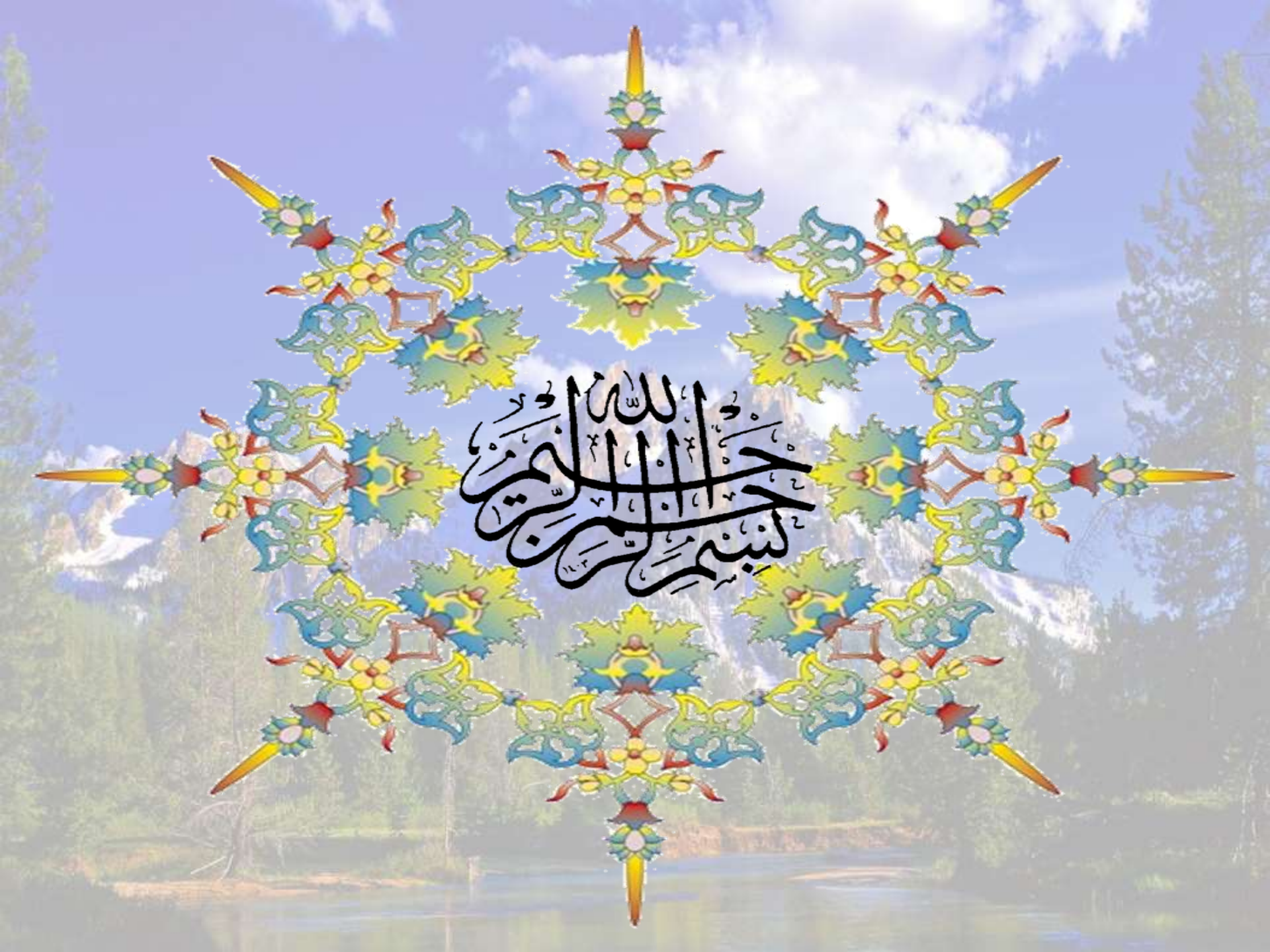

بسم الله الرحمن الرحيم

تدوین و ارائه :

حمیدرضا کاووسی

کارشناس ارشد مهندسی فناوری اطلاعات – شبکه های کامپیوتری و ارتباطی

Email: hr_kavoosi78@yahoo.com

تابستان– ۱۳۹۹

انجمن علمی
پدافند غیرعامل ایران

سازمان پدافند غیرعامل کشور

ادبیات و کارکردهای فضای سایبری

شناسایی تهدیدات سایبری

(مقدمه ای بر پدافند سایبری)

هدف ارائه

راهکارهای مصون سازی زیرساخت های حیاتی (سایبری، وابسته به سایبر)

در برابر تهدیدات سایبری

Cyber **C**ritical **I**nfrastructure **P**rotection

(**CCIP**)

روش رسیدن به هدف

تحلیل محیط

تدوین اهداف

تدوین راهبرد(ها)

تدوین اقدامات اساسی

پیاده سازی و اجرای اقدامات

چارچوب (گام‌های) ارائه

پدافند

غیر عامل

(مبانی، اصول و الزامات)

زیرساخت

(مبانی،مفاهیم)

فضای سایبری

(تعاریف،ساختار)

دفاع(پدافند) سایبری

(راهبردها، راهکارها، اقدامات اساسی)

فضای سایبری

۱. تعاریف و اصطلاحات

۲. ویژگی ها و ساختار

۳. آسیب پذیری ها و تهدیدات

تعریف فضای سایبری (Cyber Space)

شبکه های وابسته به یکدیگر ، از زیرساخت های فناوری اطلاعات ، شبکه های ارتباطی ، سامانه های رایانه ای، پردازنده های تعبیه شده(جاگذاری شده)، کنترل گرهای صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط وانسان به منظورتولید، پردازش، ذخیره سازی ، مبادله ، بازیابی و بهره برداری از اطلاعات می باشد.

پنج مولفه(لایه)فضای سایبری

۱. **ارتباطات** (شبکه های ارتباطی)

۲. **اطلاعات** (سرویس ها و خدمات. محتوا)

۳. **کاربر**(بهره برداران)

۴. **امنیت**

۵. **حاکمیت** (قانونگذار. 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)

سرمایه های ملی سایبری

- زیرساخت های کشور(حیاتی،حساس،مهم)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.

لایه های پدافند سایبری

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

سایبری شدن زیر ساخت ها
(زیر ساخت های هوشمند)

-تهدیدات سایبری شدن زیر ساخت ها:

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

داده ها درفضای سایبری

۳۰ – ۲۵ درصد(اطلاعات سازمانی):

داده هایی که سازمان ها بارگذاری می کنند

۷۵– ۷۰ درصد(اطلاعات شخصی):

داده هایی که اشخاص (فردی) بارگذاری می کنند

سطوح اهمیت (ارزش) داده ها

۱. داده های اخباری : داده های خبری

۲. داده های اطلاعاتی : داده هایی با بار اطلاعاتی

حفاظت از داده ها

هر جا داده ای وجود دارد :

۱- شخصی(اشخاصی) علاقمند به این داده ها وجود دارد .

۲- احتمال سرقت، تغییر و اختلال در آنها نیز وجود دارد.

۳-خطر(تهدید) وجود دارد.

دو سطح حفاظتی (سایبری)

- **حریم خصوصی** (Privacy Security)

عکس، فیلم ، سند ، ایمیل ، امور بانکی شخصی ،مکان یابی،سایر مشخصات فردی.

- **امنیت سازمانی/ملی** (National/ Enterprise Security)

اطلاعات / دیتای سازمانی ، اتوماسیون اداری ، وب سایت ها،IDC،Scada

جنگ(محیط ، ابزار، انگیزه)

(جنگ سایبری می تواند مقدمه جنگ نظامی باشد)

محیط نبرد

فضا

هوا

زمین

دریا

فضای سایبر

The Internet of Everything:
Networked Connections of People, Process, Data, Things

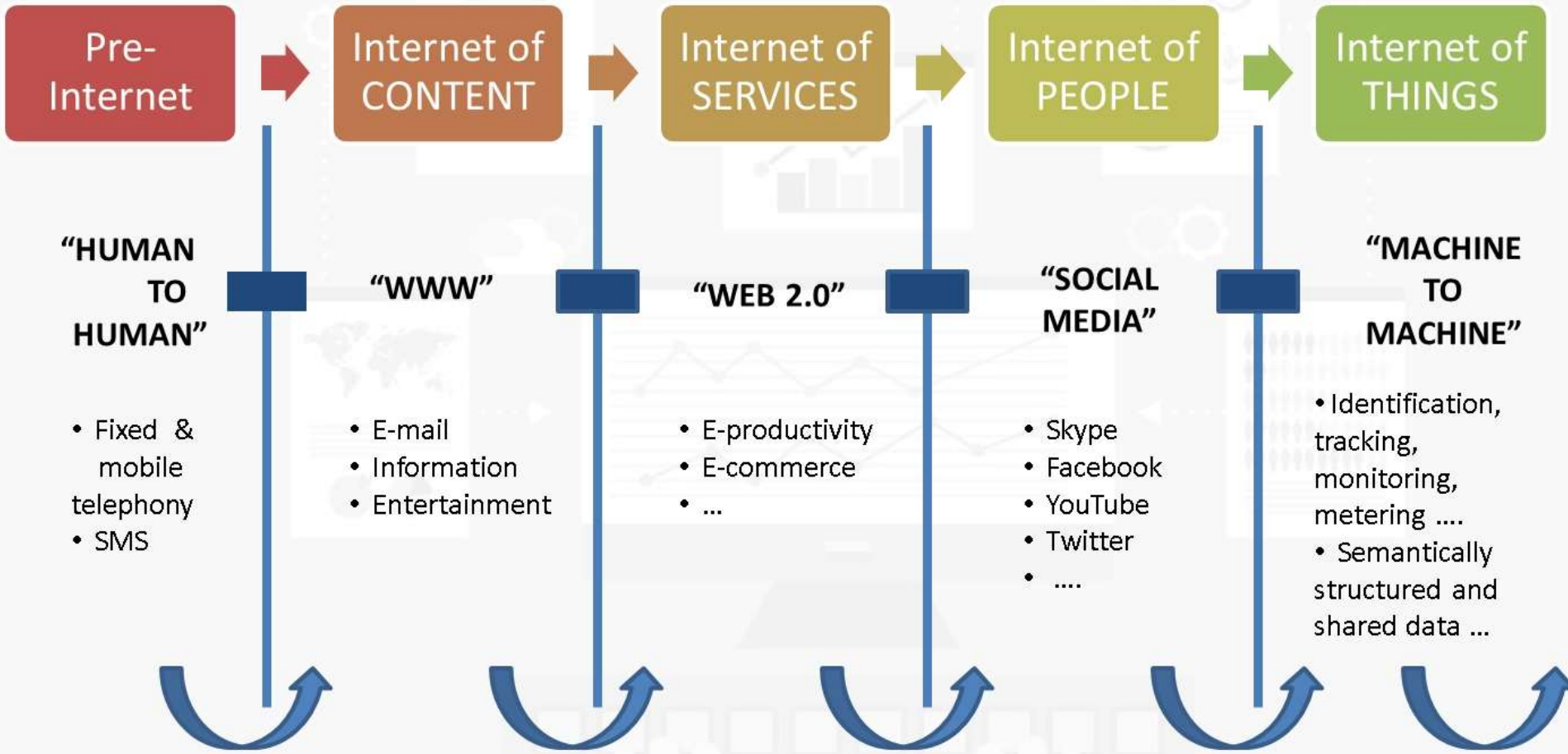
People
Connecting people in more relevant, valuable ways

Process
Delivering the right information to the right person (or machine) at the right time

Data
Turning data into more useful information for decision making

Things
Physical devices and objects connected to the Internet and each other for intelligent decision making

Evolution of Internet of Things



انواع سواد از نظر یونسکو

۱ سواد عاطفی
توانایی برقراری روابط عاطفی با خانواده، همسر و دوستان به نحو شایسته

۲ سواد ارتباطی
توانایی برقراری ارتباط و تعامل با تمامی اعضای جامعه (آداب معاشرت – روابط اجتماعی مناسب)

