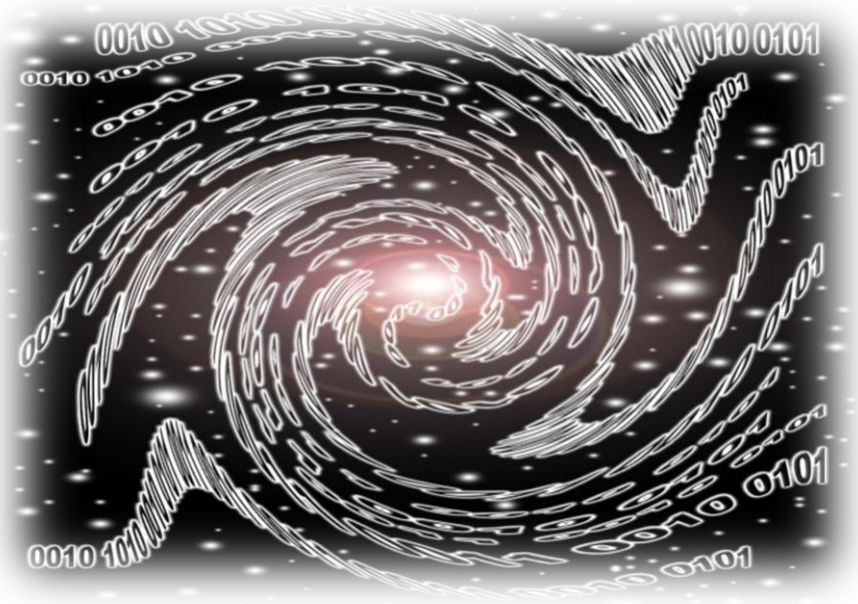
به نام خدا


0010 1010
0010 0101
0010 1010
0010 0101
0010 0101
0010 0101
0010 0101
0010 1010
0010 0101

فهرست:

مقدمه

تضمین امنیت و آسایش، همواره از بزرگترین دغدغه های حکومت ها می باشد؛ ضرورت پرداخت به این موضوع در هزاره‌ای که دشمن با استفاده از تمام امکانات ممکن، مترصد تجاوز و رخنه بمنظور پیشبرد اهداف سوء خود می باشد، امری کاملا محسوس و ملزوم است. بدون شک، دشمن از هر راه ممکن برای نفوذ و نیل به نیّات خود استفاده خواهد نمود.

امروز و با توجه به گسترش فناوری های نوین، تهدیدات، مخاطرات و نقاط رخنه پذیر متعددی بوجود آمده است که اغلب، مورد غفلت قرار می گیرند. همراه با توسعه روز افزون کاربری های رایانه در دنیا، این «فضای نوین و جذاب شکل گرفته ناشی از شبکه های رایانه ای بمنظور تبادل اطلاعات[1]» به سرعت رشد یافته است؛ بطوریکه بمنظور حفاظت از امنیت ملی و مقابله با دشمنان سایبری نیازمند تقویت نیروهای خود در این گستره و ارتقای توانمندی ها درجهت صیانت از فضای سایبر کشور می باشیم. حفاظت از فضای سایبر کشور بعنوان یکی از شریان های اصلی اطلاعات، در روزگاری که عصر اطلاعات لقب گرفته است، به اندازه حفاظت از مرزهای روی نقشه برای هر کشوری حائز اهمیت است.

[1] فضای سایبر(Cyber Space)

فصل ۱ - تاریخچه

بنظر می رسد نخستین جنگ با استفاده از فضای سایبر، اواسط دهه ۷۰ میلادی، در دوران جنگ سرد بین دو ابر قدرت آن زمان (ایالات متحده آمریکا و شوروی سابق) در گرفته باشد. شواهد حاکی از آن است که در این دوران (بین سال های ۱۹۱۷ تا ۱۹۹۱) جنگ‌های سایبری متعددی به وقوع پیوسته‌اند؛ هرچند در اغلب مستندات، مورد "کوزوو[۱]" بعنوان اولین جنگ سایبری بیان شده است.

توجه به نکات ذیل در بررسی تاریخچه جنگ‌های سایبر حائز اهمیت می باشد:

۱- ریز مستندات این جنگ‌ها (نحوه عمل، نتایج و آثار و ...) با توجه به ارتباط مستقیم با امنیت ملی کشورها بعنوان اسناد با سطح محرمانگی بالا تلقی گردیده و دولت ها مانع از فاش شدن آن ها می‌گردند.

