جنگ سایبر
تحلیلی از کاوه سیدمفیدی
سکیورتارگت، جولای ۲۰۱۴

Cyber War
An Analysis by Kaveh Seyed Mofidi
SECURE TARGET, July 2014

هدف از تحلیل جنگ سایبر، نمایش زشتی و کراهت ستیزه جویی میان انسانهاست. با دیدن چهره کریه جنگ، بدنبال تصویر زیبای صلح برویم
کاوه سیدمفیدی

مقدمه

جنگ و نزاع هرگز و در هیچ زمانی به نفع هیچ کشور و ملتی نبوده است

به راستی چرا به جای صحبت از صلح و دوستی و آسایش برای بشریت، به جنگ و ستیز بپردازیم؟ چرا با ایجاد جنگ و ناآرامی و خشونت، این سرزمین کوچک (کره زمین) را با تمام موجوداتش نابود میکنیم؟ این سوال روشن یک پاسخ منطقی هم دارد ولی حقیقت چیز دیگری است و اجتماعات انسانی همواره مورد تهدید بوده و در برابر گزند دشمنان خود معیوب اند و این حقیقتی غیر قابل گریز است.

نظر و توجه به مقوله امنیت و آسایش ملی برای هر انسان و کشوری، در هزاره‌ای که امروز زیست میکنیم، امری کاملا محسوس و ملزوم است. شاید اکنون دشمن شما در حال طرح‌ریزی حمله است و تنها یک راه نفوذ کافیست تا وی به اهداف خود برسد!

سربازان حقیقی از مرزها حفاظت می‌کنند ولی در دنیای امروز، تهدیدات و مخاطرات متعددی وجود دارند که عموما به آنها توجهی نمی‌شود، تهدیدات مرتبط با فضای سایبر. **امروز برای تضعیف دشمن لزومی ندارد حتما خطوط راه آهن آن را بمباران کنیم؛ یک مودم و یک PC کافیست!**

با گسترش روز افزون استفاده از کامپیوتر در دنیا، تشکیل و گسترش فضای مجازی و غیر فیزیکی قبلا به وقوع پیوسته است، فضایی که چه بخواهیم و چه نخواهیم، چه خوشمان بیاید و چه راضی نباشیم، در آن غرق شده ایم. اکنون با استفاده همه جانبه از کامپیوترها، فضای سایبر به اندازه کهکشان گستره دارد، اجتماعی بدون مرز و محدودیتهای رایج اجتماع واقعی. نا امنی ها و تهدیدات چنین اجتماعی به مراتب بیشتر از فضای حقیقی اجتماعات انسانی است. نگاهی به گسترش اینترنت در جهان بیاندازید تا بر این مهم ایمان آورید.

این مختصر، فقط مقدمه‌ای جهت تفهیم این امر است که حفاظت از مرزهای مجازی (Virtual Network Perimeters) به اندازه حفاظت از مرزهای روی نقشه برای هر کشوری دارای اهمیت است. مرزهای مجازی که اطلاعات، این عامل نیرو بخش و حیاتی را در درون خود جای داده‌اند؛ مرزهائی که تمام عناصر وابسته به دنیای مجازی را در خود دارند . . . آیا از دنیای مجازی خود، حفاظت میکنید؟

دو قدرت در جهان وجود دارند، شمشیر و فکر. در بلند مدت، شمشیر همیشه به درایت بازنده است.

ناپلئون بناپارت

مفاهیم اولیه

برای تفهیم جنگ سایبر ابتدا باید فضای سایبر و عناصر آن را ادراک نمائیم. بنابراین ابتدا ببینیم اصولا سایبر (Cyber) به چه مفهوم است:

سایبر، پیشوندی برای اسامی متعدد و متنوعی است که همگی براساس انتشار روزافزون کامپیوتر و کاربرد آن پدید آمده‌اند. ضمنا اغلب عناصر درگیر با اینترنت با این پیشوند قابل تشریح می باشند.

اولین اصطلاح در این وادی، Cyber Space یا همان فضای سایبر است که استعاره‌ای برای تشریح سرزمین غیرفیزیکی تشکیل شده از سیستم‌های

کامپیوتری می‌باشد. در فضای سایبر نمی‌توان بوئید و یا شنید (منظور توسط حواس پنجگانه است) ولی این گستره نیز دارای عناصر و اشیاء (object) خاص خود است؛ فایل‌ها، پیغام‌های الکترونیکی، عکس‌ها و ... این فضا دارای مدل‌های انتقالی و حمل نقل نیز می‌باشد. بر خلاف فضای حقیقی، سیر و گشت در این سرزمین بدون هیچگونه حرکتی فیزیکی مقدور است، بله تنها با حرکت ماوس یا فشردن کلیدی در صفحه کلید. اگر میخواهید تجسمی از فضای سایبر داشته باشید، تمام سیمها و اتصالات و ترمینالهای تمام شبکه های برق و تلفن و کامپیوتر باسیم و بی سیم را یکجا در ذهن خود گردآورده و به هم متصل کنید!

تعریف جنگ سایبر (لغوی، اصطلاحی)

جنگ سایبر در لغت به معنای تهاجم بر عناصر سایبر است و اصطلاحا به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستمهای اطلاعاتی با هدف به مخاطره انداختن عناصر اطلاعاتی (اطلاعات، پروسه‌های مبتنی بر اطلاعات، سیستمهای اطلاعاتی، شبکه‌های رایانه‌ای) دشمن در یک فضای سایبری است.

چنین عملیاتی بطور مشخص با اهداف نظامی، تجاری، سیاسی، فرهنگی و ... انجام می‌پذیرد. بنابراین باید دارای ارزش افزوده و به اصطلاح، بهره‌برداری از عناصر دشمن را شامل شود. چراکه عملا هر نوع جنگ دیگری نیز نهایتا به سوءاستفاده از منابع دشمن ختم خواهد شد.

جنگ سایبری دارای اهمیت روزافزون برای مراکز نظامی، سرویس‌های جاسوسی، اطلاعاتی، سری و دنیای تجارت است ولی در کل، دید نظامی و غیرنظامی را باید مدنظر داشت.

با دیگرلغات و اصطلاحات مشابه سایبری نیز آشنا شوید:

Information Warfare, I-War, IW
C4I, Cyberwar, Cyberwarfare
Netwar, Internet War, Digital War

ایمنی سایبری (Cyber Security) – امنیت و آسایش سایبر از جنبه‌های زندگی انسان امروزی است.

تروریسم سایبری (Cyber Terrorism) – مسلما تروریست‌ها نیز در فضای سایبری حضور دارند.

حمله سایبری (Cyber Attack) – برخی در این محیط اقدام به حمله و تهاجم می‌نمایند.

سلاح سایبری (Cyber Weapon) – مسلما برای حمله باید دارای سلاح و جنگ‌افزار بود.

سرباز سایبری (Cyber Soldier\Cyber Warrior) – جنگ سایبری نیز مانند هر جنگی نیاز به نیروی انسانی دارد که البته در اینجا نیروی الکترونیکی (سربازان صرفا سایبری) نیز حضور دارد.

تهدید سایبری (Cyber Threat) – مخاطرات چندی در فضای سایبری وجود دارد.