۳ سواد مالی
توانایی مدیریت اقتصادی درآمد (چگونگی پس‌انداز، سرمایه‌گذاری و مدیریت هزینه‌ها)

۴ سواد رسانه ای
این‌که بدانیم کدام رسانه‌ها معتبر و کدام نامعتبر است؛ توانایی تشخیص وثوق اخبار و دیگر پیام‌های رسانه‌ای

۵ سواد تربیتی
توانایی تربیت فرزندان به نحو شایسته

۶ سواد رایانه ای
توانایی استفاده از مهارت‌های هفت‌گانه رایانه (ICDL مفاهیم پایه فناوری اطلاعات و ارتباطات، استفاده از رایانه و مدیریت فایل‌ها و واژه‌پردازی)

انواع سواد در قرن ۲۱

اگرچه تعریف قدیمی سواد، توانایی نوشتن و خواندن است، ولی امروزه در قرن بیست‌ویکم توانایی خواندن و نوشتن، تنها بخش کوچکی از تعریف سواد است و حتی داشتن مدارک و مدارج عالیه دانشگاهی نیز دلیل باسوادی افراد نیست. در این گرافیک اطلاع رسان به برخی از انواع سواد در قرن ۲۱ اشاره می شود. نظام آموزش و پرورش ایران، با انتشار کتاب درسی «تفکر و سواد رسانه ای » در پایه دهم در سال تحصیلی ۱۳۹۶ – ۱۳۹۵، گام نخست برای آموزش یکی دیگر از سوادها با عنوان سواد رسانه ای برداشته است . (هرچند برخی از اجزای بسته آموزشی این کتاب، پیوندهایی با سواد بصری دارد) با همه این احوال، هنوز راه طولانی برای با سواد شدن در عصر حاضر باقی مانده است

استفاده بهینه و مناسب از فضای سایبری

سواد رسانه ای

(توانمندی و قابلیت درک، شناخت، تشخیص و تفکیک)

+

سواد سایبری

(توانمندی و قابلیت دانشی و مهارتی)

- ✓ آسیب پذیری سایبری
- ✓ تهدیدات سایبری
- ✓ مخاطرات سایبری
- ✓ هشدار(اعلام وضعیت)سایبری

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.

پنج عرصه دسته بندی تهدیدات حوزه سایبری

۱. حملات سایبری زیر ساختی
۲. حملات سایبری در حوزه نظامی
۳. حملات سایبری الکترومغناطیسی
۴. حملات سایبری ادراکی – شناختی
۵. حملات سایبری در حوزه شبکه های اجتماعی

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	Network exploits Wi-Fi sniffing
Physical	Lost or stolen devices

https://www.lookout.com/resources/know-your-mobile/what-is-a-mobile-threat

تهدیدات سایبری(تهدیدات در فضای مجازی)

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 ...)

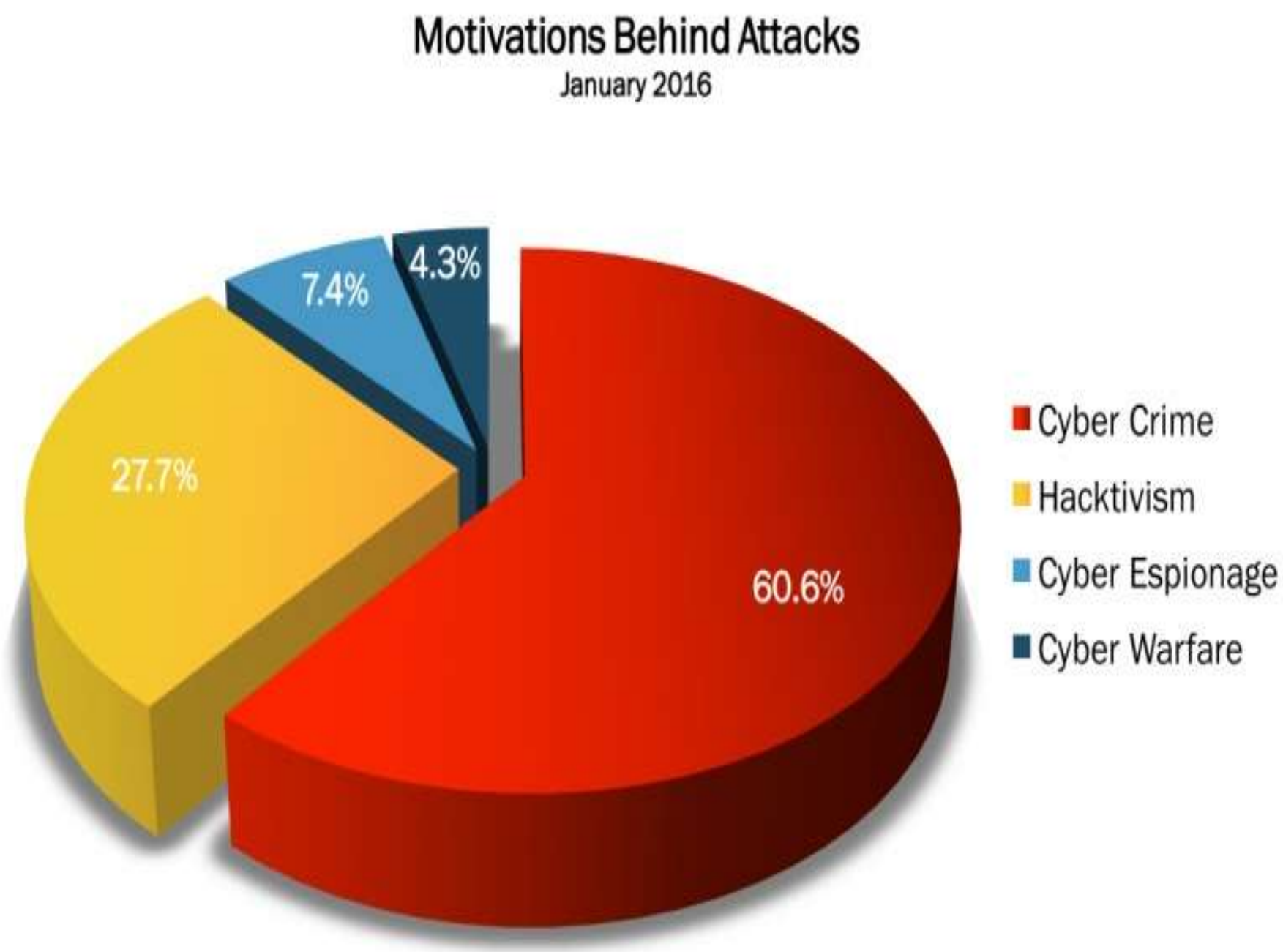
۲-۲- دزدی سایبری(جاسوسی ، سرقت و کلاهبرداری سایبری)

