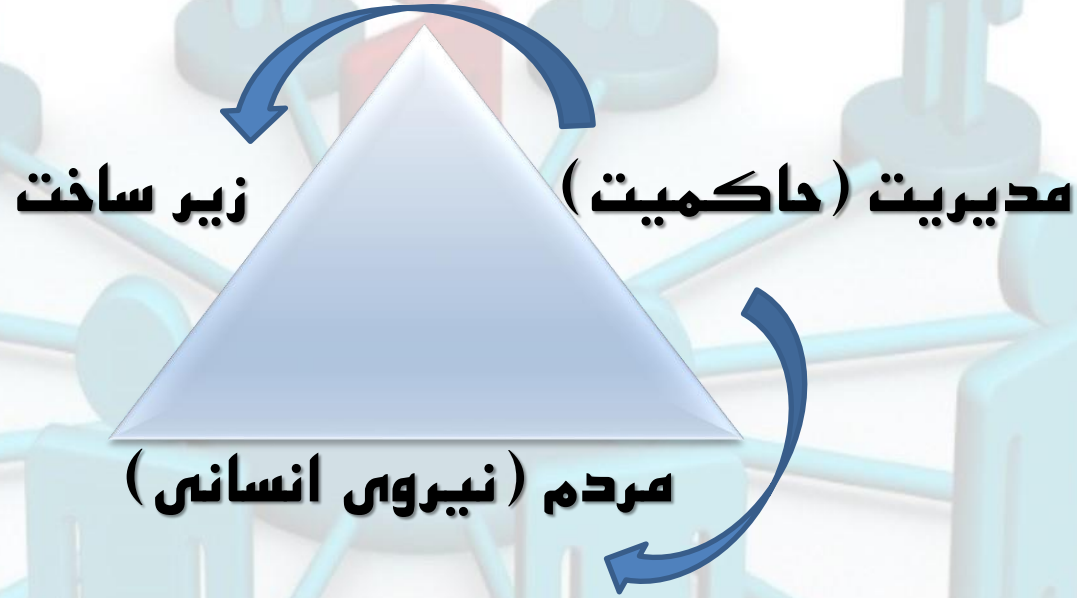
لایه های پدافند سایبری

لایه ها	عنوان		مفهوم	ویژگی
لایه اول	ایمنی سایبری	Cyber Safety	سلامت فیزیکی سرمایه ها و دارایی ها	اثر تهدید در نظر گرفته نمی شود
لایه دوم	امنیت سایبری	Cyber Security	محرمانه گی،یکپارچگی، دسترس پذیری سرمایه ها و دارایی ها	فقط یک تهدید پایه یا مبنا در نظر گرفته می شود
لایه سوم	دفاع سایبری	Cyber Defense	مقابله و مقاوم سازی سرمایه ها و دارایی ها برای شرایط جنگ سایبری	اثر وقوع جنگ(تهدید در قامت جنگ)در نظر گرفته می شود

دفاع!

- استانداردهای لایه ۱ و ۲ پاسخگوی سرویس دهی سیستم در شرایط عادی بوده و پاسخگوی تهدیدات خاص منظوره نیستند، بنابراین بایستی استانداردهای دفاعی لازم و متناسب با تهدید روز طراحی شود.
- استانداردهای دفاعی نسخه ثابتی ندارند و می بایست متناسب با الزامات محیطی و بومی طراحی، پیاده سازی و اجرا شوند.
- رصد و دیده بانی فناوری(Technology Watch) کمک شایانی به تشخیص تهدیدات روز و تدوین استانداردهای دفاعی خواهد کرد.

عناصر سه گانه مدیریت کشور



رابطه

مردم(نیروی انسانی) / حاکمیت/زیرساخت

- **مردم داری**:اداره امور مردم(در شرایط عادی و بحرانی)
- **مردم یاری**:تامین نیازمندی های اساسی(در شرایط عادی و بحرانی)
- **مردم بانی**:حفاظت از مردم(در شرایط عادی و بحرانی)

حوزه زیرساخت‌ها

هریک از عناصر اصلی شکل‌گیری زیرساخت‌ها که مطابق طرح راهبردی حفاظت از زیرساخت‌های کشور عبارتند از:

Sector

۱– انـــرژی،

۲–آب،

۳– غذا و کشاورزی،

۴ – حمل و نقل،

۵– بهداشت و سلامت،

۶– دفاعی و امنیتی،

۷– صنعت،

۸– رسانه،

۹– هســـته‌ای،

۱۰– فضـــا،

۱۱– جمـــعیت،

۱۲– حاکمیتی،

۱۳– خدمات ضروری و فوریتی،

۱۴– پولی و مالی،

۱۵– ارتباطات و فناوری اطلاعات.

16 Critical Infrastructure Sectors

Presidential Policy Directive 21:
Critical Infrastructure Security and Resilience


Nuclear


Chemical


Facilities


Dams


Manufacturing


Defense


Emergency


Comms


Financial


Energy


Agriculture


Health


Water


Transportation


IT


Gov Facilities

سایبری شدن زیر ساخت ها
(زیر ساخت های هوشمند)

-تهدیدات سایبری شدن زیر ساخت ها:

- ❑ –امکان نفوذ به زیر ساخت
- ❑ –امکان دسترسی به داده ها
- ❑ –امکان کنترل داده ها
- ❑ –امکان مدیریت و کنترل زیر ساخت
- ❑ –امکان توقف کارکرد
- ❑ –امکان تخریب زیر ساخت
- ❑ –امکان انهدام زیر ساخت

Asset

زیرساخت های با اهمیت کشور یا خود بخشی از فضای سایبر را تشکیل میدهند و یا از طریق این فضا کنترل،مدیریت و بهره برداری می شوند.

در واقع عمده اطلاعات حیاتی،حساس و مهم کشور نیز به این فضا منتقل و یا اساسا در این فضا شکل می گیرند.

مهندسی دارایی‌ها

- شناسایی و ارزیابی(کمی و کیفی) دارایی‌ها مبتنی بر مؤلفه‌های زیر :

دارایی (Asset)

تقسیم بندی بر اساس:

- ماهیت (سایبری، فیزیکی، انسانی،معنوی، ترکیبی).
- اهمیت (حیاتی،حساس،مهم،قابل حفاظت).

- **person**, **structure**, **facility**, **information**, **material**, or **process** that has **value**.

دارایی حیاتی (Critical Asset)

specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively

مجموعه **خاصی** که از **اهمیت فوق العاده** ای برخوردار است به نحوی که **ناتوانی** یا **نابودی** آن تأثیر **بسیار جدی ، موثر و تحریک کننده** بر توانایی یک ملت برای **ادامه کارکردهای اساسی** دارد. (DHS)

نکته !!

The Weaponizations of Everything:

A Field Guide to the New Way of War

پنج مولفه(لایه)فضای سایبری

۱. **ارتباطات**: شبکه ها و تجهیزات ارتباطی

۲. **اطلاعات**: سامانه ها،نرم افزارها، دیتا(محتوا)

۳. **کاربران**: بهره برداران در سطوح مختلف

۴. **امنیت**:سیاست گذاری امنیتی

۵. **حاکمیت**: قانونگذاری و تنظیم مقررات

نفوذ فضای سایبر

ارتباط با

اجتماعی از انسانها

- شبکه های ارتباطی و اجتماعی
- داده های عظیم (Big Data)
- تحلیل داده‌های عظیم (Data Mining)
- مهندسی اجتماعی (Social Engineering)

ارتباط با زیرساخت ها

(صنعتی، خدماتی، تولیدی)

- سیستم های کنترل صنعتی(ICS)
- سامانه ها، نرم افزارها، شبکه ها، سخت افزارها(ICT)

حفاظت از زیرساخت ها با رویکرد سایبری

(سایبری، وابسته به سایبر)

مهندسی اجتماعی (سایبری)

- به معنی عملی است که از طریق فریب افراد با انجام اقدامات خاص منجر به افشای اطلاعات شخصی ، مالی،سازمانی و... می‌شود.
- شیوه و ترفندی فریبکارانه برای جلب اطمینان افراد برای دریافت اطلاعات از آنان .
- استفاده از تکنیک‌های روانشناسی برای تخلیه اطلاعاتی مخاطب هدف یا فریب دادن او برای انجام دادن اشتباهات امنیتی .

اساس کار مهندسان اجتماعی سایبری

۱. اکانت‌های جعلی (درخواست کمک، دوستی و...)

۲. وب‌سایت‌های جعلی(واریز وجه،...)

۳. لینک‌های مخرب و آلوده

۴. استفاده از درایو فلش آلوده

۵. وارد کردن قربانی به تشکیلاتی جعلی

۶. تبلیغاتی که ناگهانی باز می‌شوند و اطلاعاتی می‌خواهند.

سه مرحله اصلی مهندسی اجتماعی

- **۱- انتخاب هدف**
- پرسنل دارای دسترسی سطح بالا به سیستم‌ها و اطلاعات حساس
- پرسنل دارای پایین‌ترین میزان آگاهی از تهدیدات سایبری
- پرسنل ناراضی و اخراج شده

- **۲- گردآوری اطلاعات**Information Gathering

- **۳- اجرای حمله** Execution
- پس از شناسایی هدف یا اهداف بالقوه، حمله مهندسی اجتماعی با تکنیک‌هایی اجرا می‌شود.

حملات مهندسی اجتماعی

۱. فیشینگ Phishing
۲. طعمه‌گذاری Baiting
۳. جعل هویت Impersonating
۴. رهاسازی حافظه‌های USBدر سازمان USB Drops
۵. بهانه آوردن یا پریتکستینگ pretexting

مقابله با مهندسی اجتماعی
(فنی–آموزشی – راهبردی)

۱. تقویت و به روز آوری سیستم‌های سخت افزاری و نرم افزاری امنیتی و لایه‌های دفاعی
۲. آموزش اصول امنیتی به کارکنان (آموزش های عمومی و تخصصی)
۳. تست نفوذ مهندسی اجتماعی

سطح هشدار سایبری

سطح هشدار سایبری، بیانگر وضعیت سایبری در سطح مورد نظر بوده(کشور، منطقه، دستگاه) و شامل چهار طبقه بندی است:

۱. وضعیت تحت کنترل(سفید)

۲. وضعیت تهدید سایبری(زرد)

۳. وضعیت بحران سایبری(نارنجی)

۴. وضعیت جنگ سایبری(قرمز)

جدول سطح هشدار سایبری

		احتمال وقوع جنگ سایبری				
		خیلی غیر محتمل(۰)	غیر محتمل(۱)	ممکن(۲)	محتمل(۳)	قریب الوقوع(۴)
شدت پیامدهای تهاجم سایبری	خیلی کم- رویداد(۰)	۰	۱	۲	۳	۴
	کم-حادثه امنیتی کوچک(۱)	۱	۲	۳	۴	۴
	متوسط- حادثه امنیتی عمده(۲)	۲	۳	۴	۵	۶
	زیاد- بحران(۳)	۳	۴	۵	۶	۷
	خیلی زیاد- فاجعه(۴)	۴	۵	۶	۷	۸

آسیب‌پذیری سایبری

آسیب‌پذیری، به ضعف یا نقص 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 آسیب‌پذیری سایبری

- ضعف (نقص)موجود در فناوری مورد استفاده در سامانه سایبری
- ضعف پیاده‌سازی سامانه سایبری موردنظر
- ضعف تنظیمات در سامانه سایبری موردنظر
- ضعف در بهره برداری از سامانه ها و تجهیزات سایبری

مهمترین آسیب های متصور در حوزه سایبری

- ضعف در ارائه آموزش های عمومی یا تخصصی لازم به بهره بردارن این حوزه (درسطوح مختلف).
- بهره برداری از نرم افزارها ، سخت افزارها و شبکه های سایبر ، بدون کسب اطلاعات لازم در این زمینه.
- اتصال شبکه های داخلی سازمان ها به اینترنت

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.

سه مشخصه تهدیدات سایبری

۱. گستردگی

۲. نهفتگی

۳. تنوع

عملکردهای یک عامل تهدید

۱. جاسوسی و سرقت اطلاعات (جمع آوری اطلاعات از قربانیان سایبری)

۲. تخریب داده ها، اختلال در داده ها ، پاک کردن داده ها

۳. ایجاد آسیب و اختلال در سیستم (های) آلوده شده

۴. اختلال در عملکرد نهایی سیستم

مبنای تهدیدات سایبری(ابزار–نرم افزار–شبکه)

Type	Category
Application-based	Malware Spyware Privacy threats Vulnerable applications
Web-based	Phishing Drive-by Downloads Browser exploits
Network-based	Network exploits Wi-Fi sniffing
Physical-based	Lost or stolen devices

چه چیزی و چگونه امن و ایمن شود؟

What to Secure?

Hardware

Laptops, Desktop PCs, CPU, hard disk, storage devices, cables, etc.

Software

Operating system and software applications

Information

Personal identification such as Social Security Number (SSN), passwords, credit card numbers, etc.

Communications

Emails, instant messengers, and browsing activites

تهدیدات سایبری

تهدیدات سایبری بر اساس نیت حمله ، سطح حمله و اهداف آن به دسته بندی های زیر تقسیم بندی می شود :

۱- جنگ سایبری(CyberWar)

۲- جرایم سایبری(CyberCrime)

۲-۱- تجاوز سایبری(دسترسی غیرمجاز،شنود غیز مجاز،جعل رایانه ای و ...)

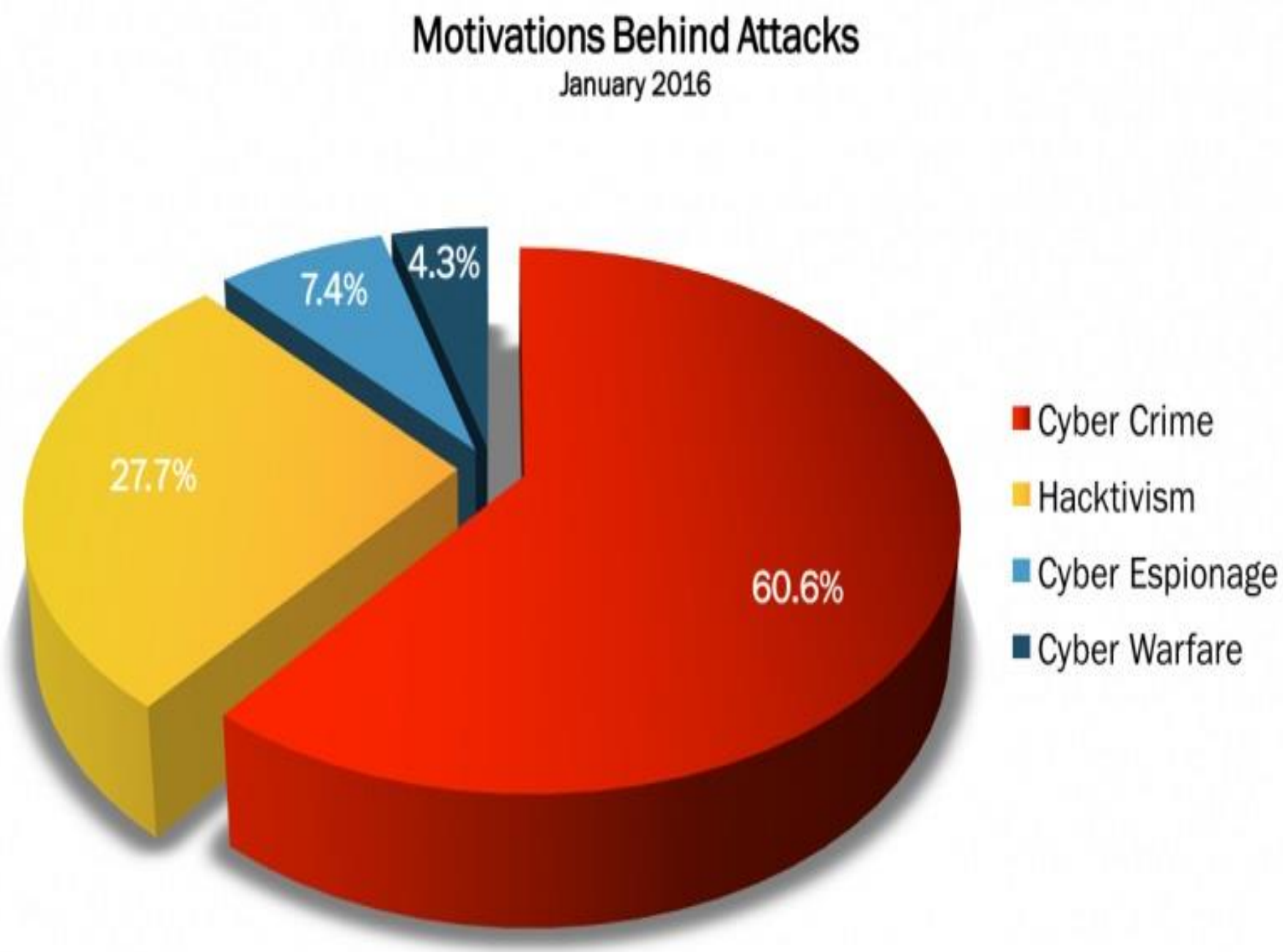
۲-۲- دزدی سایبری(جاسوسی ، سرقت و کلاهبرداری سایبری)

۲-۳- هرزه نگاری سایبری(هتک حیثیت ،جرائم علیه عفت و اخلاق فردی ، خانوادگی و عمومی)

