HOW TO ATTACK CRITICAL INFRASTRUCTURE

NO-BULLSHIT GUIDE

Cyber/Kinetic Forces – Sabotage Operations

Parastoo

U.S HISTORY

- 2003
  - Slammer worm
  - Davis-Besse Nuclear Power plant in Oak Harbor , ohio – Several hours disruption
- 2003
  - Failure in alarm processor of FirstEnergy shutdown the Grid
- 2006
  - Circulation Pumps at the Brown Ferry Nuclear Plant in Alabama failed to excessive traffic in the Control network
- 2009
  - Investigation showed hackers were able to steal Power by hacking into Smart Meters and Changing the Power Consumption reading

FIRST STEP

- OSINT your way into dox related to CIP of the target country or the region
  - Critical Infrastructure Protection
  - Usually a mix of pub and private data considered Standard
  - Who is the Regulatory ?
  - A clear understanding of how Standards and local/regional/national regulations work

  - Samples :
    - U.S : HSPD-7 (NERC CIP) , CFATS , NRC RG 5.71 (Nuclear)
    - ISA-99
  - Ops :
    - Parastoo's attack to NNSA and NRC and 7 U.S National labs to get dox
      - OSINT , SIGINT , CYBINT ops overall almost 20 months

TARGET

- SCADA
  - Industry , Plants , Grid , Utilities , Nuclear
- C4ISR
  - Military , Police
- ATC
  - Aviation
- Telecommunication
  - Satellite , Radio , Phone lines , TV , Emergency

PROTOCOLS

- The area we have covered fully or partially so far :
  - SCADA/ICS
  - C4ISR
  - Satellite
  - UAS/UAV
  - Trunk Radio
  - Radar data links
  - ATC
  - Emergency Wireless
  - Satellite TV Channels
  - Smart Grid

APT

Advanced Persistent Threats

تهدیدات پیشرفته مقاوم
در فضای تبادل اطلاعات

نویسنده و تاریخ و ارگان حذف شد - محرمانه

انفجار در سیبری

- یکی از اعضاء کابینهء ریگان در کتاب At the Abyss مینویسد : « ما میدانستیم اتحاد جماهیر شوروی قرار است خط لوله بسیار معظمی را جهت انتقال گاز در سیبری راه اندازی کند . طبیعتا این خط نیاز به ایستگاههای کنترل متعددی داشت . ما در نیروی هوائی و سازمانهای اطلاعاتی , سناریوئی ترتیب دادیم تا شوروی برای خرید نرم افزار این ایستگاههای کنترل به یک شرکت کانادائی مراجعه کند /../ ما امکان کنترل مخفی این خط لوله را داشتیم . میگفتند جنگ هسته ای محتمل است . پس اکنون وقت عمل بود . بعدا گزارش شد که انفجاری که ما ترتیب دادیم حدود ۳ کیلو تن قدرت داشته است »
- از سال ۱۹۸۲ تا کنون این بزرگترین انفجار غیر اتمی است که گزارش شده است

پیدایش مفهوم

پایان شوروی به عنوان ابرقدرت اصلی رقیب ایالات متحده که در عرصه دریا , زمین , هسته ای , بالستیک , علوم پایه و عملیات مخفی میتوانست برتری مطلق امریکا را تهدید کند در انتهای جنگ سرد , با تغییر معماری جنگ قدرت همزمان بود

در معماری فعلی , قدرت اقتصادی , نظامی و اطلاعاتی جهت ایفای نقش ابرقدرتی و القاء ارزشها فقط راهکنش است نه راهبرد . دلیل این گردش , توسعه و همه گیری فضای تبادل اطلاعات است که چینش جدیدی در عرصه های نبرد ایجاد کرد

پیدایش مفهوم

- عرصه های نبرد قبل از دههء ۹۰ میلادی :
  - زمین
  - دریا
  - هوا
  - فضا
- معماری نوین جنگ قدرت , سایبر یا فضای تبادل اطلاعات را به عرصهء پنجم سهم خواهی و تفوق طلبی تبدیل کرد