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

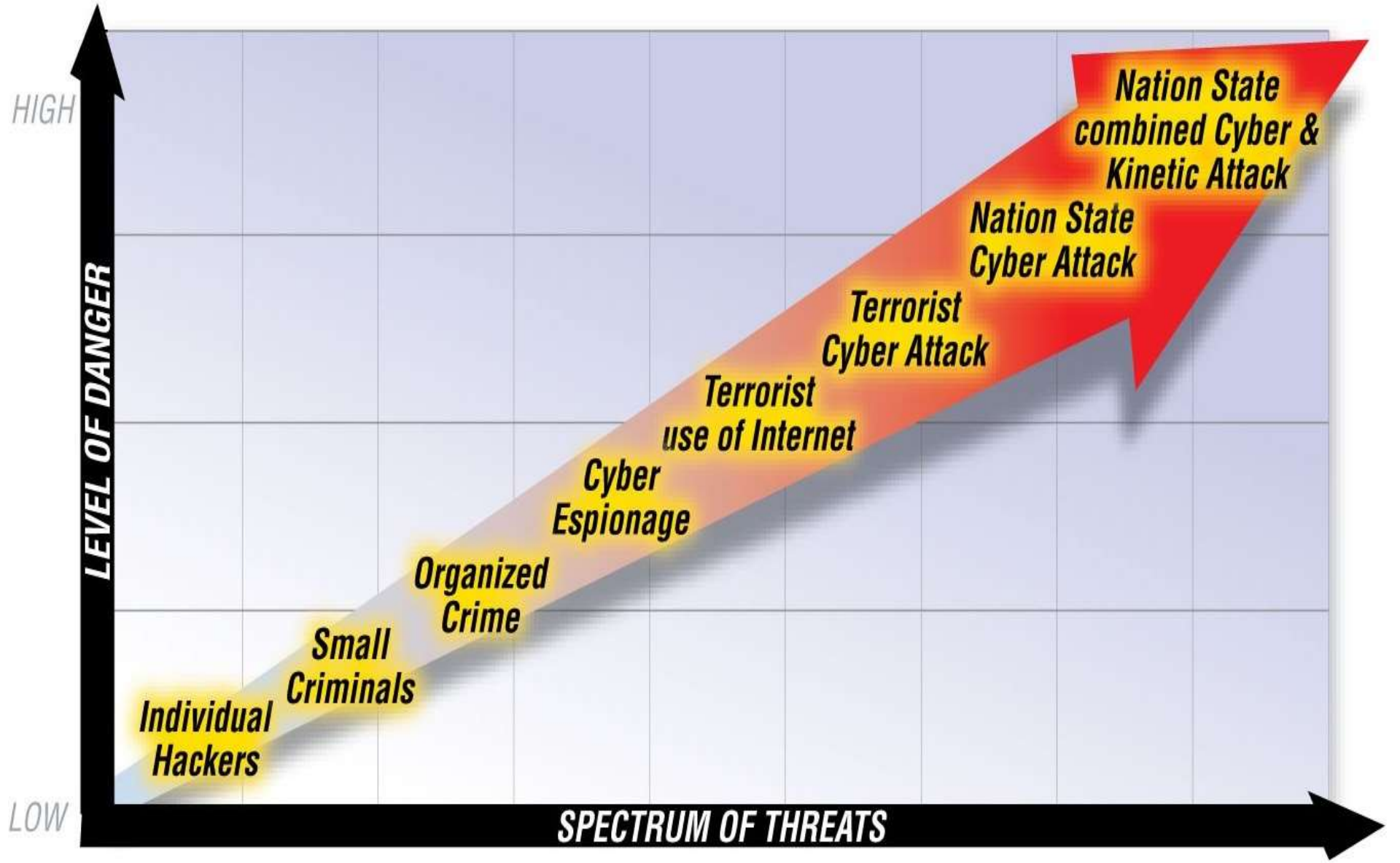
۲-۴- خشونت سایبری

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



سه مشخصه تهدیدات سایبری

۱. گستردگی

۲. نهفتگی

۳. تنوع

مبنای تهدیدات در فضای سایبری

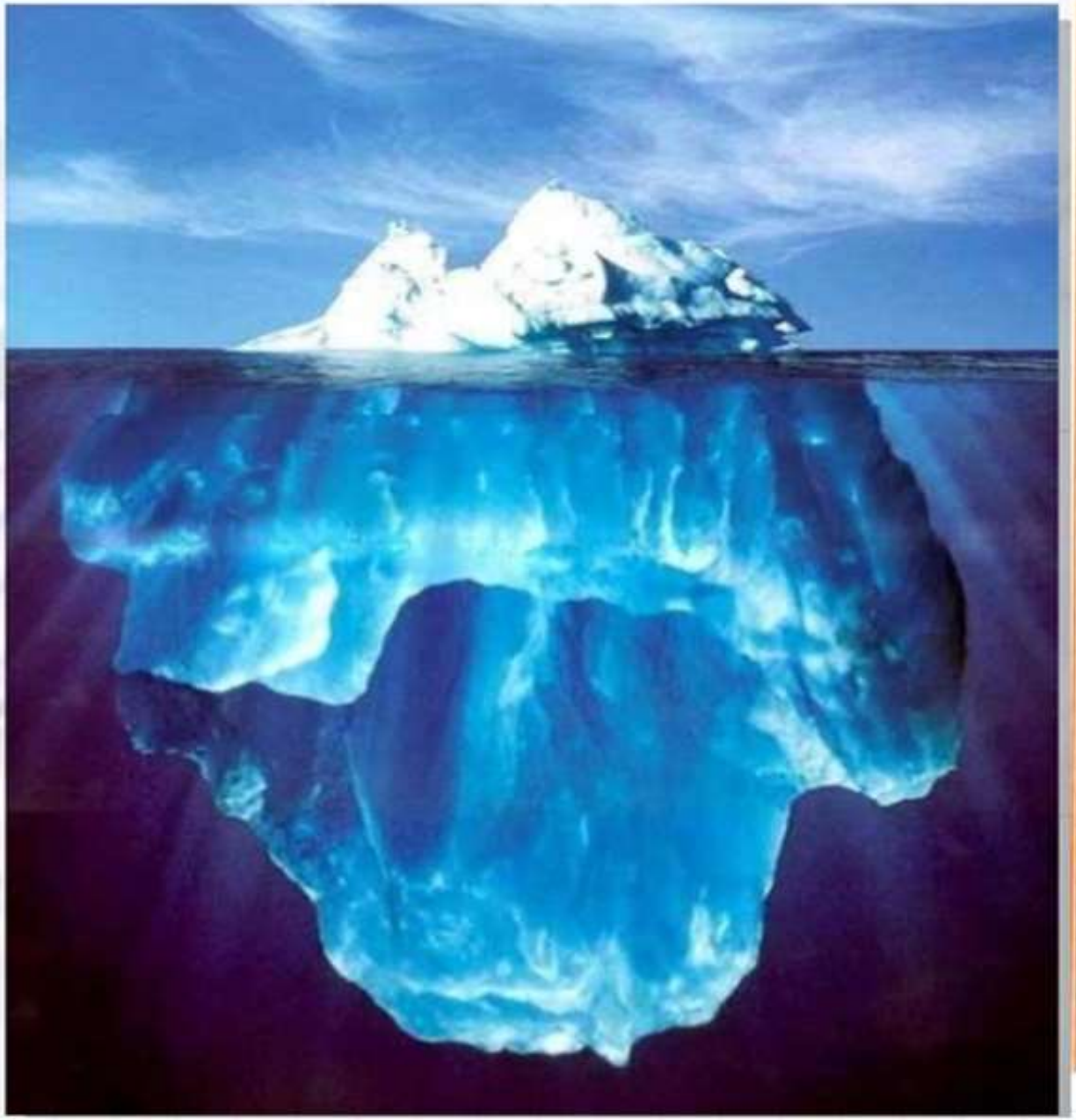
- تهدیدگران خارجی
- تهدیدگران داخلی
- تهدیدات موجود در زنجیره تأمین کالا
- تهدیدات ناشی از عدم کفایت توانمندی عملیاتی نیروهای خودی

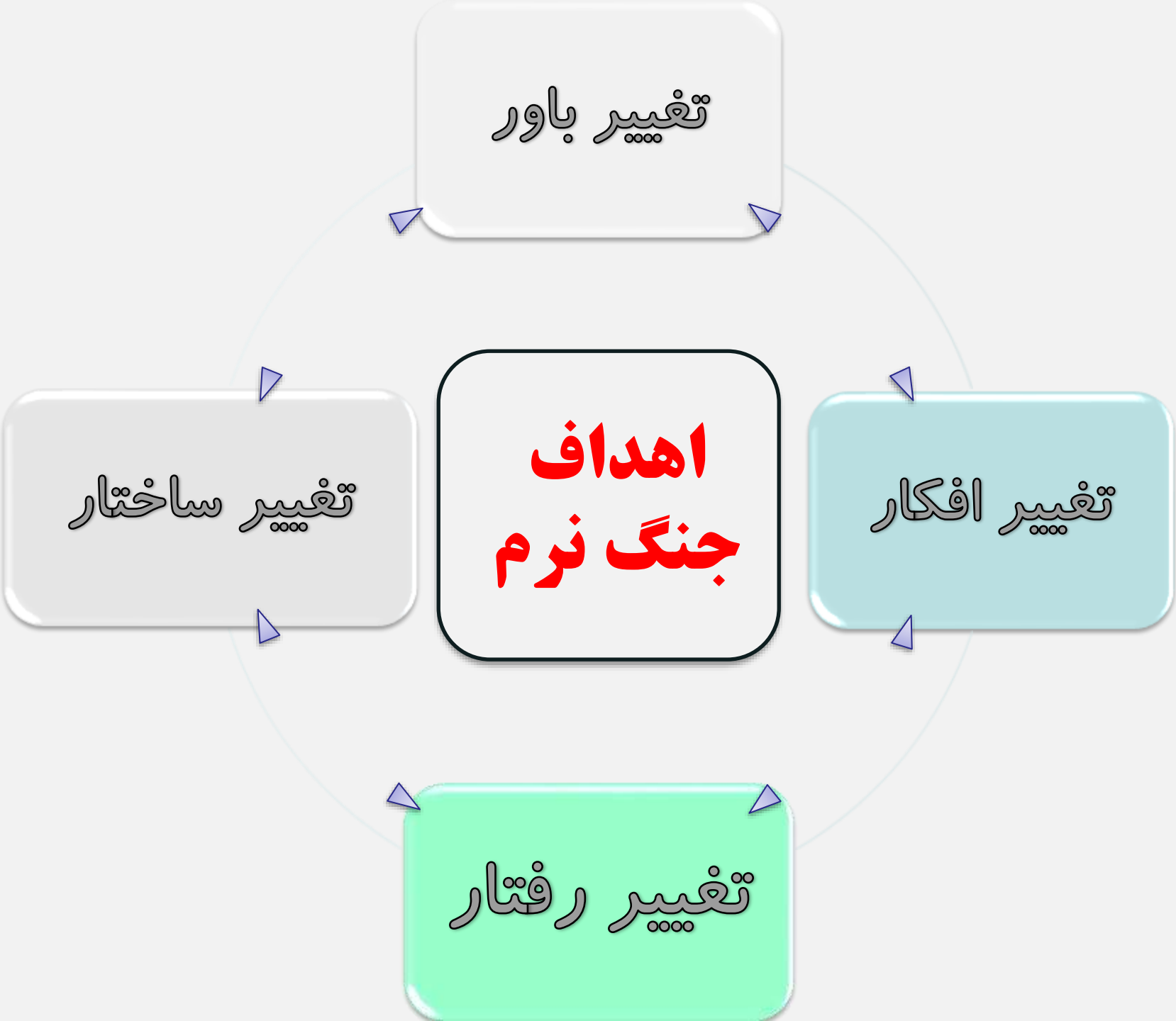
اثرگذاری تهدیدات سایبری بر تمام سرمایه ها!!!

- تهدیدات سایبری، قادر به تاثیرگذاری بر سرمایه های فیزیکی ، سایبری،انسانی،معنوی در تمام سطوح می‌باشند.

روند توسعه تهدیدات حوزه سایبری

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




تغییر باور
تغییر افکار
تغییر رفتار
تغییر ساختار
اهداف
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.

حمله سایبری منجر به تخریب فیزیکی

- **با افزایش نفوذ اینترنت اشیا و خصوصاً ورود آن به عرصه های محتلف صنعت، در سال ۲۰۱۸، حملات تخریبی سایبری که خسارات فیزیکی به همراه دارند، گسترده خواهند شد.** (به دست گرفتن کنترل سیستم ها، گرفتن باج، شنود اطلاعات و...)
- **در سال ۲۰۱۶، یک شرکت اسراییلی به نام Nation-E مدعی شد آتش‌سوزی در پتروشیمی ایران، ناشی از حملات سایبری بود.**
- **طبق آمار موسسه های تحقیقاتی ، بیشترین تهدیدات سایبری در دنیا متوجه حوزه های اقتصادی (مالی ، بانکداری) و انرژی است.**

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 .

عملکردهای متصور یک ویروس مهاجم

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

اهداف حملات !

- کسب اطلاعات
- هویت شناسی
- دسترسی به خدمات و سرویس هایی که کاربر در اختیار دارد

جاسوسی سایبری

- هنر یا تکنیک به دست آوردن اطلاعات دارای طبقه بندی ، بدون مجوز گرفتن از نگهدارنده (صاحب) اطلاعات است .
- هدف جاسوسی سایبری **سرقت** است و نه ایجاد **خسارت** ولی نباید نادیده گرفت که چنین حملاتی می‌توانند تاثیر بسزایی در خسارت داشته باشند.(یا عامل ایجاد خسارت باشند)

انواع جاسوسی

جاسوسی نوین به صورت کلی قابل تقسیم بندی به دو دسته اصلی است:

- دسته نخست، جاسوسی هدف مند از **مراکز حساس و حیاتی** تجمیعِ داده و افراد دارای روابط و اطلاعات حساس و ارزش مند.
- دسته دوم جمع آوری داده هایی که به صورت انفرادی دارای ارزش نبوده و پس از **تجمیع، چیدمان و برقراری رابطه و به صورت داده های عظیم** دارای ارزش می شوند.(جمع‌آوری اطلاعات عمومی و کم‌ارزش در خصوص هویت‌های جمعی - کلان داده ها - داده‌های عظیم(Big Data)) .

مهندسی فردی – مهندسی اجتماعی

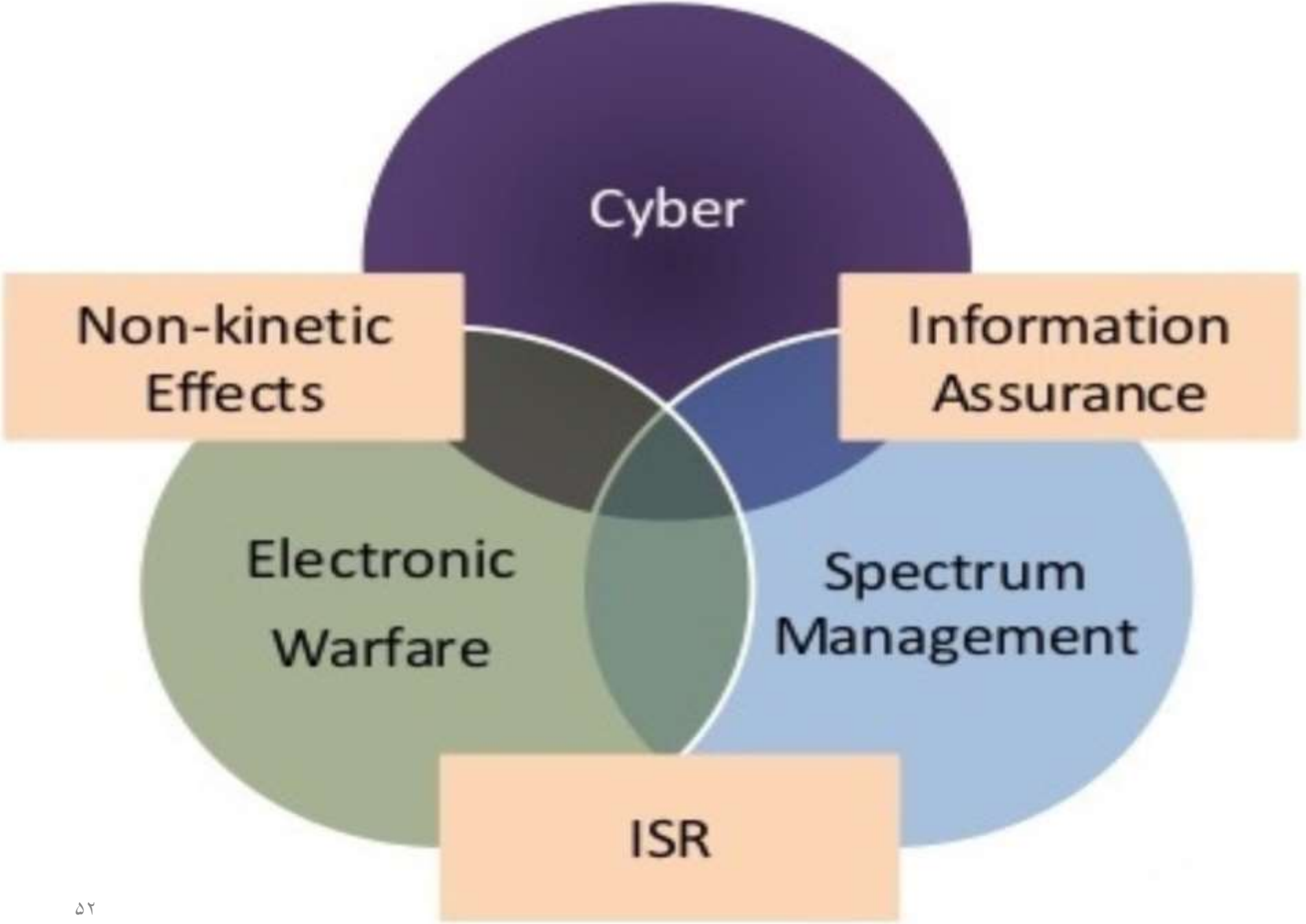
- آن چه در ذهن از لفظ جاسوسی متبادر می‌شود همراه با عملی مرموزانه، پنهانی و از روی غفلت است. ما برای جاسوسی نوین باید دو روند کلی را در نظر گرفت و از هم جدا ساخت: نخست؛ **روند تحول در ابزارها و روش‌های جاسوسی**؛ و دوم **روند تحولات ماهوی جاسوسی.**
- هدف اصلی این نوع جاسوسی به‌جای ایجاد اِشراف اطلاعاتی بر افراد و سازمان‌های دارای اهمیت، ایجاد اِشراف اطلاعاتی و چتر شناختی بر جوامع، اجتماع ها، فرهنگ‌ها و خرده‌فرهنگ‌هاست. ایجاد اِشراف شناختی با هدف دنبال کردن تغییرها، ذائقه‌ها، تفکرات و واکنش‌ها در سطح یک اجتماع به‌منظور مهندسی اجتماعی است.