شهر سایبری (Cyber City) – فضای سایبری نیز دارای شهر و کشور است.

جنایت سایبری (Cyber Crime) – تخلف و تجاوز به حقوق دیگران نیز در فضای سایبری رایج است.

پلیس سایبری (Cyber Police) – برای جلوگیری از جرائم سایبری باید دارای پلیس آن فضا نیز بود.

توجه:
- گاهی لفظ سایبر را یا پیشوند "e" که از ابتدای عبارت انگلیسی Electronic گرفته شده است نیز تعویض می‌نمایند و این درواقع تشبیهی مانوس‌تر برای عامه مردم است (مانند eMail).
- نباید مقوله سایبر را با اصطلاح سایبرنتیک (cybernetics) اشتباه کرد. این لغت دوم اولین بار در سال ۱۹۴۳ توسط شخصی به نام "نوربرت وینر" مطرح گردید و به مفهوم مطالعه و مقایسه بین دستگاه عصبی-بیولوژیکی (مغز و اعصاب) با دستگاه‌های الکتریکی/الکترونیکی و مکانیکی و نحوه تقلید از آنهاست.

تاریخچه جنگهای سایبر

بنابر شواهد، اولین جنگ این چنینی، بین ایالات متحده آمریکا و شوروی (سابق) در اواسط دهه ۱۹۷۰ در گرفته است، گروه متعددی از جنگ‌های سایبر که همگی در دوران جنگ سرد (۱۹۱۷ تا ۱۹۹۱) به وقوع پیوسته‌اند.
در مورد تاریخچه جنگ‌های سایبری باید به نکات ذیل توجه نمائیم:
- ریز مستندات این جنگ‌ها (نحوه عمل، نتایج و آثار و ...) بعنوان اسناد با سطح محرمانگی بالا تلقی گردیده و هرگز فاش نمی‌گردند.
- برخی از کارشناسان تمام تهدیدات بزرگ اینترنتی نظیر Code Red و Blaster و انواع اقسام کرمها (worms) را حملات و جنگ‌های اینترنتی می‌پندارند. با این تفسیر، تعداد و حجم حملات قابل ثبت چندین ده هزار برابر خواهد شد.
- به نوعی می توان ادعا نمود که تا به حال هیچ جنگ بزرگ و تمام عیار سایبر رخ نداده است، چیزی که آن را جنگ جهانی سایبر می نامند.
اکنون به چند عنوان از جنگ‌های معروف و ثبت شده اینترنتی توجه نمائید:

۱- کره شمالی و آمریکا – از دهه ۱۹۸۰ – کره شمالی اقدام به تاسیس مدرسه هک با بیش از ۱۰۰ سرباز آموزش دیده می‌نماید. البته این عمل در حقیقت عکس العملی در برابر توان مضاعف دشمن است. جنگ‌های این دهه را می‌توان پی‌آمدهای مشخصی از جنگ سرد دانست.

۲- سال ۱۹۹۴ - حمله به مراکز هوائی-تحقیقاتی Rome در نیویورک و همزمان به انستیتو تحقیقات اتمی کره جنوبی و نهایتا مرکز علمی در لاتویا.

۳- سال ۱۹۹۵ - بانک معروف آمریکائی، CitiBank و گروه هکرهای روسی و از دست دادن چند صد هزار دلار. در نهایت حمله‌گرهای روسی شناسائی شده و بخشی از زیان‌ها جبران شد.

۴- سپتامبر سال ۱۹۹۹ – جنگ ۷۸ روزه. وزارت دفاع آمریکا، طرح حمله به شبکه‌های کامپیوتری "سرب" را ادامه می‌دهد. مرجع: رویتر.

۵- اوایل آگوست سال ۲۰۰۰ – هنگ کنگ و استفاده از جنگ سایبری علیه چین. مرجع:Straits Times. چین، هنگ کنگ را از ایالات کشور خود می‌داند. هنگ کنگ زمانی مستعمره انگلستان نیز بوده است.

۶- مارس و آوریل سال ۲۰۰۱ - آمریکا و چین بر سر موضوع تصادم هواپیمای تحقیقاتی آمریکا با جت چینی. مرجع: Wired News. اولین قربانی، سایت دولتی چین www.travelsichuan.gov.cn بود و درصد تخریب در چین، ۱۰ برابر آمریکا بود. البته نزدیک به ۱۰۰ حمله سایبر بین آمریکا و چین درگرفته است که این فقط یکی از آنهاست.

۷- یازدهم سپتامبر ۲۰۰۱ با هزاران علامت سوال. برج‌های تجارت جهانی فقط با بمب و برخورد هواپیما منهدم نشدند و طبق شواهد، حملات تروریستی این ماه در نیویورک و واشنگتن، (حداقل) دارای پشتوانه سایبری بوده است.

۸- ماه می سال ۲۰۰۳ – آمریکا و عراق بر سر موضوع جنگ عراق. این بیشتر یک جنگ سایبر تبلیغاتی بود تا نظامی.

۹- اوایل سپتامبر سال ۲۰۰۳ – چین علیه تایوان؛ چین مبادرت به حمله سایبری به دولت تایوان می‌نماید. منبع: تایپه تایمز. این حمله از طریق انتشار اسب‌های تروآ محقق گردید.

۱۰- اکتبر سال ۲۰۰۳ – حمله به یکی از بزرگترین فرودگاه‌های ایالات متحده آمریکا در بوستون/تگزاس. منبع: روزنامه گاردین.

محدوده جنگ سایبری

عملا محدوده‌ای را نمی‌توان برای جنگ سایبر تجسم نمود. حتی اگر اپراتورهای (منظور همان سربازان) این فضا را در مکان‌های فیزیکی قرار دهیم، بازهم محدودیت مکانی در بین نیست.

محدوده عملیاتی

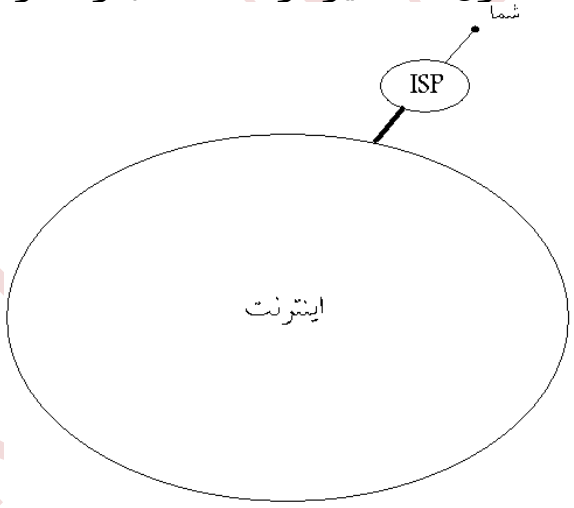
محدوده عملیات سایبر بسیار گسترده است؛ از تولید پارازیت مخابراتی گرفته تا عملیات روانی، از تغییر صفحات وب یک سایت گرفته تا بمباران ایمیلی. ولی نهایتا، اصل، تهدیدات منابع اطلاعاتی است به نحوی که امنیت ملی مورد مخاطره قرار گیرد. بنابراین بستر عملیات سایبر همانا زیرساخت‌های اطلاعاتی می‌باشد.
محدوه عملیات سایبر بطور مشخص در حدود منابع اطلاعاتی است ولی می‌تواند دربرگیرنده اشیاء خود حمله کننده نیز باشد و یا در محدوده سایبری دیگر عوامل وابسته یا غیر وابسته باشد. برای تفهیم بهتر به این سناریو دقت کنید:
. . . حمله کننده قصد دارد اقدام به دزدیدن اطلاعات و فروش آنها به شخص ثالث نماید . . . وی از طریق یک کانال واسط و ثالث نفوذ می‌کند و نهایتا اطلاعات نیز از همان کانال منتقل می‌شوند . . .
سناریوی فوق دقیقا نظیر نمونه حقیقی است که برای منابع اطاعاتی ایالات متحده آمریکا محقق گردید و در آن، حمله کننده برزیلی، اطلاعات را بطور غیر مستقیم با ولسطه اشیاء دیگر به جمهوری شوروی سابق می‌فروخت.
در مورد محدوده عملیاتی باید این نکته را مد نظر داشته باشیم که با انتخاب نادرست محدوده عملیات، بروز مشکل در محدوده سایبری خود حمله کننده

