جنگ سایبری

Cyber War

تهیه‌کننده: کاوه سیدمفیدی / سکیورتارگت
HTTP://SECURETARGET.IR
مارس/آوریل سال ۲۰۰۴

جنگ سایبری

فهرست

مقدمه

کیفر آنها که با خدا و پیامبرش به جنگ برمی‌خیزند و اقدام به فساد در روی زمین می‌کنند و با تهدید اسلحه به جان و مال و ناموس مردم حمله می‌برند، این است که اعدام شوند یا به دار آویخته گردند یا چهار انگشت از دست راست و پای چپ آنها بعکس یکدیگر بریده شود و یا از سرزمین خود تبعید گردند. این رسوائی آنها در دنیاست و در آخرت، مجازات عظیمی دارند.

قرآن کریم - سوره المائده - آیه ۳۳

ما بعنوان دارندگان دینی آسمانی و با کسب فرامین الهی از پیامبران و امامان خود، هرگز تیغ بر کس نکشیم که این راه و رسم مومنان حقیقی است. ولی دشمنان را ترسی از عقیده ما نیست. ایشان بر ما هجوم آورده و قصد جان و مال ما را خواهند نمود. پس در مقابل آنها می‌ایستیم و از دین و فرهنگ خود حفاظت می‌کنیم.

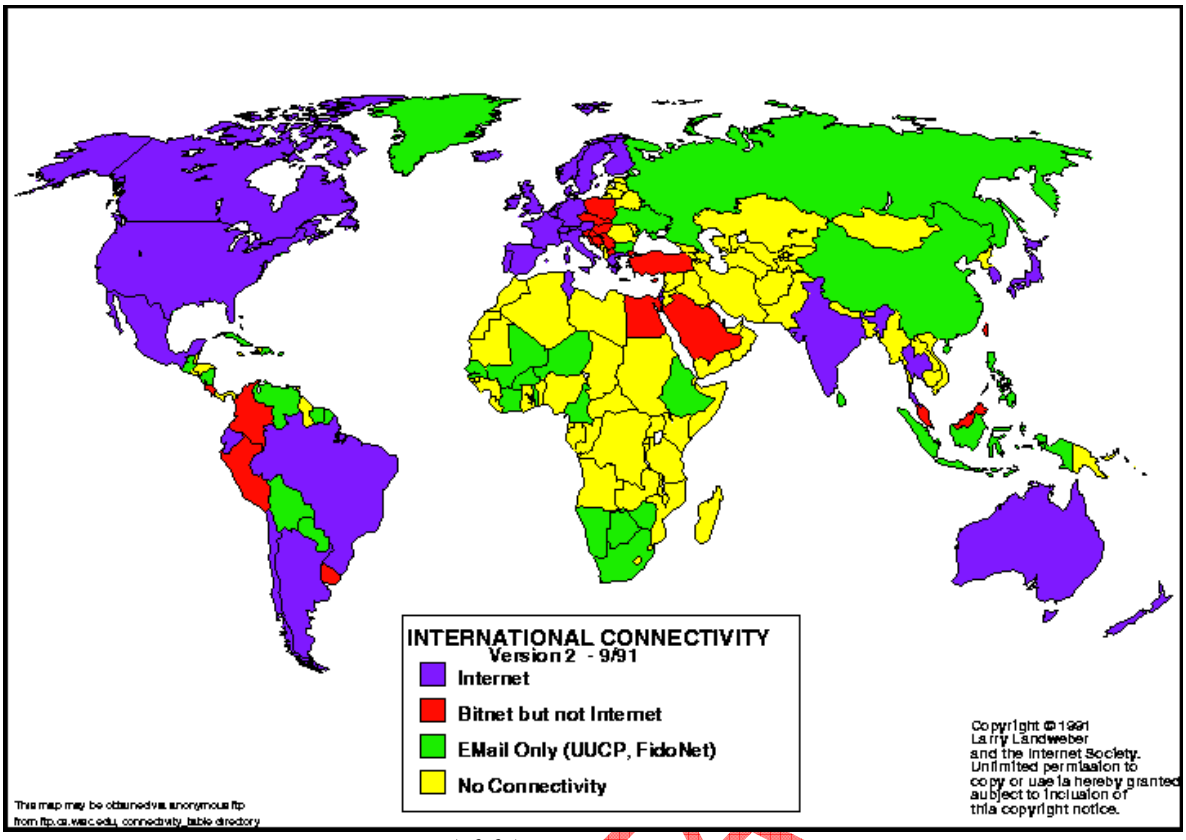
آری، به راستی چرا به جای صحبت از صلح و آسایش، به جنگ و ستیز بپردازیم؟ این گفته‌ای منطقی است ولی همواره اجتماعات انسانی در برابر گزند دشمنان خود معیوب بوده‌اند و این حقیقتی غیر قابل پوشش است. پس باید در برابر تهدیدات دشمن مقابله نمود و حتی گاهی بر وی حمله کرد.

نظر به مقوله امنیت و آسایش ملی، در هزاره‌ای که تمام نیروی دشمن متوجه و متمرکز بر تجاوز و رخنه است، امری کاملا محسوس و ملزوم است. بدون شک اکنون دشمن در حال طرح‌ریزی حمله است و تنها یک راه نفوذ کافیست تا وی به قصد خود نائل گردد.

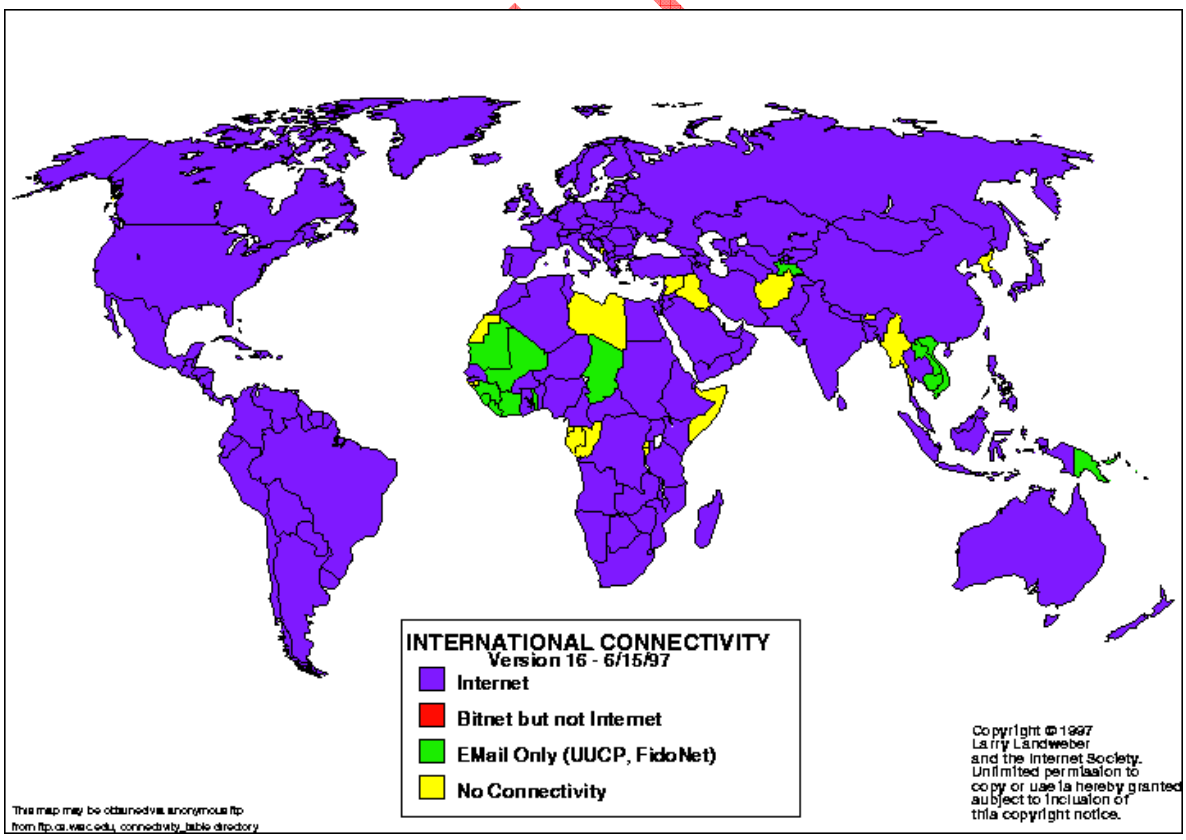
سربازان از مرزها حفاظت می‌کنند و مسئولین فرهنگی به تهاجم فرهنگی می‌اندیشند؛ اینها را با ما کاری نیست که اگر زمان آن فرا رسد، تفنگ بر دست گرفته و آتش می‌کنیم. ولی در دنیای امروز ما، تهدیدات و مخاطرات متعددی وجود دارند که عموما به آنها توجهی نمی‌شود.