حملات سایبری الکترومغناطیسی

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 ای 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

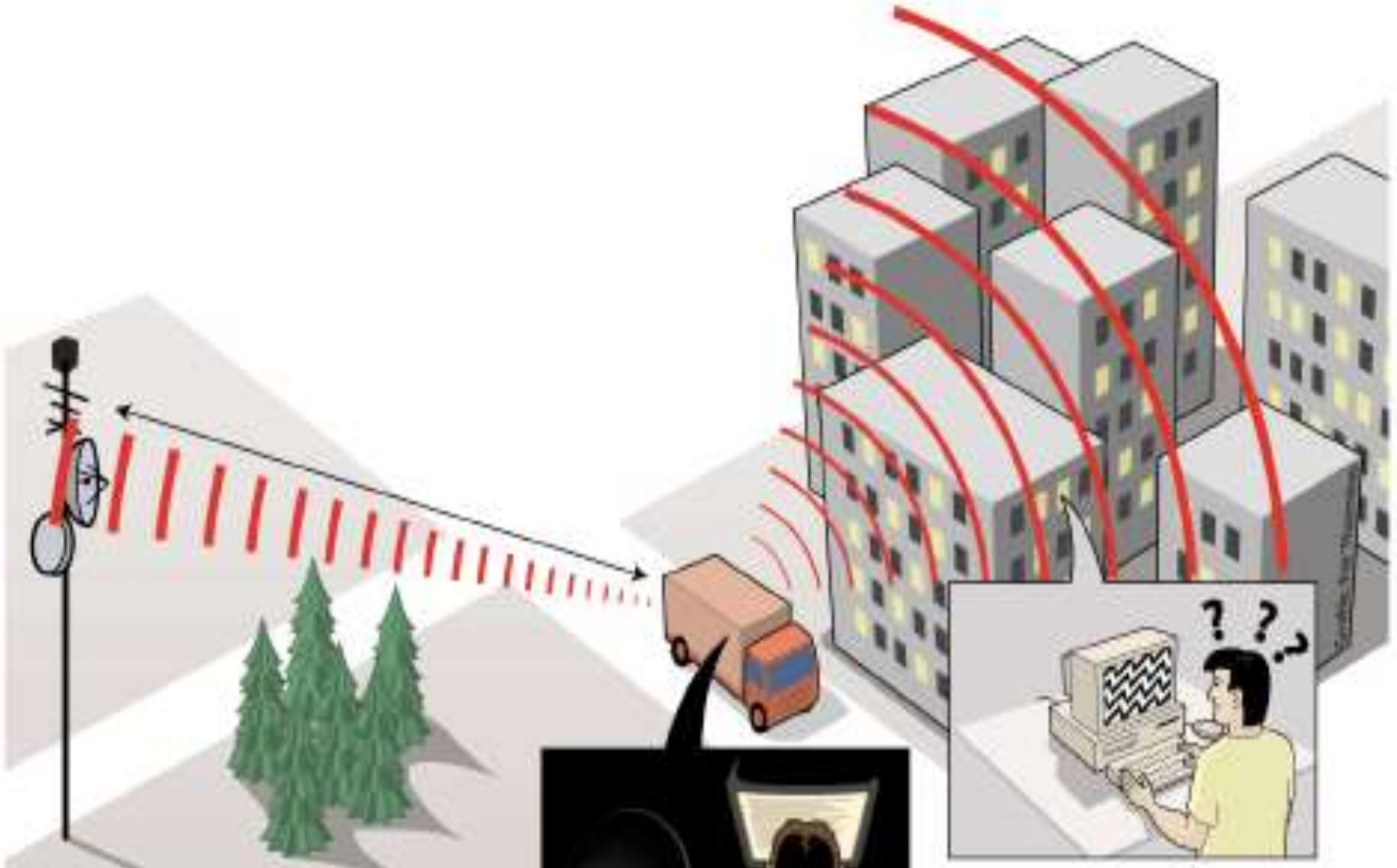
- **سلاح های الکترومغناطیسی**

- (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

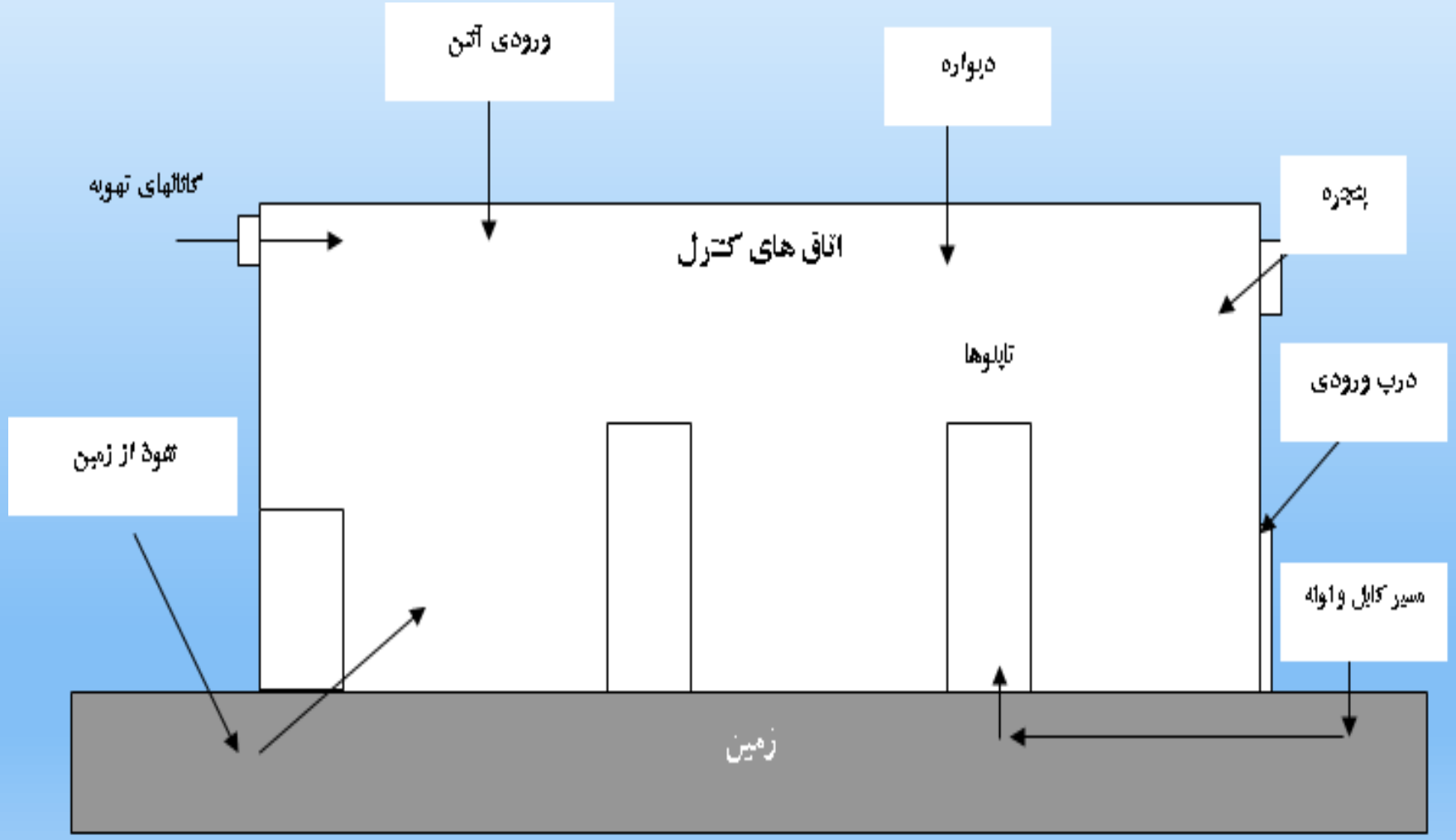
- Penetration through holes, joints etc.
- Resonance at approx. 1–3 GHz.
- Protection: shielding, filtering.

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)

جرایم سایبری(CyberCrime)

- انجام فعالیت های مجرمانه در محیط فضای سایبر و به کمک ابزار و تجهیزات رایانه ای و شبکه محور .
- ابزار انجام جرایم سایبری:ابزار و تجهیزات رایانه ای
- میدان فعالیت : فضای شبکه و اینترنت(محیط سایبر)

جرایم و مجازات ها(۱)

- جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

(دسترسی غیرمجاز- شنود غیرمجاز- جاسوسی رایانه‌ای)

- جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

(جعل رایانه‌ای - تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی)

جرایم و مجازات ها(۲)

- سرقت و کلاهبرداری مرتبط با رایانه
- جرایم علیه عفت و اخلاق عمومی
- هتک حیثیت و نشر اکاذیب
- مسؤولیت کیفری اشخاص

امنیت

ردیف	سطح	توضیحات
۱	امنیت اطلاعات	۱. امنیت، نفوذ و روش های مقابله در سطح Client & Servers ۲. امنیت، نفوذ و روش های مقابله در سطح Web
۲	امنیت ارتباطات	امنیت، نفوذ و روش های مقابله در سطح Network (Wired & Wireless)
۳	امنیت فیزیکی	کنترل دسترسی های فیزیکی
۴	مدیریت امنیت	سیاست ها، مکانیزم ها، سرویس ها

دسته بندی حملات امنیتی

- حملات فعال(active)