۲- ماهیت جنگ های سایبری، از جرایم سایبری مانند هک یا انتشار ویروس ها کاملاً متفاوت می باشد؛ یک جنگ سایبری توسط دولت یا گروهی متخاصم و بمنظور ایجاد

[۱] Kosovo

اختلال و یا صدمه زدن به زیرساخت های هدف طرح ریزی و اجرا می شود. آنچه که تحت عنوان جرم سایبری شناخته می شود، در واقع می تواند بعنوان ابزارهای یک جنگ سایبری مورد استفاده قرار گیرد.

از جمله جنگ‌های معروف و ثبت شده سایبری می توان به موارد ذیل اشاره نمود:

۱- دهه ۸۰ میلادی؛ کره شمالی و آمریکا:

در این دهه کره شمالی در عکس العمل به توان مضاعف دشمن، اقدام به تأسیس مدرسه هک با بیش از ۱۰۰ سرباز آموزش دیده می‌نماید. جنگ‌های این دهه را می‌توان پیامدهای مشخصی از جنگ سرد دانست.

۲- سال ۱۹۹٤؛ حملات همزمان:

در این سال به مراکز هوائی،تحقیقاتی Rome در نیویورک، انستیتو تحقیقات اتمی کره جنوبی و نهایتاً مرکزی علمی در لاتویا (از کشورهای تازه استقلال یافته شوروی سابق) سه حمله همزمان صورت گرفت؛ درحالیکه کنترل شبکه در دستان حمله کننده‌ها بود ولی منبع آن کاملاً

نامشخص بود. در این حملات ردپاهایی از انگلستان مشاهده شده است.

۳- سال ۱۹۹۵؛ حمله به Citibank آمریکا:

در این حمله ۴۰۰هزار دلار توسط گروه هکرهای روسی بسرقت رفت. البته در نهایت با شناسائی مهاجمین روسی بخشی از زیان‌ها جبران شد.

٤- سال ۱۹۹۹؛ حمله به یوگسلاوی:

در ماه می این سال براساس دستور بیل کلینتون، رئیس جمهور وقت ایالات متحده آمریکا، سازمان امنیت و اطلاعات این کشور طرح حمله به سامانه های رایانه‌ای یوگوسلاوی را پی‌ریزی می‌نماید. به سبب فاش شدن اسرار این حمله، مقامات آمریکائی گریزی از آن نمی‌بینند و آن را رسماً تأیید می‌نمایند. از جمله اقدامات انجام شده در این حمله می‌توان به موارد ذیل اشاره نمود:

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

۵- سال ۱۹۹۹؛ جنگ ۷۸ روزه:

در ماه سپتامبر این سال خبرگزاری رویتر رسماً اعلام می کند که وزارت دفاع آمریکا، طرح حمله به شبکه‌های کامپیوتری "صرب" را بمنظور تهدید تسلیحات نظامی و خدمات اجتماعی با جدیت ادامه می‌دهد. این حمله ۷۸ روز ادامه داشته است.

٦- سال ۲۰۰۰؛ حمله علیه چین:

در ماه آگوست این سال Straits Times اعلام می کند که هنگ کنگ که خواهان استقلال خود از کشور چین بوده است؛ از این نوع جنگ بمنظور ضربه زدن و اعمال فشار به چین استفاده نموده است. هنگ کنگ در این حملات با استفاده از ویروس های خود مراکز انرژی، نظامی وبانک‌های چین را تحت تأثیر قرار داد و توانست فعالیت آن ها را مختل نماید.

۷- سال ۲۰۰۱؛ آمریکا و چین:

در این سال بر سر موضوع برخورد هواپیمای جاسوسی آمریکا با جت چینی جنگ سایبری دنباله داری بین دو کشور در گرفت که دامنه های آن تاحدودی به اروپا نیز کشیده شد. سایت دولتی چین، اولین قربانی این جنگ بود. در بین جنگ های سایبری در گرفته بین آمریکا و چین، این مشهورترین نمونه می باشد. درصد آسیب های وارده به زیرساخت ها و تخریب در چین بر اثر این جنگ ها ۱۰ برابر آمریکا بوده است.

۸- سال ۲۰۰۱؛ آمریکا و روسیه:

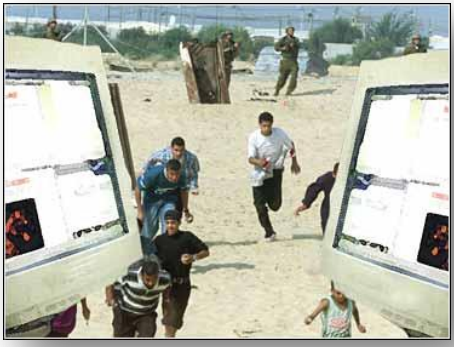
در آوریل این سال روزنامه روسی Moskovsky Komsomolets از استخدام هکرهای روسی، برای نفوذ به شبکه خدمات امنیتی این کشور توسط امریکا خبر می دهد.