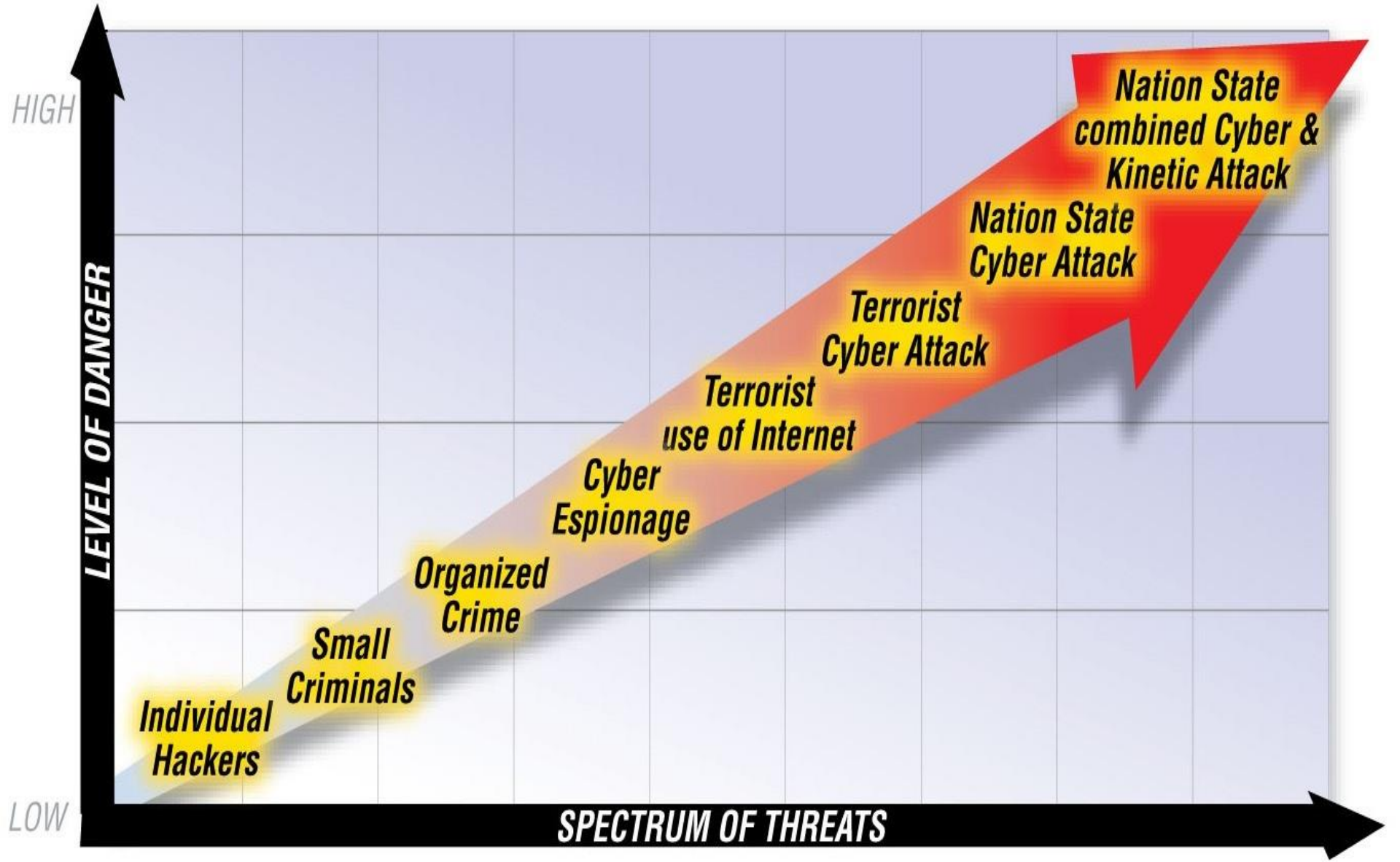
۲-۴- خشونت سایبری

۳- تروریسم سایبری(CyberTerrorism)

۴- هک تیویسم سایبری(Cyber HackTivism)


Motivations Behind Attacks
January 2016
60.6%
27.7%
7.4%
4.3%
Cyber Crime
Hacktivism
Cyber Espionage
Cyber Warfare

طیف کلی تهدیدات سایبری و سطوح رو به افزایش خطر



مبنای تهدیدات در فضای سایبری

- تهدیدگران خارجی
- تهدیدگران داخلی
- تهدیدات موجود در زنجیره تأمین کالا
- تهدیدات ناشی از عدم کفایت توانمندی عملیاتی نیروهای خودی

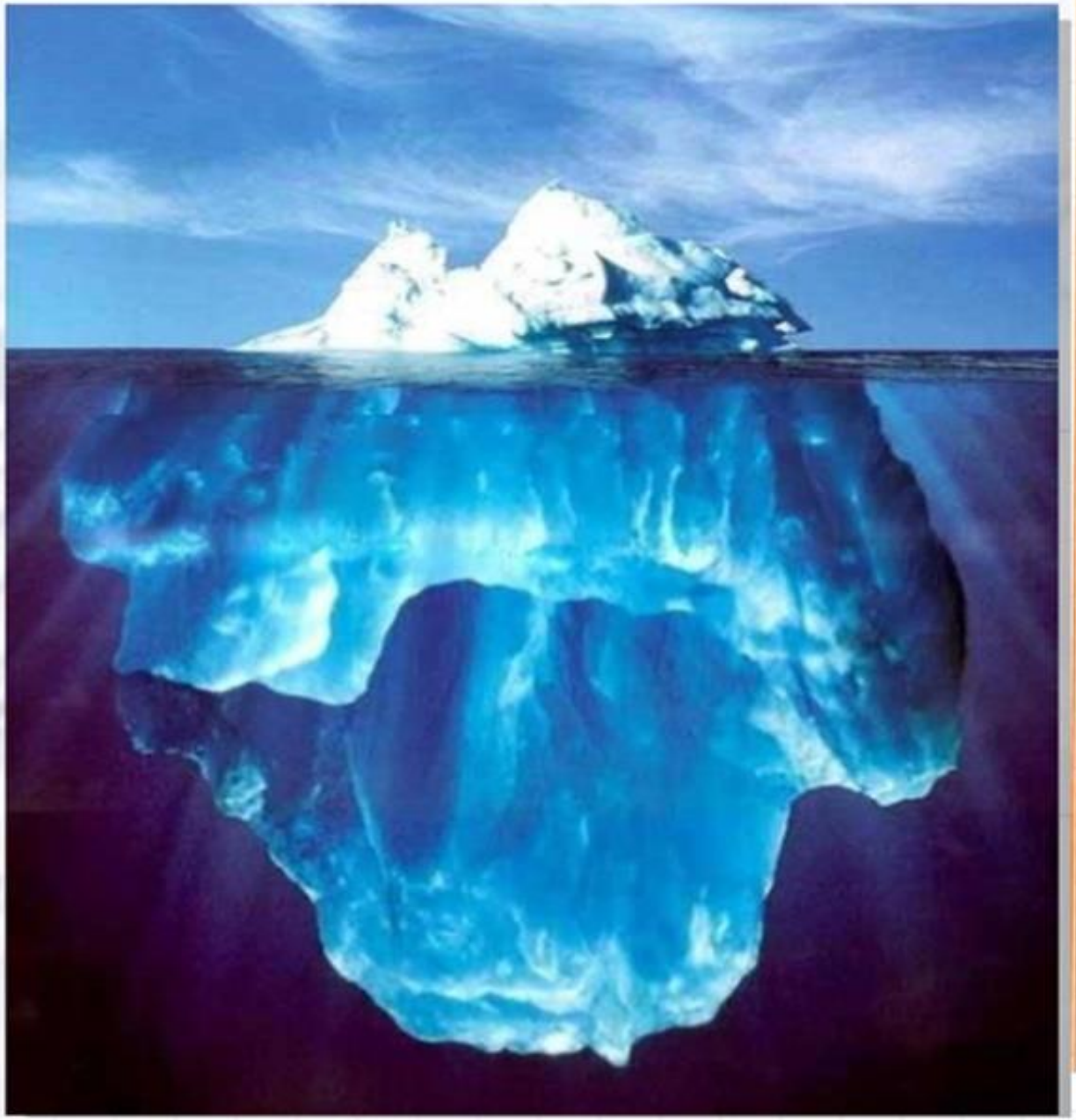
جنگ(محیط ، ابزار، انگیزه)

(جنگ سایبری می تواند مقدمه جنگ نظامی باشد)

محیط نبرد

روند توسعه تهدیدات حوزه سایبری

- هکرها و مجرمین سایبری
- بد افزارها
- جنگ سایبری
- جنگ نرم



جنگ سایبری(Cyberwarfare)

- «جنگ سایبری» به نوعی از نبرد اطلاق می شود که طرفین جنگ(کشورها) در آن از رایانه و شبکه‌های رایانه‌ای (به خصوص شبکه اینترنت) به عنوان ابزار تهاجم استفاده کرده و نبرد را در فضای سایبری به راه می اندازند.
- اصطلاح «جنگ سایبری» معمولاً به استفاده از یک سلاح سایبری برای وارد کردن خسارت فیزیکی اطلاق می گردد.

عرصه های تهدیدات سایبری(در قامت جنگ سایبری)

ردیف	حوزه	عامل تهدید (ابزار)
۱	جنگ سایبری زیرساختی صنعتی	مبتنی بر ویروس های صنعتی
۲	جنگ سایبری زیرساختی غیر صنعتی	مبتنی بر ویروس های غیر صنعتی و فعالیت های مخرب ICT
۳	جنگ سایبر الکترونیک و الکترومغناطیس	مبتنی بر سیگنال/ الکترونیک/ پالس EMP
۴	جنگ سایبری مبتنی بر شبکه های اجتماعی(شناختی،افکار عمومی)	مبتنی بر داده/ داده کاوی / محتوا/ تحلیل محتوا
۵	جنگ سایبری پولی، مالی و بانکی	مبتنی بر فناوری (بلاک چین، رمزارز و ..)
۶	جنگ سایبری نظامی	مبتنی بر تجهیزات و تسلیحات سایبری نظامی
۷	جنگ سایبری ترکیبی	ترکیبی از عوامل تهدید سایبری

جنگ سایبری زیرساختی

عنصر مورد هدف– دارایی کلیدی	مولفه کلیدی تحت تاثیر	مولفه های تهدید	آسیب پذیری کشور	پیامد اولیه	پیامد ثانویه	پیامد نهایی
تجهیزات و شبکه های کنترل صنعتی/غیر صنعتی	شبکه های زیرساختی کشور و آسیب به استمرار خدمات اساسی	بدافزارها و سلاح های سایبری- استفاده از فناوری های نوین مانند هوش مصنوعی و یادگیری ماشین	بالا- استفاده از محصولات و خدمات خارجی در نقاط کلیدی زیرساختی کشور- در حال مهاجرت به محصولات و زیست بوم داخلی	بروز اختلال در سیستم های صنعتی بصورت نقطه ای	بروز اختلال حوزه ای در شبکه های صنعتی ای کشور مانند حوزه برق، گاز و ...	بروز اختلال عمده در زیرساخت های حیاتی کشور- پیامد های آبشاری

جنگ سایبری مبتنی بر شبکه های اجتماعی

عنصر مورد هدف– دارایی کلیدی	مولفه کلیدی تحت تاثیر	مولفه های تهدید	آسیب پذیری کشور	پیامد اولیه	پیامد ثانویه	پیامد نهایی
داده – محتوا	مردم و افکار عمومی	سازماندهی و جریان سازی مردم در بستر شبکه های اجتماعی خارج پایه، جایگزینی و تغییر انگاره های سنتی و دینی مردم با تزریق اطلاعات غلط و جعلی و ذائقه سازی مخاطبان متناسب با نیاز جریان استکباری	بسیار بالا– به دلیل استفاده از شبکه های اجتماعی خارج پایه	تاثیر گذاری بر اذهان مردم– جهت دهی و سازماندهی افکار عمومی	بروز نارضایتی ها و سوار شدن بر امواج گسست های قومی، سیاسی و ...	بروز آشوب ها و تاثیر مخرب بر مولفه های امنیت ملی

جنگ سایبری پولی، مالی و بانکی

عنصر مورد هدف– دارایی کلیدی	مولفه کلیدی تحت تاثیر	مولفه های تهدید	آسیب پذیری کشور	پیامد اولیه	پیامد ثانویه	پیامد نهایی
تراکنش ها و شبکه های مالی و اقتصادی	شبکه های اقتصادی و مالی	بدافزارها و سلاح های سایبری- استفاده از فناوری های نوین مانند هوش مصنوعی و یادگیری ماشین	بسیار بالا- وابستگی بالا به تجهیزات عمدتا امریکایی	اختلال در تراکنش های مالی شبکه اقتصادی کشور	اختلال در مولفه های کلیدی اقتصادی کشور و بروز نارضایتی های اجتماعی	اختلال عمده در شبکه تجارت و اقتصاد کشور و تاثیر عمده بر مولفه های امنیت ملی کشور- پیامد های آبشاری

جنگ سایبری نظامی

عنصر مورد هدف– دارایی کلیدی	مولفه کلیدی تحت تاثیر	مولفه های تهدید	آسیب پذیری کشور	پیامد اولیه	پیامد ثانویه	پیامد نهایی
تجهیزات نظامی مانند هواپیما، موشک و ...	شبکه دفاعی کشور	استفاده از فناوری های نوین مانند هوش مصنوعی، اینترنت اشیا، سایبرالکترومغناطیس و ...	نسبتا پایین- خودکفایی کشور در تولید محصولات پایه و استراتژیک دفاعی	اختلال در حوزه دفاعی کشور بصورت حوزه ای	اختلال عمده در شبکه دفاعی کشور و برتری نظامی دشمنان	تاثیر عمده بر امنیت ملی و مولفه های کلیدی قدرت ملی

جنگ سایبری ترکیبی (هیبریدی)

عنصر مورد هدف– دارایی کلیدی	مولفه کلیدی تحت تاثیر	مولفه های تهدید	آسیب پذیری کشور	پیامد اولیه	پیامد ثانویه	پیامد نهایی
ترکیبی از موارد بالا	ترکیبی از موارد بالا	ترکیبی از موارد بالا	بالا	بروز نارضایتی های حوزه ای در حوزه های اجتماعی، اقتصادی و ...	بروز نارضایتی ها و آشوب های محلی و منطقه ای	بروز نارضایتی ها و آشوب ها و اعتراضات در سطح ملی- پیامد های آبشاری

جنگ سایبر الکترونیک و الکترومغناطیس

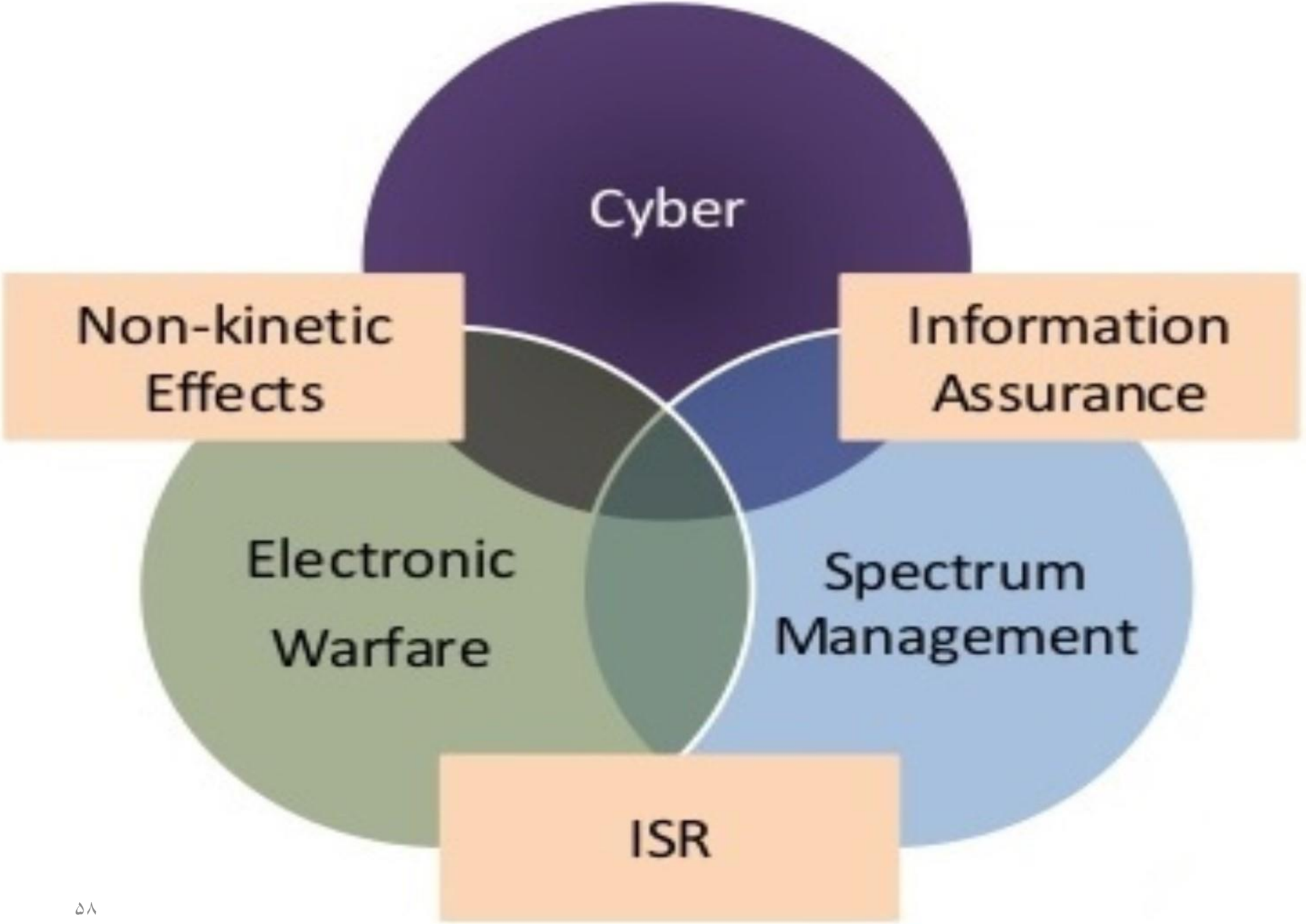
عنصر مورد هدف– دارایی کلیدی	مولفه کلیدی تحت تاثیر	مولفه های تهدید	آسیب پذیری کشور	پیامد اولیه	پیامد ثانویه	پیامد نهایی
تجهیزات و بوردهای الکترونیکی و هادی ها	تجهیزات مخابراتی و رایانه ای	طیف الکترومغناطیس و جنگ الکترونیک که از آن بعنوان ابعاد سایبر الکترونیک نام برده میشود. ربات های هوشمند برای اختلال و یا انهدام تجهیزات، امواج الکترومغناطیسی برای ارسال داده بر روی تجهیزات هدف که به صورت ایزوله و فاقد ارتباط با شبکه عمومی است، تزریق انواع بدافزار به شبکه های ایزوله و ... استفاده خواهد شد.	بسیار بالا– وابستگی مطلق به محصولات خارجی و عمدتا امریکایی	اختلال در شبکه های مخابراتی و شبکه های رایانه ای بصورت نقطه ای	اختلال و نفوز به شبکه های کلیدی مخابراتی و رایانه ای زیرساخت های اساسی کشور	تاثیر عمده بر امنیت ملی و مولفه های کلیدی قدرت ملی– پیامد های آبشاری

تهدیدات سایبر الکترومغناطیس

Cyber Electromagnetic

تقاطع فضای سایبر و فضای الکترومغناطیس

(پالس های الکترومغناطیس)


Cyber
Non-kinetic Effects
Information Assurance
Electronic Warfare
Spectrum Management
ISR

تهدیدات الکترومغناطیسی

- تهدیدات الکترومغناطیسی : امواج (پالس های) الکترومغناطیسی مخرب که از یک سلاح الکترومغناطیسی(رادیویی،مخابراتی ،ژنراتورهای مولد، بمب های انفجاری)بوجود می‌آید(انتشار می یابد).
- سلاح الکترومغناطیسی: تجهیزاتی هستند که می توانند یک منبع کنترل شده EMP باشند.