پیدایش مفهوم

- ساختار کاپیتالیستی ایالات متحده و کانونهای غیر آشکار قدرت عمدتا غربی با غفلت از نقش زیرساخت و علوم پایهء این عرصه جدید با تحفظات اقتصادی صحنه تولید و مهندسی را به مرور به چین واگذار کردند
- در کمتر از یک دهه چین به ابرقدرت اصلی عرصه سایبر تبدیل شد . سنای ایالات متحده در گزارشی اعلام کرد قدرت سایبری چین به نحوی رشد کرده است که برتری ایالات متحده در سایر عرصه ها به ویژه هوا و فضا را نیز زیر سوال برده است

پیدایش مفهوم

- موسسه RAND متعلق به نیروی هوائی ایالات متحده و اصلی ترین کانون تولید فکر و نوآوریهای مفهومی در امریکاست .
- مفهوم تهدید پیشرفته مقاوم توسط این موسسه جهت بررسی و ایجاد ظرفیت تقابلی با تهدید سایبری چین در سال ۲۰۰۶ مطرح شد
- در فاصله کوتاهی قدرتهای سایبری جدیدی مانند هند , پاکستان , روسیه , برزیل و گروهکهای مجرم سازمان یافته نیز مانند چین به تهدیدات ماهیتی برای امریکا تبدیل شدند
- رئیس جامعه اطلاعاتی ایالات متحده در یک سخنرانی عمومی نام ایران را نیز به فهرست تهدیدات جدی سایبری امریکا اضافه کرد

تعریف تهدید پیشرفته مقاوم

- سلسله ای از عملیات سایبری و بشری که توسط یک ارگان قدرتمند و هوشمند سازماندهی شده و برای لطمه به زیرساختها یا داشته ها و توانائیهای اطلاعاتی حریف با روشهای مدرن و بصورت توزیع شده و سرسخت اجرا گردد
- حمله سایبری از عوامل فناوری اطلاعات یا خطاهای بشری استفاده میکند اما تهدید پیشرفته مقاوم مبتنی بر یک طراحی پیچیده شامل استفاده از سلسله ای از عناصر شامل جاسوسی فردی , تحریمهای هوشمند , نقائص سایبری , تحقیق و توسعه ابزارهای مخرب لازم که اغلب زمان بر و گرانقیمت هستند میشود
- امروزه برای توصیف لطمات اطلاعاتی کوچک مقیاس یا ساده از حمله سایبری استفاده میشود اما برای اشاره به اقدامات سازمان یافته و هدفمند که به زمان و برنامه ریزی و بردارهای حمله متعددی نیاز دارند از مفهوم APT استفاده میشود