امروز برای تضعیف دشمن لزومی ندارد حتما خطوط راهن آن را بمباران کنیم؛ یک مودم و یک PC کافیست!

با گسترش روز افزون استفاده از رایانه در دنیا، تشکیل و گسترش فضای مجازی و غیر فیزیکی به وقوع پیوسته است که غرق شدن در آن ناگزیر هر فرد انسان است. اکنون با استفاده همه جانبه از رایانه‌ها، فضای سایبر به اندازه کهکشان گستره دارد. پس باید در این گستره نیز نیرومند شد و توانائی مقابله با دشمن سایبری را داشت.



شکل: اینترنت، سپتامبر سال ۱۹۹۱ میلادی



شکل: اینترنت، ژوئن سال ۱۹۹۷ میلادی

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 . . . از دنیای مجازی خود، حفاظت کنیم.

توجه:

– در این مستند به کرات از اصطلاحات زبان انگلیسی استفاده شده است. هدف ارائه عناوین رایج این علم است و باید ایمان داشته باشیم که این تنها چالشی کوچک از حضور در فضای سایبری است.

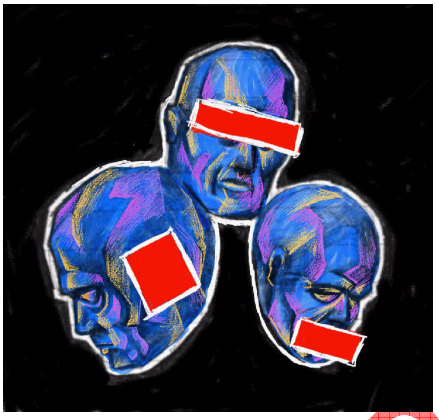
– اطلاعات مرتبط با مقوله جنگ سایبری معمولا فاش نمی‌گردد. لذا این مستند فقط بر شواهد موجود تکیه نموده و از حدس و گمان و یا دورغ و فریب دوری جسته است.

پس اگر در جنگ بر ایشان دست یافتی، چنان تار و مارشان کن که عبرت آیندگانشان شود؛ باشد که پند گیرند.
قرآن کریم – سوره الانغال – آیه ۵۷

مفاهیم اولیه

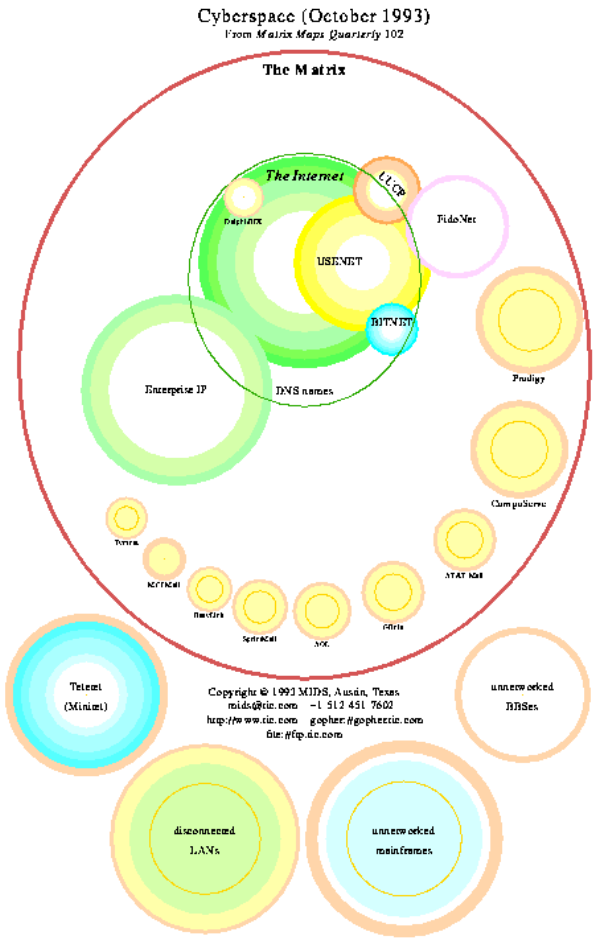
برای تفهیم جنگ سایبری ابتدا باید فضای سایبری و عناصر آن را ادراک نمائیم. بنابراین ابتدا ببینیم اصولا سایبر (Cyber) به چه مفهوم است:

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



شکل: تجسمی از عدم وجود حواس در فضای سایبری

اولین اصطلاح در این وادی، Cyber Space یا همان فضای سایبری است که استعاره‌ای برای تشریح سرزمین غیرفیزیکی تشکیل شده توسط سیستم‌های کامپیوتری می‌باشد. در فضای سایبری نمی‌توان بوئید یا شنید (منظور توسط حواس رایج 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 موشواره یا فشردن کلیدی در صفحه کلید.



شکل: فضای سایبری، اکتبر ۱۹۹۳ میلادی

تعریف جنگ سایبری (لغوی، اصطلاحی)

جنگ سایبری در لغت به معنای تهاجم بر عناصر سایبری 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. کما اینکه هر نوع جنگ دیگر 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.

خالی از لطف نیست که با لغات و اصطلاحات مشابه سایبری نیز آشنا شویم:

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

با دیگر لفات سایبری نیز آشنا شوید:

ایمنی سایبری (Cyber Security) – امنیت و آسایش سایبری نیز 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.

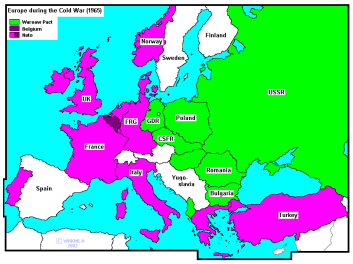
توجه:

– 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.

– نباید مقوله فضای سایبری را با اصطلاح سایبرنتیک (cybernetics) ادغام نمود. این لغت 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 سایبری در جهان و کشورهای مختلف از جمله کشور ایران

به گزارش منابع غربی، اولین جنگ سایبری در "کوزوو (Kosovo)" رخ داده است ولی چنین نیست! این ادعا به نوعی سبب پوشش جنگ‌های متعدد سایبری می‌گردد که همگی در دوران جنگ سرد (۱۹۱۷ تا ۱۹۹۱ در ۲۴ شکل و دوره متفاوت) به وقوع پیوسته‌اند. بنابر شواهد، اولین جنگ این چنینی، بین ایالات متحده آمریکا و شوروی (سابق) در اواسط دهه ۱۹۷۰ در گرفته است.



شکل: اروپا در دوران جنگ سرد

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. این مسئله تنها به شکلی بسیار نا محسوس در مورد جنگ‌های سال‌های ۲۰۰۲ و ۲۰۰۳ میلادی رعایت نگردیده‌اند و چه بسا در سال جاری میلادی با آشکار شدن اسناد بیشتری روربرو شویم.

– برخی از کارشناسان تمام تهدیدات بزرگ اینترنتی نظیر Code Red و Blaster را حملات و جنگ‌های اینترنتی می‌پندارند. با این تفسیر، رقم و حجم حملات قابل ثبت چندین هزار برابر خواهد شد.

– به نوعی می توان ادعا نمود که تا به حال هیچ جنگ بزرگ و تمام عیار سایبری رخ نداده است، چیزی که آن را جنگ جهانی سایبری می نامند.

حال به عناوین 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. بنابراین انگیزه‌ها کاملا مشخص هستند.

۲– سال ۱۹۹۴ – حمله به مراکز هوائی–تحقیقاتی Rome در نیویورک و همزمان به انستیتو تحقیقات اتمی کره جنوبی و نهایتا مرکزی علمی در لاتویا (از کشورهای تازه استقلال یافته شوروی سابق).

– شبکه در دستان حمله کننده‌ها بود ولی منبع آن کاملا نا مشخص بود تا اینکه ردی از انگلستان کشف شد.

۳– سال ۱۹۹۵ – بانک معروف آمریکائی، CitiBank و گروه هکرهای روسی و از دست دادن ۴۰۰هزار دلار! – در نهایت حمله‌گرهای روسی شناسائی شده و بخشی از زیان‌ها جبران شد.

۴– ماه می سال ۱۹۹۹ – براساس دستور بیل کلینتون، رئیس جمهور وقت ایالات متحده آمریکا، CIA طرح حمله به سیستم‌های رایانه‌ای یوگوسلاوی را پی‌ریزی می‌نماید. این همان جنگی است که به سبب فاش شدن اسرار آن، مقامات آمریکائی گریزی از آن نمی‌بینند و آن را

رسما تائید می‌نمایند؛ بله، گروهی از جنگ‌ها علیه "کوزوو" و "سربستان". مرجع: مجله Newsweek. از پیامدهای این جنگ می‌توان به موارد ذیل اشاره نمود:

- نفوذ به حساب‌های بانکی
- قطع نمودن خطوط تلفن
- تهدید مراکز سوخت‌رسانی و غذا

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

- اهداف: تهدید تسلیحات نظامی و خدمات اجتماعی

۶- 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 ولی آنها به دنبال استقلال بوده و هستند.