۹- سال ۲۰۰۱؛ برج های دو قلو:

هرچند آمریکا مسئولیت مستقیم عملیات یازدهم سپتامبر را بطور مشخص به القاعده و عمل انتحاری اعضای این گروه نسبت می‌دهد، اما باید توجه داشت شواهد نشانگر طرح‌ریزی بسیار دقیق و اجرای عملیات، طی حدود یک سال و نیم است که بدون پشتوانه جنگ سایبری امکان پذیر نبوده است.

۱۰- سال ۲۰۰۳؛ آمریکا و عراق:

در ماه می این سال امریکا با طرح ریزی و اجرای یک جنگ تبلیغاتی سایبری راه را برای تجاوز به عراق و توجیه اقدام خود برای افکار عمومی جهانی باز نمود.



۱۱- سال ۲۰۰۳؛ حمله علیه تایوان:

در این سال چین مبادرت به حمله سایبری به دولت تایوان می‌نماید. ابزار مورد استفاده در این حمله انتشار اسب‌های تروآ که نوعی از ویروس های خطرناک رایانه ای می باشد، بوده است.

۱۲- سال ۲۰۰۶؛ جنگ ۳۳ روزه:

در حالیکه آمریکا، اسرائیل، متحدان اروپایی آنها و برخی از سران سازشکار عرب، در آغاز این جنگ با قاطعیت و اطمینان از نابودی حداکثر ۳ روزه حزب ا... سخن می گفتند؛ به دلیل عدم توجه اسرائیل به تکنیک های دفاع غیرعامل و برتری حزب ا... در نبردهای اطلاعاتی با بکارگیری تکنیک های پدافند غیر عامل در حوزه فناوری اطلاعات و استفاده از ابزارآلات و تجهیزات بومی، موجب ناکامی اسرائیل در دستیابی به اهداف خود شد.

تهدید سایت‌های اینترنتی طرفین، حملات متناوب DoS[۱] که بمنظور ایجاد اختلال در سرویس دهی با ایجاد حجم بالای ترافیک صورت می گیرد ، استفاده از تکنیک های شنود و جاسوسی از جمله اقدامات انجام شده در حوزه فضای سایبری در جنگ ۳۳ روزه می باشد.

[۱] Denial of Service

۱۳- سال ۲۰۰۷؛ حمله به استونی :

در آوریل این سال، پس از تصمیم استونی برای نابود کردن مجسمه برنزی شکست شوروی در جنگ جهانی دوم سایت های احزاب سیاسی، بانک ها، روزنامه ها و وزارتخانه های این کشور حدود ۳ هفته تحت حملات سایبری قرار گرفت.

۱٤- سال ۲۰۰۸؛ اوستیای جنوبی:

در نخستین ساعات آغاز جنگ روسیه و گرجستان، آتش این جنگ در فضای سایبر نیز روشن شد. بسیاری از کارگزار[۱]های شبکه گرجستان کمی قبل از آغاز عملیات نظامی روسیه به مناطق استقلال طلب اوستیای جنوبی مورد حملات سایبری قرار گرفتند؛ بطوریکه سایت های وزارت امور خارجه، وزارت دفاع گرجستان، سایت رسمی میخائیل ساکاشویلی رئیس جمهور گرجستان و شبکه های اصلی تلویزیونی این کشور بر اثر حملات مستمر DoS کاملاً مسدود و بلااستفاده شده بودند. در نتیجه این حملات سایت ها

---

[۱] سرور (Server)

بروزسازی نمی شدند و نمی توانستند اخبار جدید را دریافت یا اعلام کنند.

فصل ۲ – فضای سایبر

فضای سایبر مجموعه‌ای از شبکه‌های ارتباطی کامپیوتری شامل وسایل ارتباطی، انتقالی، کنترلی و سیستم‌های مدیریتی با یکسری اهداف ارزشمند برای پردازش‌ها و زیرساخت ها می‌باشد. اینترنت بزرگترین مؤلفه از فضای سایبر می‌باشد.

بیشتر سامانه هایی که به فضای سایبر وابسته اند و از آن استفاده می‌کنند، از این فضا به عنوان یک ضعف امنیتی یاد می‌کنند که می‌توان از آن در جهت انجام حملات استفاده نمود. بیشتر این سامانه ها به گونه‌ای طراحی شده‌اند که بتوانند استفاده ارزان و وسیعی از دسترسی به شبکه داشته باشند و این موضوع، توانایی سوء استفاده مهاجمین بمنظور استثمار و آسیب‌پذیر نمودن شبکه‌ها و سرویس های هدف را افزایش داده است.