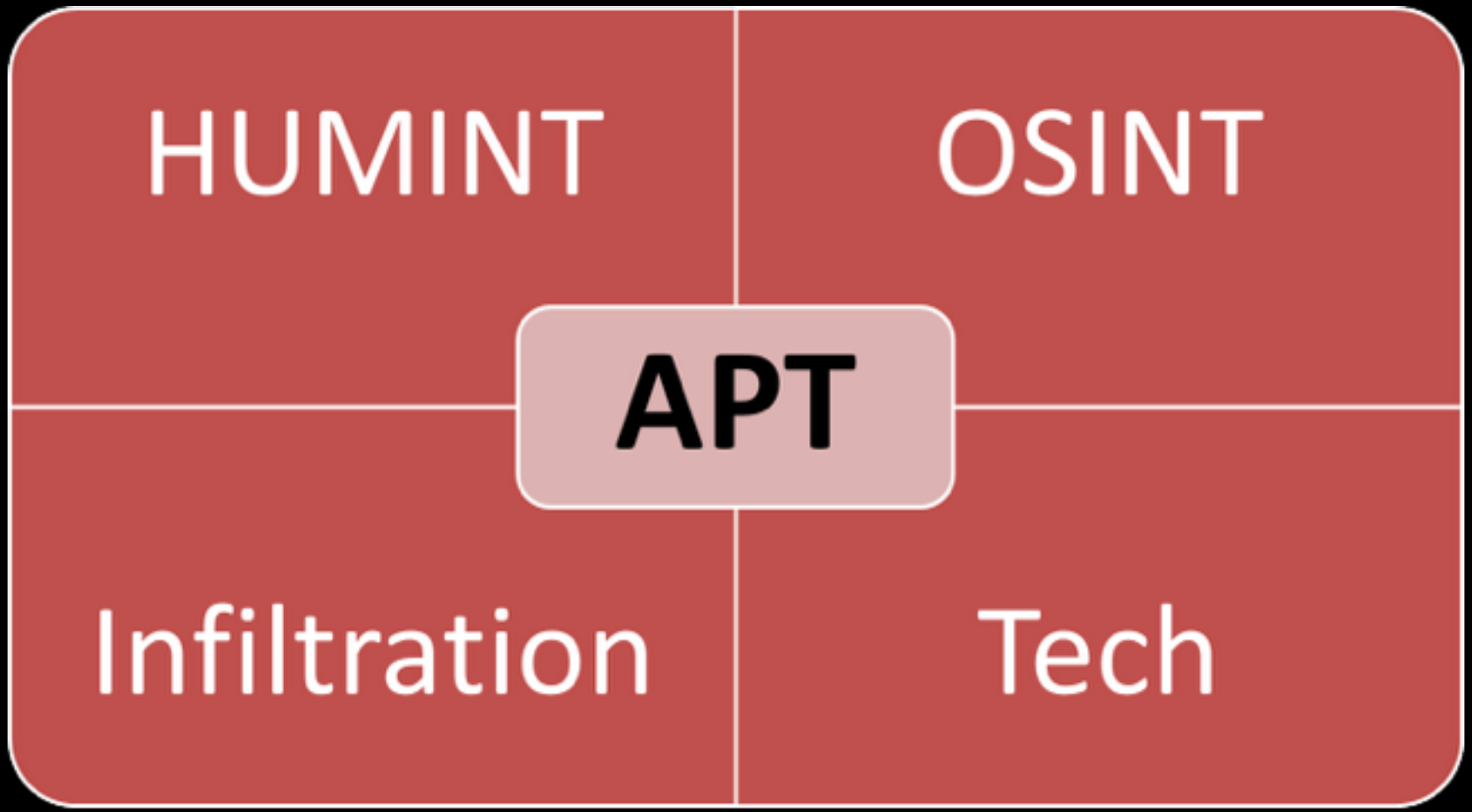
بردارهای عملیاتی

- جمع آوری و سازماندهی اطلاعات آشکار
- نفوذ پنهان
- منابع انسانی و جاسوسی
- اشراف و تجزیه اطلاعات از طریق برتری فناوری

Attack Vectors

- OSINT
  - Open Source Intelligence
- Infiltration
  - System & Network Penetration
- HUMINT
  - Human Intelligence
- Technological Advancements
  - SIGINT , COMINT , GEOINT & Satellite Imagery , Phone and Internet Interception , Breaking Encryption

مربع تهدید



اطلاعات آشکار

- بر خلاف باور غلط عام و متداول , اطلاعات آشکار مهمترین منابع برداشت داده توسط سرویسهای اطلاعاتی و مجرمان حرفه ای هستند و با پویش و پایش منابع آشکار از اشخاص گرفته تا شبکه ها یا سازمانها , بخش مهمی از هر سناریوی آفندی شکل میگیرد
- جهت حراست از منافع , پویش و پایش دائمی منابع آشکار جهت مشاهده اطلاعات موجود یا نشت کرده ابتدائی ترین قدم حفاظتی است
- به این منظور روشها و ابزارهای مختلفی وجود دارند که در اختیار داشتن این دانش و فناوریها ضروری است اما مهمتر , درک صحیح از نحوهء برداشت و سازماندهی اطلاعات آشکار با مقاصد آفندی و پدافندی است . در دانشکده های اطلاعاتی و نظامی , رئوس آموزشی به همین منظور تحت عنوان کلی « جمع آوری » وجود دارد .

منابع انسانی و جاسوسی

- بین افسران با تجربه اطلاعاتی که بعضا کتابهائی بصورت خاطرات یا موضوعی نوشته اند قطعه حکمت مشهوری وجود دارد که به زبانها و گویشهای مختلف تکرار شده است :

– یک منبع (مهره) بشری قرار گرفته در جای مناسب زمین حریف از هر راهبرد و سلاحی موثرتر است .