نیز محتمل است. این به علت نزدیکی و تداخل مرزهای سایبر است که در ادامه بیشتر روشن می‌گردد.
تصور کنید که حمله کننده سایبری مبادرت به تهاجم به یک سایت اینترنتی می‌نماید و نهایتا موجب پائین آمدن آن سایت می‌گردد...ولی علت پائین آمدن سایت هدف، انهدام (crash) سرور اصلی بوده است...و یکی از سرورهای محدوده جغرافیائی حمله کننده بطور ناخواسته در محدود عملیاتی بوده است...این مشکل به ویژه با انتشار و نامتمرکز بودن خدمات ثبت دامنه، میزبانی فضای وب، ثبت آدرس اینترنتی و ارائه پهنای باند بسیار محتمل و رایج است.
به محدوده‌هائی از عملیات سایبری توجه نمائید:

- اشیاء بسترساز شبکه (روترها، سوئیچ‌ها، ماهواره‌ها و ...)
- عناصر وب (سایت‌های وب، پایگاه‌های اطلاعاتی مبتی بر وب و ...)
- ایمیل، رایج‌ترین عنصر گذشته و حال در فضای سایبری

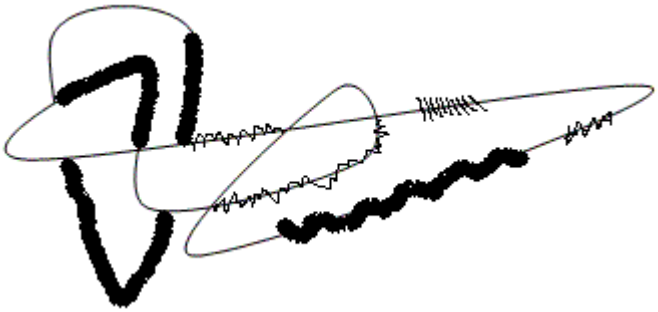
محدوده جغرافیائی

برای فضای سایبری نمی‌توان محدوده جغرافیائی تصور نمود. بنابراین جنگ سایبری نیز دارای مرز نیست. ولی درنظر داشته باشید که این تجسم به علت مقایسه مستقیم فضای سایبری با دنیای حقیقی و براساس دانسته‌ها و قراردادهای فیزیکی می‌باشد. در عمل، فضای سایبری نیز دارای مرز است.
تصور کنید که سیستم کامپیوتری شما از طریق خطوط تلفن شهری به اینترنت متصل باشد؛ اکنون شما نیز در فضای مجازی قرار دارید:



شکل: هنگام اتصال/ارتباط با اولین عنصر سایبری، در محدوده جغرافیائی آن قرار می‌گیریم

ولی مالکیت اشیاء درگیر بعضا کاملا مشخص است، لذا می‌توان مرزها را تعیین نمود. تنها تفاوتی که بین مرز سایبری با مرز حقیقی وجود دارد، همانا عدم محدودیت در ترسیم مرز و "مدار بسته بودن آن" است. به شکل صفحه بعد دقت کنید:



شکل: مرزهای مجازی با مرزهای فیزیکی متفاوت‌اند، ولی حضور دارند

در حقیقت مرزها در عین همبستگی، کاملا گسیخته هستند و این تصور نیز به سسب تجسم فیزیکی حاصل می‌گردد.

مشخصات عملیات سایبر

شاید بتوان مشخصه‌های یک عملیات سایبر را عینا از روی عملیات جنگی فیزیکی نمونه‌برداری نمود. نحوه عملکرد که همان حمله و دفاع است، باید دارای آیتم‌های ذیل باشد:

عملیات سایبر کاملا مشابه پایه های مقدماتی مبحث ایمنی و نفوذ است

۱- انگیزه

بدون شک، حمله‌کننده باید ابتدا دارای انگیزه‌ای مشخص باشد. امکان دارد این انگیزه مستقیما تولید شده (مانند زمانی که شما مورد حمله سایبر قرار گرفته باشید و در عین دفاع قصد دارید پیشروی کنید) یا به شکلی غیر مستقیم (مانند زمانی که یک نزاع سیاسی شما را به راه حمله می‌کشاند) نیرو وارد نماید. به هر صورت، باید انگیزه تعیین و تفسیر گردد، در غیر این صورت، مراحل بعدی دارای بستر و پایه منطقی نخواهند بود.

۲- هدف

با توجه به انگیزه حمله، محدوده عملیات مشخص می‌گردد. این همان چیزی است که آن را هدف یا Target می‌نامیم. هدف می‌تواند به بزرگی و گستره سیستم و شبکه توزیع نیرو در یک کشور باشد، و یا می‌تواند به کوچکی یک سیستم مشخص در یک شبکه محلی باشد. دقت نمائید که بزرگی و کوچکی هدف نیست که تعیین کننده ارزش آن است؛ در عملیات سایبر، یک هدف که در شکل فیزیکی بسیار کوچک است می‌تواند دارای ارزشی بزرگتر و بیشتر از یک پالایشگاه عظیم داشته باشد.

۳- جمع‌آوری اطلاعات

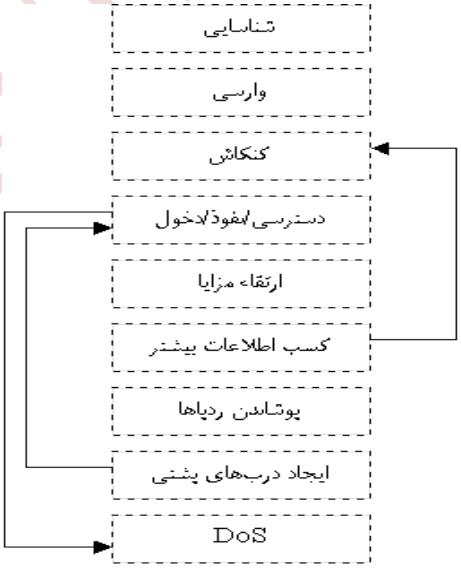
هر عملیاتی، چه فیزیکی و چه سایبر باید با چشمان کاملا باز صورت پذیرد. اجرای عملیات سایبر بدون اطلاعات مانند بمباران مکانی است که از مسکونی یا نظامی بودن آن مطلع نیستید؛ بدون اطلاعات فقط نیرو و منابع خود را از دست می‌دهید. ضمنا احتمال ردیابی و شناسائی خود را برای دشمن افزایش خواهیم داد.