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

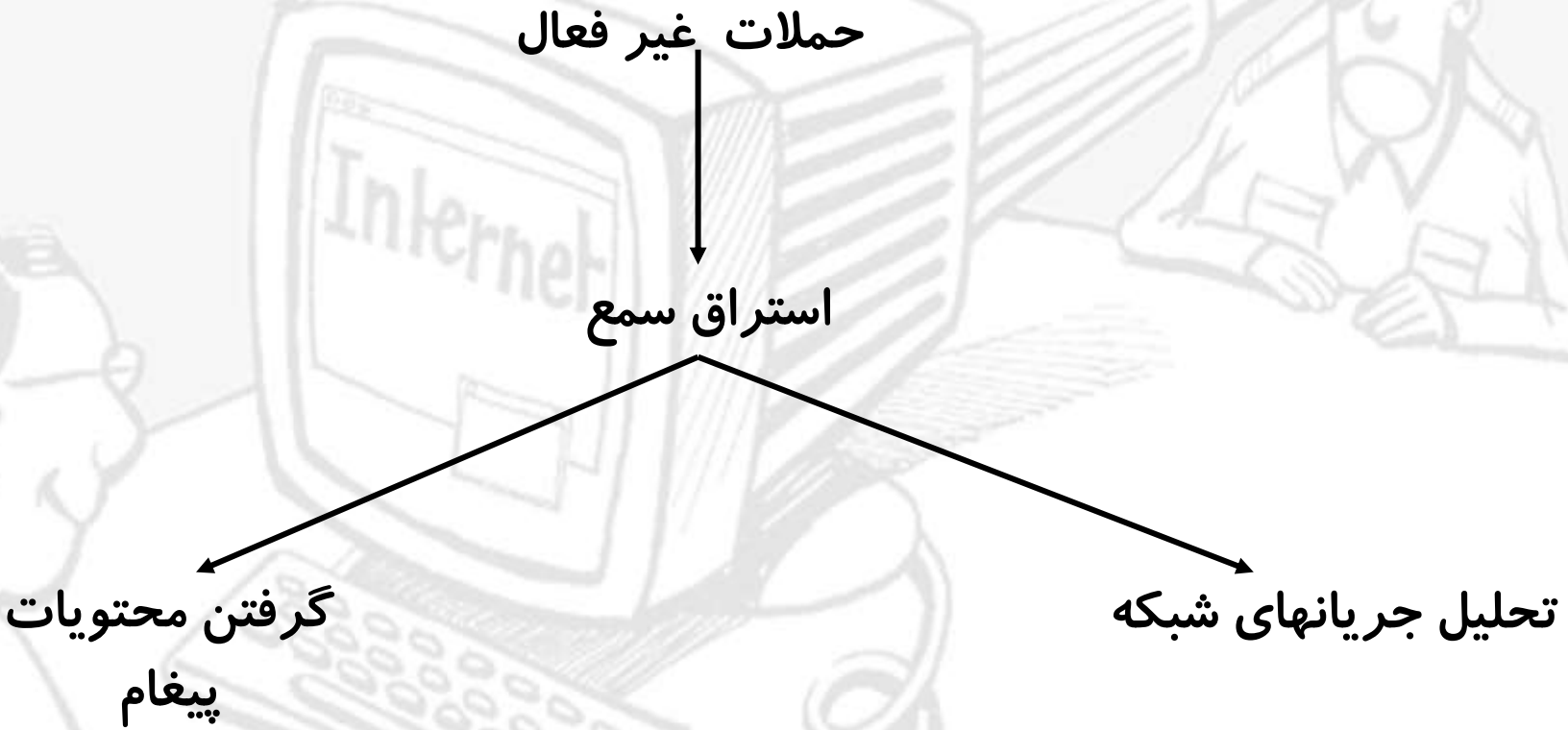
- حملات غیرفعال (passive)

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

حملات امنیتی

- بعضی از تغییرا ت رشته‌های داده

حملات امنیتی



- 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

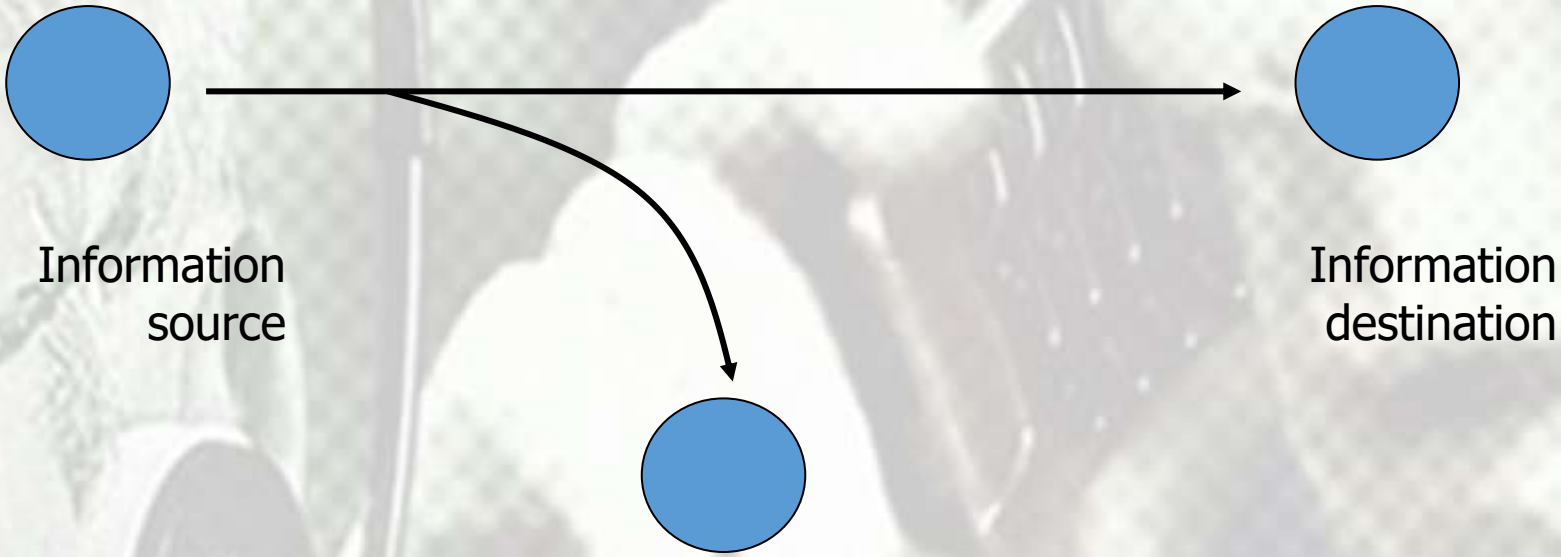
جریان عادي

حملات امنیتی

قطع ارتباط

- حمله به دسترس پذيري(Availability)

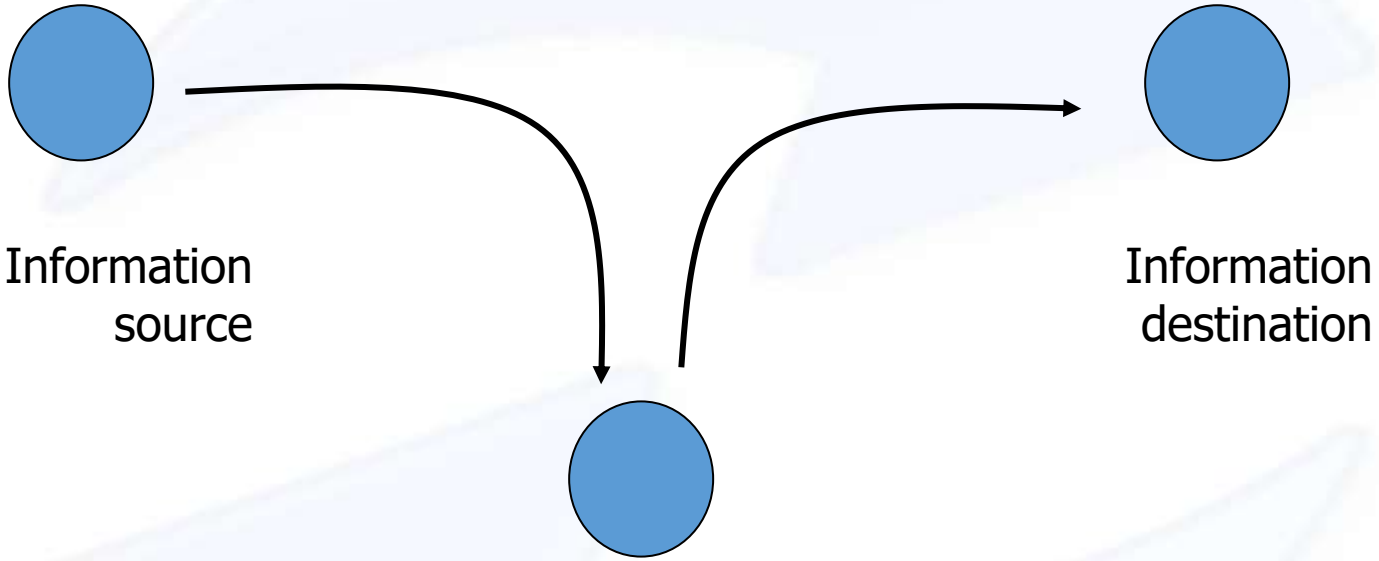
حملات امنیتی



استراق سمع(شنود یا interception)

- حمله به محرمانگي

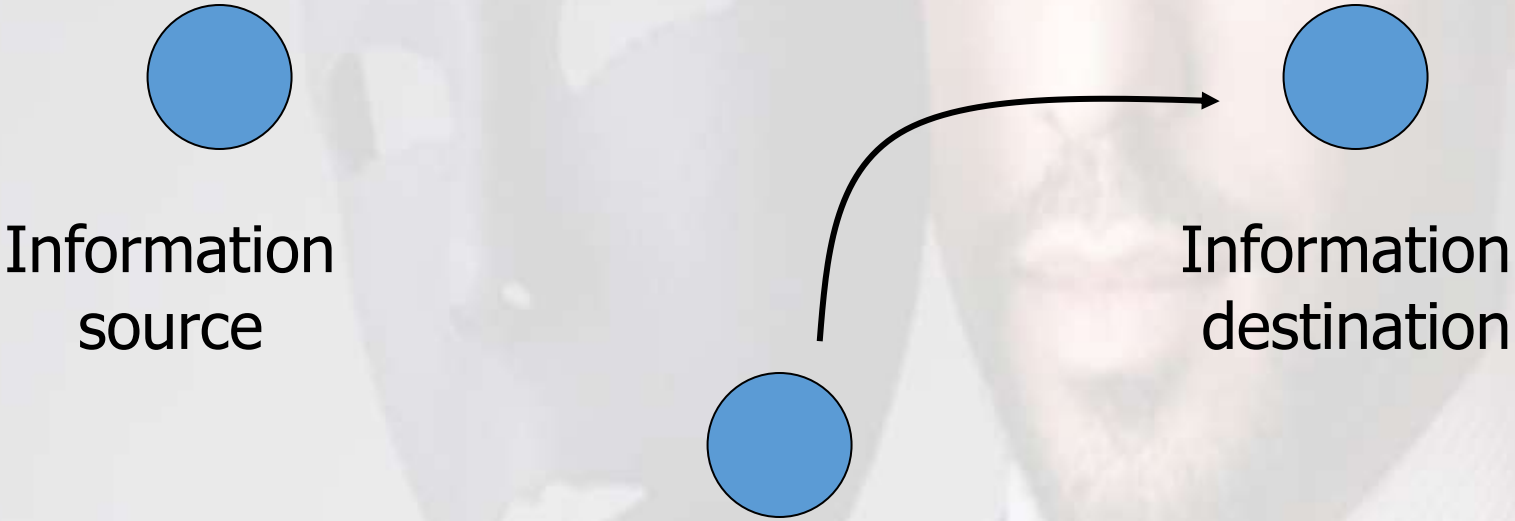
حملات امنیتی



تغییر(تغییر اطلاعات یا modification)

- حمله به جامعیت

حملات امنیتی



جعل هویت

- **حمله به هویت شناسي**

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

انواع حملات سایبری	توصیف
انکار خدمات DOS	در این روش دسترسی سامانه به کاربران مجاز 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 اینترنت 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 برای حمله به هدف صورت می گیرد.
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.
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.
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.
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.