شکل: چین، سال ۲۰۰۳

- استفاده از ویروس‌ها در هدف قرار دادن مراکز انرژی، نظامی وبانک‌ها.
- ارائه نقشه هنگ کنگ/چین بدون تاریخ دقیق امکان پذیر نیست. هنگ کنگ زمانی مستعمره انگلستان نیز بوده است.

شکل: چین، سال ۱۹۸۴

۷- اسرائیل و فلسطین، جنگ اعراب و اسرائیل و نهایتا کشیده شدن جنگ به آمریکا.

- تهدید سایت‌های اینترنتی طرفین
- حملات متناوب DoS.
- حضور اعراب در برابر اسرائیل در این جنگ‌ها محسوس است. بنابراین نمی‌توان فقط فلسطین را مد نظر داشت.
- تکرار زمانی: اوایل نوامبر سال ۲۰۰۰ و اواسط آوریل ۲۰۰۲

توجه: DoS به مفهوم Denial of Service یا عدم قابلیت خدمت رسانی است.

۸- مارس و آوریل سال ۲۰۰۱ – آمریکا و چین بر سر موضوع تصادم هواپیمای جاسوسی آمریکا با جت چینی. مرجع: Wired News.
– سایت دولتی چین www.travelsichuan.gov.cn، اولین قربانی.
– این جنگ تا حدودی به اروپا نیز کشیده شد.
– درصد تخریب در چین، ۱۰ برابر آمریکا بود.
– نزدیک به ۱۰۰ حمله سایبری بین آمریکا و چین درگرفته است که این مشهورترین آنهاست.

۹- ۱۱ آوریل سال ۲۰۰۱ – آمریکا و روسیه. مرجع: روزنامه روسی به نام Moskovsky Komsomolets.
– استفاده از/استخدام هکرهای روسی برای نفوذ به شبکه خدمات امنیتی/کشوری روسیه

۱۰- یازدهم سپتامبر ۲۰۰۱ – یک شروع مجدد و هزاران علامت سوال.

شکل: برج‌های تجارت جهانی فقط با بمب منهدم نشدند!

طبق شواهد، حملات تروریستی این ماه در نیویورک و واشنگتن، حداقل دارای پشتوانه سایبری بوده است.
– آمریکا مسئولیت را بطور مشخص به گروه القاعده نسبت می‌دهد.
– شواهد نشانگر طرح‌ریزی بسیار دقیق و اجرای عملیات طی حدود یک سال نیم است.

۱۱- ماه می سال ۲۰۰۳ – آمریکا و عراق بر سر موضوع تجاوز به عراق.
– این بیشتر یک جنگ سایبری تبلیغاتی بود تا نظامی.

۱۲- 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.
– ایالات "هوبای" و "فوژان" چین بطور مشخص لشکرکشی نموده بودند.

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

۱۴- مارس سال ۲۰۰۴- آخرین جنگ دونفره! - Netsky و MyDoom - آیا حقیقتا دو نفر در این جنگ آسیب می‌بینند؟

۱۵- منبع ذیل را نیز برای دسترسی سریعتر مشاهده نمائید:

“ Resources | Oh, the humanity! A current list of 'cyber wars' “
http://vmyths.com/resource.cfm?id=23&page=1

بد نیست به آمار بسیار کوچکی از جنگ‌های سایبری توجه نمائید:

- سالانه ۲۵۰هزار جمله سایبری به مراکز نظامی آمریکا صورت می‌گیرد که فقط اندکی از آنها تاثیر گذار می‌شوند.
- سالانه حدود نیم میلیارد دلار به آمریکا خسارت وارد می‌شود.
- کارشناسان معتقد هستند در بین کشورهای پیشرفته، ژاپن به علت نداشتن سیاست‌های امنیت اطلاعاتی، یکی از ضعیف‌ترین اهداف سایبری محسوب می‌گردد.
- آخرین آمار از حملات ثبت شده ویروسی در دنیای سایبری (منبع: پستینی)

ردیف	نام ویروس	تعداد حمله
۱	netsky	۵۱۹۹۳۸۱۸
۲	mydoom	۲۶۷۹۷۷۷
۳	bagle	۱۹۸۳۹۹۶
۴	klez	۱۲۰۴۰۵۰
۵	dumaru	۱۲۰۲۴۰۰
۶	sober	۳۷۹۳۳۰
۷	swen	۲۶۸۹۸۶
۸	sobig	۱۶۶۴۷۹
۹	mimail	۱۵۴۰۹۰
۱۰	bugbear	۱۱۶۶۲۲

شکل: ۱۰ حمله ویروس برتر در مارس ۲۰۰۴

در ایران ما چه می‌گذارد؟

تابستان ۲۰۰۳، نیروهای مسلح ایران به عربستان سعودی نزدیک می شوند تا تولید نفت در خاور میانه را کنترل کنند. ایالات متحده متفقین خود را برای دفع ایران جمع می کند ولی ناگهان در می یابد که بطور مجازی و توسط کامپیوترهای مهاجم پنهان و غیرقابل ردیابی فلج شده است؛ آنها شبکه نیرو را می خوابانند ، باعث تصادم قطارها می شوند، تبادلات مالی را مختل می کنند و سیستمهای مخابرات را تهدید می نمایند. جنگ دوم خلیج فارس تبدیل به اولین جنگ سایبری می گردد.

فصل اول از رمان تام کلنسی

شواهدی از درگیری سایبری میان ایران و هیچ کشوری در دنیا در دست نیست ولی با توجه به اصول اولیه این جنگ‌ها، شاید ما مطلع نباشیم! تنها تاثیری از برخی جنگ‌های اینترنتی را می‌توان در ایران مشاهده کنیم. بطور مثال، جنگ معروف سال ۲۰۰۱ بین آمریکا و چین و نهایتا جنگ ماه می سال ۲۰۰۳ بین عراق و آمریکا که تاثیرات نه چندان عمیقی بر فضای سایبری ایران گذاشتند.

محدوده جنگ سایبری

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

. . . ملیت مفهومی ندارد زیرا می توان استخدام نمود و یا فقط جاسوسی را به کافی نت فرستاد . . .

محدوده عملیاتی

محدوده عملیات سایبری 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 دشمن مورد مخاطره قرار گیرد. بنابراین بستر عملیات سایبری همانا زیرساخت‌های اطلاعاتی می‌باشند.

محدوه عملیات سایبری بطور مشخص در حدود منابع دشمن است ولی می‌تواند دربرگیرنده اشیاء خود حمله کننده نیز باشد و یا در محدود سایبری دیگر عوامل وابسته یا غیر وابسته باشد. برای تفهیم بهتر به این سناریو دقت کنید:

. . . حمله کننده قصد دارد اقدام به دزدیدن اطلاعات دشمن و فروش آنها به شخص ثالث نماید . . . وی از طریق یک کانال واسط و ثالث به دشمن 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 سایبری است که در ادامه بیشتر روشن می‌گردد.

تصور کنید که حمله کننده سایبری مبادت 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.

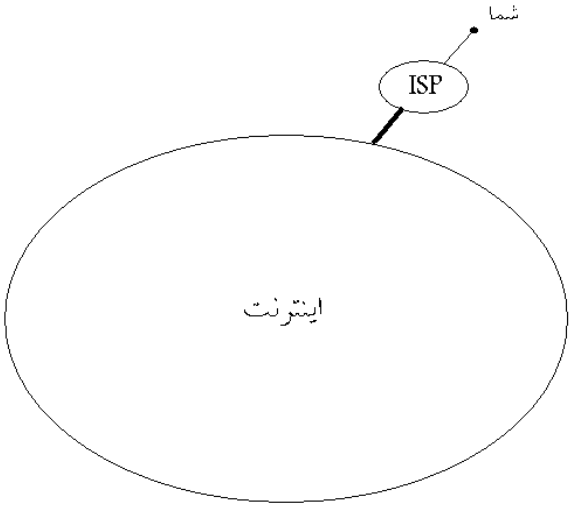
به محدوده‌هائی از عملیات سایبری توجه نمائید:

- 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

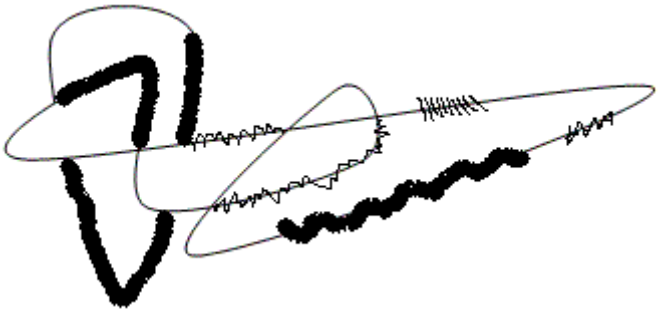
برای فضای سایبری نمی‌توان محدوده جغرافیائی تصور نمود. بنابراین جنگ سایبری نیز دارای مرز نیست. ولی درنظر داشته باشید که این تجسم به علت مقایسه مستقیم فضای سایبری با دنیای حقیقی و براساس دانسته‌ها و قراردادهای فیزیکی می‌باشد. در عمل، فضای سایبری نیز دارای مرز است.