کسب اطلاعات از عناصر سایبر بعنوان مهم‌ترین بخش از عملیات سایبر مورد توجه است. از دید کارشناسان، جمع‌آوری اطلاعات از اهداف سایبری به مفهموم انجام ۵۰درصد از کل عملیات است. در اینجا، اطلاعات به مفهوم

هر جنبه از هدف است که به نحوی با ایمنی سایبری آن در ارتباط باشد؛ بلوک‌ها و آدرس‌های اینترنتی/اینترانتی (IP Addresses)، اسامی دامنه‌های عمومی و خصوصی، سرویس‌های مبتنی بر پروتکل اینترنت (TCP/IP)، معماری سیستم‌ها و شبکه‌ها، مکانیسم‌های امنیتی و کنترل دسترسی، سیستم‌های شناسائی و ردیابی، شماره‌های تلفن، مکانیسم‌های تصدیق و ... ما این مرحله را به سه بخش شناسائی، وارسی و کنکاش تقسیم می‌نمائیم.
اصل Security through Obscurity را همیشه مد نظر داشته باشید

۴- نقاط ضعف
وقتی اطلاعات حمله کننده درباره ماهیت سایبری هدف کامل شد، مرحله تعیین نقاط ضعف آغاز می‌شود. این بخش از کار به واقع ساده‌ترین قسمت عملیات است. با دانستن مشخصات هدف، تعیین عیوب سخت‌افزاری و نرم‌افزاری چندان دشوار نبوده و فقط زمان لازم است. اگر دشمن در مورد شما به چنین مرحله‌ای برسد، فقط تیک تاک عقربه‌های ساعت را دنبال نمائید تا حمله آغاز شود!

۵- نفوذ
پس از تعیین نقاط ضعف و با در نظر گرفتن اطلاعات بدست آمده و با آگاهی از مکانیسم‌های ردیابی، عملیات سایبری در جهت نفوذ به هدف پیش می‌رود. این مرحله، اگرچه بخش پایانی عملیات است ولی زمان بیشتری را به خود اختصاص داده زیرا دارای قسمت‌های متعدد است.
عموما لفظ hack را با عبارت "نفوذ" همراه می‌کنند ولی منظور ما از نفوذ با عبارت دقیق Penetration همراه است. نفوذ همیشه به مفهوم دسترسی کامل به منابع هدف نیست؛ حمله کننده گاهی وادار به ارتقاء مزایا می‌گردد، مجبور می‌شود اطلاعات بیشتری کسب نماید، ردپاهای خود را بپوشاند، درب‌های پنهان و پشتی ایجاد نماید یا حتی در نهایت فقط به یک حمله DoS اکتفا نماید.



شکل: متدلوژی حمله سایبر

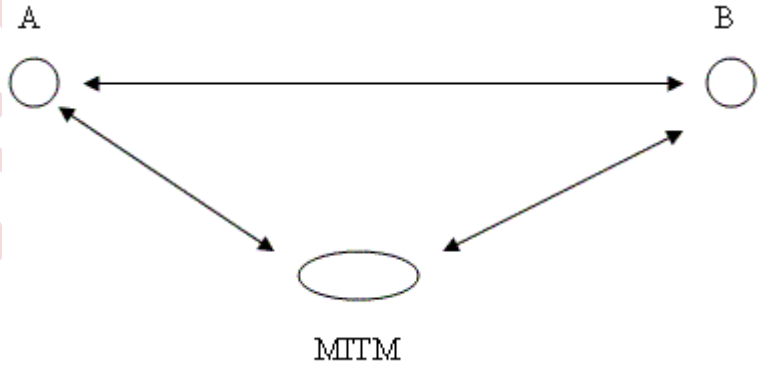
در مورد عملیات سایبری باید توجه داشته باشیم که تنها مدیوم رایج در این فضا، مدیوم شبکه‌های مبتنی بر TCP/IP نیست. در اینترانت‌ها ممکن است پروتکل‌ها و با عبارتی، عناصر سایبری متفاوتی حضور داشته باشند. ضمنا

هنوز هم رایج‌ترین مدیوم ارتباطی شبکه، خطوط تلفن شهری یا همان PSTN است. بنابراین حملاتی نظیر Wardialing یا جنگ با مودم‌ها به عنوان یک تهدید بزرگ محسوب می‌گردند.
مثال دیگر، مدیوم بدون سیم یا همان Wireless است که نوع عملیات موسوم به Wardriving را ایجاد می‌نماید.

ویژگی جنگ‌های سایبر

جنگ فیزیکی با جنگ سایبری از برخی جهات کاملا شبیه به هم هستند. مثلا هدف اصلی در جنگ، از هر نوع که می‌خواهد باشد، وارد آوردن ضرر و زیان به دشمن است. انگیزه اصلی در جنگ باید قاعدتا تصاحب منابع دشمن باشد. در حقیقت فلج نمودن دشمن بدون در اختیار گرفتن منابع آن چندان معقول به نظر نمی‌رسد.
بهترین روش برای شناخت ویژگی‌های جنگ سایبر این است که تصور و تجسم فیزیکی را از میان برداریم و صرفا سایبری تفکر کنیم. بیائید برای اینکه بهتر به این درک برسیم، فقط خصائص دیگر انواع جنگها را در کنار خصوصیات سایبری مشاهده کنیم:

۱- حمله از راه دور
اولین تفاوت جنگ سایبری با دیگر انواع جنگها و بالاخص جنگ فیزیکی و حقیقی، قابلیت طراحی، اجرا و نتیجه‌گیری از راه دور یا اصطلاحا به شکلی remote است.
برای حمله سایبری نیازی به حرکت فیزیکی ندارید و طبیعی است که این تفاوت از منشا فضای سایبری و حقیقی ناشی می‌گردد. سربازها و نقاط حمله می توانند در دنیا پخش شوند؛ نظیر عملی چنین تجسمی را می‌توان در حملات DoS به اثبات رساند.
بارزترین نشانه این ویژگی، انواع حملات موسوم به MITM یا MTM یا همان Man in the Middle است. در این حملات، مهاجم مابین دو منبع (معمولا معتمد) قرار گرفته و اطلاعات ایشان را ربوده یا صحت آنها را مورد مخاطره قرار می‌دهد.