انواع حملات سایبری	توصیف
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
شماره گیری مکرر	برنامه ساده ای که شماره تلفن های متوالی را شماره گیری می کند تا مودمی را پیدا کند.
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.
ارسال هرزنامه	ارسال نامه های پست الکترونیک تجاری ناخواسته که می تواند حاوی سازوکار تحویل نرم افزار های مخرب و سایر تهدیدات سایبری باشد.
سرقت کلمه های عبور و اطلاعات مالی	با استفاده از هرزنامه افراد را فریب می دهد تا اطلاعات حساس خود را افشا نمایند.
ساخت وب سایت جعلی	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.
فریب	روشی که دزدان کلمه عبور برای فریب کاربران و متقاعد کردن آنها از ارتباط با وب سایت معتبر بکار می برند.
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.

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)

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)

امنیت فیزیکی یا امنیت در دسترسی

(Availability Security)

- امنیت فیزیکی ارتباطات(End2End)
- امنیت فیزیکی ایستگاههای کاری
- امنیت فیزیکی سرورها ، سوییچ ها ، روترها و فایروال ها
- امنیت فیزیکی ارتباطات بی سیم

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

پدافند سایبری

راهبردها، راهکارها، اقدامات اساسی

پدافند سایبری(Cyber Defense)

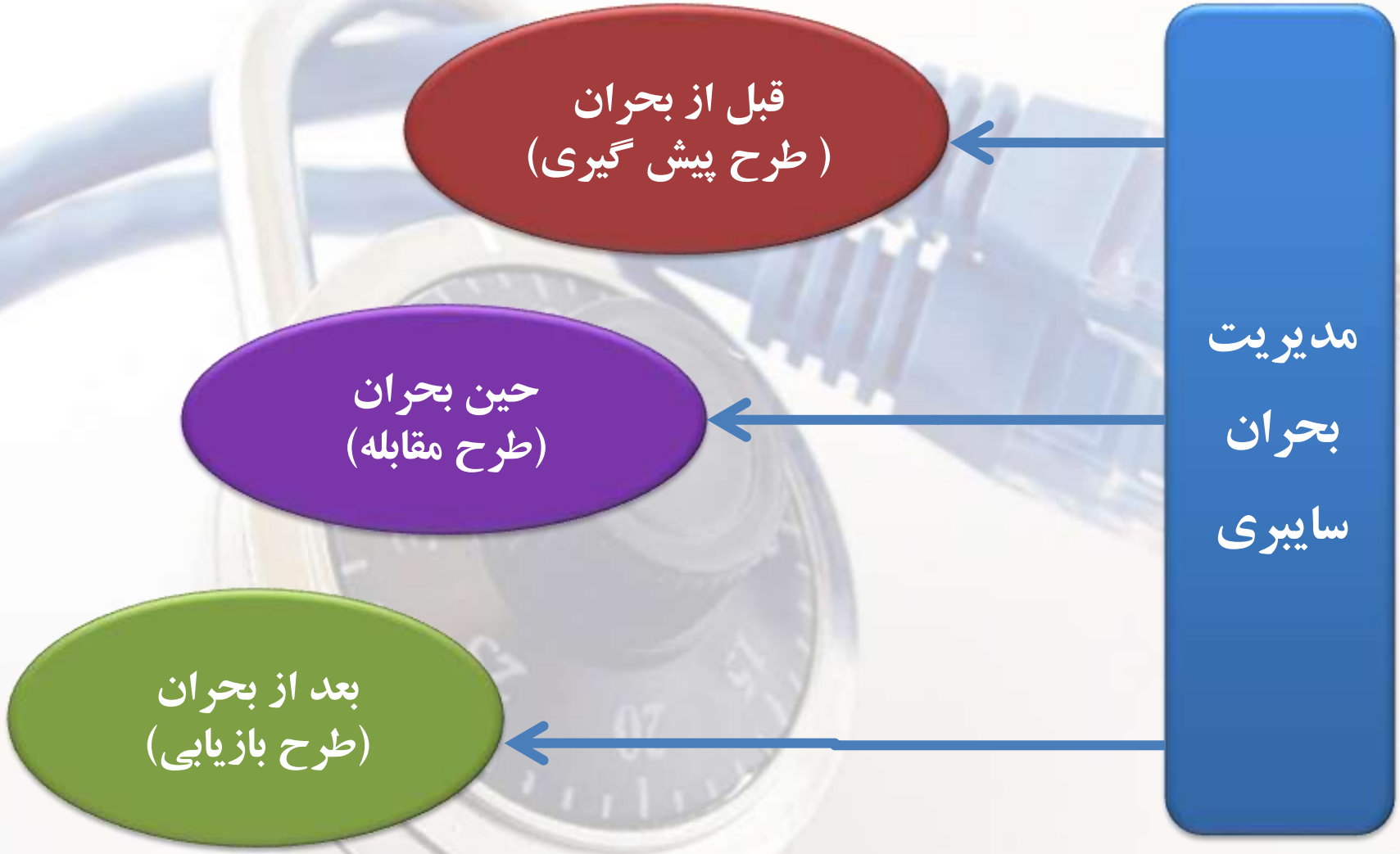
بهره‌گیری از کلیه امکانات سایبری و غیرسایبری کشور، به منظور ایجاد بازدارندگی، پیش‌گیری، ممانعت از انجام، تشخیص به موقع، مقابله موثر و بازدارنده با هرگونه تهاجم سایبری به سرمایه‌های ملی سایبری کشور، توسط متخاصمین سایبری .

رسالت پدافند سایبری

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

اهداف نهایی پدافند سایبری

- کاهش آسیب پذیری و ایمن سازی زیرساخت های سایبری
- افزایش پایداری و تداوم فعالیت های ضروری سایبری کشور
- ارتقاء پایداری ملی زیرساخت های سایبری کشور
- ارتقاء کمی و کیفی منابع انسانی در حوزه پدافند سایبری
- گسترش و تقویت تولید داخلی و بومی سازی خدمات و محصولات روزآمد پدافند سایبری
- ارتقاء سطح آگاهی، دانش و مهارتهای بومی و فرهنگ سازی در حوزه پدافند سایبری
- تسهیل مدیریت بحران در زیرساخت های سایبری کشور


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


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


بازسازی
بازیابی
بعد از بحران
ساماندهی
ویادگیری

پدافند سایبری چگونه باشد ؟

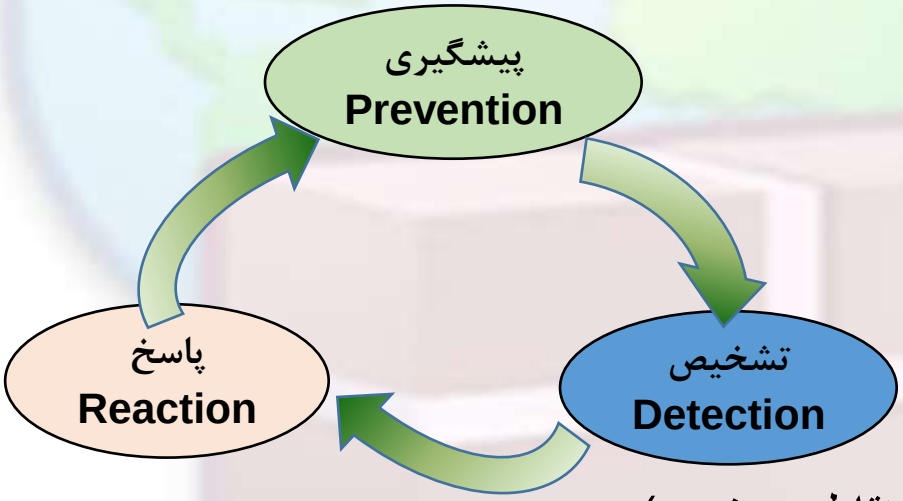
- رعایت اصول فنی و استانداردهای موجود در حوزه فعالیت مربوطه(تکنیک)
- رعایت خلاقیت و ابتکار (تاکتیک)

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

راهبردهای سایبری(۱)

۱. 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



راهبردهای سایبری(۲)

۲. سطح بندی سامانه ها و شبکه های کاربردی در سطح سازمان.

۳. ، 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 .

۴. 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).

۵. استقلال شبکه های اینترانتی سازمان از بستر اینترنت.

راهبردهای سایبری(۳)

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

۷. ، طراحی و اجرای رزمایش های عملیاتی در بخش فناوری اطلاعات و ارتباطات سازمان برای مقابله با تهدیدات سایبری.

۸. استفاده از تجهیزات و سرویس های بومی حوزه سایبری در سطح سازمان.

۹. تاکید بر وجود قابلیت بومی سازی درخرید تجهیزات و خدمات فناوری اطلاعات خارجی.

راهبردهای سایبری(۴)

۱۰. کشف و رفع آسیب پذیری های سخت افزاری و نرم افزاری و سامانه ها.

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

۱۲. آموزش و نهادینه سازی اصول پدافند سایبری (در سطوح مدیران و کارشناسان).

۱۳. اعلام هشدارهای لازم.

۱۴. دفاع حقوقی در برابر تهدیدات.

راهبردهای سایبری(۵)

۵۱. سازمان دهی ساختار و دفاع سایبری صنعتی

- ایجاد سامانه های امداد و نجات رایانه ای صنعتی (CERT)در سطح زیرساخت
- ایجاد سامانه های امنیتی صنعتی SOC در سطح زیرساخت

۶۱. بومی سازی و مصون سازی سامانه های پایه پدافند سایبری صنعتی

راهبردهای سایبری(۶)

۷۱. طراحی نظام عملیاتی سایبری صنعتی با تأکید بر آموزش، تجهیز و رزمایش

- 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

راهبردهای سایبری(۷)

۸۱. 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

راهبردهای سایبری(۸)

۹۱. لایه بندی کردن شبکه های ارتباطی به اجزای زیر و طراحی، پیاده سازی و اجرای دفاع سایبری در هر کدام از آن‌ها

- لایه پسیو یا لایه فیزیکی
- لایه اکتیو
- لایه ذخیره سازها
- لایه نرم افزارها و سامانه های کاربردی
- لایه انتقال (ارتباطات)
- لایه بهره بردار (کاربر)

راهبردهای سایبری(۹)

۱۰. طراحی، پیاده سازی و اجرای مراکز داده مورد نیاز مطابق الزامات پدافند غیر عامل

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

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

- ارتینگ
- فیلترینگ
- شیلدینگ

راهبردهای سایبری(۱۰)

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

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

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

103
103

اقدامات اساسی (دفاع و پدافند لایه ای)

۱) تدوین دستورالعمل های اجرایی(مدیریتی و فنی)

۲) دفاع فیزیکی(دوربین های مداربسته مبتنی بر IP- روشهای شناسایی بیومتریک – و ...)