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:



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

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

مشخصات عملیات سایبری

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

عملیات سایبری کاملا مشابه روند مقدماتی 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 سایبری 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 سایبری، یک هدف که در شکل فیزیکی بسیار کوچک است می‌تواند دارای ارزشی بزرگتر و بیشتر از یک پالایشگاه داشته باشد.

۳- جمع‌آوری اطلاعات

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

کسب اطلاعات از عناصر سایبری دشمن بعنوان مهم‌ترین بخش از عملیات سایبری 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

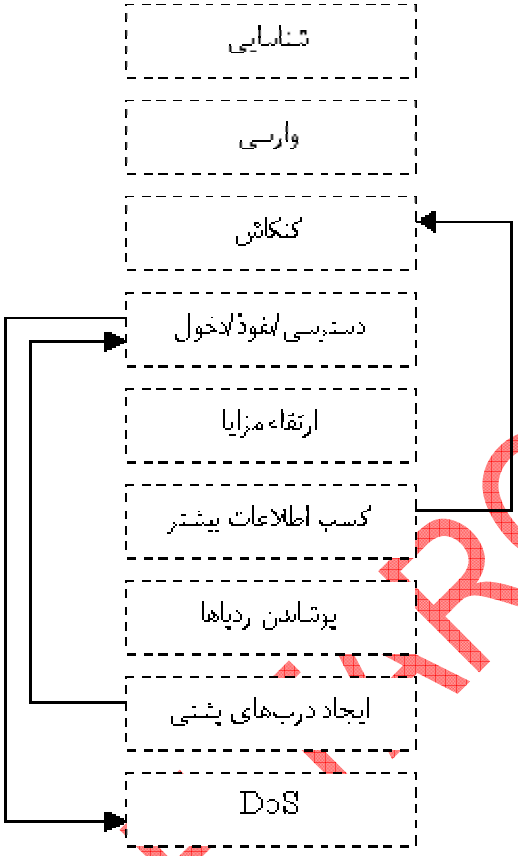
۴- نقاط ضعف

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 سایبری

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.

ویژگیهای جنگ‌های سایبری نسبت به سایر انواع جنگ‌ها

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.

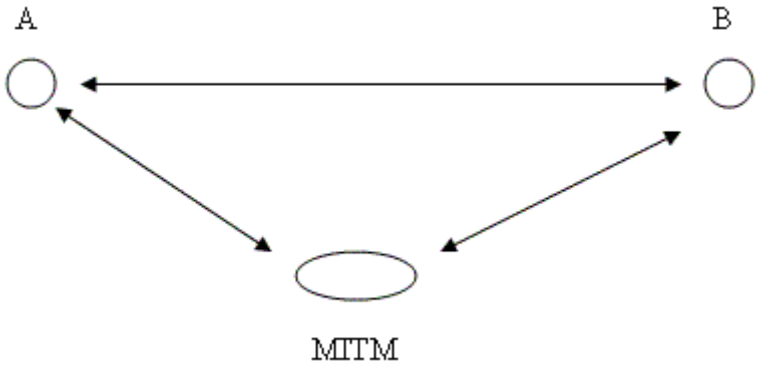
بهترین روش برای شناخت ویژگی‌های جنگ سایبری این است که تصور و تجسم فیزیکی را از میان برداریم و صرفا سایبری تفکر نمائیم. بیائید برای اینکه بهتر به این درک برسیم، فقط خصائص دیگر انواع جنگها را در کنار خصوصیات سایبری مشاهده کنیم:

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.



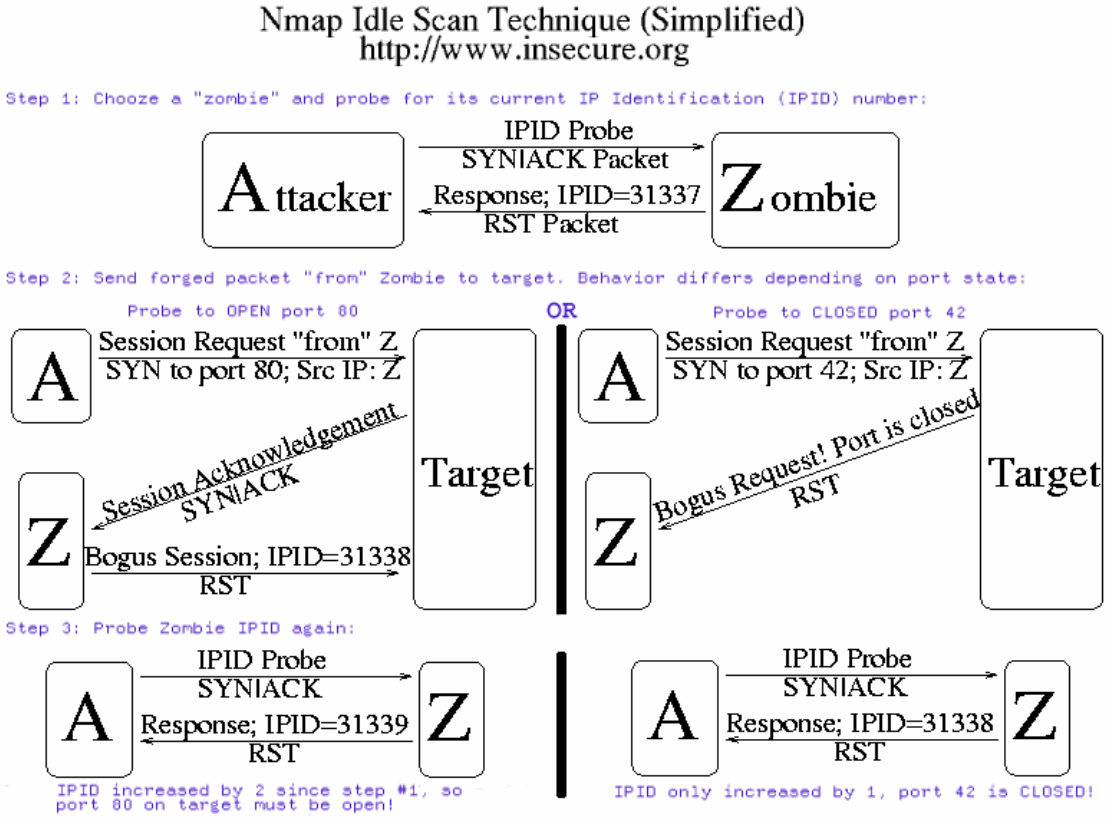
۲- دشواری در شناسائی و ردیابی

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

تشریک مساعی در شناسائی و ردیابی (مانند حملات داس و استفاده از لاگها در روترهای میان راه)

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 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 سایبری 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.

۶- 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 DDoS، DRDoS 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.

Information Warfare: Zeroes I Win, One you lose

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.

نیازمندی‌های یک عملیات سایبری

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.