منابع تهدید الکترومغناطیسی

- **منابع طبیعی**

- صاعقه، رعد و برق

- **منابع سیستمی یا ابزاری**

- سوئیچینگ - موتورها – دستگاه های جوشکاری - ترانسفورماتورها

- ژنراتورها -سیستم های تهویه

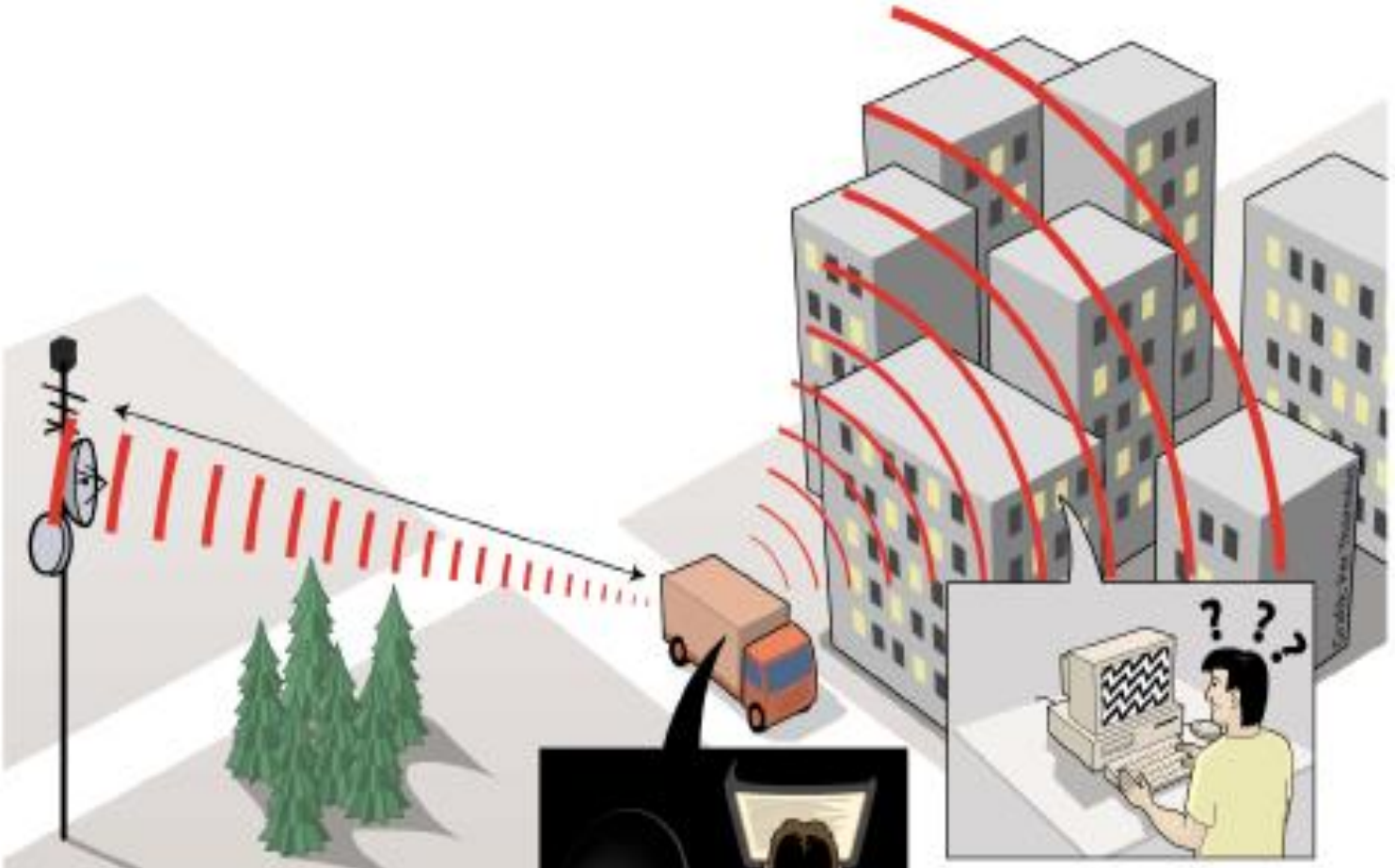
- **سلاح های الکترومغناطیسی**

- (HEMP)انفجار های هسته ای

-بمب های الکترومغناطیسی انفجاری

-تسلیحات الکترومغناطیسی سیار زمینی با تغذیه الکتریکی

High Power Microwaves (HPM). Coupling to Systems



Front-Door Coupling

- Through antennas, sensors etc.
- For microwave receivers: HPM frequency within receiving band.
- Protection: transient protectors, filters.

Back-Door Coupling

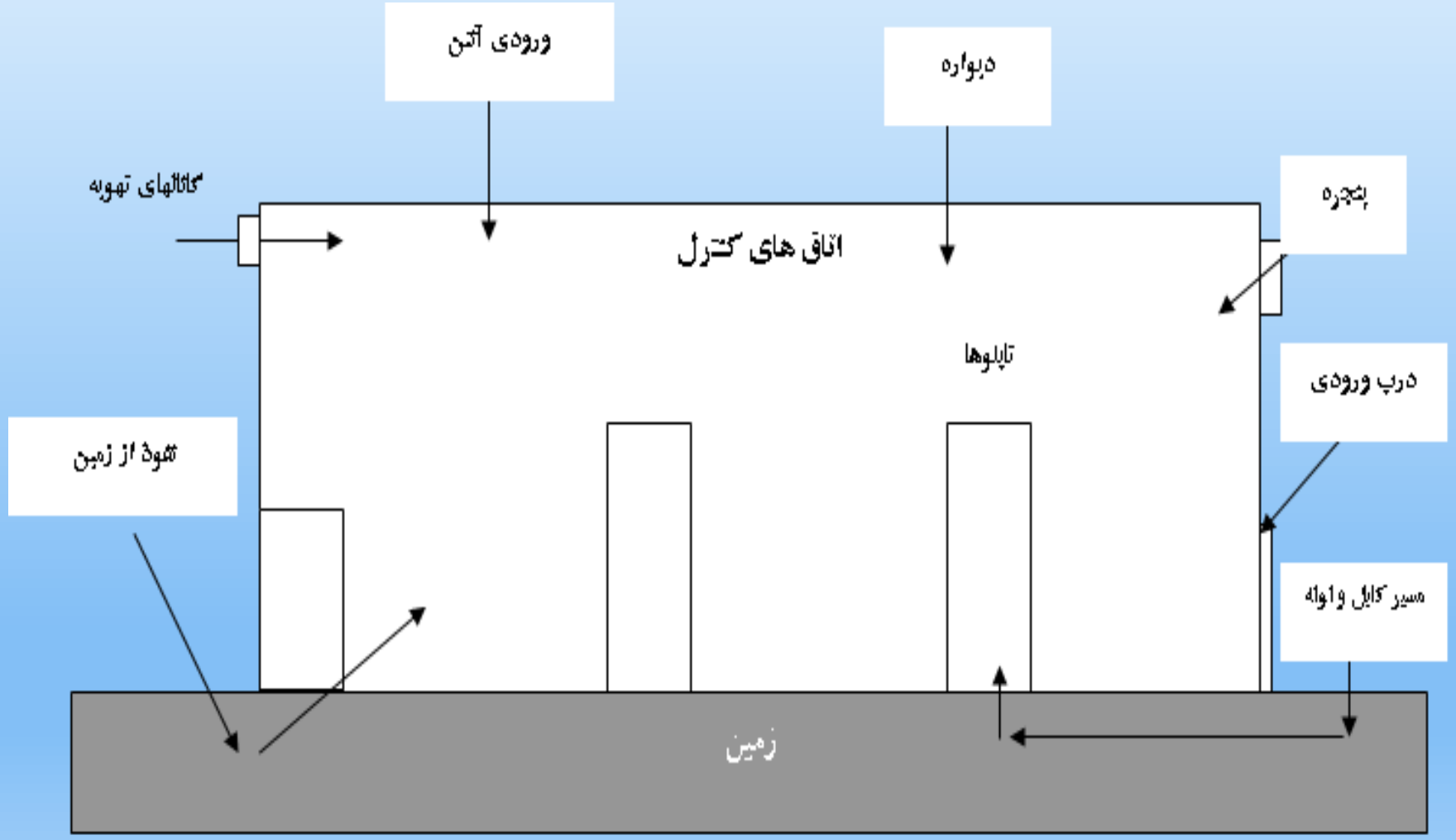
- Penetration through holes, joints etc.
- Resonance at approx. 1–3 GHz.
- Protection: shielding, filtering.

Illustrat

FO

TOTALFÖ
FORSKNI

مدل کلی نفوذ پالس(امواج) الکترومغناطیسی



ویژگی های تهدیدات الکترومغناطیسی

- از یک سلاح الکترومغناطیسی بوجود می‌آیند(انتشار می یابند).
- این امواج به صورت پالس می باشند.
- دارای انرژی زیادی می باشند.
- میدان الکترومغناطیسی حاصل از این امواج، می تواند ولتاژ وجریان بالاتر را به صورت لحظه ای بر کلیه رساناهای موجود، نظیرسیم‌ها، مدارات ولوازم الکتریکی والکترونیکی القاء کند.

راهکارهای مقابله

- شیلدینگ مناسب فضا و تجهیزات (Shielding)
- فیلترینگ مناسب کابل های دیتا و تغذیه برق(Filtering)
- ارتینگ مناسب در محل سایت ها(Earthing)

فلج کردن سایبری کشورها

Cyber Sabotage

- اصطلاح «سابوتاژ سایبری» یا همان «فلج کردن سایبری»، به **حملات سایبری** به زیرساخت‌های حیاتی اطلاق می‌شود که **تخریب فیزیکی** را در پی دارد.
- مختل ساختن عملکرد عادی سیستم
- نفوذ کردن رایانه ای خدشه زننده

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.

برخی عوامل زمینه ساز جنگ سایبری

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

طرح نیترو زئوس(Nitro Zeus)

- در اوایل دوران ریاست‌جمهوری اوباما طرحی کلید خورد که در آن هزاران پرسنل نظامی و اطلاعاتی مشارکت داشتند و ده‌ها میلیون دلار برای آن هزینه شد، این طرح نیترو زئوس نام داشت.
- نیترو زئوس، برنامه یک جنگ سایبری گسترده است و قرار بود در صورتی که تلاش‌های دیپلماتیک به منظور محدود کردن برنامه هسته‌ای بی‌نتیجه بماند و توافق هسته‌ای به جایی نرسد، اجرایی شود.
- آمریکا مدعی است که اگر این سلاح سایبری مورد استفاده قرار می‌گرفت، سامانه‌های پدافند هوایی، ارتباطی و بخش‌های حیاتی شبکه توزیع برق ایران از کار می‌افتاد.

بدافزارهای مرتبط با طرح نیترو زئوس

- فلیم (Flame) : سلاحی علیه زیرساخت های حیاتی کشور
- استاکس‌نت (Stuxnet) : وسعتی به اندازه بمب هیروشیما
- دوکو (Duqu) : جاسوسی از مذاکرات هسته‌ای ایران
- گاوس (Gauss) : از کار انداختن زیرساخت‌های کشورها

هدف : اطمینان خاطر آمریکا و متحدان. از داشتن گزینه‌ای دیگر در صورت تبدیل شدن ایران به تهدیدی جدی .

مخاطره سایبری

به احتمال بهره‌برداری یک تهدید سایبری، از یک یا چند آسیب‌پذیری سایبری موجود در یک سرمایه ملی سایبری را مخاطره سایبری گویند .

منشاء مخاطره سایبری

منشاء مخاطره سایبری، عبارت است از دو عامل:

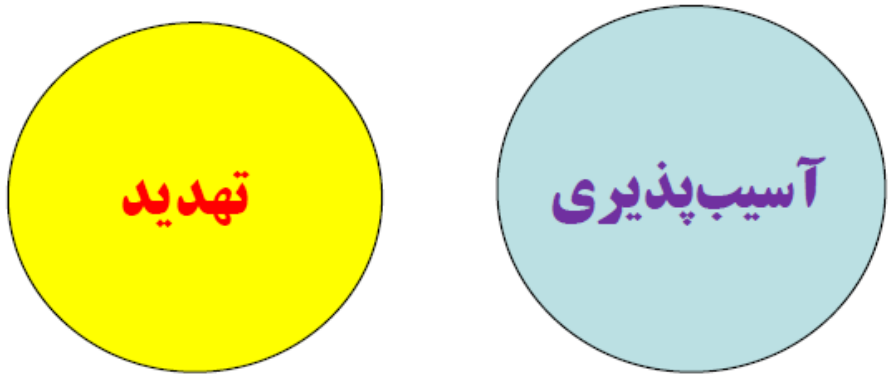
- تهدید سایبری موجود علیه سرمایه سایبری
- آسیب‌پذیری سایبری موجود در داخل سرمایه سایبری

اهداف مخاطره سایبری

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

ارتباط تهدید و آسیب پذیری(۱)

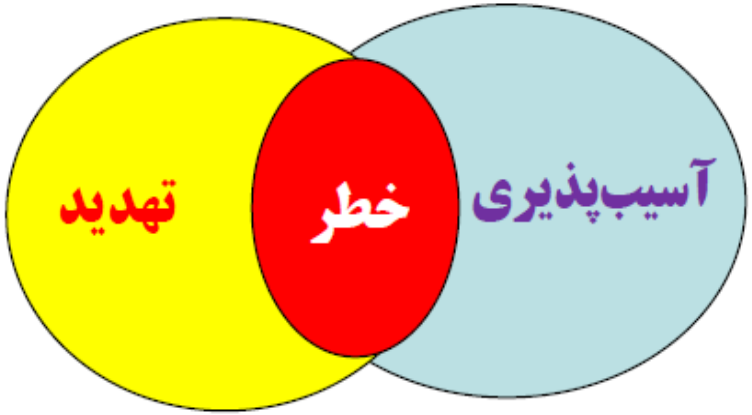
حالت اول: ارتباطی میان آسیب‌پذیری‌ها و تهدید وجود ندارد.



چگونگی ارتباط حوزه‌های تهدید خارجی و آسیب‌پذیری در حالت عدم‌ارتباط

ارتباط تهدید و آسیب پذیری(۲)

در حالت دوم: ارتباط محدود، طیفی از ارتباط و تعامل میان این دو حوزه قابل تصوّر است.

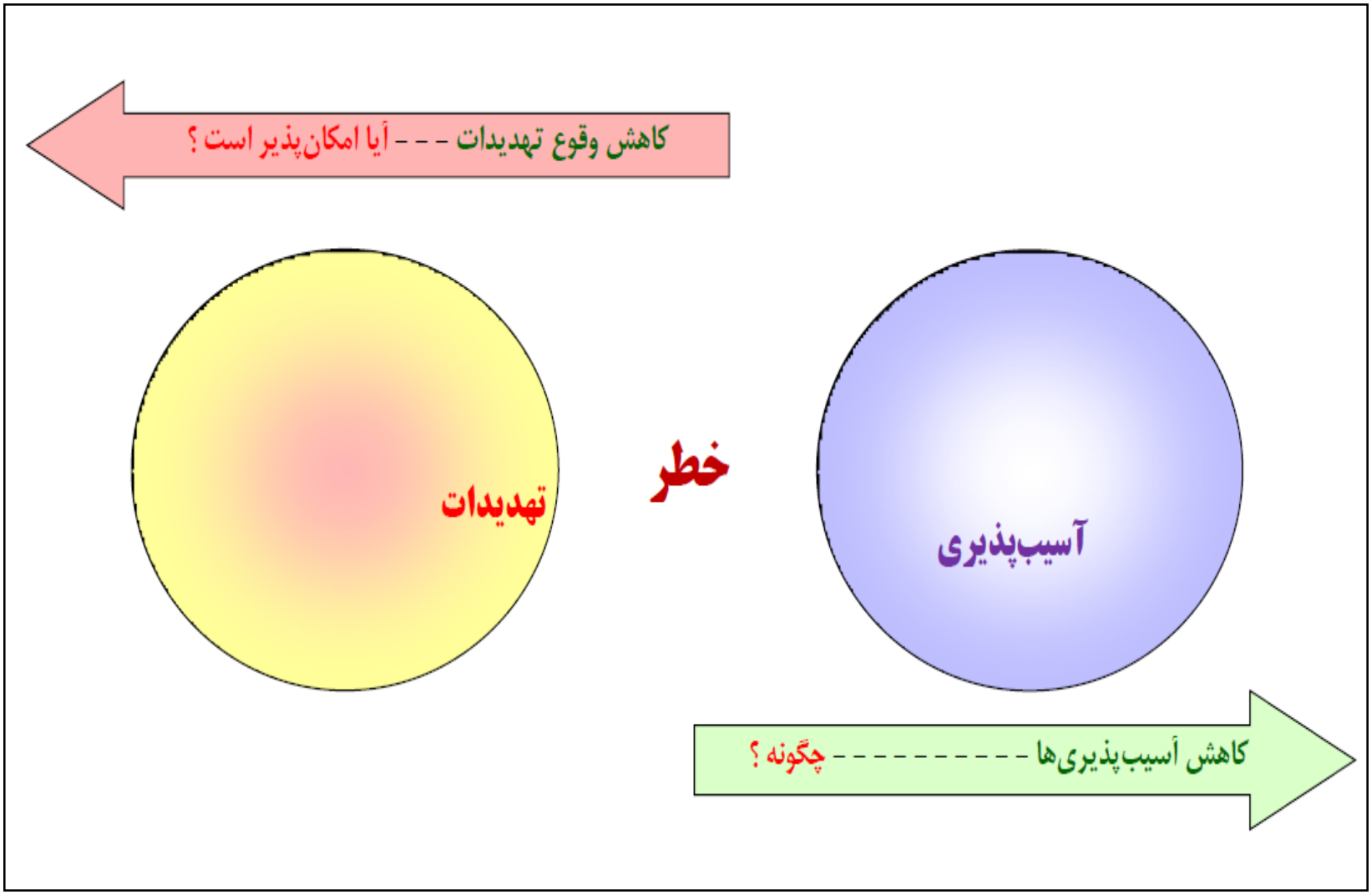


چگونگی ارتباط تهدید و آسیب‌پذیری در حالت ارتباط محدود

ارتباط تهدید و آسیب پذیری(۳)

در حالت سوم: آسیب‌پذیری و تهدید موجود بر یکدیگر منطبقند.