۳) دفاع پیرامونی و مرزبانی (UTM-Firewall-Honeypot)

۴) دفاع در شبکه (Router-Switch L2/L3)

۵) دفاع در سطح برنامه های کاربردی(دیتابیس- DB Monitoring/Scanning)

اقدامات اساسی (دفاع و پدافند لایه ای)

۶) دفاع در سطح داده و محتوا(Data Encryption-Recovery Data-PKI)

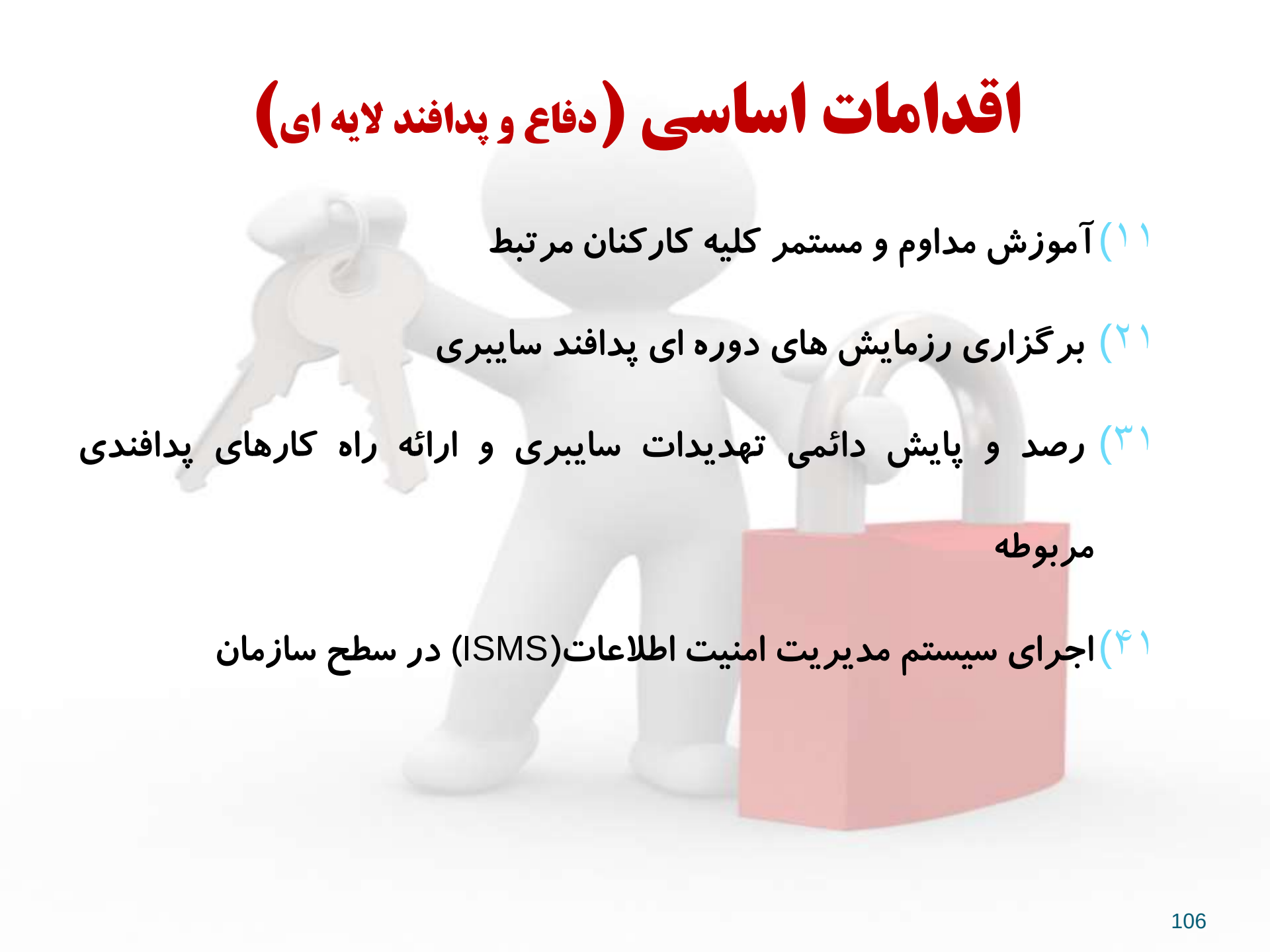
۷) تهیه نسخه های پشتیبان از اطلاعات موجود(Redundant)

۸) دفاع در سطح سیستم عامل(Industrial -CPU/Proccesor-Virtualization Computer)

۹) دفاع در نقاط پایانی(ضدبدافزارها- سامانه های تشخیص نفوذ)

۱۰) انجام عملیات تست نفوذ(Penetration Test) به شبکه و سامانه های موجود به صورت دوره ای

اقدامات اساسی (دفاع و پدافند لایه ای)



۱) آموزش مداوم و مستمر کلیه کارکنان مرتبط

۲) برگزاری رزمایش های دوره ای پدافند سایبری

۳) رصد و پایش دائمی تهدیدات سایبری و ارائه راه کارهای پدافندی مربوطه

۴) اجرای سیستم مدیریت امنیت اطلاعات(ISMS) در سطح سازمان

Clean Room اتاق های

Checking Devices **&** Soft wares

- ✓Data recovery
- ✓Safety Device
- ✓Security Device
- ✓Security Software

Devices : Pc- Laptop- Smartphone-Cd-Ram-Flash - HDD

اصول ده گانه حفاظت سایبری

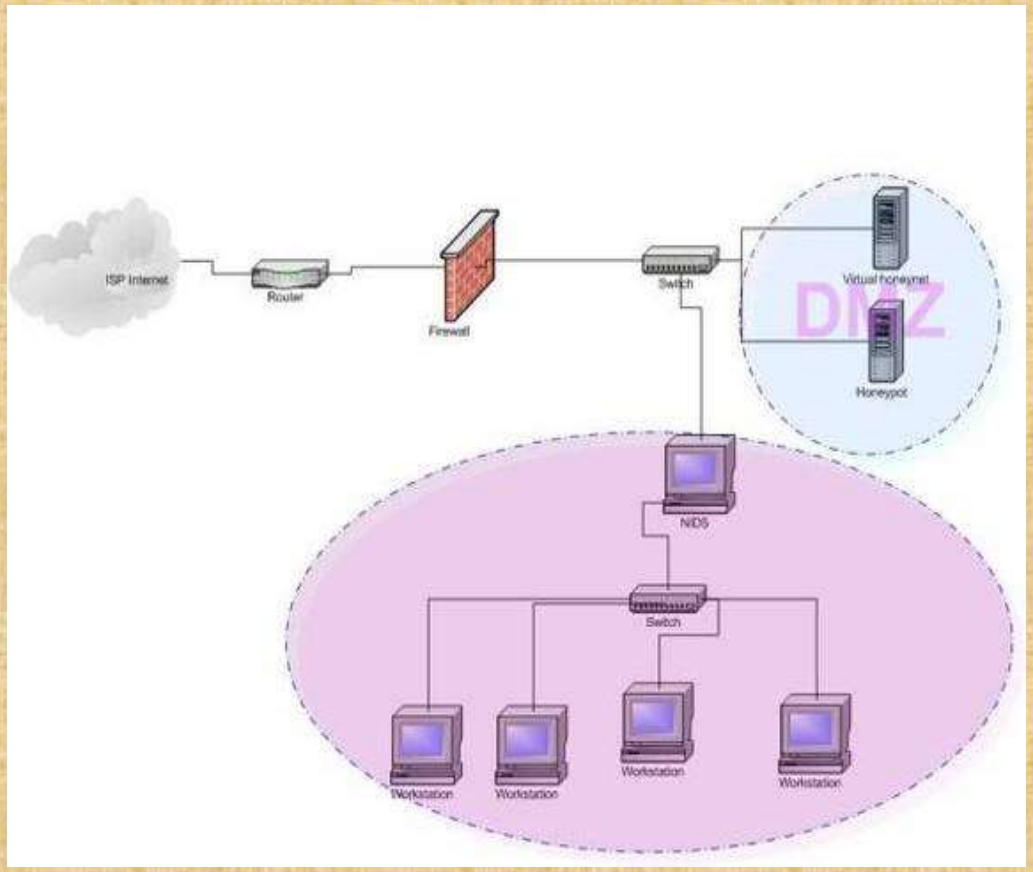
- اصل فریب
- اصل جداسازی
- اصل تنوع
- اصل دفاع در عمق (Defense In Depth)
- اصل واکنش
- اصل ارتباط
- اصل آگاهی
- اصل اشتراک
- اصل جمع آوری
- اصل احتیاط

اصول حفاظت از زیرساخت های ملی(با رویکرد سایبری)

❑اصل فریب

- فریب دادن مهاجم و ارجاع آن به منابع و دارایی های غیر واقعی .
- با هدف ایجاد عدم قطعیت برای تصمیم گیری های دشمن.

روش کوزه عسل (Honeypot)



یک منبع سیستم اطلاعاتی با اطلاعات کاذب است که برای مقابله با هکرها و کشف و جمع‌آوری و تحلیل فعالیت‌های غیرمجاز در شبکه‌های رایانه‌ای بر روی شبکه قرار می‌گیرد.

هانی پات‌ها به دو دلیل استفاده می‌شوند:

- شناخت نقاط ضعف سیستم(مقابله با آسیب پذیری)
- جمع‌آوری اطلاعات لازم برای تعقیب و ردگیری نفوذگران(مقابله با تهدید)

اصول حفاظت از زیرساخت های ملی(با رویکرد سایبری)

❑ **اصل جدا سازی**

- با هدف جلوگیری از خرابکاری و تاثیر متقابل زیر ساخت ها بر یکدیگر
- معماری و طراحی صحیح شبکه
- چینش صحیح تجهیزات(ارتباطی، امنیتی)
- کنترل دسترسی (داخلی – خارجی)

اصول حفاظت از زیرساخت های ملی(با رویکرد سایبری)

❑اصل جدا سازی

- جداسازی دارایی ها فرآیندی است شامل توزیع ، تکثیر(تکرار) و تجزیه دارایی های ملی به منظور کاهش ریسک.
- مانند ایجاد شبکه تولید و توزیع محتوا (CDNs)

اصول حفاظت از زیرساخت های ملی(با رویکرد سایبری)

❑اصل تنوع

- متنوع سازی استفاده از سامانه ها برای کاهش خطرات و آسیب پذیری ها
- با هدف جلوگیری از بهره برداری دشمن از یک ضعف مشترک در زیر ساخت ها

اصول حفاظت از زیرساخت های ملی(با رویکرد سایبری)

❑اصل دفاع در عمق(Defense In Depth)

- « دفاع در عمق» بر این نظریه تاکید دارد که هر یک از لایه های امنیتی می تواند در هر لحظه دچار خطا گردد.
- ایجاد لایه های چند گانه دفاعی برای افزایش احتمال متوقف کردن و یا حداقل کند کردن یک حمله است.
- قراردادن عناصر(لایه) دفاعی بین دارایی و مهاجم (**کارآیی** لایه ها از **تعدد** آنها مهمتر است)
- با هدف افزایش سطح امنیتی دارایی های حیاتی و کاهش ریسک پیامد حملات
- کاهش امکان (مشکل و یا غیرممکن)سطح دسترسی مهاجم به دارایی ها(منابع-اطلاعات)

اصول حفاظت از زیرساخت های ملی(با رویکرد سایبری)

- **اصل واکنش** : با هدف واکنش به موقع در برابر حوادث و کاهش آسیب پذیری حاصل از وقوع آن
- **اصل ارتباط** : با هدف کاهش آسیب پذیری با جمع آوری اطلاعات از تمامی نقاط
- **اصل آگاهی** : با هدف حفاظت از اطلاعات موقعیتی و مکانی زیر ساخت ها

اصول حفاظت از زیرساخت های ملی(با رویکرد سایبری)

- **اصل واکنش** : با هدف واکنش به موقع در برابر حوادث و کاهش آسیب پذیری حاصل از وقوع آن
- **اصل ارتباط** : با هدف کاهش آسیب پذیری با جمع آوری اطلاعات از تمامی نقاط
- **اصل آگاهی** : با هدف حفاظت از اطلاعات موقعیتی و مکانی زیر ساخت ها

اصول حفاظت از زیرساخت های ملی(با رویکرد سایبری)

- **اصل اشتراک:** با هدف افزایش سطح ویژگی های امنیتی زیر ساخت ها با توجه به درجه ای از اشتراک موجود میان آنها
- **اصل جمع آوری** : با هدف افزایش ضریب امنیتی زیر ساخت ها با استفاده از جمع آوری اطلاعات ممیزی
- **اصل احتیاط** : با هدف جلوگیری از افشای اطلاعات حساس،پنهان کردن دارایی ها با ایجاد لایه های محافظتی

مصون سازی در سطح مفاهیم عملیاتی

- دسته بندی دارائی های سایبری
- احصا ، بررسی و ارزیابی تهدیدات
- احصاء ، بررسی و ارزیابی آسیب پذیری ها
- احصاء وابستگی های بین زیر ساختی
- محاسبه و ارزیابی ریسک
- بررسی سناریو های تهدید و سناریوی پایه
- بررسی انواع رویکردی پدافند غیرعامل

- بررسی انواع راهکارهای پدافند غیرعاملی
- مهندسی ارزش و انتخاب راه کار بهینه
- تهیه طرح مفهومی پدافند غیرعامل زیر ساخت
- تهیه طرح جامع پدافند غیرعامل زیر ساخت
- تهیه طرح های تفصیلی هر نوع پدافند غیرعامل تخصصی

گوشی هوشمند
Smart Phone

گوشی هوشمند

به آن گروه از گوشی های تلفن همراه گفته می شود که علاوه بر امکانات ساده یک گوشی مانند مکالمه و پیامک(بدلیل وجود سیستم عامل و پردازش گرهای قوی) قابلیت های دیگری از جمله : مدیریت رایانامه ، دسترسی به اینترنت ، تصویر برداری ، موقعیت یابی ، برنامه های کاربردی متنوع و بسیاری از قابلیت های دیگر را در اختیار کاربر قرار می دهد .