شکل: سربازان قدیم

شکل: سربازان جدید

شکل: سربازان سایبری

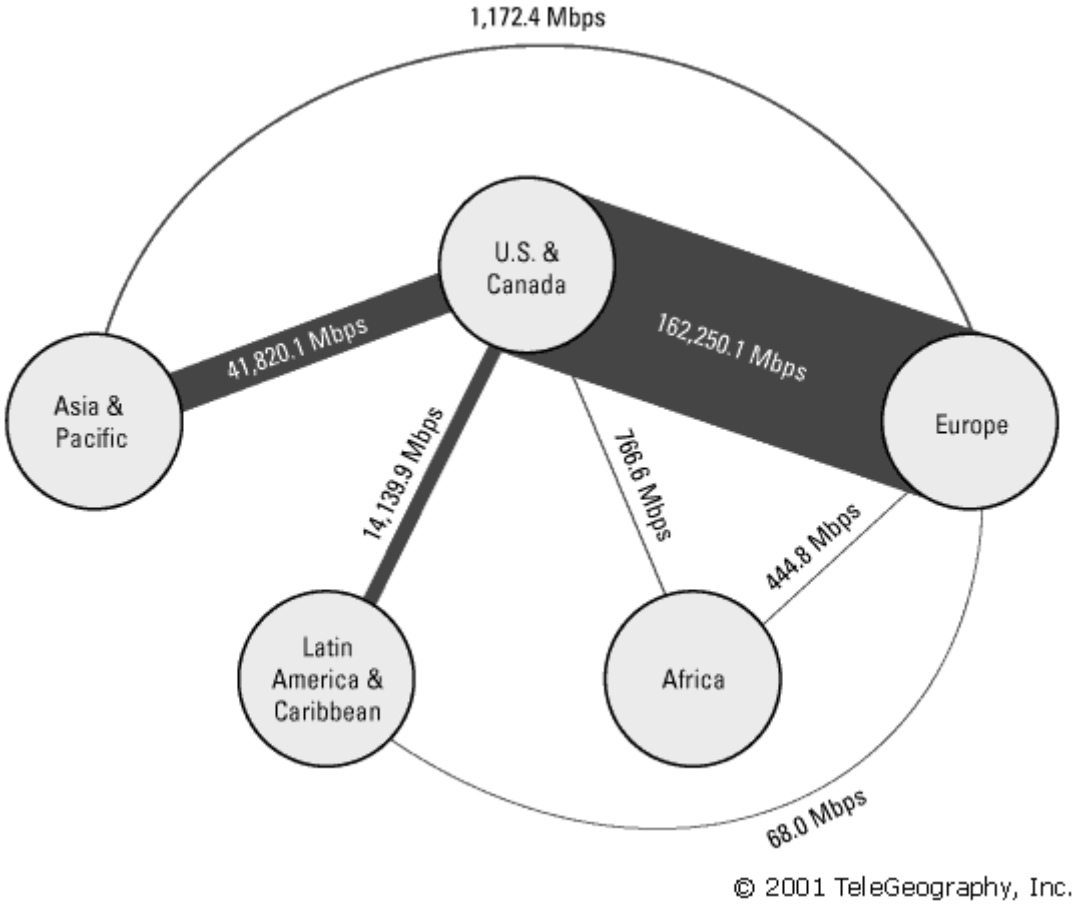
به هر صورت، نیروی انسانی، راهبر عملیات سایبری است. از طرح‌ریزی و جمع‌آوری اطلاعات گرفته تا تحلیل و اجرای حمله. بطور مشخص، اولین توان تخصصی مورد لزوم در یک عملیات سایبری، دانش شبکه یا اصطلاحا Networking است. سرباز سایبری باید بداند که بستر ارتباطی چگونه عمل می‌نماید و مدیوم شبکه دارای چه خصوصیات ذاتی است. در مورد اینترنت با تمام گستردگی آن، نقطه اتکاء پروتکل TCP/IP است. در این محیط باید حداقل با مدلهای اینترنتی (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 سایبری محسوب می‌گردند زیرا به شکل بسیار ظریفی بر تعامل بین این فضا و محیط فیزیکی تکیه دارند.

توان تجهیزاتی

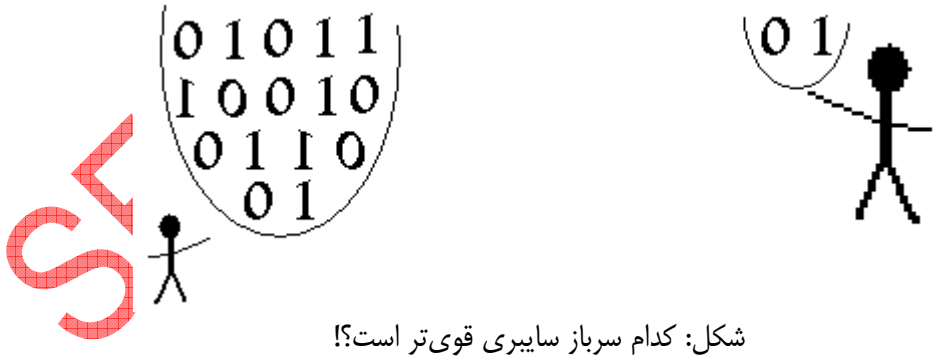
مسلما تجهیزات عام یک عملیات سایبری همانا عناصر رایج و عمومی فضای سایبری هستند. ولی برای انجام حرکات خاص باید دارای تجهیزات خاص بود یا به عبارت دیگر باید عناصر خاصی از فضای سایبری را در دست داشت.

مثلا تصور نمائید که از ISPائی استفاده می‌نمائید که مبادرت به سانسور نمودن صفحات وب نموده یا 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.



شکل: پهنای باند خطوط ارتباطی اصلی، سال ۲۰۰۱

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؟!

ابزار و سلاح‌های جنگ‌های سایبری

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 سایبری را می‌توان در اجتماع نفوذگران (Hacker Community) یافت. ضمنا توجه داشته باشید که اجتماع نفوذگران از بسیاری از ابزارهای جامعه ایمن‌گران برای تهدید ایشان استفاده می‌نمایند.

اگر بخواهیم سلاح‌های سایبری 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 می‌گردند.
- 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 کنکاشکر عموما در خورد سیستم‌های عامل حضور دارند. این ابزارها مبادرست 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:

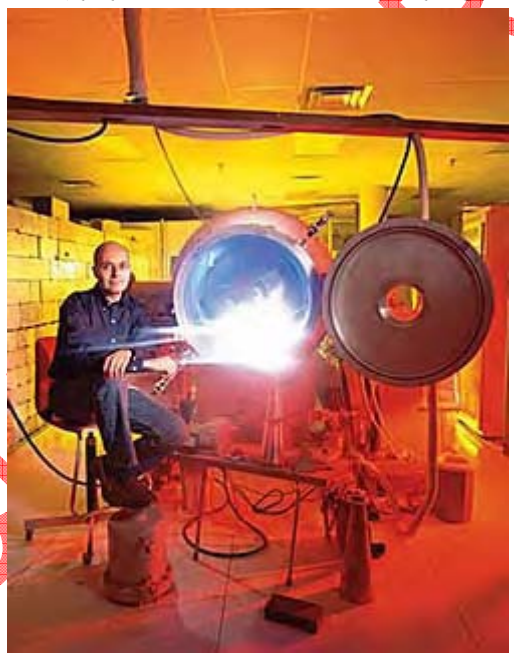
- ابزارهای کنکاش در کاربران و گروه‌های فعال و غیرفعال یک سیستم عامل
- ابزارهای کنکاش در سیاست‌های احتمال حاضر و جاکم بر OSها
- ابزارهای ربودن و گرفتن نشانه‌ها (banner)

توجه: سربازان سایبری 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/سایبری. مانند امواج کوتاه و بلند دستکاری شده که موسوم به E-Bomb یا بمب الکترونیکی نیز می‌باشند.



شکل: محقق سلاح‌های مایکرو-ویو، Edl Schamiloglu در کنار شتاب‌دهنده خود موسوم به Pulserad-110A در دانشگاه نیومکزیکو نشسته است. این ابزار قادر است پالس‌های ۱۰۰ نانو ثانیه‌ای از الکترون‌ها تولید نماید که هر پالس، ۱۰۰ها مگاوات قدرت دارند.

The computer-killing 'gun' featured at InfowarCon.

شکل: دستگاهی موسوم به تفنگ کامپیوتری که شخصی به نام David Schriner در اواسط سال ۱۹۹۹ میلادی در نمایشگاهی در واشینگتون به نمایش گذاشته شد. این تفنگ نابودکننده قادر بود در فاصله ۱۰۰ متری خود هر سیستم الکترونیکی را از کار بیاندازد و حتی در فواصل کمتر باعث منهدم شدن مانیتورها شده بود. هزینه ساخت این دستگاه مخرب حدود ۵۰۰ دلار آمریکا برآورد شد و تکنیک استفاده از HERF یا همان High Energy Radio Frequency را دارا بود.

جدیدترین انواع این سلاح‌ها را با فن‌آوری NEMP یا همان Nuclear Electro Magnetic Pulse تولید می‌نمایند.

– 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)

– 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

– 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.

– 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.