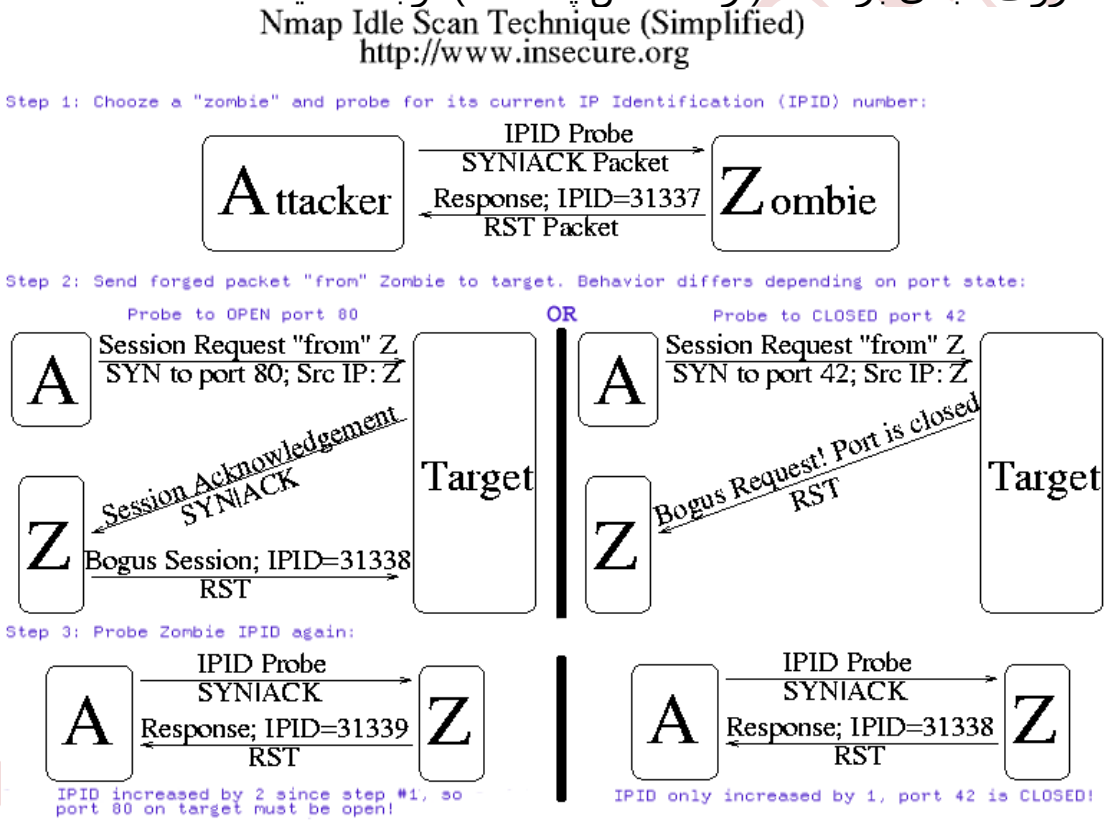


۲- دشواری در شناسائی و ردیابی
به سبب خصائصی که در ذات پروتکل‌های ارتباطی در فضای سایبری وجود دارد، عملا شناسائی و ردیابی منبع اصلی حمله و حمله کننده اصلی، بسیار دشوار و گاهی غیرممکن است. در حقیقت اگر در این خصوص، تشریک مساعی مرزهای سایبری را نادیده بانگاریم، شناسائی غیر ممکن است. به اسکلت هدر/فریم IP توجه نمائید:

4	8	16	32 bits
Ver.	IHL	Type of service	Total length
Identification		Flags	Fragment offset
Time to live	Protocol	Header checksum	
Source address			
Destination address			
Option + Padding			
Data			

شکل: اسکلت IP

تغییر فیلد آدرس مبداء یا همان Source Address و سپس تزریق پکت در شبکه به سادگی و حتی توسط کاربران بسیار مبتدی در اینترنت مقدور است. بنابراین مبداء ناشناس و مبهم خواهد ماند. به نمونه‌ای از حملات معروف مبتنی بر IPID (از خصائص پکت IP) توجه نمائید:



شکل: تکنیک وارسی IDLE در برنامه معروف Network Mapper

۳- محدودیت در انتقال

به سبب وابستگی فعلی فضای سایبری به معدود پروتکل‌های ارتباطی، انتقال و عوامل وابسته به آن (نظیر سرعت، حجم، کیفیت، اعتبار و ...) با چالش محدودیت در این پروسه روبرو هستند. بله، TCP/IP همچون چسبی تمام اینترنت را به هم متصل نموده است ولی این چسب (حتی در نسخه ششم) دارای نواقص و محدودیت‌هائی است.

۴- تهدید سه جنبه ایمنی

در جنگ فیزیکی، حمله کننده سعی در تهدید جنبه‌های فیزیکی زندگی انسان می‌نماید. در جنگ سایبری، تهدید یکی از سه جنبه ایمنی اطلاعاتی، شامل محرمانگی (Confidentiality)، صحت و تمامیت (Integrity) و در دسترس بودن (Availability)، موجب تهدید عنصر سایبر و اشیاء مرتبط با آن می‌گردد.

۵- اندازه هدف
بزرگی و کوچکی هدف/تارگت در جنگهای فیزیکی فوق العاده با اهمیت است. اگر قرار باشد پالایشگاه یا پمپ بنزینی هدف قرار گیرند، بدون شک اولویت با پالایشگاه است. ولی در جنگهای سایبری، بزرگی عناصر به با بزرگی حقیقی آنها قابل فهم و مقایسه نیست و باید اندازه سایبری آنها را مد نظر داشت.
در جنگهای فیزیکی به دنبال تخریب مناطق جغرافیائی بزرگتر هستند، ولی در جنگ سایبری باید اهداف مهم و اساسی "از نظر سایبری و نقش آنها در آن فضا" را هدف قرار داد. این اهداف ممکن است از نظر فیزیکی بسیار ناچیز باشند ولی نقش بزرگی در فضای سایبری ایفا نمایند.

٦- انتشار حمله
حمله سایبری می‌تواند به سادگی از چندین منبع/کانال صورت پذیرد. هدایت و راهبری حمله‌های فیزیکی که از چندین محل آغاز می‌گردند بسیار دشوار است ولی نظیر حملات سایبری DRDoS، DDoS و Mini-DDoS به سادگی و اثر زیاد و محسوس از چندین صد/هزار/ده هزار نقطه قابل اجرا هستند.

۷- هزینه
بدون شک هزینه جنگ حقیقی از جنگ سایبری بیشتر است و این خصوصیت بارز فضای سایبری است که عوامل و عناصر سهل الوصول‌تر و ارزان‌تر هستند.

۸- مسئولیت‌پذیری
از آنجائی که قوانین مدون و مشخص بین‌المللی برای مبارزه و ایجاد دعاوی سایبری وجود ندارد، کشورها به سادگی از زیر بار مسئولیت حملات سایبری خود شانه خالی می‌کنند. تنها هشت کشور عضو گروه هشت هستند که در این زمینه کمی با هم مدارا می‌نمایند.

۹- محدودیت در عناصر پایه
تنها عناصر پایه در یک جنگ سایبری، صفر و یک هستند. البته ذهن انسان را نیز نباید جدا دانست زیرا به هر شکل، فضای سایبری زائیده تفکر و خیال آدمی است.

۱۰- راهبری سهل
راهبری و هدایت جنگ سایبری به مراتب ساده‌تر از جنگ‌های حقیقی است. گاهی با فشار یک کلید و یا اشاره به یک شیء سایبری می‌توان آن را در موقعیت حمله و یا دفاع قرار داد؛ نیروها را گسترش داد یا عقب نشیتی نمود.

۱۱- پایان و شروع
پایان و شروع مشخصی برای اینگونه جنگ‌ها وجود ندارد. زیرا به سبب عوامل درگیر در جنگ که همگی دارای ماهیت سایبری هستند (یا می‌توانند باشند)، عملا شروع و خاتمه یا مجازی است و یا فوق العاده متعدد.