چگونگی ارتباط حوزه تهدید و آسیب‌پذیری در حالت ارتباط حداکثری و انطباق کامل


کاهش وقوع تهدیدات - - - آیا امکان‌پذیر است ؟
تهدیدات
خطر
آسیب‌پذیری
کاهش آسیب‌پذیری‌ها - - - - - - - - - - چگونه ؟

دسته بندی حملات امنیتی

- حملات فعال(active)

اطلاعات را تغییر میدهد و یا بر عملیات تاثیر می گذارد.

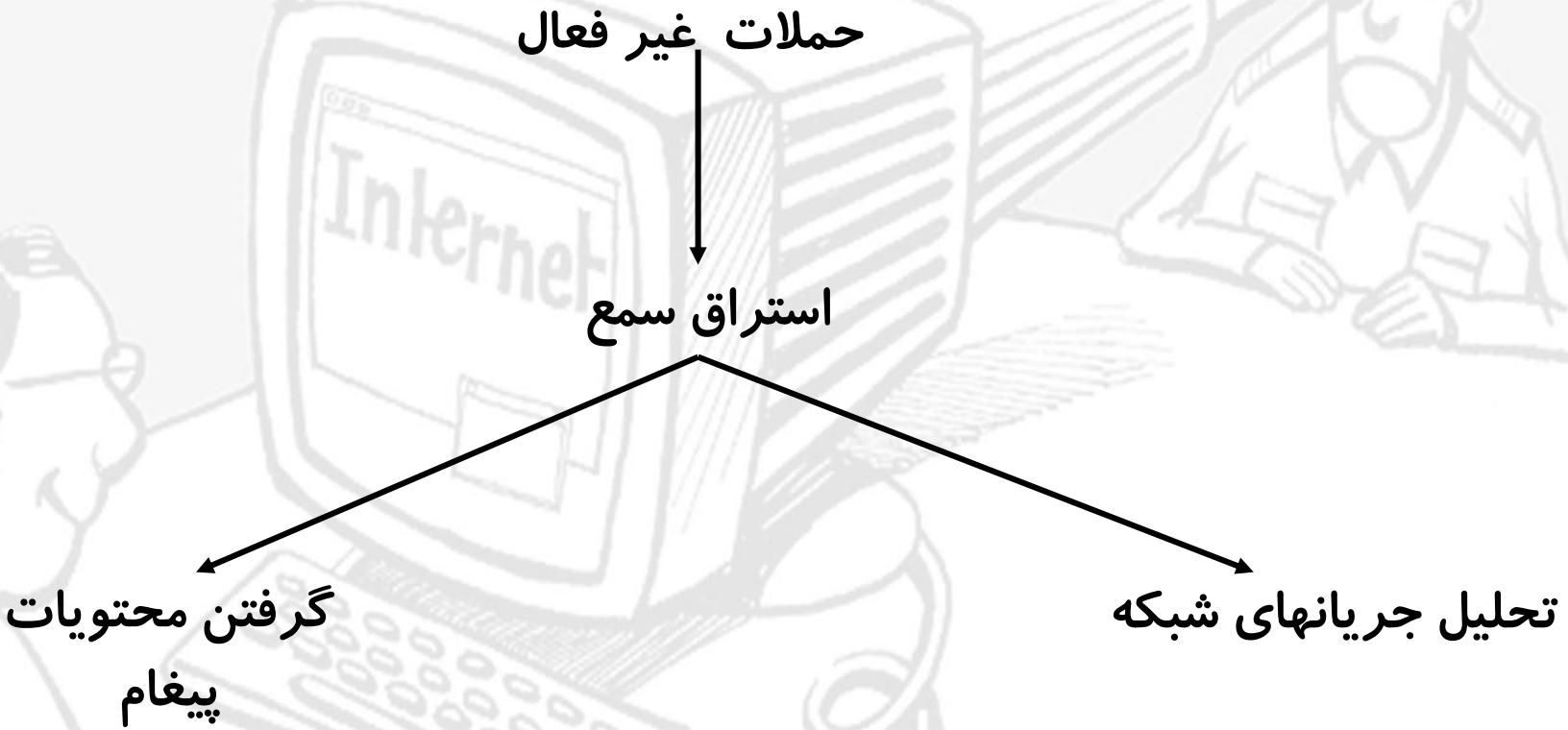
- حملات غیرفعال (passive)

فقط اطلاعات را خوانده و از آنها استفاده میکند ولی تغییری در اطلاعات نمی دهد.

حملات امنیتی(۱)

- بعضی از تغییرا ت رشته‌های داده

حملات امنیتی(۲)



- استراق سمع، نظارت بر جریانهای شبکه

انواع حملات نفوذگران

- شنود یاinterception

در این روش نفوذ گر می‌تواند به شکل مخفیانه از اطلاعات نسخه برداری کند.

- تغییر اطلاعات یاmodification

در این روش نفوذگر به دستکاری و تغییر اطلاعات می‌پردازد.

- افزودن اطلاعات یاfabrication

در این روش نفوذگر اطلاعات اضافی بر اصل اطلاعات اضافه می‌کند.

- وقفهinterruption

در این روش نوع نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود.

حملات امنیتی

Information source

Information destination

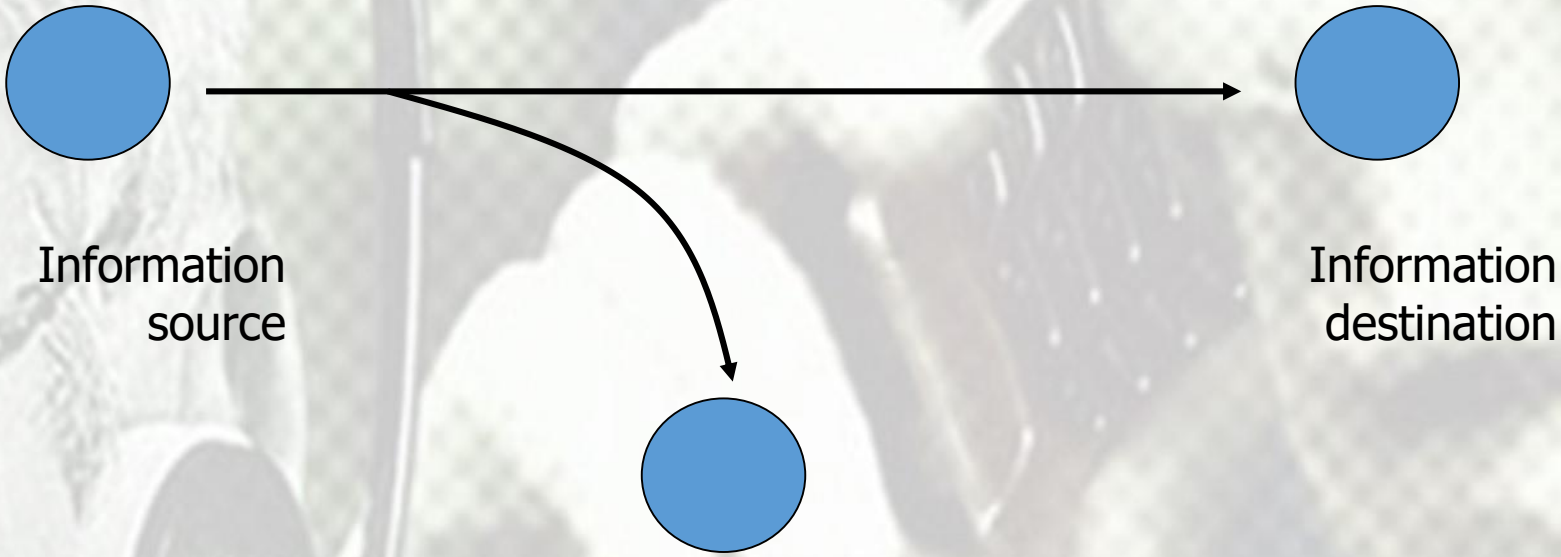
جریان عادي

حملات امنیتی

قطع ارتباط

- حمله به دسترس پذيري(Availability)

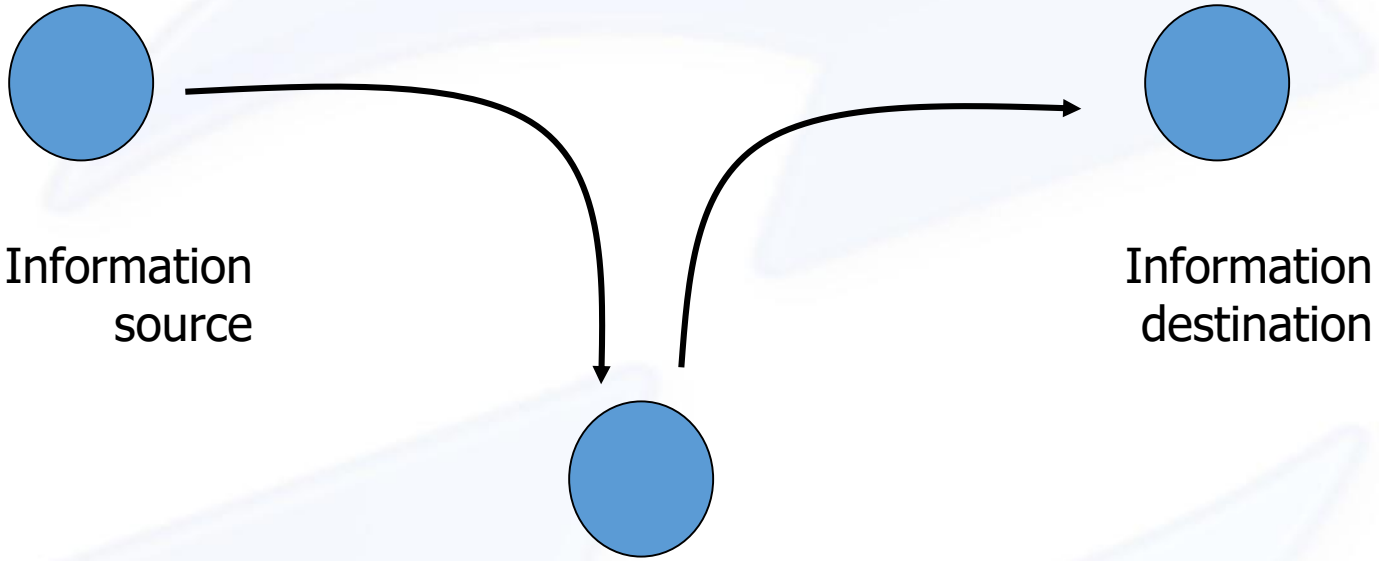
حملات امنیتی



استراق سمع(شنود یا interception)

- حمله به محرمانگي

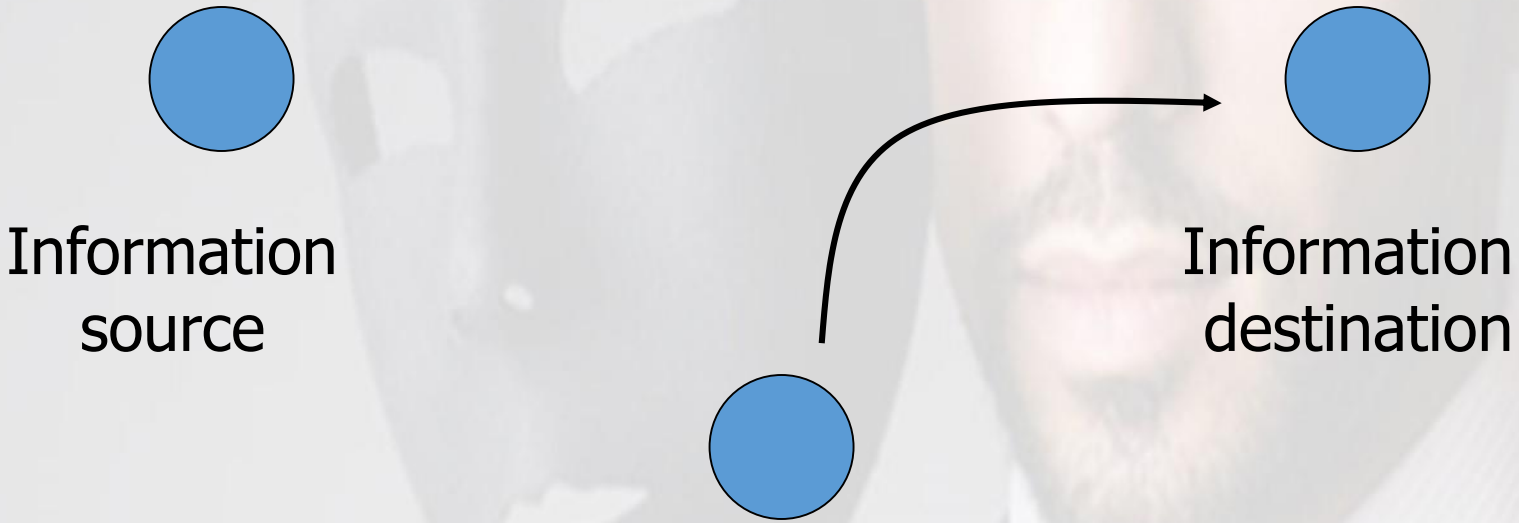
حملات امنیتی



تغییر(تغییر اطلاعات یا modification)

- حمله به جامعیت

حملات امنیتی



جعل هویت

- حمله به هویت شناسي

Web Attacks: The Biggest Threat to Your Network

برخی تهدیدات(حملات) امنیتی(۱)

تهدیدات (۱)	
انکار خدمات DOS	در این روش دسترسی کاربران مجاز به سامانه و بالعکس از دست می رود. در واقع حمله کننده از یک نقطه شروع به غوطه ور کردن کامپیوترهای هدف در پیام های مختلف و انسداد آمد و شد قانونی داده ها می نماید. این باعث می شود که هیچ سامانه ای نتواند از سرویس استفاده و یا با سامانه های دیگر ارتباط برقرار کند.
انکار گسترده خدمات DDOS	در این روش به جای شروع حمله از یک منبع، همزمان از تعداد زیادی سامانه توزیع شده اقدام به حمله می کنند. غالباً این کار با استفاده از کرم ها و تکثیر آنها در رایانه های متعدد بری حمله به هدف صورت می گیرد.
اسنیفر	برنامه ای است که داده های مسیریابی شده را شنود نموده و با بررسی هر بسته در جریان داده ها به دنبال اطلاعات خاصی مانند کلمه های عبور می گردد.
اسب تروا	برنامه ای رایانه ای که کدی خطرناک را مخفی می کند. معمولاً اسب تراوا دارای ظاهری مشابه برنامه های مفیدی است که کاربر تمایل به اجرای آنها دارد.

برخی تهدیدات(حملات) امنیتی (۲)

تهدیدات(۲)	
بمب منطقی	نوعی خرابکاری که در آن برنامه نویس کدی وارد برنامه می کند که در صورت بروز اتفاقی خاص برنامه خود به خود یک فعالیت تخریبی را صورت می دهد.
ویروس	برنامه ای است که فایل های رایانه ای که معمولاً برنامه های اجرایی هستند را با وارد کردن نسخه ای از خود در آن فایلها آلوده می سازد با بارگذاری فایل های آلوده در حافظه، این نسخه ها اجرا و به ویروس امکان آلوده کردن سایر فایل ها را می دهد. بر خلاف کرم ها ویروس برای انتشار نیازمند دخالت انسانی است.
کرم	برنامه ای رایانه ای مستقل که با نسخه برداری از خود از یک سامانه به سامانه دیگر در شبکه تکثیر می شود. بر خلاف ویروس های رایانه ای کرم ها نیازی به دخالت انسان برای انتشار ندارند.
جاسوس افزار	بدافزار نصب شده بدون اطلاع کاربر برای ردیابی و یا ارسال داده ها به طرف سوم غیر مجاز به صورت پنهانی
باج افزار	Ransomware، گونه‌ای از بدافزارها هستند که دسترسی به فایل‌ها را محدود می کنند و ایجادکننده آن برای برداشتن محدودیت درخواست باج می‌کند. برخی از انواع آن‌ها روی فایل‌ها رمزگذاری انجام می‌دهند و برخی دیگر ممکن است به سادگی سامانه را قفل کنند.

برخی تهدیدات(حملات) امنیتی (۳)

تهدیدات(۳)	
ابزارهای سوء استفاده	این ابزار ها در دسترس عموم قرار دارد که می توانند با برخورداری از سطوح مهارتی مختلف آسیب پذیری های موجود در شبکه ها را کشف و از آن طریق وارد شوند.
ارسال هرزنامه	ارسال نامه های پست الکترونیک تجاری ناخواسته که می تواند حاوی سازوکار تحویل نرم افزار های مخرب و سایر تهدیدات سایبری باشد. با استفاده از هرزنامه افراد را فریب می دهد تا اطلاعات حساس خود را افشا نمایند(سرقت کلمه های عبور و اطلاعات مالی)
ساخت وب سایت جعلی (فریب)	ایجاد یک وب سایت فریب برای تقلید از یک سایت واقعی و مشروع و معمولاً در مورد پست الکترونیک این عمل هنگامی رخ می دهد که آدرس فرستنده و دیگر بخش های مشخصات نامه الکترونیک تغییر داده می شود به طوری که گیرنده تصور می کند نامه از مبدأ معتبری ارسال شده است.
بات نت	شبکه ای از سامانه های کنترل از راه دور که برای هماهنگی حملات، توزیع بدافزار و هرزنامه و پیام های سرقت اطلاعات بکار برده می شود. بات ها معمولاً به صورت مخفیانه در سامانه هدف نصب می شوند و امکان کنترل از راه دور رایانه مورد هدف را به کاربر غیر مجاز می دهند تا اهداف خرابکارانه خود را محقق کنند.
جنگ شبکه ای بی سیم	روشی برای امکان ورود به شبکه های رایانه ای بی سیم با استفاده از لپ تاپ، آنتن و کارت شبکه بی سیم که شامل گشت زنی در موقعیت های خاص برای دسترسی غیر مجاز می باشد.