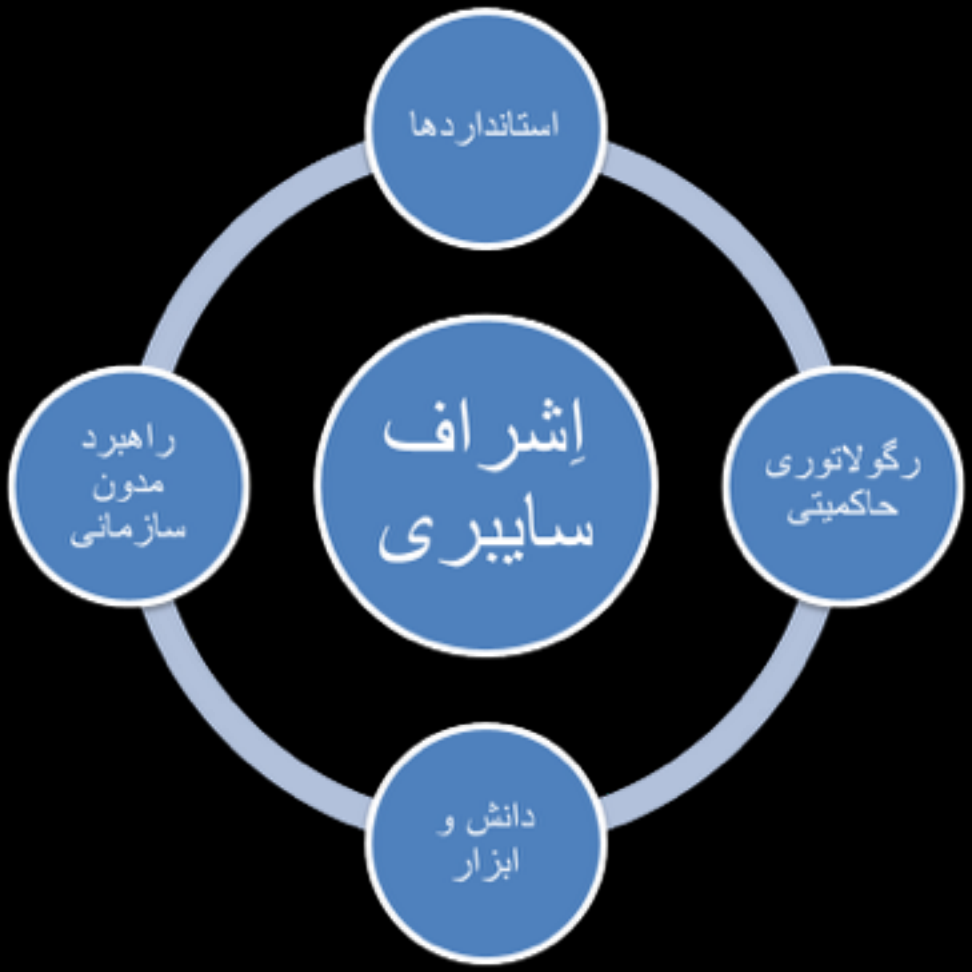
نفوذ پنهان

- فقدان تدابیر هوشمندانه گسترده در مقیاس ملی مانند :
- استانداردها
- رگولاتوری حاکمیتی
- راهبرد مدون سازمانی مدیریت امنیت اطلاعات
- دسترسی به دانش , آموزش و ابزارهای مناسب

باعث میشوند نفوذ پنهان به سامانه های زیرساختی یا کاربردی در فضای تبادل اطلاعات حتی برای افراد کم تجربه و سازماندهی نشده نیز امری دستیافتنی باشد

اولین قدم جهت مقابله به این وجه تهدید , فراهم آوردن اِشراف سایبری در مقیاس سازمان یا بصورت ملی است .

مقابله با مخاطره نفوذ پنهان



تهدید برتری فناوری دشمن

میراث آلبرتا

لا مالَ أعوَدُ مِنَ العَقل

هیچ دارائی بهتر از عقل نیست

امام صادق (ع)

درک صحیح از وضعیت

- برای مقابله با دشمن باید نوع تهدیدها و بردارهای احتمالی حمله شناسائی شوند
- در فضای تبادل اطلاعات , تهدیدهای ذیل متعارف بوده و بصورت روزمره رخ میدهند :

  – جرائم سایبری
  – جاسوسی سایبری
  – درگیری سایبری

درک صحیح از وضعیت : جرائم سایبری

- سرقتهای مالی و اعتباری
- دست اندازی به حریم خصوصی
- باج خواهی
- فریب
- جعل هویت

جرائم سایبری توسط افراد یا گروههای کوچک با انگیزه های مالی یا شخصی مانند انتقام یا خودنمائی و جبران کمبودهای فکری و شخصیتی رخ میدهند