(تبلت ها ،فبلت ها و سایر ابزار مشابه در زمره گوشی های تلفن همراه در نظر گرفته می شوند).

بهره برداری از گوشی های هوشمند در ایران!!!!

۱. بازی های رایانه ای (آنلاین – آفلاین)

۲. شبکه های ارتباطی (پیام رسان های موبایلی)

۳. عکس برداری و فیلم برداری

۴. مشاهده فیلم و عکس

۵. شبکه های اجتماعی

۶. ارتباطات صوتی

۷. سایر اپلیکیشن ها

۸. پیامک

فروش ۴۶۰ میلیارد تومانی بازی رایانه‌ای در ایران

بر اساس پیمایشی که در سراسر کشور و با ارائه ۷۰ هزار پرسشنامه در میان مردم انجام‌شده، آمار مصرف بازی‌های رایانه‌ای تا پایان سال گذشته در کشور مشخص شده است

٪۵ ایرانی

٪۹۵ خارجی

۲۳ میلیون نفر

۷۹ دقیقه متوسط زمان روزانه هر نفر

٪۲۵ بازی کامپیوتری

٪۷۵ بازی موبایلی

انواع شبکه های ارتباطی

1. **Social networks** (**Facebook, Twitter, Linkdin**): To connect with people and brands
2. **Messenger Networks** (**Telegram, Viber, Line**) :To send/receive MMS
3. **Media sharing networks** (**Instagram, Snapchat, YouTube**)To find and share photos, video, live video, and other media online.
4. **Discussion forums** (**Reddit, Quora, Digg**):To find, discuss, and share news, information, and opinions.

مهمترین کارکردها!

۱-تبادل اطلاعات

۲-کسب و کار (شبکه‌های اجتماعی سلول‌های آینده اقتصاد جهانی هستند اما ما فقط بر بستر رسانه و در حوزه پیام‌رسان از آنها استفاده می‌کنیم)

۱- جمع آوری اطلاعات (شخصی- خانوادگی-سازمانی- کشوری)

۲- مهندسی اجتماعی (سنجش و ارزیابی افکار و رفتار جامعه)

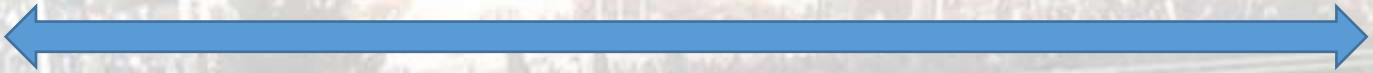
تحلیل رفتار در فضای مجازی

- گاهی رفتارها در فضای مجازی با رفتارها در فضای حقیقی کاملا متفاوت است .

اتاق فرمان حقیقی

اتاق فرمان مجازی

(میدان داری شبکه های اجتماعی پیام رسان در مدیریت صحنه)



اعتراض یا اغتشاش

تروریست یا ستیزه جو

اشتباهاتی راهبردی

- **شبکه های مجازی فقط یک پیام رسان نبوده و با ارائه خدمات گسترده، جزیی ترین مسائل زندگی انسان ها را تحت تاثیر قرار می دهند.**
- **قرار گرفتن بیگ دیتاهای ۴۰ میلیون نفر در اختیار بیگانه (که باعث شده بعضا احاطه اطلاعاتی دشمن نسبت به دستگاه های اطلاعاتی خودمان بیشتر باشد).**
- **عدم تمایل کاربر ایرانی به استفاده از محصول داخلی**(رغبت کمتر از ۵ درصدی کاربران ایرانی به پیام‌رسان‌های داخلی) .
- **رها کردن کاربران ایرانی در شبکه‌های مجازی بیگانه .**

اشغال سرزمینی

- اشغال فیزیکی (**خاک**)
- اشغال مجازی (**اشغال فضای سایبر کشور توسط بیگانگان**)

تنها ۸ درصد از محتوای تلگرام؛ تولیدی است و ۹۲ درصد آن کپی و ارسال مطالب است . (**ایجاد و القا مطلب**)

- آشوب های اخیر نوعی اشغالگری سایبری بوده که در نظر بود با کمک امکانات فضای سایبر با ایجاد تغییرات گسترده اجتماعی و تلاش برای وارد آوردن ضربات سنگین ، کشور را به سمت فروپاشی و تحت سیطره خود قرار دادن ، سوق دهند. .

بیش از ۶۰٪ ترافیک تلگرام در دنیا مربوط به ایرانی هاست!!!

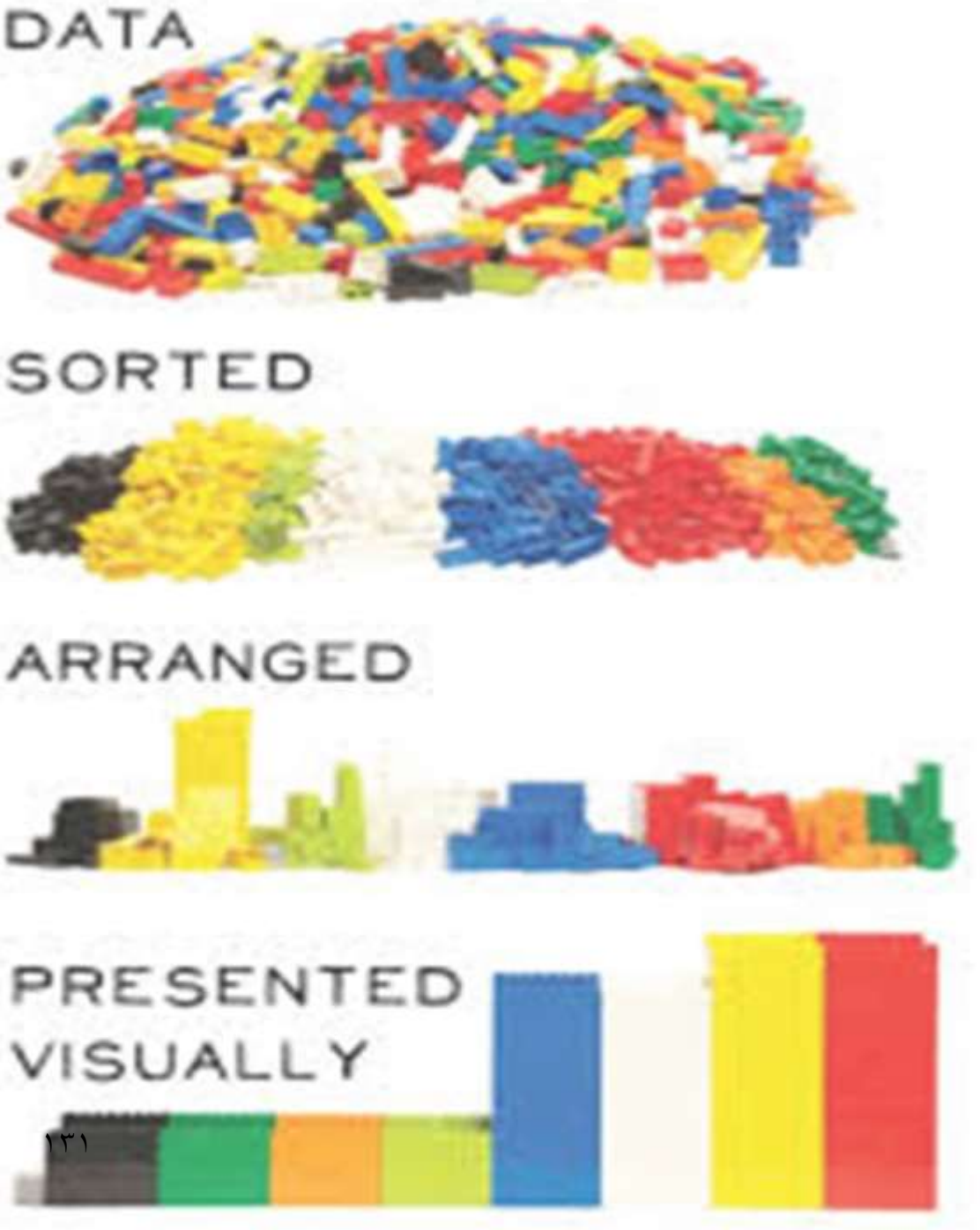
Country	Percent of Visitors	Rank in Country
Iran	44.9%	29
Russia	6.0%	940
Brazil	4.5%	698
Saudi Arabia	4.3%	231
Italy	3.5%	642

- **بیش از ۴۰ میلیون ایرانی عضو تلگرام هستند !**
- **اگر هر ایرانی روزانه 100M دیتا از طریق تلگرام منتقل کند(حدود ۲۵۰ تومان هزینه انتقال این مقدار دیتا است):۴۰M *۲۵۰ = ۱۰.۰۰۰.۰۰۰.۰۰۰ تومان**

آسیب ها و آسیب پذیری ها

- برقراری ارتباط غیر مفید و کنترل نشده (خانواده-سازمان)
- حضور بی‌مورد و نامناسب در فضای مجازی(هرزگردی)
- سرویس های فضای مجازی جایگزین ارتباطات بین خانواده ها
- کم بودن سواد رسانه ای / سایبری کاربران
- قرار گیری در معرض انواع شایعات

روند تحلیل داده ها



هرم سلسله مراتب دانش (علم اطلاعات)

چند نکته در مورد استفاده از
شبکه های اجتماعی و شبکه های ارتباطی و تجهیزات وابسته

- تنظیم کردن کلمه عبور مناسب (چند کاراکتری و ترکیبی) بر روی گوشی ، تبلت، لپ تاپ و یا رایانه مورد استفاده و تعویض این کلمه عبور در بازه های زمانی .
- تنظیم کردن کلمه عبور مناسب (چند کاراکتری و ترکیبی) بر روی شبکه اجتماعی (ارتباطی) مورد استفاده، ایمیل ها(یا جیمیل ها) و تعویض این کلمه عبور در بازه های زمانی .
- انجام تنظیمات حریم خصوصی (Privacy Policy) بر روی شبکه های مورد استفاده.
- حفاظت فیزیکی از گوشی ، تبلت،لپ تاپ و رایانه های شخصی و اداری و دور از دسترس دیگران قرار دادن آنها.

چند نکته در مورد استفاده از
شبکه های اجتماعی و شبکه های ارتباطی و تجهیزات وابسته

- اطلاعات کامل شناسنامه ای،شخصی و مالی
- موقعیت مکانی(GPS)
- اشتراک‌گذاری مکان (Sharing location) تقریبا در همه شبکه‌های اجتماعی فراهم است که این امکان را به دیگران می‌دهد بتوانند رد شما را بیابند.
- ارسال تصاویر خود و یا اطرافیانتان به همراه نام آن ها
- آدرس منزلتان و شماره واقعی تلفن تان(ثابت- همراه)
- اطلاعات در مورد برنامه تعطیلات خود،خانواده و یا اطرافیانتان

چند نکته در مورد استفاده از
شبکه های اجتماعی و شبکه های ارتباطی و تجهیزات وابسته

- وضعیت روابط شخصی تان
- تصاویر با برچسب مشخص‌کننده مکانی(Geotags)
- اطلاعات در مورد کار و یا پروژه‌های شغلی محل کارتان
- صحبت در مورد روحیات و خلقیات شخصی و خانوادگی
- بر روی لینک‌ها،ضمایم و پیوست های موجود در پیام هایی که از منابع ناشناس ارسال می‌شوند کلیک نکنید.
- مراقب جعل هویت باشید و به هر ناشناسی اعتماد نکنید

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 رسول الله