امنیت

عنوان	توضیحات
برنامه مدیریت امنیت سایبری	سیاست های امنیتی، مکانیزم های امنیتی، سرویس های امنیتی
امنیت اطلاعات	۱. امنیت، نفوذ و روش های مقابله در سطح Client & Servers ۲. امنیت، نفوذ و روش های مقابله در سطح Web
امنیت ارتباطات	امنیت، نفوذ و روش های مقابله در سطح Network (Wired & Wireless)
امنیت فیزیکی	کنترل دسترسی های فیزیکی

امنیت اطلاعات

امنیت اطلاعات مبتنی است بر تحقق سه ویژگی زیر:

✓محرمانگی (Confidentiality)

- عدم افشای غیرمجاز داده‌ها

✓صحت (Integrity)

- عدم دستکاری(تغییر) داده‌ها توسط افراد یا نرم‌افزارهای غیرمجاز

✓دسترس‌پذیری (Availability)

- دسترسی به داده هاتوسط افراد مجاز در هر مکان و در هرزمان

خط مشی امنیتی

- خط‌مشی (سیاست) امنیتی(Security Policy): نیازمندیهای امنیتی یک سازمان و یا یک سیستم اطلاعاتی/ ارتباطی را بیان می‌نماید.
- در تعریف سیاست‌های امنیتی:
  - باید بدانید تا چه اندازه و در چه نقاطی نیاز به اقدامات محافظتی دارید.
  - سیاستهای سازمان در دسترسی افراد به منابع اطلاعاتی چیست؟
  - باید بدانید چه افرادی، چه مسؤولیت‌هایی در اجرای اقدامات محافظتی سازمان دارند.

مکانیزم امنیتی

- **مکانیزم امنیتی (Security Mechanism)**: به هر روش، ابزار و یا رویه‌ای که برای اعمال یک سیاست امنیتی به کار می‌رود، یک مکانیزم امنیتی گویند.

تکنیک ها و تاکتیک های امن سازی ارتباط (امنیت ارتباطات)

۱. استفاده از محدوده فرکانس های بالا (باند مایکروویو)

۲. استفاده از روش های طیف گسترده(DSSS–FHSS)

۳. پایین آوردن(مدیریت مناسب) سطح توان ارسالی

۴. استفاده از دیتا(ارتباطات دیجیتال) به جای صوت(ارتباطات آنالوگ)

۵. بهره گیری از فناوری فیبر نوری

۶. رمز نگاری (کد گذاری) دیتای ارسالی (استفاده از تکنیک های رمز نگاری پیچیده)

۷. ایجاد لایه‌های ارتباطی متنوع(بی سیم ، با سیم)

۸. رعایت اصول پدافند غیر عامل (طراحی، پیاده سازی ، اجرا، بهره برداری)

امنیت فیزیکی(محیطی)

- در نظرگرفتن سیستم های دوربین مدار بسته ، زنگ اخبار برای اماکن
- در نظرگرفتن سیستم تهویه مناسب برای تاسیسات، تجهیزات و اماکن.
- تهیه فهرست افراد مجاز دارای دسترسی های لازم و مجاز .
- در نظرگرفتن سیستم های کنترل دسترسی به اماکن .
- توجه به امنیت محیط کار درساعات غیر اداری.

امنیت فیزیکی(محیطی)

- استفاده از منبع تغذیه برق بدون قطع (UPS) .
- استفاده ازسیستم های هوشمند اعلام ، کنترل و اطفاء حریق.
- جلوگیری از ورود و خروج و تکثیر غیرمجاز ذخیره سازها (شامل انواع لپ تاپ، هارد اکسترنال،نوار،CDیا DVD، فلاپی، حافظه فلش) .
- جلوگیری از نصب برنامه های کاربردی (توسط کاربران) .
- اجرای مسیرکابل کشی مجزا برای سیستم برق و دیتا .
- ایجاد سیستم بایگانی دیتا بصورت سخت افزاری(پشتیبان گیری).

امنیت فیزیکی(محیطی)

- ایجاد سیستم امحا کامل تجهیزات،اسناد و مدارک اسقاطی و بدون استفاده.
- ایجاد حصار یا دیوار امن برای محدوده تجهیزات شبکه ای(اتاق سرور،اتاق تجهیزات شبکه ،مرکز داده امن).
- ایجاد سیستم حفاظت الکترومغناطیسی
  - ارتینگ(Earthing)
  - فیلترینگ(Filtering) دیتا و برق
  - شیلدینگ(Shielding)-قفس فارادی

امنیت شبکه(لایه اکتیو)

- طراحی ، اجرا و مستندسازی تمامی ساختار شبکه بر اساس مدل لایه ای Core,Distribution,Access
- امنیت ، طراحی و پیاده سازی سیستم سوییچینگ شبکه بر اساس مدل L3 Switching & STP
- نصب و راه اندازی Firewallو ایجاد Zoneهای امنیتی توسط آن و تعریف سطوح دسترسی
- نصب و راه اندازی IDSو IPSدر شبکه
- امنیت ، طراحی و پیاده سازی IP Address Management
- امنیت ، طراحی و پیاده سازی LAN & WANو مدیریت سوییچها ، روترها و کنترل ترافیک آنها

امنیت سیستم عامل و لایه کاربردی

- پیکربندی امنیتی روی تمامی سیستم عامل های شبکه ای و اینترنتی NOS & IOS
- پیکربندی امنیتی روی تمامی سیستم عامل های کلاینت ها OS
- پیکربندی امنیتی و ایمن سازی سرویس های شبکه
- نصب و راه اندازی سیستم Automatic Backup & Restore
- نصب و راه اندازی سیستم WSUSدر شبکه های Microsoft Base(*Windows Server Update Services*)
- پیکربندی امنیتی و ایمن سازی Active Directory & Group Policy

امنیت و پیاده سازی Network Monitoring

- نصب و راه اندازی سیستم Network Monitoring & Analyzer
- نصب و پیاده سازی Network Performance Monitor
- نصب و پیاده سازی Application Performance Monitor
- نصب و پیاده سازی NetFlow Traffic Analyzer
- نصب و پیاده سازی IP Address Manager
- نصب و پیاده سازی IP SLA Manager
- طراحی ، نصب و راه اندازی سیستم Bandwidth Management & Caching
- نصب و راه اندازی سیستم Anti Virus (Network Base & Host Base)

امنیت و پیاده سازی سیستم Centralize AAAو مدیریت یکپارچه

- نصب و راه اندازی سیستم LAS (LAN Accounting Suite)به همراه تمامی اجزاء مورد نیاز
- راه اندازی و پیاده سازی سیستم Centralize AAAدر غالب LASو اتصال ADبه آن
- ایجاد و پیاده سازی Redundancy & Fault Toleranceجهت بالا بردن سطح امنیتی شبکه

➢ طراحی و پیاده سازی سیستم Access Control

➢ طراحی و پیاده سازی Server Farm & Site Room

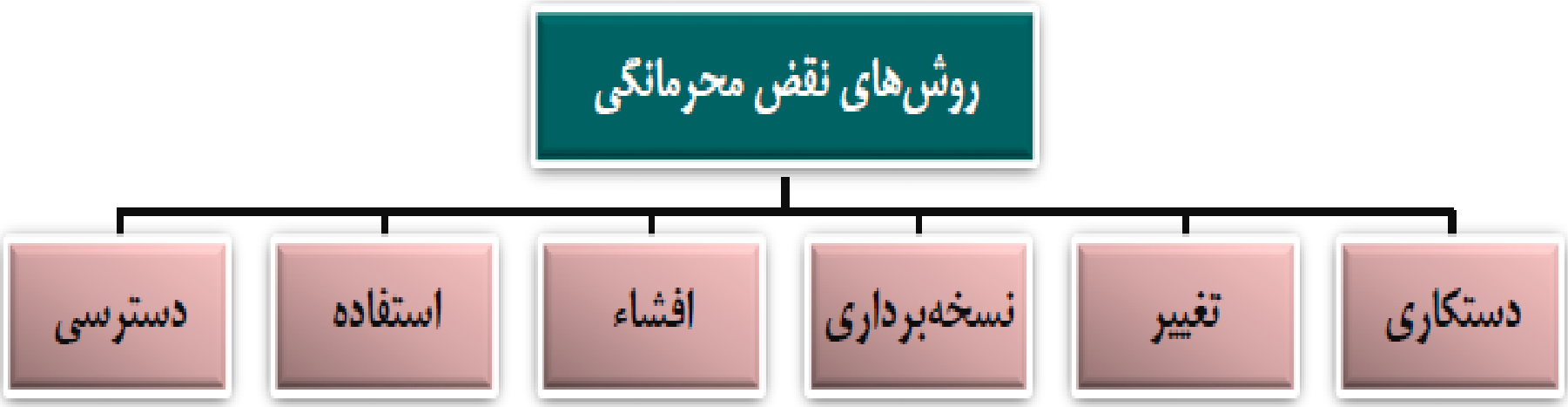
ارکان مهم امنیت

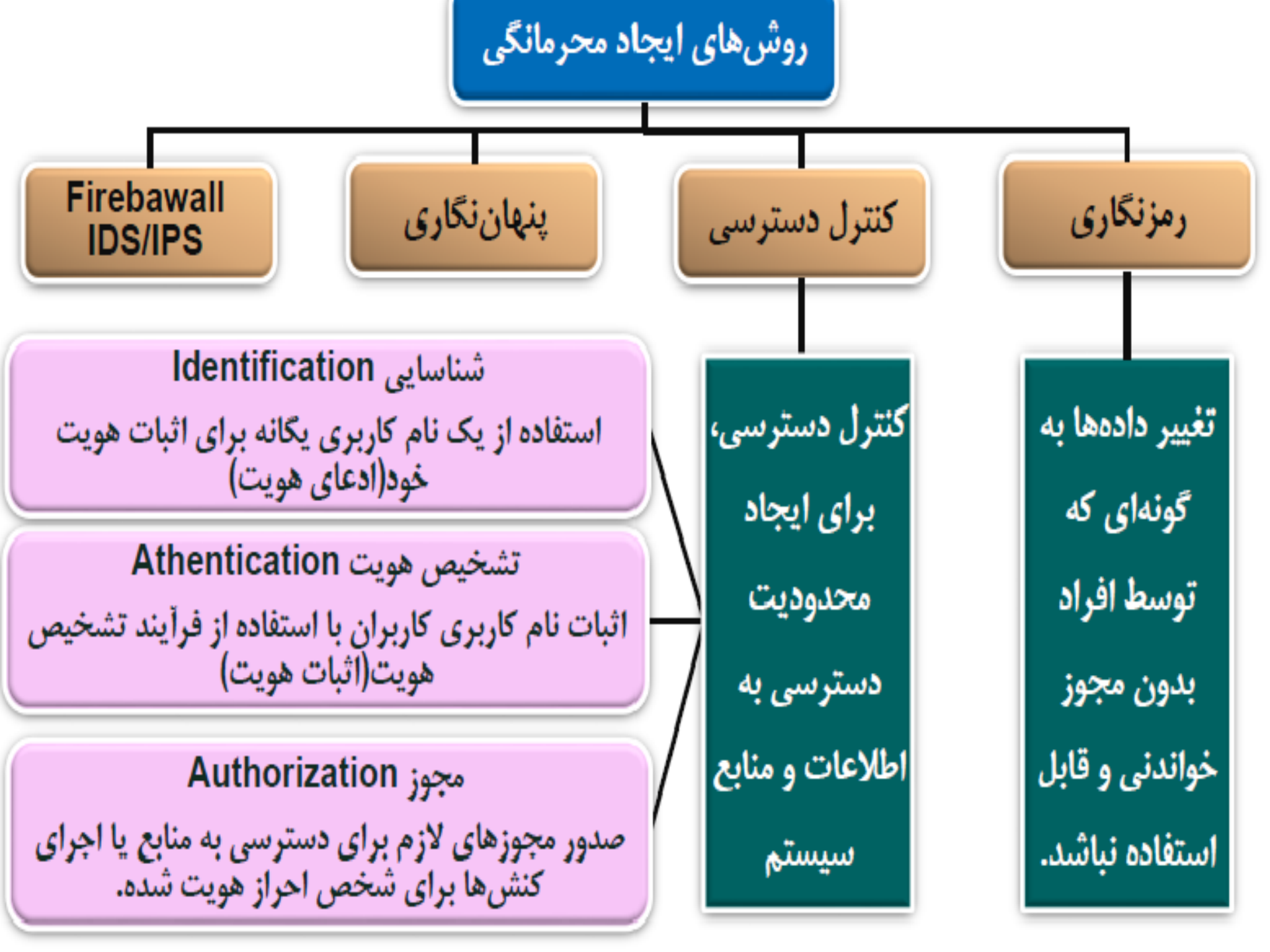
Expanded to include

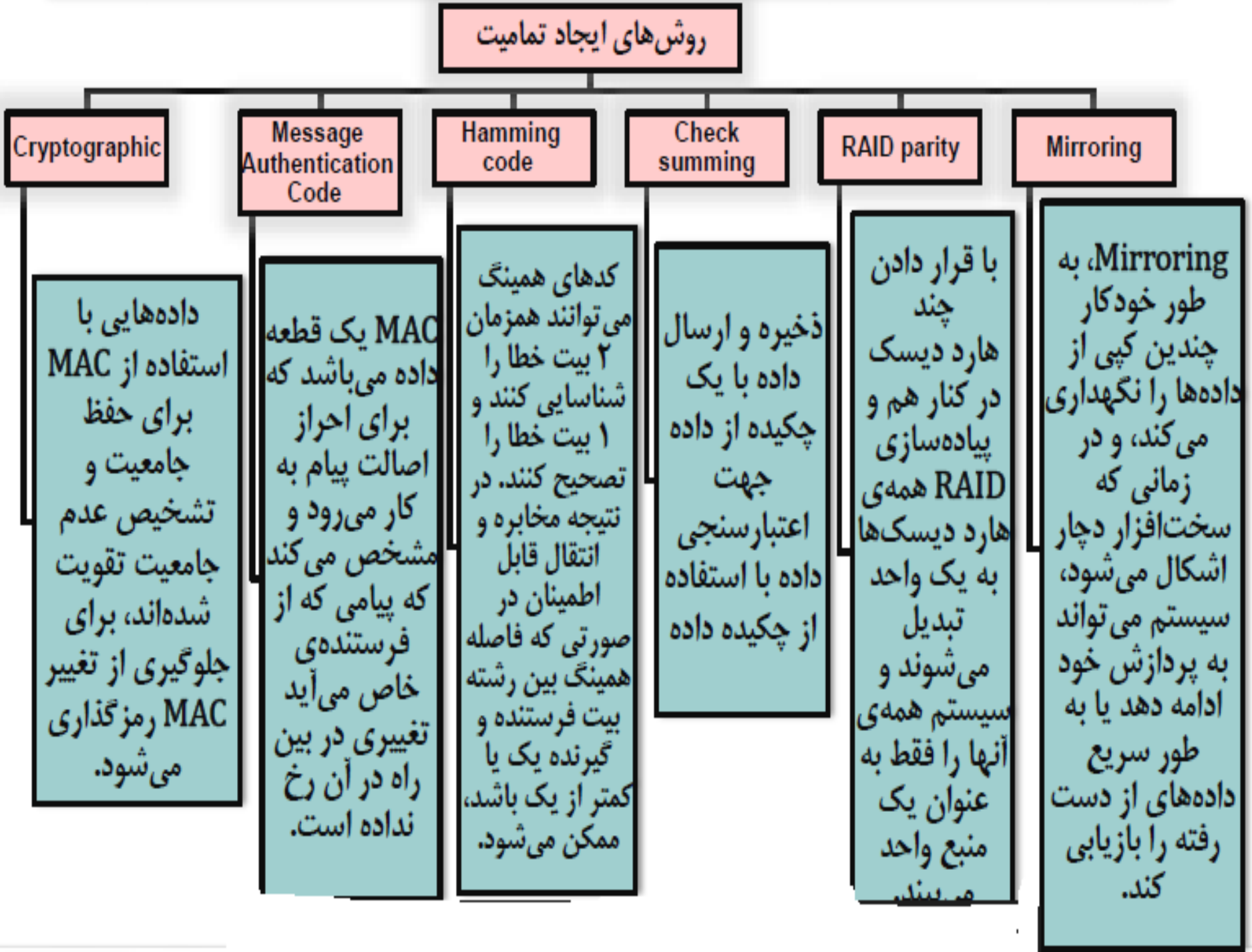
- ✓Identification
- ✓Authentication
- ✓Authorization
- ✓Privacy
- ✓Accountability

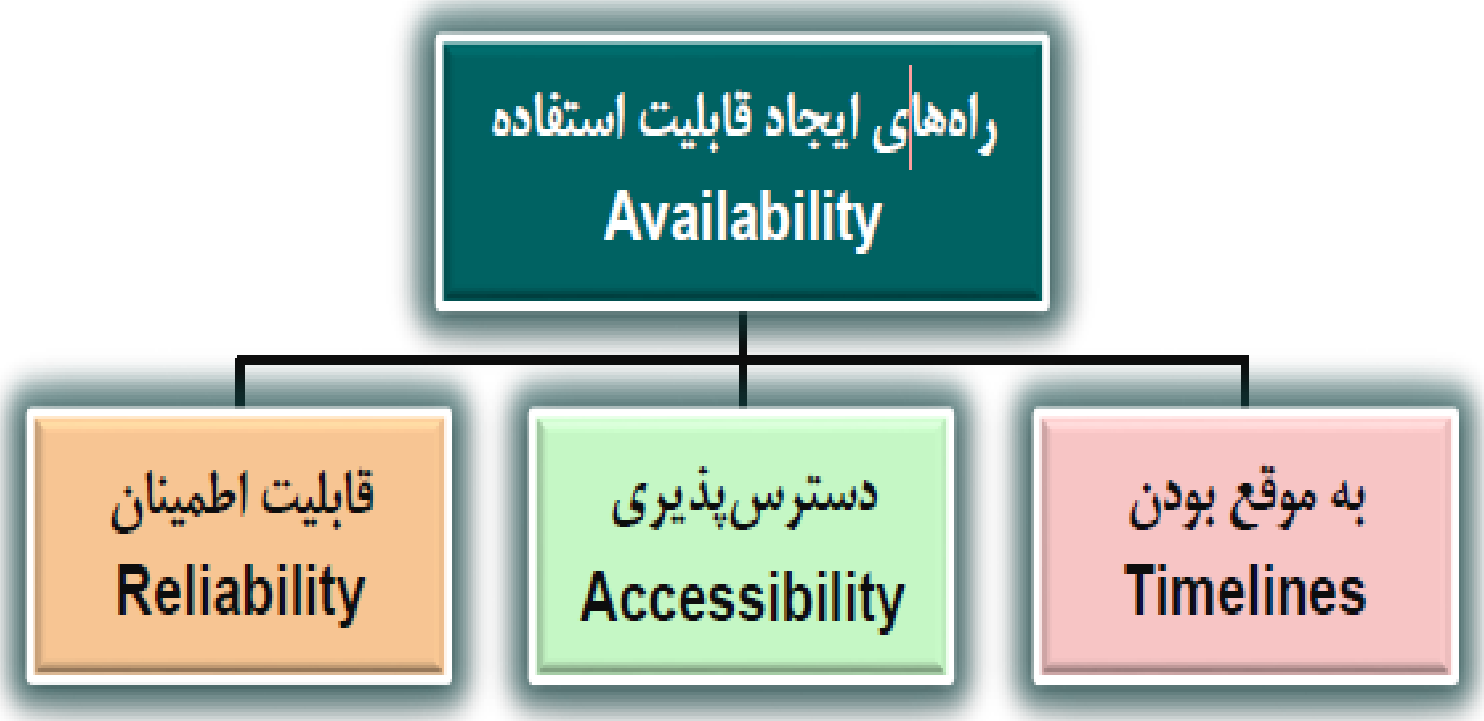
اصل محرمانگی

- داده‌ها صرفا برای افراد مجاز و در زمان مورد نیاز در دسترس باشند.
- مثال از نقض محرمانگی:
  - شنود غیر قانونی محتوای یک ایمیل در حال انتقال
    - راه حل: رمزنگاری پیام




روش‌های ایجاد محرمانگی
رمزنگاری
کنترل دسترسی
پنهان‌نگاری
Firebawall
IDS/IPS
تغییر داده‌ها به گونه‌ای که توسط افراد بدون مجوز خواندنی و قابل استفاده نباشد.
کنترل دسترسی، برای ایجاد محدودیت دسترسی به اطلاعات و منابع سیستم
شناسایی Identification
استفاده از یک نام کاربری یگانه برای اثبات هویت خود(ادعای هویت)
تشخیص هویت Athentication
اثبات نام کاربری کاربران با استفاده از فرآیند تشخیص هویت(اثبات هویت)
مجوز Authorization
صدور مجوزهای لازم برای دسترسی به منابع یا اجرای کنش‌ها برای شخص احراز هویت شده.