نیازهای عملیات سایبر

بدون شک عملیات سایبری دارای ملزومات خاص خود است؛ توان انسانی متخصص و تجهیزات مورد لزوم. البته اولین نیاز این نوع عملیات، حضور و اتصال در این فضا است. اشیائی که در فضای سایبری حضور نداشته باشند عملا هم از گزند حمله مصون هستند و هم خود هرگز مبادرت به حمله نمی‌نمایند.

نیروی انسانی، توان تخصصی

عمده‌ترین نیاز، توان تخصصی است ولی به یاد داشته باشیم که شرط لازم، داشتن اطلاعات از دشمن است. در مورد نیروی انسانی متخصص باید اذعان کنیم که کیفیت بیش از کمیت دارای اهمیت است. در حقیقت تعداد نیروی انسانی یک عملیات سایبری ملاک نیست بلکه متدهای مورد استفاده ایشان و نحوه عملکرد آنها مد نظر است.

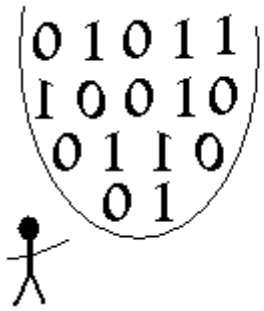
به هر صورت، نیروی انسانی، راهبر عملیات سایبری است. از طرح‌ریزی و جمع‌آوری اطلاعات گرفته تا تحلیل و اجرای حمله. بطور مشخص، اولین توان تخصصی مورد لزوم در یک عملیات سایبری، دانش شبکه یا اصطلاحا Networking است. سرباز سایبری باید بداند که بستر ارتباطی چگونه عمل می‌نماید و مدیوم شبکه دارای چه خصوصیات ذاتی است. در مورد اینترنت با تمام گستردگی آن، نقطه اتکاء پروتکل TCP/IP است. در این محیط باید حداقل با مدلهای ایترنتی (Shared Ethernet) و سوئیچی (Switched) آشنا بود.
دومین قابلیت مهم در یک عملیات سایبری، شناخت اجتماعات مختلف است، به عبارت دیگر، سربازان سایبری شما باید به نوعی مهندسان اجتماعی (Social Engineer) باشند. آمار و ارقام مستند حاکی از این موضوع هستند که مهندسی اجتماعی اکنون بالاترین تهدید فضای سایبر محسوب می‌گردد زیرا به شکل بسیار ظریفی بر تعامل بین این فضا و مجیط فیزیکی تکیه دارند.

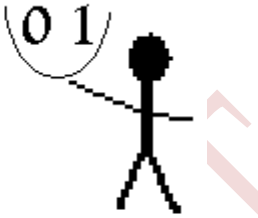
توان تجهیزاتی

مسلما تجهیزات عام یک عملیات سایبر همانا عناصر رایج و عمومی فضای سایبر هستند. ولی برای انجام حرکات خاص باید دارای تجهیزات خاص بود یا به عبارت دیگر باید عناصر خاصی از فضای سایبری را در دست داشت.
مثلا تصور نمائید که از ISPائی استفاده می‌نمائید که نوعی از پکت را رد نمی‌کند (Drop). مسلما تحت چنین شرایطی، شما عضو و عنصری ناقص از فضای سایبری محسوب می‌گردید و محتملا به مرزهای ناشناخته دسترسی ندارید.
ضمنا یکی از مهم‌ترین بخش‌های فضای سایبری، قدرت نقل و انتقال بوده که با عامل پهنای باند (bandwidth) ارتباط مستقیم دارد. در صورتیکه دارای

پهنای باند مکفی نباشید، باید از بسیاری از حملات چشم‌پوشی نموده و عملا نمی‌توانید در برابر انواع حملات DoS دفاع کنید.

توجه: بخشی از اجتماع سایبری را زیرزمینی یا اصطلاحا underground تلقی می‌نمایند. اگر توان صد در صد سایبری را مد نظر داشته باشیم، باید به تمام مناطق آن دسترسی داشته باشیم.





شکل: کدام سرباز سایبری قوی‌تر است؟!

ابزارها و سلاح‌های جنگ‌های سایبر

سلاح جنگ سایبری، مخلوطی از دانش و تجهیزات است. ما بر این باور هستیم که دانش تخصصی بالاترین اثر را دارد ولی بدون شک ابزار نیز ملزوم است.
در مورد استفاده از ابزار باید به این نکته توجه نمائیم که هرگز راه عکس را نپیمائیم؛ ابتدا باید تکنیک طراحی گردد و سپس ابزار آن تولید گردد.
با حضور در بزرگراه اطلاعاتی نظیر شبکه اینترنت، بسیاری از ابزارها، بدون صرف وقت زیادی در دسترس هستند و مجددا خاطر نشان می‌کنیم که نحوه استفاده از آنها و زمینه دانش مهم است.
ابزارهای جنگ‌های سایبر را می‌توان در اجتماع هکرها (Hacker Community) یافت. ضمنا توجه داشته باشید که جمع هکرها از بسیاری از ابزارهای جامعه ایمن‌گران برای تهدید ایشان استفاده می‌نمایند.
اگر بخواهیم سلاح‌های سایبر را دسته‌بندی نمائیم می‌توانیم گروه‌های ذیل را در نظر بگیریم:

۱- ابزارهای شناسائی
عموم سلاح‌های شناسائی در خود فضای سایبری یا همان اینترنت وجود دارند. قاعدتا اهداف سهل‌الوصول‌تر دارای ماهیت و هویت سایبری مشخصی بوده و می‌توان آن اهداف را به سادگی تعقیب نمود. به نمونه‌های کلی این ابزارهای توجه نمائید:

- اطلاعات عمومی
- موتورهای جستجوی دامنه‌ها
- ثبات دامنه اینترنتی
- ثبات آدرس اینترنتی
- تکنیک‌های Trace Routing
- ابزارهای شناسائی DNS
- ابزارهای شناسائی شبکه و همبندی آن
- ابزارهای متفرقه

۲- ابزارهای وارسی
وارسی هدف، همانند کوبیدن به دیوارها برای پیدا کردن درب‌ها و پنجره‌هاست. سرباز سایبری با اقدامات قبلی به لیستی از شبکه‌ها و آدرس‌های IP دست خواهد یافت و می‌دانیم که این تکنیک‌ها اطلاعات ذی قیمتی را برای وی فراهم خواهند نمود. با سلاح‌های وارسی باید سیستم‌های زنده و فعال (alive) و آنهایی را که از طریق اینترنت قابل دسترسی هستند (Internet Reachable) را مشخص نمود. به نمونه‌های عام این ابزارها توجه نمائید:

- انواع جاروب کننده‌ها (Sweep)
- انواع وارسی کننده‌های پورت‌های TCP و UDP

توجه:
- وقتی سربازان از ابزارهای وارسی استفاده می‌نمایند. (محتملا) اولین ردپاهای حاکی از یک حمله نزدیک، ثبت می‌گردد.
- در بخش سلاح‌های وارسی و تعقیب و شناسائی بطور مشخص از پروتکل ICMP بهره‌برداری بیشتری می‌گردد.
- تکنیک‌های وارسی پنهان و بدون صدا در این بخش، از اهمیت بالائی برخوردارند.