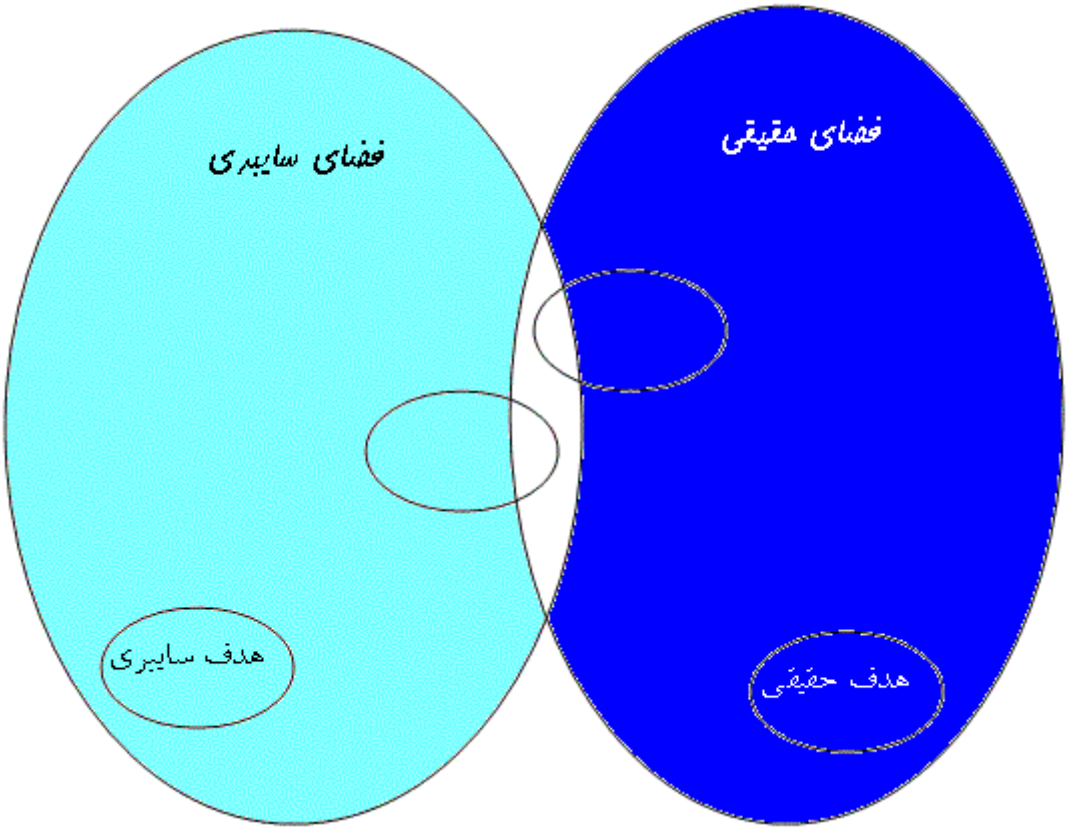
اهداف جنگ سایبری

مسلما اولین هدفی که در ذهن نقش می‌بندد، اهداف نظاامی 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 جمله 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 مبادرت به ربودن اشخاص و هواپیماها می‌نمودند، با انتقال ارقام نجومی بصورت الکترونیکی، اکنون درآمد ایشان می‌تواند سهل‌تر، ایمن‌تر و بیشتر گردد.

تاثیرات جنگ‌های سایبری

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 نقطه و 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.

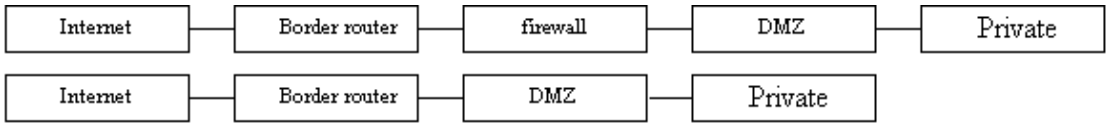
– بمباران سرورهای دامنه و بانکها.

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 سایبری

بدون شک نقاطی آسیب‌پذیرتر هستند که دارای درگیری بیشتری در فضای سایبری 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.



شکل: مسلما عناصر DMZ در خطر بیشتری قرار دارند

میزان آسیب پذیری ایران

با توجه به توانمندی ایران در IT میزان آسیب پذیری ایران در حوزه های نظامی، اقتصادی، اجتماعی و صنعتی کشور چندان زیاد نیست. البته متاسفانه دولت ایران هیچ سیاست و استراتژی مدون و مشخصی برای امنیت اطلاعات ندارد. در حقیقت اگر هم برخی مراکز اقدامی کرده اند یا می کنند، نظیر بازی فوتبالی است که هر کدام از بازیکنان فقط بی هدف توپ را شلیک می کنند، حال به هر طرف رفت، که رفت.

هر چه وابستگی به سیستمهای اطلاعاتی رایانه‌ای افزایش یابد، ضعف در برابر چنگ سایبری افزایش خواهد یافت.

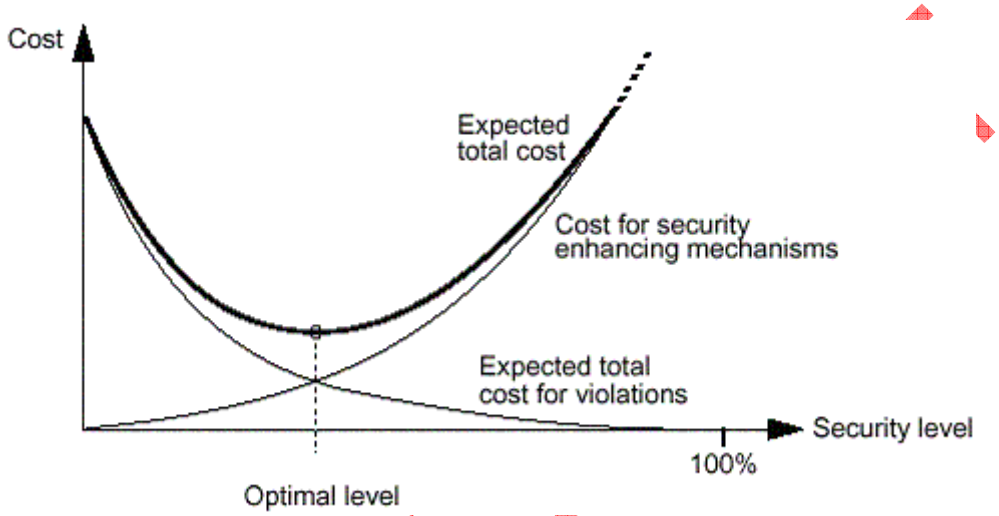
در حقیقت نقص اصلی، در اتصال منابع اطلاعاتی اساسی به یکدیگر است.

عملا ایالات متحده آمریکا مالک منابع اصلی سایبری بوده و به نواع مالک فضای سایبری است.

راه‌های جلوگیری یا پدافند جنگ سایبری

بهترین دفاع و حمله در جنگ سایبری همانا بالا بردن سطح ایمنی عناصر درگیر است و این میسر نخواهد بود، جز با افزایش اطلاعات. ولی به راستی جه سطح از ایمنی برای اشیاء سایبری ملزوم است؟ آیا باید هر عنصری را تا حد توان خود حفاظت نمائیم و آیا تمام عناصر دارای ارزش یکسان امنیتی هستند؟

جواب این سوال بسیار کوتاه، در صدها صفحه در استانداردهای امنیتی فعلی (ISO 17799, BS 7799) آمده است. بطور خلاصه می‌توان اینگونه بیان نمود که هر یک از عناصر درگیر در فضای سایبری (فن‌آوری اطلاعاتی)، باید به اندازه ارزش خود حفاظت گردند. در غیر این صورت، انتخاب مکانیسم‌های دفاعی چندان بهینه نخواهد بود و بدون شک دارای هزینه‌های سربار است.



شکل: انتخاب نقطه بهینه در ایمن‌سازی اشیاء سایبری

البته این موضوع بر دفاع سایبری حاکم است و اگر قصد حمله را داشته باشیم باید تا دندان مسلح شویم. پس باید ابتدا دارائی‌ها و عناصر اصلی و اساسی اطلاعاتی (اشیاء مهم در فضای سایبری) را تعریف و تعیین نموده و براساس سیاست‌های کلان و با در نظر گرفتن تهدیدات موجود در برابر آن عناصر، تمهیدات دفاعی را پی‌ریزی نمائیم.

نکات مهم:

- نکته مهم در دفاع، همکاری دولت با تجارت عمومی و خصوص است.
- تمهیدات دفاعی، ساده‌تر و ارزان‌تر هستند. یک تیم مجرب در امور امنیتی به مراتب ارزانتر از یک خلبان است.

جمع‌بندی

- تهدید و جنگ سایبری را باید به اندازه نمونه‌های فیزیکی مهم پنداشت.
- فضای سایبری را نمی‌توان مطلق تصور نمود.
- علی‌رغم خالص دانستن فضای سایبری، فاکتور انسانی را نمی‌توان در نظر نگرفت.
- مسلما کشورهائی آسیب‌پذیرتر هستند که دارای هویت سایبری محسوس‌تری هستند.
- جنگ و نزاع هرگز و در هیچ زمانی به نفع هیچ کشوری نبوده است.
- علی‌رغم وسعت فضای سایبری در ایران، لزوم افزایش توانمندی‌های کشورمان بسیار محسوس است.
- هرگز نباید با کشوری وارد جنگ سایبری شد که دارای اشیاء محدودتر در این فضا است.