روش‌های ایجاد تمامیت
Mirroring
RAID parity
Check summing
Hamming code
Message Authentication Code
Cryptographic
Mirroring، به طور خودکار چندین کپی از داده‌ها را نگهداری می‌کند، و در زمانی که سخت‌افزار دچار اشکال می‌شود، سیستم می‌تواند به پردازش خود ادامه دهد یا به طور سریع داده‌های از دست رفته را بازیابی کند.
با قرار دادن چند هارد دیسک در کنار هم و پیاده‌سازی RAID همه‌ی هارد دیسک‌ها به یک واحد تبدیل می‌شوند و سیستم همه‌ی آنها را فقط به عنوان یک منبع واحد
ذخیره و ارسال داده با یک چکیده از داده جهت اعتبارسنجی داده با استفاده از چکیده داده
کدهای همینگ می‌توانند همزمان ۲ بیت خطا را شناسایی کنند و ۱ بیت خطا را تصحیح کنند. در نتیجه مخابره و انتقال قابل اطمینان در صورتی که فاصله همینگ بین رشته بیت فرستنده و گیرنده یک یا کمتر از یک باشد، ممکن می‌شود.
MAC یک قطعه داده می‌باشد که برای احراز اصالت پیام به کار می‌رود و مشخص می‌کند که پیامی که از فرستنده‌ی خاص می‌آید تغییری در بین راه در آن رخ نداده است.
داده‌هایی با استفاده از MAC برای حفظ جامعیت و تشخیص عدم جامعیت تقویت شده‌اند، برای جلوگیری از تغییر MAC رمزگذاری می‌شود.

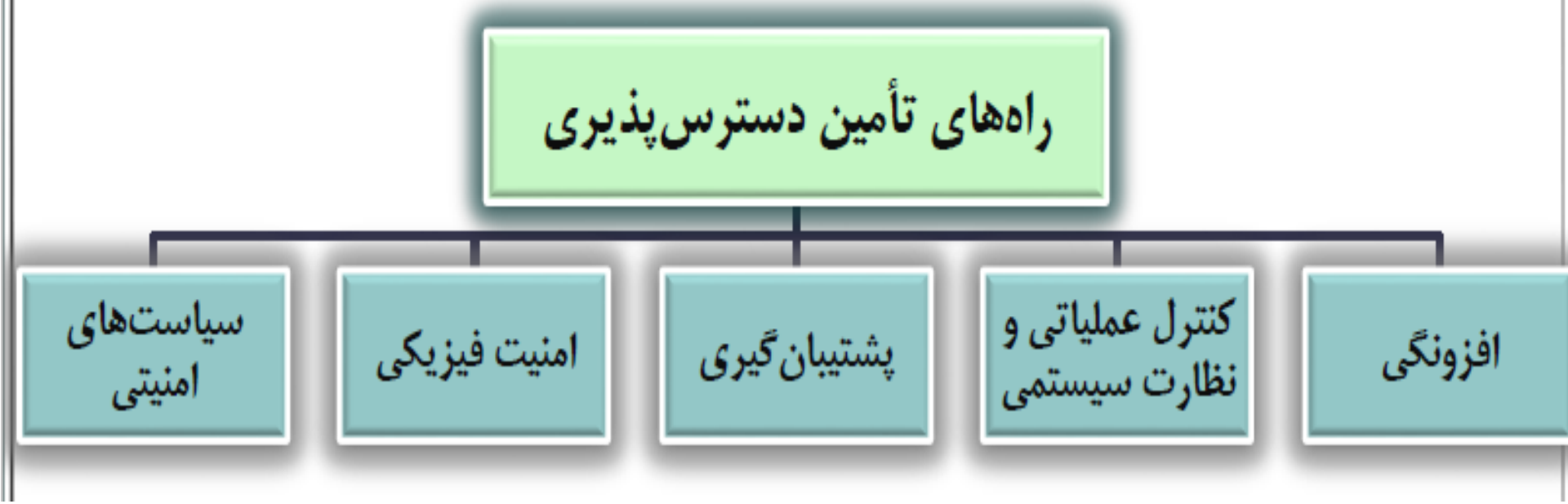

راه‌های ایجاد قابلیت استفاده
Availability
قابلیت اطمینان
Reliability
دسترس‌پذیری
Accessibility
به موقع بودن
Timelines

قابلیت اطمینان Reliability

احتمال کارکرد سالم و بدون عیب برای مدت زمان مشخص طبق شرایط موجود و از پیش تعیین شده

دسترس‌پذیری Accessibility

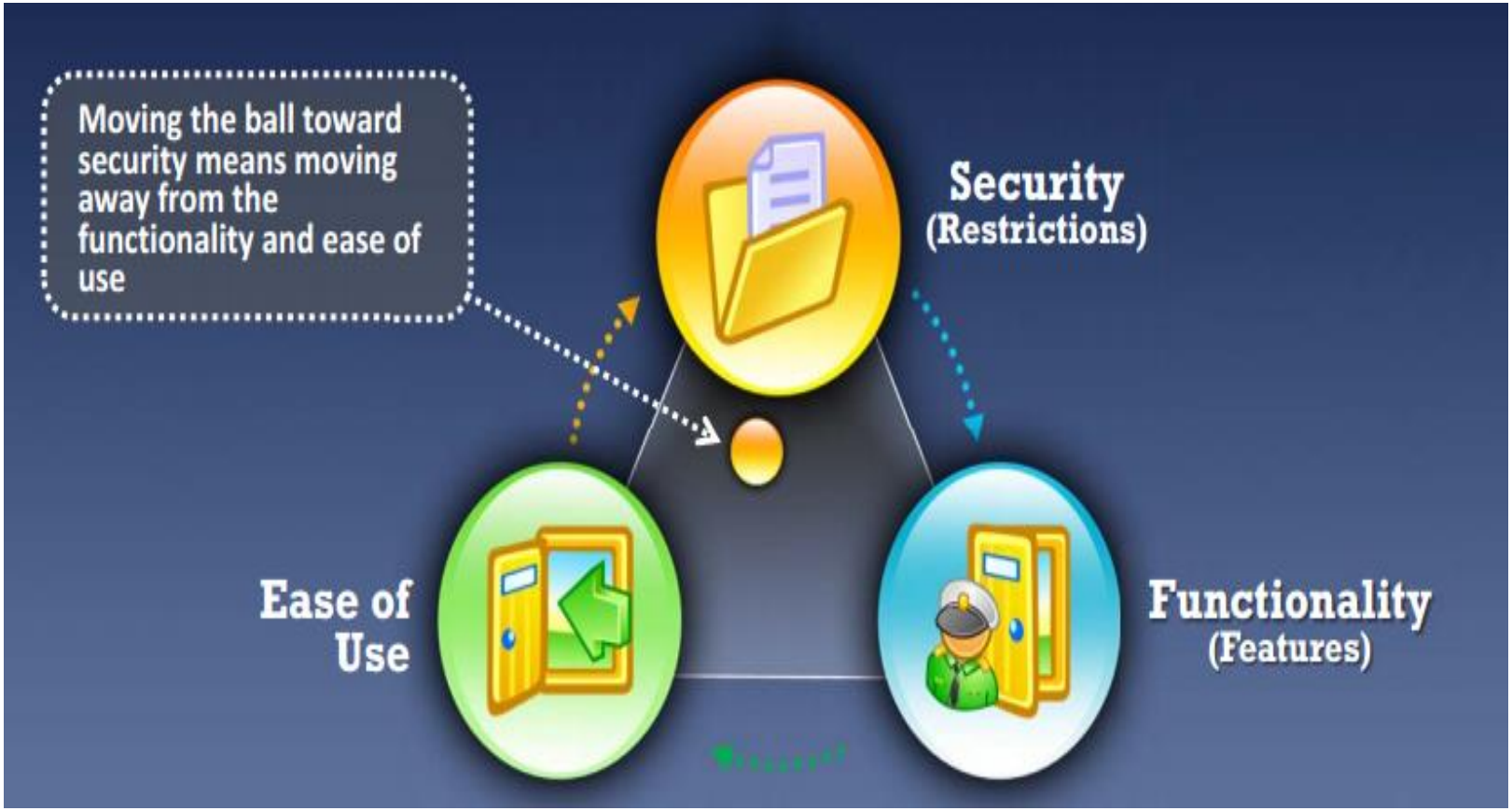
درجه‌ای که یک سیستم توسط بسیاری از **کاربران قابل استفاده است** و امکان تغییر وجود ندارد.

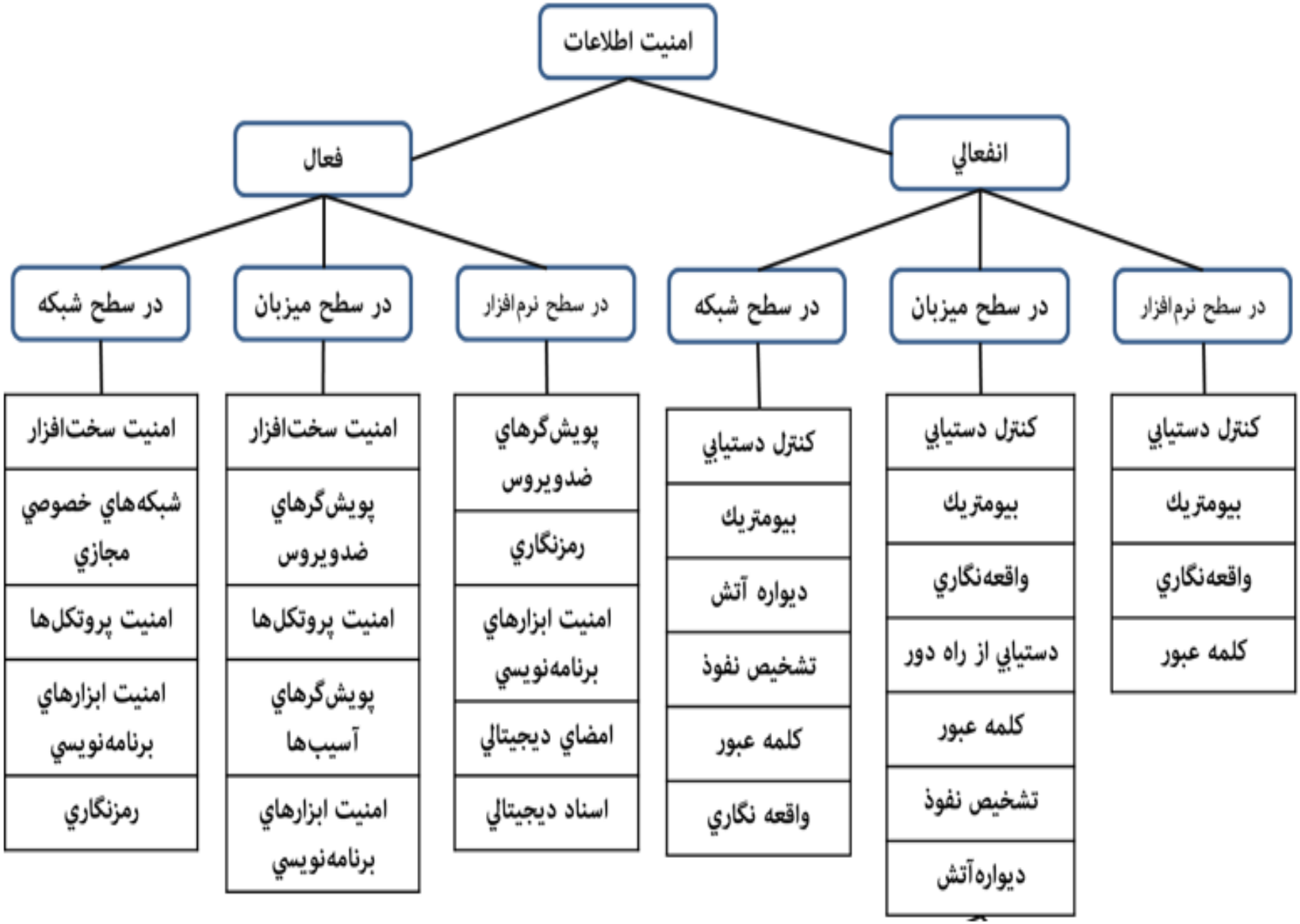


Timelines

به موقع بودن پاسخ سیستم و یا تامین منابع به درخواست کاربر

Trade-off توازن امنیت




امنیت اطلاعات
انفعالي
فعال
در سطح نرم‌افزار
در سطح میزبان
در سطح شبکه
در سطح نرم‌افزار
در سطح میزبان
در سطح شبکه
کنترل دستیابي
بیومتریك
واقعه‌نگاري
کلمه عبور
کنترل دستیابي
بیومتریك
واقعه‌نگاري
دستیابي از راه دور
کلمه عبور
تشخیص نفوذ
دیواره‌آتش
کنترل دستیابي
بیومتریك
دیواره آتش
تشخیص نفوذ
کلمه عبور
واقعه نگاري
پویش‌گرهاي ضدویروس
رمزنگاري
امنیت ابزارهاي برنامه‌نویسي
امضاي دیجیتالي
اسناد دیجیتالي
امنیت سخت‌افزار
پویش‌گرهاي ضدویروس
امنیت پروتکل‌ها
پویش‌گرهاي آسیب‌ها
امنیت ابزارهاي برنامه‌نویسي
امنیت سخت‌افزار
شبکه‌هاي خصوصي مجازي
امنیت پروتکل‌ها
امنیت ابزارهاي برنامه‌نویسي
رمزنگاري

برخی ریسک های متصور(۱)

Resource Exhaustion	اصطلاک منابع
Interception of Data in Transmission	رهگیری(شنود) داده ها در حین انتقال
Insecure or Ineffective Deletion of Data	حذف ناامن و یا بی اثر داده
Distributed Denial of Service (DDoS)	حملات انکار سرویس توزیع شده
Loss or Compromise of Encryption Keys	از دست دادن یا سازگاری کلید های رمزگذاری
Loss of Operation Logs	از دست دادن لاگ ها(گزارش عملیات ها)
Backups Lost or Stolen	از دست رفتن یا سرقت فایل های پشتیبان

برخی ریسک های متصور(۲)

Malicious Probes	نرم افزارهای مخرب
Conflicts between customer	تداخل بین مشترکین در محیط ابر
Licensing Risks	ریسک های صدور مجوز
Network Failure	تخریب/ شکست شبکه
Networking Management issues	مسایل مربوط به مدیریت شبکه
Social Engineering Attacks	حملات مهندسی اجتماعی
Big data Attacks	حملات دادهای عظیم
Theft of Computer Equipment	سرقت تجهیزات رایانه ای

برخی ریسک های متصور(۳)

Unauthorized Access to Premises, Including Physical Access to Machines and Other Facilities	دسترسی ها غیر مجاز (مانند دسترسی به ماشین ها و ابزار)
Availability -Authorization -Accounting	نقض AAA (دسترسی-مجوز-حسابرسی)
Insecure storage of cloud access credentials by customer	دخیره سازی ناامن دسترسی های ابر توسط مشترک
Data leakage on Upload/Download	نشت اطلاعات
Scanners	اسکن کنند ه ها(پویش(**Scanning**) دیتای تبادلی در شبکه ها و سامانه ها)

- آمادگی دفاع سایبری
- پدافند سایبری(راهبردها، راهکارها، اقدامات اساسی)
- تدوین طرح های امنیت و پدافند سایبری

پدافند سایبری(Cyber Defense)

بهره‌گیری از کلیه امکانات سایبری و غیرسایبری کشور، به منظور ایجاد بازدارندگی، پیش‌گیری، ممانعت از انجام، تشخیص به موقع، مقابله موثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری کشور، توسط متخاصمین سایبری .

پدافند سایبری (Cyber Defense)

- به مجموعه اقدامات و تدابیر سایبری و غیر سایبری گفته می شود که به کارگیری آنها موجب کاهش آسیب پذیری، تداوم کارکردهای اساسی و ضروری سایبری و وابسته به فضای سایبر، تسهیل مدیریت بحران سایبری در برابر طیف تهدیدات پایه سایبری(*)، ارتقا پایداری و تاب آوری سایبری ملی و توسعه و به روز رسانی بازدارندگی سایبری و دفاعی در برابر تهدیدات پایه سایبری دشمن می شود.

رسالت پدافند سایبری

مصون سازی و پایدارسازی سرمایه های ملی سایبری و فضای سایبری کشور در برابر تهدیدات و حملات سایبری دشمن .