۳- ابزارهای کنکاش
سلاح‌های کنکاشگر عموما در خود سیستم‌های عامل حضور دارند. این ابزارها مبادرت به بیرون کشیدن اطلاعات خاص OSها و شبکه‌ها، نظیر عناصر کاربری و تولیدات نرم‌افزاری می‌نمایند.
هدف اصلی جنگجو بطور مشخص کسب اطلاعات بیشتر در خصوص منابعی است که شاید تابحال بر وی مستتر بوده‌اند ولی این اطلاعات در نظر اول کاملا بی‌ضرر به نظر می‌رسند: منابع اشتراکی (share)، کاربران (user)، گروه‌ها (group) و برنامه‌ها (application). به عناوین عام این ابزارها دقت نمائید:

- ابزارهای کنکاش در کاربران و گروه‌های فعال و غیرفعال یک سیستم عامل
- ابزارهای کنکاش در سیاست‌های احتمال حاضر و جاکم بر OSها
- ابزارهای ربودن و گرفتن نشانه‌ها (banner)

توجه: سربازان سایبر می‌دانند که تکنیک‌ها و ابزارهای این مرحله عموما نفوذی یا اصطلاحا intrusive هستند.

۴- ابزارهای نفوذ
همانطور که قبلا هم اشاره شد، با دارا بودن اطلاعات کافی از هدف، تکنیک و ابزار نفوذ چندان دور از دسترس نیست.

- ابزارهای صرفا سایبری
- سلاح‌های فیزیکی/سایبر. مانند امواج کوتاه و بلند دستکاری شده که موسوم به E-Bomb یا بمب الکترونیکی نیز می‌باشند. مانند سلاح‌های مایکرو-ویو و شتاب‌دهنده ها که قادرند پالس‌های ۱۰۰ نانو ثانیه‌ای از الکترون‌ها تولید نماید که هر پالس، ۱۰۰ها مگاوات قدرت دارد. و یا دستگاههایی موسوم به تفنگهای کامپیوتری که قادرند در فاصله ۱۰۰ متری خود هر سیستم الکترونیکی را از کار بیاندازد و حتی در فواصل کمتر باعث منهدم شدن مانیتورها شوند (تکنیک استفاده از HERF یا همان High

Energy Radio Frequency و فن‌آوری NEMP یا همان Nuclear Electro Magnetic Pulse).

۵- ابزارهای ارتقاء مزایا
حمله‌کننده همیشه پس از نفوذ به تمام امکانات هدف خود دسترسی ندارد. بنابراین باید به دنبال روش‌ها و ابزارهائی باشد تا مزیت وی را به روی هدف افزایش و ارتقاء دهند. به عناوین تکنیک‌های این گروه توجه نمائید:
- روش‌ها و ابزارهای تزریق
- متدهای فریبکارانه (Art of Deception)
- استراق سمع (Phreaking/Eavesdropping/Sniffing)

٦- سلاح‌های پنهان
گاهی نفوذ مجدد به یک هدف سایبری شامل تکرار تمام مراحل کنکاشگرانه و نفوذ است. لذا حمله کننده باید مبادرت به جادادن سلاح‌های پنهان نماید تا بعدا نیز به دخول نائل گردد. به عناوین این بخش از ابزارها توجه کنید:
- انواع اسب‌های تروآ
- انواع ویروس‌ها و کرم‌ها
- نقاط پنهان در سیستم‌های عامل

۷- جنگ افزارهای حملات DoS
شاید سرباز سایبری که نتواند نهایتا به عنصر سایبری نفوذ نماید، مبادرت به تعدید جنبه در دسترس بودن آن هدف نماید. بنابراین استفاده از متدها و ابزارهای حملات DoS محتمل است.

۸- سلاح مهندسی اجتماعی
برای بهره‌برداری از عیوب کاربران، شناخت ایشان لازم است و این شناخت براساس کنکاش در جامعهٔ دربرگیرنده آنها میسر می‌گردد؛ پروسه‌ای که آن را Social Engineering یا مهندسی اجتماعی می‌نامند (به نام حملات try-and-true و حملات masquerade هم شناخته می‌شود). شیوه کلاسیک اجرای چنین حملاتی با جا زدن اشیاء به جای اشیاء دیگر مورد اعتماد در مجموعه هدف است.
مهندسی اجتماعی، نیازی به استفاده از رایانه ندارد و سلاح‌های مهندسی اجتماعی، بخشی ابتدائی (low-tech) از فن‌آوری‌های پیشرفته فضای سایبری محسوب می‌گردند.

توجه:
- در تمام سلاح‌ها، آنکه قابلیت اسکریپت نمودن یا همان اتوماتیزه نمودن را دارد، دارای ارزش بیشتری نزد سربازان سایبری است.
- در نهایت، اغلب سلاح‌های سایبری مطلق، به دنبال تائید و جلب اعتماد هدف خود هستند (Trust) و این خصوصیا بارزی از فضای سایبری است؛ هر عنصری، تحت شرایط خاص، می‌تواند خود را به جای شیء دیگری جای بزند. ساده‌ترین نماد چنین برخوردی، حدس زدن کلمه رمز شیء است که به شما تعلق ندارد.