پلیس سایبری گرچه دارای وظایف کلان حاکمیتی مانند نظارت و رصد فضای تبادل اطلاعات را دارد اما بدون وجود ضروریات مدیریت امنیت اطلاعات , تحقیقات پلیسی و قضائی با مشکلات بسیاری روبرو میشوند

سرویس دهندگان خدمات و محتوا , سازمانها و ادارات , دانشگاهها و .. باید ضمن تعامل با فضای تبادل اطلاعات , ملزومات نظارتی و امنیتی جهت جلوگیری از تضییع حقوق فردی و توسعه جرم را فراهم کنند

نمونه : تعامل FBI & FCC در مورد CALEA و حق شکایت شهروندان و مسئولیت سرویس دهندگان و ارگانها

درک صحیح از وضعیت : جاسوسی سایبری

- نفوذ به زیرساخت یا سامانه های حساس جهت تخلیه یا بهره برداری از اطلاعات شامل جاسوسی مالی , صنعتی , فناوری , سیاسی , علمی و..
- ارگانهای زیرساختی و حساس و مراجع اطلاعاتی با ارزش مانند بانکها جهت حراست از داده های خود باید برنامه امنیتی نظارتی مدون و پویشهای لازم برای نفوذ اخلاقی جهت آزمایش دائمی سازگاری با استانداردها را به روال متعارف سازمان تبدیل کنند
- حاکمیت میبایست لوازم رگولاتوری و نظارت بر تخلف , نشت احتمالی , عدم سازگاری با قراردادها و استانداردها و .. را فراهم و به عنوان وظیفهء حفاظتی حاکمیت از عرصهء تبادل اطلاعات اجرا نماید

درک صحیح از وضعیت : درگیری سایبری

- شامل زد و خوردهای محدود میان کشورها یا برخی گروهها به دلائل رسانه ای و سیاسی
- عمدتا کوتاه مدت و کم هزینه
- نمونه ها :
  - زد و خورد دائمی هکرهای هندی – پاکستانی و بنگلادشی
  - درگیریهای گروههای عرب و ترک با گروههای اسرائیلی
  - درگیری گروههای موسوم به ناشناس به دلائل مختلف با سازمانها یا ارگانهای متفاوت

درک صحیح از وضعیت : تهدید پیشرفته مقاوم

- نیاز به برنامه ریزی بلند مدت
- کاربرد تخصصهای متفاوت
- بودجه هنگفت
- بهره مندی از عوامل و منابع انسانی حریف
- در اختیار داشتن پیمانکاران شایسته
- اهداف مشخص و واقع بینانه

گرچه محال نیست گروههای خلافکار سازمان یافته بتوانند چنین ظرفیتهائی را در اختیار گرفته و عملیاتی کنند اما بدیهی است که حکومتها به ویژه در صورتیکه خود را در معرض خطر احساس کنند از چنین تهدیدی چه در قالب عامل بازدارنده چه به عنوان اقدام آفندی استفاده خواهند کرد

بازیگران اصلی

- مطالعه و شناخت فعلی ما از وضعیت نشان میدهد که اکنون چین و ایالات متحده بازیگران اصلی این عرصه هستند و سایر نظامها یا هنوز نتوانسته اند به ظرفیت مشابهی دست پیدا کنند یا اساسا برنامه و رویکرد تهدید آمیزی در این عرصه ندارند
- منفعت/هزینه
- کره شمالی , روسیه , هند , برزیل و ایران جزو کشورهائی هستند که گزارشهای مختلفی در مورد اقدامات تهدید آمیز و آفندی آنها در قالب APT گزارش شده است