سطوح پدافند سایبری

پدافند نقطه ای(در لایه زیر ساخت و کارگاه)مانند نیروگاه برق	پدافند سایبری دستگاهی و حوزه ای مانند حوزه هسته ای	پدافند سایبری استانی	پدافند سایبری در سطح ملی در سطوح زیرساخت و شبکه های ارتباطی ملی	پدافند جمعی فراملی در قالب پیمانهای مشترک دفاع سایبری منطقه ای

رویکردهای پدافند سایبری

پدافند سایبری پیش‌بینانه (رصد، پایش، کنترل و تشخیص تهدید)	پدافند سایبری پیش‌گیرانه(کاهش آسیب پذیری، امن سازی اضطراری، ارتقا آمادگی)	پدافند سایبری پیش‌دستانه(دفاع فعال و حمله پیش دستانه)	پدافند سایبری واکنش-گرایانه(مقابله، اضطراری یا جامع)	پدافند سایبری انفعالی(پاسخ و مقابله در شرایط غافلگیری)

Resilience

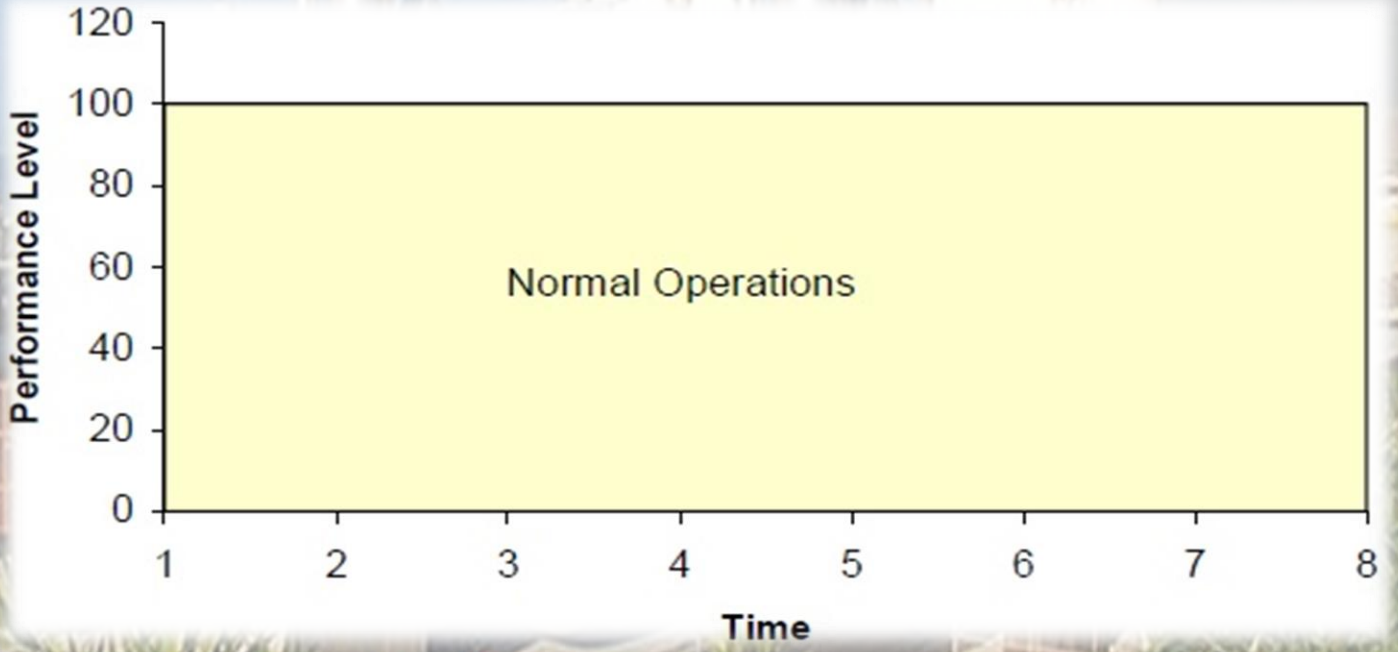
PPD-21 تاب آوری را به عنوان مقاومت در برابر تغییرات ناخواسته ، توانایی انطباق با شرایط و سرعت بخشیدن به بازیابی پس از اختلال تعریف می کند.

تاب آوری ، توانایی مقاومت و بازیابی از حملات عمدی، حوادث، تهدیدات یا حوادث طبیعی تعریف می شود.

resilience is brought about through a combination of

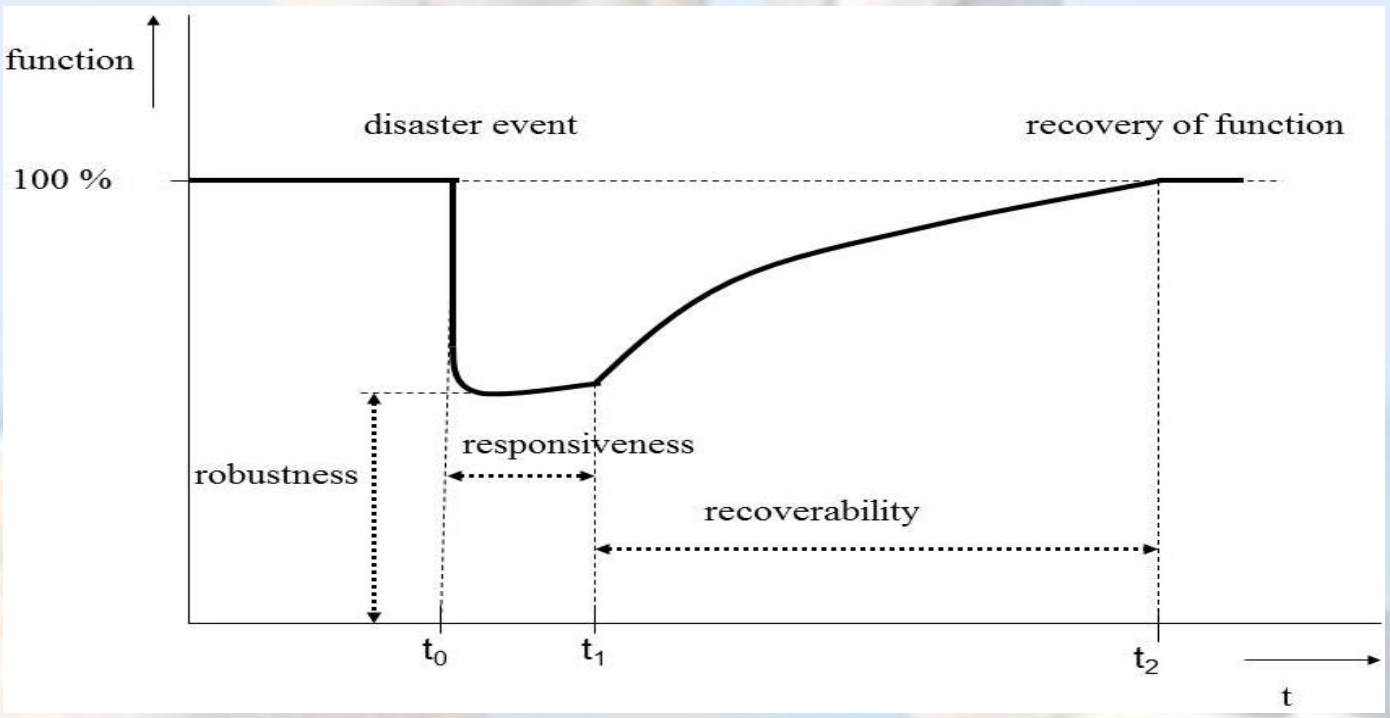
- مقاومت Resistance
- افزونگی Redundancy
- قابلیت اطمینان Reliability
- پاسخ Response
- بازیابی Recovery

عملکرد مطلوب سیستم



Resiliency

- حفظ سطح قابل قبول عملکرد در حین و بعد از وقایع مخرب و ناگوار
- بازیابی قابلیت های کامل سیستم در یک دوره زمانی مشخص



تاب آوری سایبری (Cyber Resilience)

- تاب‌آوري، توانایی تداوم یا بازگشت به عملیات عادی در صورت وقوع برخی از اختلال‌ها، اعم از طبیعی یا انساني، و عمدي یا غیرعمدی است.
- برای تاب‌آوري سامانه‌هاي سایبری، باید برنامه‌های سامانه جایگزین، فرآیندهاي اضطراری پشتیبان‌گیری و گزینه‌های پیکربندی جایگزین/راه‌اندازی مجدد وجود داشته باشد.

بازدارندگی سایبری (Cyber Deterrence)

- بازدارندگی، پیش‌گیری از اقدام غیرقابل پذیرش توسط یک تهدید موثّق و/یا باور به این نکته است که هزینه‌ی اقدام، بیش از مزایای قابل‌دریافت است.

- گزینه‌های بازدارنده، یک دوره اقدام است که براساس بهترین قضاوت‌های اقتصادی، دیپلماتیک و نظامی، به‌منظور دلسردکردن (منصرف‌کردن) یک دشمن از یک دوره اقدام جاری یا عملیات موردنظر (فکرشده)، طراحی‌شده است.

تست نفوذ (Penetration Test)

- تست نفوذ فرآیندی است که آسیب پذیری ها و حفره های امنیتی سرور، شبکه و منابع و برنامه های متصل به آن را از طریق شبیه سازی یک حمله واقعی هکری، بررسی می کند **(هدف : ارزیابی سطح امنیتی سیستم)** .

- ✓ تست شفاف یا جعبه سفید (transparent box testing)
- ✓ تست جعبه سیاه (black box testing)
- ✓ تست جعبه خاکستری (gray box testing)

رزمایش سایبری

- روش ها و فرآیندهای بکار گرفته شده برای حمله به زیر ساخت های اطلاعاتی و ارتباطاتی و دفاع از این زیر ساخت ها در یک تمرین تیمی مشترک.
- بکار گیری مجموعه ای از برنامه ها برای تصرف، حذف، جلوگیری از ارایه سرویس و دفاع توسط گروه های حاضر در رزمایش.

انواع رزمایش سایبری(۱)

الف- رزمایش سایبری هجومی

۱. **رزمایش های نفوذی:** جمع آوری اطلاعات حیاتی

۲. **رزمایش های موضعی:** تصرف نقاط کلیدی فیزیکی / منطقی

۳. **رزمایش های تاثیرگذار :** نفوذ و تاثیر گذاری بر تصمیمات

انواع رزمایش سایبری(۲)

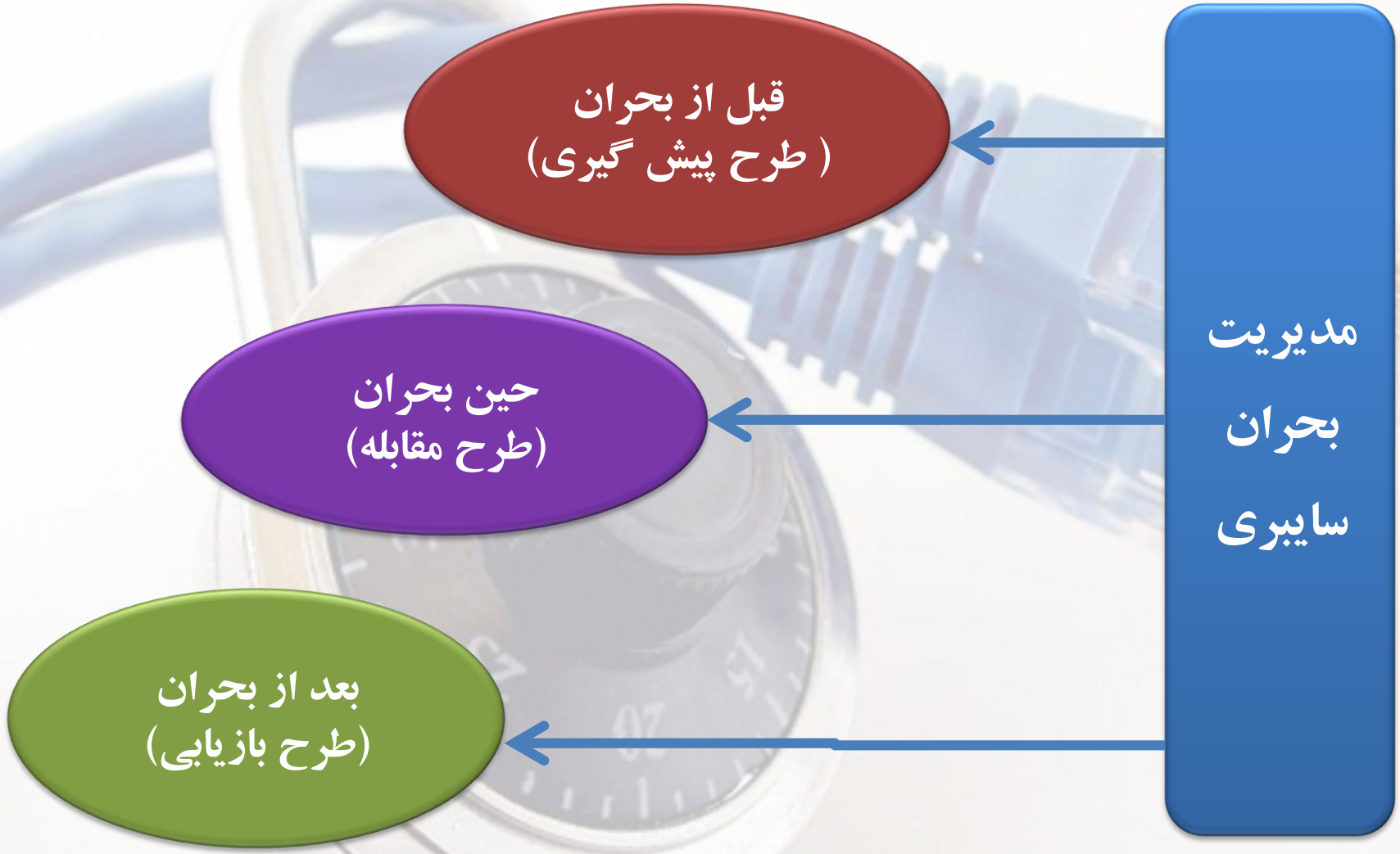
ب- رزمایش سایبری دفاعی

۱. **دفاع در عمق:** محافظت از سیستم ها و اطلاعات

۲. **دفاع هدف متحرک:** دفاع با تغییر مکان فیزیکی و غیر فیزیکی

۳. **دفاع فریبنده:**دور کردن مهاجم و ضبط فعالیت های او

۴. **ضد حمله:** کسب اطلاعات از دشمن و انجام حمله متقابل


مدیریت
بحران
سایبری
قبل از بحران
(طرح پیش گیری)
حین بحران
(طرح مقابله)
بعد از بحران
(طرح بازیابی)


پیش بینی
پیش گیری
آمادگی
قبل از بحران


هشدار ومصونیت
ارزیابی مقدماتی
حین بحران
پاسخگویی سریع
امداد ونجات
عملیات ویژه
مهار وکنترل


بازسازی
بازیابی
بعد از بحران
ساماندهی
ویادگیری

پدافند سایبری چگونه باشد ؟

- رعایت اصول فنی و استانداردهای موجود در حوزه فعالیت مربوطه(تکنیک)
- رعایت خلاقیت و ابتکار(تاکتیک)

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

جمع‌بندی مأموریت‌های پدافند سایبری

زمان	قبل از جنگ سایبري			آستانه جنگ سایبري	حین جنگ سایبري	پس از جنگ سایبري	
موضوع	سرمایه سایبري	تهدید سایبري	آسیب‌پذیري سایبري	مخاطره سایبري	جنگ سایبري قریب‌الوقوع	جنگ سایبري	پیامد جنگ سایبري	امنیت و آمادگي سایبري	قدرت و بازدارندگي سایبري
رویکرد دفاع	پیش‌گیرانه	پیش‌گیرانه	پیش‌گیرانه	پیش‌گیرانه	پیش‌دستانه و قانوني	واکنش‌گرایانه و بازدارنده و قانوني	منفعلانه و واکنش گرایانه و بازدارنده	پیش‌گیرانه	بازدارنده
	پیش‌بینانه	پیش‌بینانه			پیش‌بینانه	پیش‌بینانه		پیش‌بینانه	
مأموریت		رصد و پایش تهدید سایبري	استخراج آسیب‌پذیري سایبري	تجزیه و تحلیل تهدید و آسیب‌پذیري و پیش‌بیني مخاطرات سایبري	رصد و پایش تهدید سایبري استخراج آسیب‌پذیري سایبري تجزیه و تحلیل شواهد و قرائن و پیش‌بیني جنگ سایبري ثبت ادلّه دفاع قانوني	مدیریت صحنه جنگ سایبري تجزیه و تحلیل جنگ سایبري و پیش‌بیني پیامدهاي احتمالي آن ثبت ادلّه دفاع قانوني	بازیابي و ریشه‌کني پیامدهاي جنگ سایبري	امن‌سازي و ارتقاء آمادگي پدافند سایبري تولید قدرت پاسخ به تهدید سایبري احقاق حقوق کشور (دفاع قانوني) تجربه‌اندوزي و بهره‌گیري از تجارب ارزشمند دفاع سایبري

گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری(۱)

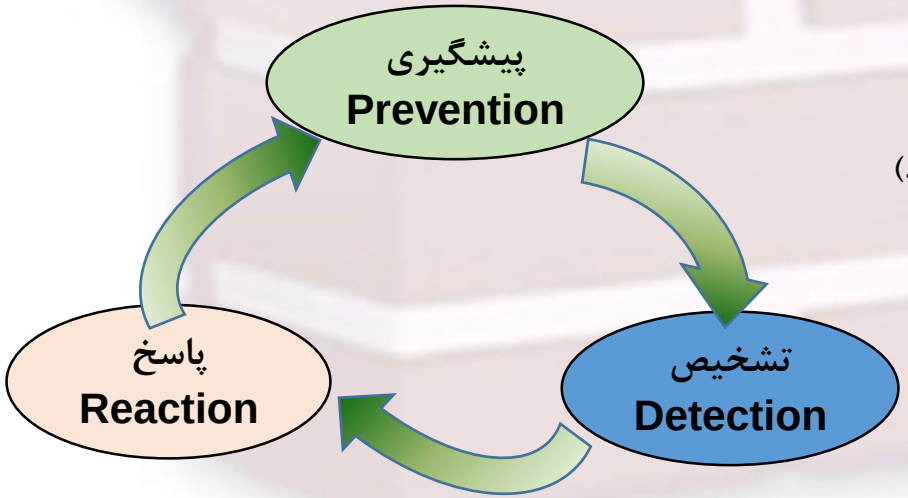
۱. **شناسایی دارایی ها، مراکز و شبکه ها و زیرساخت‌های سایبری و متکی به سایبر**

- تکمیل پرسشنامه درخصوص دارایی های سایبری و وابسته به سایبر
- تعیین سطح اهمیت دارایی‌ها، مراکز، شبکه‌ها و زیرساخت‌های سایبری و وابسته به سایبر به سطوح ویژه حیاتی، حساس و مهم، فاقد طبقه بندی
- اجرای اقدامات پیش بینی شده در اسناد امن سازی اضطراری پدافند سایبری به منظور کاهش و رفع آسیب پذیری‌های عمومی و نسبتا ساده

گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری(۱)

۲. رصد و پایش، پیشگیری و ارتقاء توان بازدارندگی در مقابل تهدیدات سایبری شامل:

- پیشگیری (Prevention)
  - جلوگیری از خسارت
- تشخیص و ردیابی (Detection & Tracing)
  - تشخیص (Detection)
    - میزان خسارت
    - هویت دشمن
    - کیفیت حمله (زمان، مکان، دلایل حمله، نقاط ضعف...)
- پاسخ (Reaction)
  - ترمیم، بازیابی و جبران خسارات
  - جلوگیری از حملات مجدد



گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری(۲)

۳. رصد دائمی تهدیدات سایبری سامانه ها، مراکز و شبکه های تعیین سطح شده.