توصیه‌های شخصی تهیه‌کننده جهت مقابله با حملات سایبری

ما فاقد کارشناسان حرفه‌ای در امور امنیتی رایانه‌ها نیستیم؛ تنها چالش موجود، مدیریت بهینه منابع انسانی متخصص است. لذا توصیه‌های ذیل را کامل و مکفی تلقی ننمائید.

مراکز و مسئولین تصمیم‌گیری IT کشور

- اشتراک، همکاری و ارتباط میان آژانس‌های سری و اطلاعاتی کشور
- گزینش استانداردها و استفاده از استانداردهای ISO
- اطلاع‌رسانی
- تقویت متخصصین رایانه در جهت فراگیری زبان‌های انگلیسی، روسی و چینی
- حفاظت از زیرساخت‌های اصلی (Critical Infrastructure Protection) و مشخصا زیرساخت‌های فن‌آوری اطلاعاتی کشور
- عدم تکیه مطلق بر هرگونه منبع خارجی و غیر معتمد و انتخاب مدل Trust بهینه و مقتضی
- تعلیم و تربیت و بکارگیری متخصصین علوم سایبری از جنبه‌های فنی و حقوقی تا مجریان قانون
- افزایش مکانیسم‌های کنترل و مانیتورینگ و تخصصی نمودن قابلیت‌های ردیابی و جمع‌آوری مدرک
- آزمایش و انتخاب فن‌آوری‌های جدید و تطبیق آنها با نیازهای امنیتی کشور
- تدوین و تثبیت قوانین داخلی
- برخورد جدی با مجرمین داخلی
- تدوین و بکارگیری و اعمال سیاست‌های مرتبط

کارشناسان و متخصصین IT کشور

- طراحی استانداردها و الگوهای رمزنگاری ایرانی؛ این بدان مفهوم نیست که الگوهای فعلی/غربی به نا کارآمد هستند، بلکه به کار ما نمی‌آیند. مثلا فن‌آوری پیشرفته و بسیار مستحکم در رمزنگاری PGP (Pretty Good Privacy) در دستان وازرت دفاع آمریکا است.
- تبعیت از اصول ایمنی و حفاظت شامل مکانیسم‌های جلوگیری (Prevention)، ردیابی (Detection) و ترمیم (Recovery)
- استفاده گسترده‌تر از IDSها و NIDSها در جهت تقویت امر کنترل و ردیابی
- بکارگیری هانی‌نت (HoneyNet) در جهت تحقیق و توسعه فنون نظامی سایبری
- تحقیق و نفحص (R&D)؛ راه حل ایمنی همیشه ساده است. کارشناسان معتقدند گروه تروریستی القاعدا به سادگی با جا دادن اطلاعات رمز شده در عکس‌ها (BMP, JPEG, TIFF, GIF, ...)، مبادرت به تبادل ایمن آنها می‌نموده‌اند.

کاربران شبکه های رایانه‌ای

- همکاری و اجرای صحیح سیاست‌های دولت
- تقویت و حفاظت از مسائل خصوصی یا همان Privacy، تنها شکل تهدید کاربران نهائی فضای سایبری است. بنابراین ایشان باید در حفظ آن بکوشند.

توصیه‌هائی برای همگان

۱- عدم انتقال اطلاعات (حتی طبقه بندی نشده) نظامی در اینترنت.

۲- بخاطر داشته باشیم که اندازه ایمنی ما به مقدار ضعیف‌ترین نقطه است.

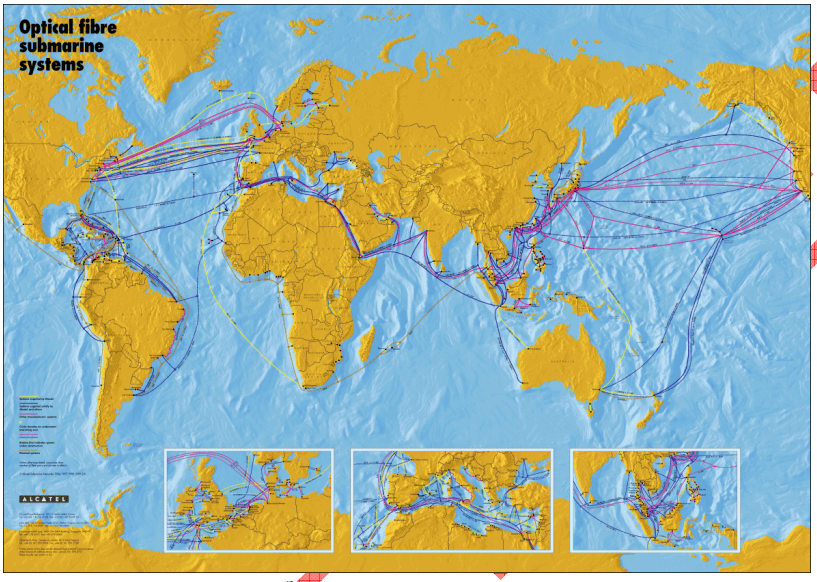
یافته‌های تخصصی تهیه‌کننده

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

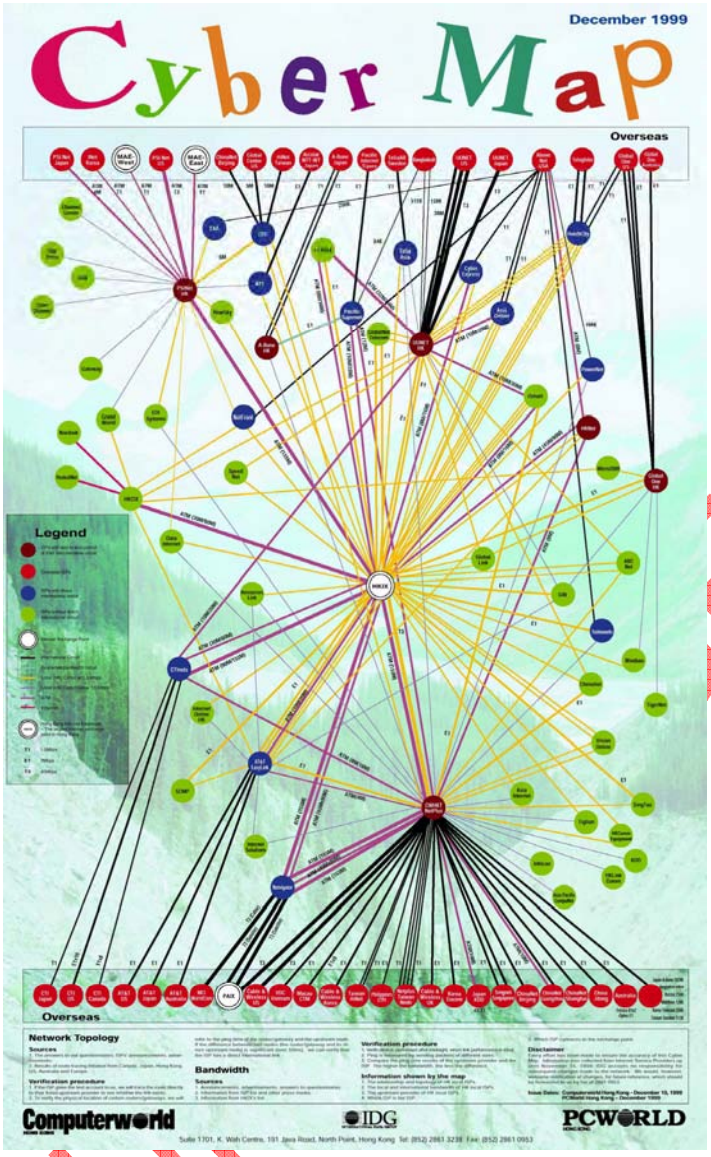
ناپلئون بناپارت

– برای بودن در فضای سایبری باید نقشه آن را دانست (CyberAtlas, CyberGeography)

چگونه می‌توان از منابع مهم حفاظت نمود بدون آنکه نحوه قرارگیری و ارتباط آنها را با هم بدانیم؟! لذا ترسیم و تشبیه فضای سایبری فوق العاده دارای اهمیت است.