بازیگران اصلی

- دپارتمانهای سوم و چهارم واحد اطلاعات ارتش چین و همچنین وزارت امنیت داخلی چین دارای اسناد آشکار منتشر شده ای هستند که نشان میدهد این ارگانها دست کم بیش از یک دهه در زمینه طراحی آفندهای پیشرفته سایبری فعالیت میکنند
- دانشگاههای متعددی در چین شامل دانشگاههای عمومی و نظامی , عناوین درسی یا رشته هائی با عنوان جنگ سایبری یا امنیت شبکه و .. دارند
- واحد اطلاعات ارتش چین آنچنان بی پروا در زمینه آفند سایبری فعالیت میکند که نتیجه یک آزمایش روی نفوذ به شبکه برق یکی از ایالتهای امریکا و امکان صدمه حیاتی به اموال و انسانها را بصورت آشکار همراه با مستندات منتشر کرده است که در گزارش کمیته روابط چین—امریکای سنای امریکا نیز به آن اشاره شده است .
- سرقت اطلاعات هواپیمای اف—۳۵ و بهره برداری از آن در ساخت اولین هواپیمای استیلث چینی و اذعان علنی مقامات نظامی چین نشان میدهد دکترین دفاعی این کشور در عرصه سایبر بصورت آشکار و بی درنگ بر اساس قدرتنمائی و شفافیت در بروز ظرفیتها به عنوان عامل بازدارنده میباشد
  - برآورد ارزش اطلاعات سرقت شده : ۳۰۰ میلیارد دلار

بازیگران اصلی

- بر اساس اطلاعات آشکار در کره شمالی فقط در ۸ مرکز متعلق به دولت یا ارتش دسترسی به اینترنت بصورت گسترده وجود دارد و ظرفیت دانشگاهی , فردی یا گروهی بدون عنایت نظام سیاسی حاکم عملیاتی نمیشود
- گزارشاتی در مورد سرقت برخی نرم افزارهای مرتبط با انرژی اتمی توسط کره شمالی وجود دارد که آزمایشات هسته ای این کشور نشان میدهد یا این گزارشات صحیح بوده یا خود این کشور توانسته است دانش نرم افزاری که حدود ۵۰ سال عمر و سرمایه گزاری لازم دارد را تولید کند که در هر دو صورت دست کم نشان دهندهء توان نرم افزاری بالای حکومت کرهء شمالی است

بازیگران اصلی

- مطالب اغراق آمیز و نادرست و آمیخته با توهم و متاثر از کارتلهای رسانه ای اسرائیلی در مورد توان سایبری رژیم صهیونیستی منتشر میشود و باور عمومی نادرستی در مورد قدرت بالای آنها وجود دارد
- مطالعه و تجربیات ما نشان میدهد که این باورها نادرست بوده و گرچه برخی فناوریهای پیشرفته در اختیار رژیم صهیونیستی قرار دارند اما عوامل متعددی نظیر کوچک بودن این رژیم , فساد شدید نظام سیاسی داخلی , درگیریهای گسترده دو حزب عمده جهت کسب قدرت و وابستگی تاریخی سرویسهای اطلاعاتی این رژیم به امریکا و بریتانیا باعث شده است که این رژیم به تهدید حقیقی سایبری تبدیل نشود
- اظهار نظرهای ناآگاهانه و بعضا غیر مسئولانه برخی مقامات مبنی بر اجرا شدن حملات جدی علیه ایران توسط این رژیم شاید به دلیل عدم آگاهی کافی از جزئیات باشد . هدف ما در این گفتگوی فنی استخفاف دشمن نیست اما بر اساس تجربه به ذکر همین آیهء شریفه کفایت میکنیم که «ان اوهن البیوت لبیت العنکبوت»

بازیگران اصلی

- مخاطره اصلی سایبری که میتواند تهدید پیشرفته مقاوم علیه جموری اسلامی طراحی و حتی بصورت آفندی به عمل در آورد , ایالات متحده است
- حکومت فدرال ایالات متحده نه تنها در این امور بلکه بصورت کلی در تهیه فناوریهای پیشرفته و خدمات کاربردی آنها از پیمانکاران دفاعی خود استفاده میکند که اغلب آنها شناخته شده هستند
- بر خلاف باور عام و متعارف , که این تهدیدات در اتاقهای تاریک و مخوف و موهوم زیرزمین سیا انجام میشود , مطالعات ما و شواهد نشان میدهد که توسعه این تهدیدات , مانند ساختن پیشرفته ترین رادار یا شنود یا کدهای هسته ای در شرکتهای پیمانکار و آزمایشگاههای تحقیقاتی انجام میگردند