- ❑ احصای تهدیدات سایبری مترتب در مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر و ترسیم بردار تهدیدات
- ❑ دسته بندی تهدیدات مترتب به مراکز، شبکه ها و زیرساخت های سایبری و وابسته به سایبر
- ❑ تدوین سناریوی تهدید پایه و سناریوهای تهدیدات محتمل

۴. رصد و شناسایی دائمی و دسته بندی آسیب پذیری های سایبری سامانه ها، مراکز و شبکه های تعیین سطح شده (کشف و رفع آسیب پذیری های سخت افزاری و نرم افزاری و سامانه ها).

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

۶. تعیین پیامدهای تهدیدات و آسیب پذیری ها

گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری(۳)

۷. محاسبه و ارزیابی ریسک و تعیین ریسک قابل قبول.

۸. ارائه راهکارهای پدافندی به منظور مقابله با حملات سایبری، کاهش آسیب پذیری ها و مقابله با تهدیدات سایبری.

۹. ارائه طرح تداوم خدمات و فعالیت های ضروری در صورت بروز بحران سایبری.

۱۰. پیاده سازی و اجرای راهکارهای ارائه شده.

۱۱. نظارت، ارزیابی، کنترل و به روز آوری اقدامات.

۲۱. برگزاری رزمایش های سایبری(طراحی و اجرای رزمایش های عملیاتی در بخش فناوری اطلاعات و ارتباطات سازمان برای مقابله با تهدیدات سایبری)

گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری(۴)

۳۱. استفاده از تجهیزات و سرویس های بومی حوزه سایبری در سطح سازمان و تاکید بر وجود قابلیت بومی سازی درخرید تجهیزات و خدمات فناوری اطلاعات خارجی.

۴۱. برگزاری آموزش های ارتقاء توانمندی های سایبری(آموزش و نهادینه سازی اصول پدافند سایبری در سطوح مدیران و کارشناسان).

۵۱. همکاری و هماهنگی با سازمان های متولی حوزه امنیت فضای سایبر کشور(قرارگاه پدافند سایبری، مرکز ماهر ، مراکز آپا).

۶۱. پشتیبان از محتوی و اطلاعات موجود در شبکه در بازه های زمانی برنامه ریزی شده.

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

گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری(۵)

۸۱. طراحی، پیاده سازی و اجرای مراکز داده مورد نیاز مطابق الزامات پدافند غیر عامل(شاخص های عمومی، شاخص های پدافندی)

- الزامات مکان یابی (Site Selection)
- الزامات سازه و معماری
- الزامات تاسیسات
- الزامات سایبری(پسیو، اکتیو، حفاظت الکترومغناطیس)

۹۱. طراحی، پیاده سازی و اجرای اصول حفاظت الکترومغناطیسی در برابر تهدیدات الکترومغناطیسی (شامل منابع طبیعی، سیستمی و سلاح‌های الکترومغناطیسی)

- ارتینگ
- فیلترینگ
- شیلدینگ

143

گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری(۶)

۲.۰ ارتقاء سطح امنیتی لایه های فناوری اطلاعات و ارتباطات (ICT)

- ایجاد سامانه های امداد و نجات رایانه ای (CERT)در سطح زیرساخت
- ایجاد سامانه های امنیتی SOC در سطح زیرساخت
- طراحی، پیاده سازی و اجرای اصول امنیت اطلاعات، امنیت ارتباطات و امنیت فیزیکی
- 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.
- استفاده از سیستم عامل های متن باز-linux base- به جای سیستم عامل ویندوزی در سطح مدیریت داده های سازمان.
- استفاده از توپولوژی مناسب ارتباطی و حتی الامکان از توپولوژی Full Mesh

گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری(۷)

۱۲.سازمان دهی ساختار و دفاع عملیات سایبری صنعتی

- ایجاد سامانه های امداد و نجات رایانه ای صنعتی (CERT)در سطح زیرساخت
- ایجاد سامانه های امنیتی صنعتی SOC در سطح زیرساخت
- تربیت نیروی انسانی متخصص سایبری و ارتقاء توانمندی آن‌ها
- فرهنگ سازی، آموزش و افزایش آگاهی و مهارت های عمومی در حوزه سایبری
- مصون سازی و بومی سازی چرخه مدیریت صنعتی زیرساخت
- بومی سازی و مصون سازی سامانه های پایه پدافند سایبری صنعتی

گام های اساسی جهت امن سازی زیرساخت های سایبری و پیاده سازی نظام پدافند سایبری(۸)

۲۲. کنترل دسترسی های فیزیکی و یا الکترونیکی به سامانه ها ، شبکه ها ، نقاط مختلف سایت ها و مراکز (حیاتی، حساس و مهم) مطابق با سطح بندی صورت پذیرفته

۳۲. اجرای پروژه های متکی به سایبر براساس اصول و ضوابط پدافند سایبری (مطالعه، امکان سنجی،مکان یابی، طراحی، تامین کالا، اجرا،نگهداری و بهره برداری).

۴۲. استقلال فیزیکی/منطقی شبکه های طبقه بندی دار و فاقد طبقه بندی (اینترانتی سازمان از بستر اینترنت).

۵۲. تدوین برنامه مدیریت بحران سایبری سازمان با تشریح وظایف بخش های مختلف سازمان.

۶۲. تدوین و انتشار نظامات(ملاحظات،مقررات،الزامات واصول) سایبری.

۷۲. اعلام هشدارهای لازم.

۸۲. دفاع حقوقی در برابر تهدیدات.

رعایت الزامات و ملاحظات (اقدامات اساسی) در امن سازی اضطراری سایبری

- الزامات و ملاحظات سازمانی و مدیریتی
- الزامات و ملاحظات حوزه معماری شبکه و معماری امنیتی
- الزامات مرکز عملیات امنیت (SOC)
- الزامات و ملاحظات حوزه نرم افزاری
- الزامات و ملاحظات مدیریت مخاطرات
- الزامات و ملاحظات در حوزه ارتباطات
- الزامات و ملاحظات حوزه سخت افزاری
- الزامات و ملاحظات حوزه پشتیبان گیری

- الزامات و ملاحظات حوزه نیروی انسانی
- الزامات و و ملاحظات حوزه برون سپاری ، تعمیرات و زنجیره تامین
- الزامات امن سازی حوزه سیستم ها و تجهیزات کنترل صنعتی
- اقدامات امنیتی در سیستم کنترل زیمنس
- الزامات امن سازی حوزه سیستم ها و تجهیزات کنترل صنعتی
- اقدامات امنیتی در سیستم کنترل یوکوگاوا امن سازی RTU سیستم‌های اسکادا
- امن سازی بستر RTUها و مرکز کنترل اسکادا
- امن سازی مرکز کنترل اسکادا
- الزامات امن سازی حوزه های عمومی سیستم ها و تجهیزات کنترل صنعتی

الزامات و ملاحظات سازمانی و مدیریتی

اهداف

- مشخص و شفاف ساختن سیاست ها، روال ها و خط مشی های عملیاتی
- اطمینان از آمادگی لازم برای مواجهه با تهدیدات و حملات محتمل
- تشکیل، آموزش و ارتقای تخصصی کمی و کیفی تیم عملیات سایبری
- اطمینان از توجیه مدیران ارشد زیرساخت
- اطمینان از حمایت ها و پشتیبانی های مالی و قانونی از اجرای اقدامات امن سازی اضطراری

الزامات و ملاحظات سازمانی و مدیریتی

چالش‌های عمده

- ساختار امنیت و پدافند سایبری زیرساخت
- بودجه و تخصیص منابع مالی
- توجیه مستمر مدیران ارشد زیرساخت

الزامات و ملاحظات حوزه معماری شبکه و معماری امنیتی

اهداف

- تنظیم روابط، ارتباطات، پروتکل ها و شیوه چینش و هم بندی تجهیزات شبکه و امنیت و پدافند سایبری با رویکرد ارتقای سطح امنیت و حفاظت از کل و تک تک اجزای شبکه

الزامات و ملاحظات حوزه معماری شبکه و معماری امنیتی

چالش‌های عمده

- ساختار امنیت و پدافند سایبری زیرساخت
- معماری امنیتی شبکه مبتنی بر معماری دفاع در عمق، دفاع لایه به لایه
- معماری شبکه
- مقابله و کاهش نشت اطلاعات (Data Leakage)
- توجه جدی به اصل Multi-Branding
- استفاده حداکثری از تجهیزات، محصولات و خدمات بومی و امن مورد تایید
- مدیریت دسترسی (افراد کلیدی، کاربران عادی و پیمانکاران)
- جلوگیری و کاهش حملات DDoS

الزامات مرکز عملیات امنیت

چالش‌های عمده

- ایجاد سازوکار رصد، پایش، تشخیص و هشدار سایبری (مرکز عملیات امنیت – SOC)
- ایجاد ساختار و سازوکار تشکیل تیم های واکنش به رخدادهای سایبری (CSIRT)
- سازوکار شناسایی و کاهش مخاطرات بدافزارهای پیچیده (APT، AET، Zero Day، Botnet و ...)
- استفاده حداکثری از تجهیزات، محصولات و خدمات بومی و امن مورد تایید

الزامات و ملاحظات حوزه نرم افزاری

چالش‌های عمده

- **به روزرسانی تجهیزات شبکه، امنیت شبکه و ارتباطات**
- **توجه جدی به اصل** Multi-Branding
- **استفاده حداکثری از تجهیزات، محصولات و خدمات بومی و امن مورد تایید**

الزامات و ملاحظات مدیریت مخاطرات

چالش‌های عمده

- **هاردنینگ تجهیزات شبکه، امنیت شبکه و ارتباطات**
- **سازوکار شناسایی و کاهش مخاطرات بدافزارهای پیچیده (**APT، AET، Zero Day، Botnet **و ...)**
- **اسناد مرتبط با تداوم کارکرد زیرساخت (**BCP، DRP، CERP**)**

الزامات و ملاحظات در حوزه ارتباطات

چالش‌های عمده

- ارتباط با شبکه های بیرونی سازمان
- بسترهای ارتباطی (فیبر نوری، MPLS، APN، NIX و ...)
- توجه جدی به اصل Multi-Branding
- استفاده حداکثری از تجهیزات، محصولات و خدمات بومی و امن مورد تایید
- بهره گیری حداکثری از شبکه ملی اطلاعات
- استقرار بر روی DNS داخلی (Iran Access)

الزامات و ملاحظات حوزه سخت افزاری

چالش‌های عمده

- **به روزرسانی تجهیزات شبکه، امنیت شبکه و ارتباطات**
- **توجه جدی به اصل** Multi-Branding
- **استفاده حداکثری از تجهیزات، محصولات و خدمات بومی و امن مورد تایید**

الزامات و ملاحظات حوزه پشتیبان‌گیری

چالش‌های عمده

- سازوکار پشتیبان گیری تمیز و ارتقای درجه اطمینان آن
- استفاده حداکثری از تجهیزات، محصولات و خدمات بومی و امن مورد تایید

الزامات و ملاحظات حوزه نیروی انسانی

چالش‌های عمده

- **تهدیدات درونی** (Insider Threat)
- **دسترسی پیمانکاران**

الزامات و و ملاحظات حوزه برون سپاری ، تعمیرات و زنجیره تامین

چالش‌های عمده

- **اسناد مرتبط با تداوم کارکرد زیرساخت (**BCP، DRP، CERP**)**
- **استفاده حداکثری از تجهیزات، محصولات و خدمات بومی و امن مورد تایید**
- **بودجه و تخصیص منابع مالی**

مصون سازی سایبری در سطح مفاهیم عملیاتی (در پدافند غیر عامل)

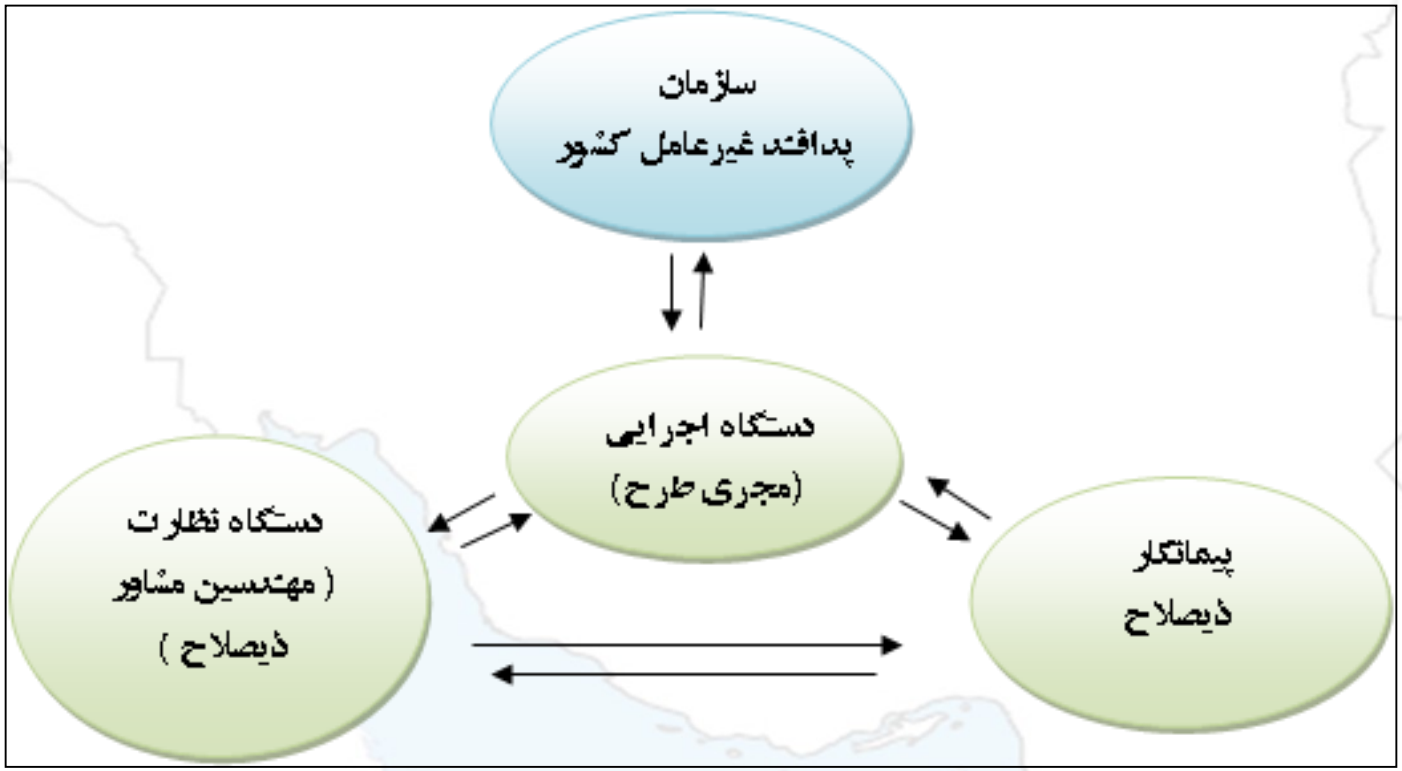
- احصا ، بررسی و ارزیابی(کمی،کیفی) دارایی های سایبری
- احصا ، بررسی و ارزیابی(کمی،کیفی) تهدیدات سایبری
- احصاء ، بررسی و ارزیابی(کمی،کیفی) آسیب پذیری های سایبری
- احصاء ، بررسی و ارزیابی(کمی،کیفی) وابستگی های بین زیر ساختی
- محاسبه،ارزیابی و مدیریت ریسک
- بررسی سناریو های تهدید و سناریوی پایه

- بررسی انواع رویکردهای پدافند سایبری
- بررسی انواع راهکارهای پدافند سایبری
- مهندسی ارزش و انتخاب راه کار بهینه
- تهیه طرح مفهومی پدافند سایبری زیر ساخت
- تهیه طرح جامع پدافند سایبری زیر ساخت
- تهیه طرح های تفصیلی

ارکان و ارتباط عوامل ذیربط در اجرای طرح‌های پدافند غیرعامل

الف ـ سازمان پدافند ب- دستگاه اجرایی

ج ـ دستگاه نظارت (مهندسین مشاور) د – پیمانکار ذیصلاح پدافند



اپراتورهای امنیت فضای سایبری کشور

ردیف	متولی		حوزه عملکردی	
۱	سازمان پدافند غیر عامل کشور	قرارگاه پدافند سایبری (با همکاری افتا)	زیرساخت های حیاتی و حساس	انرژی حمل و نقل
۲	وزارت اطلاعات	مرکز افتا (با همکاری سازمان پدافند)	زیرساخت های حیاتی و حساس	پولی،مالی،بانکی ارتباطات
۳	وزارت ارتباطات و فناوری اطلاعات	مرکز ماهر	خدمات عمومی	سازمان ها و نهادهای غیرزیرساختی
۴	نیروی انتظامی	پلیس فتا	خدمات عمومی	امنیت سایبری فردی، اسنپ،تپسی،...

اگر امنیت نباشد..... !!!!!

اقتصاد هم نیست.

عدالت اجتماعی هم نیست .

دانش و پیشرفت علمی هم نخواهد بود .

تلاش برای سازندگی و افتخارآفرینی هم نیست.

ناامنی، بزرگترین خطری است که یک ملت را تهدید می‌کند.


محمد صلی اللہ علیہ وسلم