شکل: فیبرهای نوری زیر آبی



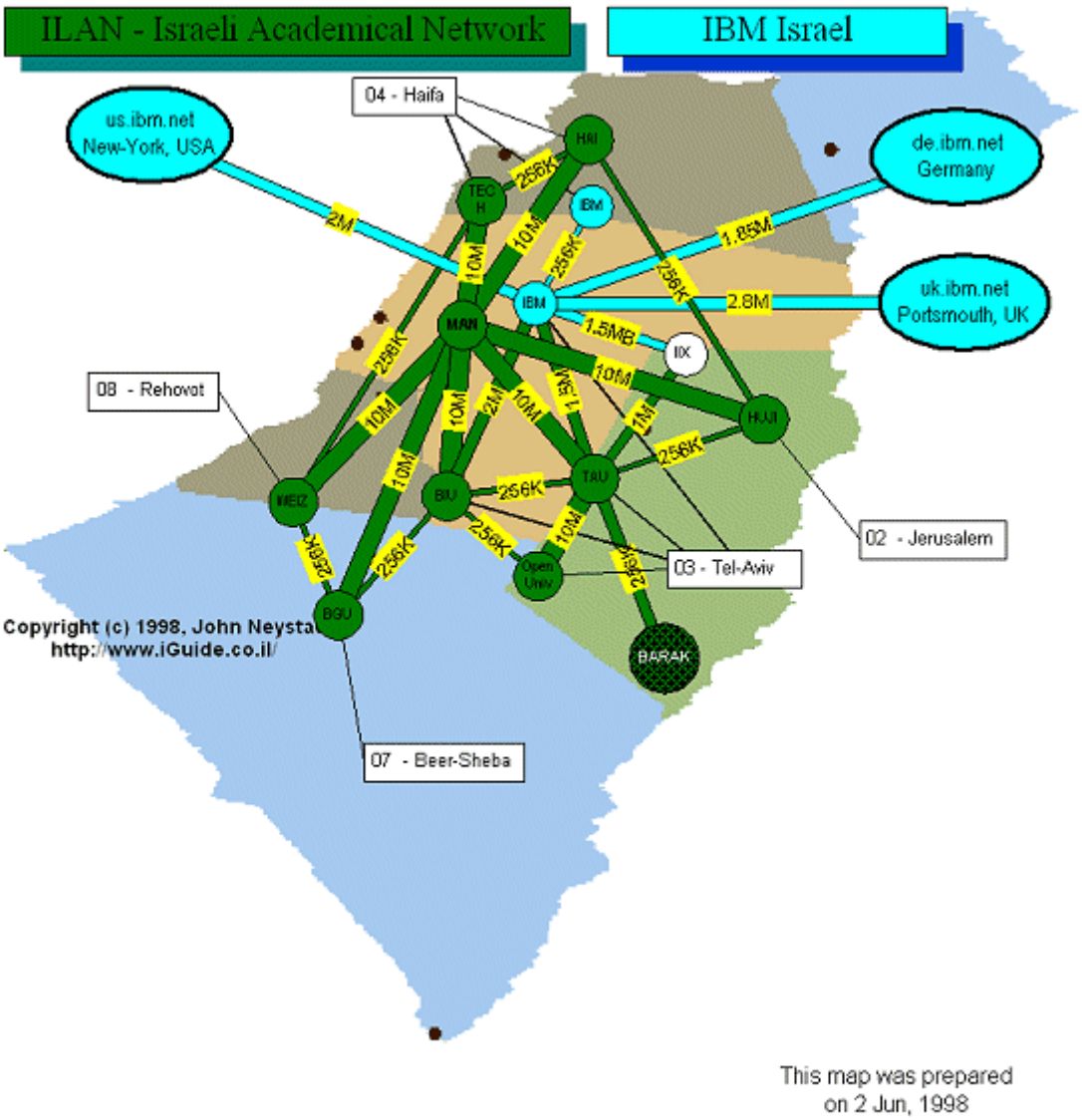
شکل: نقشه سایبری، دسامبر ۱۹۹۹

– مطلق نیاندیشید!

اگر به دنبال جنگ سایبری باشید که فقط در فضای سایبری ادامه می‌یابد، این قرن را چشم پوشی نمائید! زیرا بستگی انسان امروزی به فضای سایبری هنوز آنچنان نیست که این فضا را بطور جداگانه در نظر داشته باشیم.

– ایران و اسرائیل

اگر باور داشته باشیم که اسرائیل، بعنوان کشوری متجاوز و درست در مقابل منافع ملی و مدهبی کشور ماست، لزوم طرح‌ریزی و شروع یک جنگ سایبری علیه اسرائیل کاملا مطابق با امنیت ملی کشور ما، ایران است.



شکل: نقشه سایبری اسرائیل در سال ۱۹۹۸

متاسفانه، عملا مالک فضای سایبری، ایالات متحده آمریکا است که متفق اصلی و بی چون چرای اسرائیل است ولی می‌توان با اتخاذ روش‌های مناسب، از این نکته بر علیه وی و متفقینش بهره جست.

– هوش مصنوعی

استفاده ار هوش مصنوعی برای اتوماتیزه نمودن و جهت‌دار نمودن جنگ‌ها فوق العاده کاربردی است. زیرا اگر قرار باشد بخش اعظم این عملیات با حضور نوع انسان انجام شود، کیفیت و کمیت آن کاهش خواهد یافت.

– زیرساختهای اطلاعاتی

باید ابتدا زیرساختهای اطلاعاتی (Information Infrastructures) را بهینه نمود و بدین شکل، مستند و مدون به امور نظامی سایبری پرداخت.

– سیاست‌های دولت

سیاست‌های دولت نباید موجب سرخوردگی و بی میلی بخش خصوصی گردد؛ چیزی که در برخی موارد شاهد آن هستیم.

– عملی نمودن

سیاست‌های دولت ما شاید در حد تئوری باقی می مانند و هرگز عملی نشده‌اند.

– سانسور

سانسور باید کاملا برچیده شده (این خلاف نظرات شورای عالی انقلاب فرهنگی است) و به جای آن، کنترل و مانیتورینگ مستحکم‌تر گردد.

در پایان، ذکر بخش ابتدایی خطبه ۱۰۵ نهج البلاغه، از امیرمؤمنان علی (ع) خالی از لطف نیست:

... سپاس خداوندی که دین اسلام را پدید آورد و احکام دین را برای مسلمین سهل کرد و احترام به ارکان دین را در ضمیر مسلمین جای داد و هر که وارد دین اسلام شد از آرامگاه امن برخوردار گردید و ...

مراجع

سایتهای اینترنتی:

http://cve.mitre.org/
http://usinfo.state.gov/
http://www.2600.com/
http://www.altavista.com/
http://www.astalavista.com/
http://www.cia.gov/
http://www.cis.unisa.edu.au/
http://www.clickz.com/
http://www.defenselink.mil/
http://www.fbi.gov/
http://www.glreach.com/
http://www.google.com/
http://www.guardian.co.uk/
http://www.hartford-hwp.com/
http://www.lnkworld.com/
http://www.mit.edu/
http://www.nipc.gov/
http://www.nsa.gov/
http://www.packetstormsecurity.org/
http://www.psycom.net/
http://www.securityfocus.com/
http://www.taipeitimes.com/
http://www.usdoj.gov/
http://www.yahoo.com/

مقالات جالب توجه:

http://vmyths.com/hoax.cfm?id=281&page=3
http://www.mosnews.com/news/2004/08/27/internetterror.shtml

کتب:

* Cyberwar 2.0: Myths, Mysteries & Reality (Alan D. Campen, Douglas H. Dearth)
* Cyberwar 3.0: Human Factors in Information Operations and Future Conflict (Alan D. Campen, Douglas H. Dearth)
* Cyberwar: Point. Click. Destroy (Francha Roffe Menhard, Francha Roffe Menhard)
* Cyberwar: Security, Strategy, and Conflict in the Information Age (Alan D. Campen)
* Cyberwars: Espionage on the Internet (Jean Guisnel)
* Hacktivism and Cyberwars: Rebels With a Cause (Tim Jordan, Paul A. Taylor)
* Mapping Cyberspace (Martin Dodge, Rob Kitchin)
* Secrets and Lies : Digital Security in a Networked World (Bruce Schneier)
* The Art of War (Sun Tzu)
* The Atlas of Cyberspace (Martin Dodge, Rob Kitchin)
* The New Face of War: How War Will Be Fought in the 21st Century (Bruce D. Berkowitz)

کنفرانس‌ها:

* University of South Australia – Australian Information Warfare & IT Security Conference – December 2003

ما یقین داریم، هرگز نمی‌توانیم بر اراده خداوند در زمین غالب شویم و نمی‌توانیم از پنجه قدرت او بگریزیم.

قرآن کریم – سوره الجن – آیه ۱۲

هیچ کس از عذاب پروردگارش در امان نیست.

قرآن کریم – سوره المعارج – آیه ۲۸