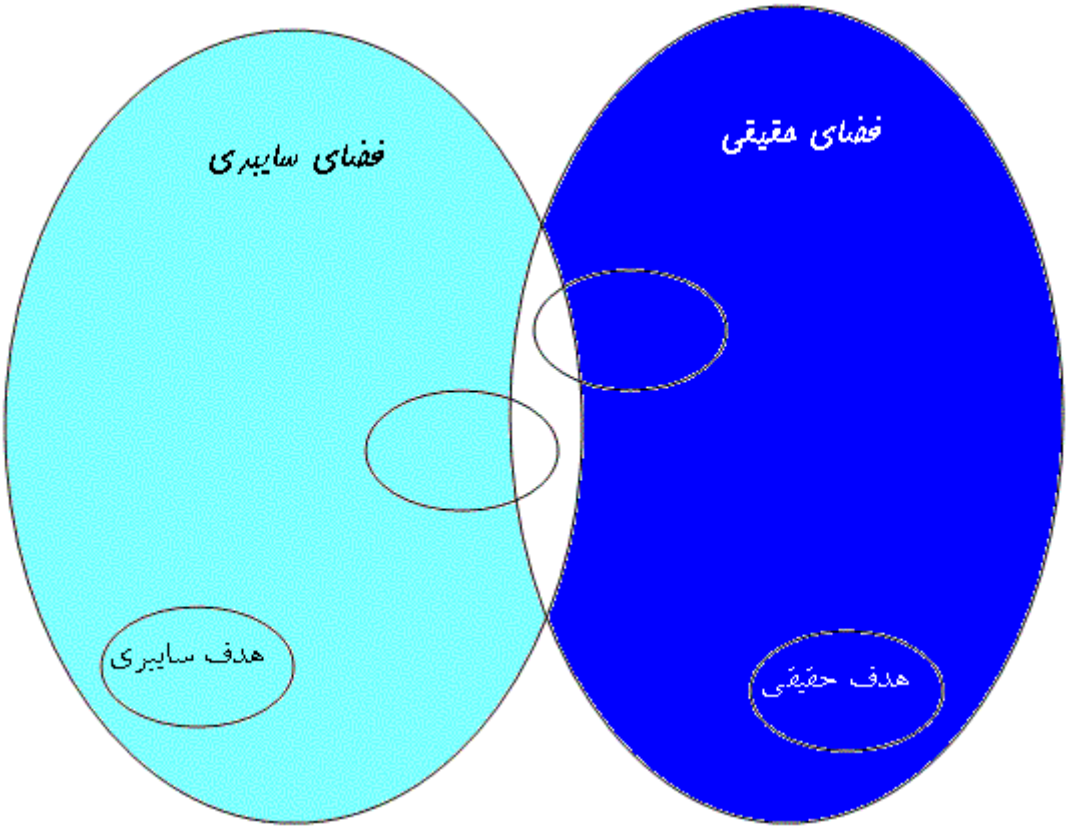
اهداف جنگ سایبر

مسلما اولین هدفی که در ذهن نقش می‌بندد، اهداف نظامی است. زیرا به هر شکل، هنوز هم در واقعیت، آنچه که به شکلی بسیار محکم با زندگی و بقای فیزیکی کشورها مرتبط است، نیروی نظامی آنهاست. ولی دومین نقطه توجه به عقیده کارشناسان و تجربه‌های بدست آمده، عناصر مرتبط با خدمات اجتماعی است.

در یک جنگ سایبری اهمیت خدمات اجتماعی به اندازه مراکز نظامی است

اینکه مهاجم سایبری هدفی اقتصادی و یا سیاسی را دنبال نموده و مورد حمله قرار می‌دهد یا اینکه بر اهداف نظامی و یا اجتماعی تکیه دارد، دقیقا بر انگیزه مبتنی است. آنچه که مسلم است این است که دشمن سعی خواهد کرد اهدافی را انتخاب نماید که بیشتر با فضای سایبری عجین هستند. چراکه مورد تهدید قرار دادن اهداف تنها و آنهائی که گسیخته از فضای سایبری هستند بطور مشخص دارای اثر (Impact) کمتری خواهد بود.

در حقیقت این انگیزه جنگ بعلاوه تعامل بین عناصر مرتبط سایبری (Information Component) و فیزیکی است که تعیین کننده هدف نهائی است. در اینجا ذکر این نکته بسیار مهم لازم است که اصولا مهاجم، قصد کدام بخش و عامل درگیر و مرتبط با انگیزه خود را دارد. اگر تجسمی کاملا سایبری داشته باشیم، هدف باید کاملا سایبری باشد؛ لذا اثر آن نیز در همان فضاست. ولی در عمل و آنچه که امروز شاهد آن هستیم، هنوز هم هدف نهائی بر تاثیر نهادن بر عوامل فیزیکی است.



شکل: تقابل و تعامل اهداف فیزیکی و سایبری

بنابراین حمله کننده در بهترین شرایط، اهدافی را منتخب می‌کند که تاثیر بیشتری بر عوامل فیزیکی و حقیقی زندگی ما داشته باشد تا اینکه صرفا

سایبری باشد. به سختی می‌توان فضای سایبری را از فضای فیزیکی جدا نمود؛ آیا می‌توان جنبه فیزیکی زندگی انسانها را نادیده انگاشت؟!
اگر بخواهیم فهرستی اجمالی از اهداف محتمل سایبری تهیه نمائیم باید چنین تصور کنیم:
- اهداف نظامی؛ در جهت بدست گیری یا صرفا فلج نمودن مکانیسم‌های دفاع و حمله فیزیکی. مانند سایت‌های موشکی.
- اهداف خدمات اجتماعی؛ با هدف تضعیف نیروی انسانی. مانند سوخت رسانی، تغذیه و ...
- نقاط درگیر با پروسه نقل و انتقال (چه سایبری و چه فیزیکی)، مخابرات و نیرو/انرژی (Denial of Power).

در دهه‌های ۱۹۷۰ و ۱۹۸۰ تروریست‌ها برای ایجاد درآمد اشخاص و هواپیماها را می‌ربودند. با امکان انتقال ارقام نجومی بصورت الکترونیکی، اکنون درآمد ایشان می‌تواند سهل‌تر، ایمن‌تر و بیشتر گردد

تائیرات جنگ‌های سایبر

میزان تاثیر چنین جنگی بستگی کامل به میزان تداخل فضای سایبری با فضای حقیقی دارد. هر چه از زیرساخت‌های اطلاعاتی مبتنی بر رایانه بیشتر استفاده گردد، تاثیر پذیری بیشتر است.
بدون شک انتخاب نوع هدف حمله کننده نیز بی تاثیر نیست. حمله به بانک اطلاعاتی یک بیمارستان را با حمله به برج مراقبت فرودگاه مقایسه نمائید.!
شاید بتوان کمترین اثر حمله سایبری را، از دسترس دور نمودن منابع سایبری دانست:
۱- در بهترین شرایط:
- حملات DoS
- ویروس‌ها و کرم‌های رایانه‌ای
۲- در شرایط خوب:
- حمله کننده‌ها به سیستمهای کامپیوتری دولتی نفوذ نموده و اسرار نظامی و فن‌آوری رمزبندی را می‌ربایند.
- خطوط نیرو مختل می‌گردند.
- سیستمهای اورژانسی مورد مخاطره قرار گرفته، بدین شکل سعی و کوشش در رساندن کمک و نجات مختل می‌گردد.
۳- در شرایط بد:
- فیبرهای نوری مابین نقاط اصلی تهدید می‌گردند.
- بمباران سرورهای دامنه و بانکها.
۴- در بدترین شرایط:
در نهایت: بمباران عناصر اینترنتی محقق گردیده و پائین آوردن اینترنت محتمل است. البته این دیدی صرفا سایبری است ولی تصور نمائید که میزان اشتراک فضای فیزیکی با سایبری بالا باشد.

نقاط آسیب‌پذیر در جنگ‌های سایبر

بدون شک نقاطی آسیب‌پذیرتر هستند که دارای درگیری بیشتری (ارتباطات و لینکها) در فضای سایبر هستند. در حقیقت میزان آسیب‌پذیری، ارتباط مستقیم با میزان وابستگی دارد. ولی بطور مشخص، عناصر تنها (سیستم‌های Stand-alone، شبکه‌های خصوصی و ...) در مقایسه با فضاهای عمومی (اینترنت، وب و...) امن تر هستند. هر چه وابستگی به سیستمهای اطلاعاتی رایانه‌ای افزایش یابد، ضعف در برابر چنگ سایبری افزایش خواهد یافت. در حقیقت نقص اصلی، در اتصال منابع اطلاعاتی اساسی به یکدیگر است. بنابراین کشورهائی آسیب‌پذیرتر هستند که دارای هویت سایبری محسوس‌تری هستند و هرگز نباید با کشوری وارد جنگ سایبر شد که دارای اشیاء محدودتر در این فضا است.

جنگ را بشناسیم و از آن دوری کنیم تا صلح و آرامش برای ملتها فراهم شود

توجه: این تنها نسخه حقیقی از تحلیل جنگ سایبر است که در دست دارید و نسخ دیگر فاقد اعتبار میباشد

پایان