تسلیحات سایبری

- پس از وقایع دو سال اخیر , مفهوم سلاح سایبری و شکل و ترکیب دادن به ابعاد نظری و عملی آن در حال گسترش است
- وضعیت فعلی فضای تبادل اطلاعات به شرایط نزدیک به جنگ اتمی زمان کارتر و خروشچف بسیار شبیه است
- کانونهای قدرت باید حریف را دچار « معادلهء تهدید آمیز و چند بعدی » کنند که یا توان حل آن را نداشته باشد یا درک کند که این روند در صورت ادامه به نابودی خواهد انجامید و بدین ترتیب از موضع مخاصمه کوتاه بیاید
- تهدید پیشرفته مقاوم , مانند یک سلسله از معادلات پیچیده است که در فضای در هم تنیده تبادل اطلاعات ضمن ایجاد بازدارندگی یا آفند اطلاعاتی , ذهن و برنامه ریزی حاکمیت را مختل میکند
- تهدید پیشرفته مقاوم , سلاحی توزیع شده , نرم , مرکب از عناصر فکری و لمسی است که دست کم در ۵۰ سال آینده , مانند عرصه های فضا و هسته ای به عاملی یکتا در تعیین تفوق و دست بالا در اداره حکومت خواهد داشت

عملیات روانی

- یکی از نتایج غیر قابل چشم پوشی تهدید پیشرفته مقاوم , اثرات مخرب روانی آن بین مردم و مسئولین است . بدیهی است که به دلیل ماهیت فضای تبادل اطلاعات , اخبار اعم از درست یا نادرست و ضد اطلاعات عمدی دشمن به سرعت مخابره میشود
- نمونه : قبل از حمله دوم به عراق , ارتش امریکا با استفاده از ترفندهای تلفنی و نرم افزاری با تعداد زیادی از افسران عالیرتبه عراقی که تلفن آنها قبلا از نفوذ به مخابرات عراق تخلیه شده بود تماس گرفت و به آنها اخطار کرد که حمله امریکا به عراق حتمی است (که بود) و جهت حفظ خانواده و منافعتان از مسیرهای مشخصی از عراق خارج شوید . این امر , باعث جو روانی و عصبی شدیدی بین افسران و شایعه پراکنی و ضعف فکری آنها شد که به دلیل عکس العملهای مختلف , استخبارات صدام برخی افسران متخلف را اعدام کرد و برخی نیز که فرار کرده بودند توسط افراد ناشناس کشته شدند .
- بهره برداری روانی از نتایج یک عملیات پیچیده در فضای تبادل اطلاعات گاهی تبدیل به بزرگترین نتیجهء آن عملیات میشوند
  - استاکس نت

پدافند

- طرح و گفتگوی مسائل نظری و پایه پیرامون این موضوع منجر به رشد فکری و گسترش افق بینش فعالان این حوزه میشود به همین دلیل برگزاری پنلهای آزاد گفتگو در دانشگاهها , مراکز آپا , موسسات و کانونهای فکر ضروری به نظر میرسد
- سازماندهی استانداردهای ملی و رگولاتوری ارگانها جهت سازگاری اولین وظیفه حاکمیت به نظر میرسد . پاسخگو شدن حاکمیت به تدابیر خود و پاسخگو کردن ارگانها نسبت به تهدیدات و رخدادها و مدیریت آنها قدم ابتدائی در حراست از فضای تبادل اطلاعات است
- مدیریت امنیت در فضای تبادل اطلاعات , بیشتر از آشنائی با فنون و الفاظ و عناوین , به قابلیتهای مدیریتی نیاز دارد . انتخاب مدیران شایسته و دارای سوابق «مدیریتی» روشن و مرتبط , ضروری تر از لشگرکشی های فنی ـ مهندسی متعارف در این حوزه است

اهداف غیر متعارف

- ایستگاههای برق
- ماهواره ها
- سامانه های کنترل نظامی – سی ۴
- سامانه های مدیریت اطلاعات ستاد – آی اس آر
- خطوط تلفن اضطراری
- اطلاعات و سریال پاسپورتها از دستگاههای چاپ
- دستگاههای کنترل حضور و غیاب با اثر انگشت
- کارتهای پرسنلی کانتکتلس

Confidential اسلاید غیر عمومی

و آخر دعوانا ان الحمدلله رب العالمین

- با تشکر صمیمانه از :
  - شرکت پرورش داده ها
  - سازمان فناوری اطلاعات
  - وزارت ارتباطات و فناوری اطلاعات
  - واجا
  - سایبری سپاه
  - حفاظت اطلاعات وزارت دفاع
  - حفاظت اطلاعات ارتش