❖ **ویژگی های فضای سایبر**

از جمله ویژگی های اساسی فضای سایبر که باعث ایجاد محیطی مناسب برای سربازان جنگ های سایبر می‌شود، می توان به موارد ذیل اشاره نمود:

۱- گمنامی:

شناسایی و ردیابی یک سرباز جنگ سایبر در فضای سایبر و پیدا کردن مکان فیزیکی وی با توجه به تکنیک های خاص پنهان سازی در این فضا، بسیار مشکل است.

۲- تجهیزات ارزان و دردسترس:

سهولت دسترسی به ابزارهای حمله و جاسوسی و هزینه آنها نسبت به جنگ افزارهای حملات دیگر، سازمان های

تروریستی را قادر ساخته تا با استفاده از تجهیزات پیچیده، پیشرفته، بروز سایبری و از طریق ارتباطات پنهان به زیرساخت های هدف، حمله و به اهداف خود دست یابند.

۳- در دسترس بودن هدف:

اینترنت و ارتباطات به طور روزافزون در حال گسترش می‌باشد، و یک سرباز سایبری قادر است ۲۴ ساعته در حال ارتباط با هدف باشد.

از دیگر مؤلفه های این فضا می توان از توجه رسانه‌ای، تأثیرگذاری بر میزان نیرو، تأثیرات فیزیکی، هوشمندی و سادگی استفاده نام برد.

فصل ۳ - جنگ سایبر

جنگ سایبر، به معنی استفاده از کامپیوترها و فضای تبادل اطلاعات به عنوان یک اسلحه یا به عنوان ابزاری برای انجام کارهای خشونت بار جهت ترساندن، تغییر عقیده و یا نابودی یک گروه یا کشور می باشد. جنگ سایبر به قصد کارهای سیاسی انجام می گیرد و مکان‌ها و زیرساخت هایی مانند انرژی، حمل‌ونقل، ارتباطات و سرویس‌های خدماتی ضروری را هدف قرار می‌دهد. در جنگ

سایبر از شبکه‌های کامپیوتری به عنوان بستر انجام این اعمال خرابکارانه استفاده می‌شود.

❖ اهداف جنگ های سایبر

اهداف نظامی، خدمات اجتماعی، سامانه های نقل و انتقال، مخابرات، نیرو، انرژی و هر زیرساخت حیاتی می تواند قربانی این جنگ ها بوده و امنیت، ایمنی و پایداری آن به خطر افتد.

❖ ویژگی های جنگ سایبر نسبت به سایر انواع جنگ‌ها

جنگ فیزیکی و سایبر از برخی جهات کاملا شبیه به هم هستند؛ بعنوان مثال هدف اصلی در جنگ - از هر نوع - وارد آوردن ضرر و زیان به دشمن است و روش اصلی در جنگ قاعدتاً تصاحب منابع دشمن خواهد بود.

نقاط افتراق جنگ سایبر نسبت به سایر جنگ ها را می توان به صورت زیر دسته بندی نمود:

۱- حمله از راه دور[۱]

اولین تفاوت جنگ سایبر با دیگر جنگ ها و بالاخص جنگ فیزیکی و حقیقی، قابلیت طراحی، اجرا و نتیجه‌گیری از راه دور است.

۲- دشواری در شناسائی و ردیابی

به سبب خصائصی که در پروتکل‌های ارتباطی در فضای سایبر وجود دارد، عملاً شناسائی و ردیابی منبع اصلی حمله و مهاجم اصلی، بسیار دشوار و گاهی غیرممکن است.

---

[۱] Remote

۳- تهدید سه جنبه امنیت

در جنگ سایبر، هر سه جنبه امنیت (امنیت، ایمنی و پایداری)، می تواند مورد تهدید قرار گیرد.

٤- اندازه هدف

در جنگ های فیزیکی عموماً به دنبال تخریب مناطق جغرافیائی بزرگتر هستند، ولی در جنگ سایبر باید اهداف مهم و اساسی "از نظر سایبری و نقش آن ها" را هدف قرار داد. این اهداف ممکن است از نظر فیزیکی بسیار ناچیز باشند ولی نقش بزرگی ایفا نمایند.

٥- انتشار حمله

حمله سایبری می‌تواند به سادگی از چندین منبع/کانال صورت پذیرد در حالی که هدایت و راهبری حمله‌های فیزیکی که از چندین محل آغاز می‌گردند بسیار دشوار است.

٦- هزینه

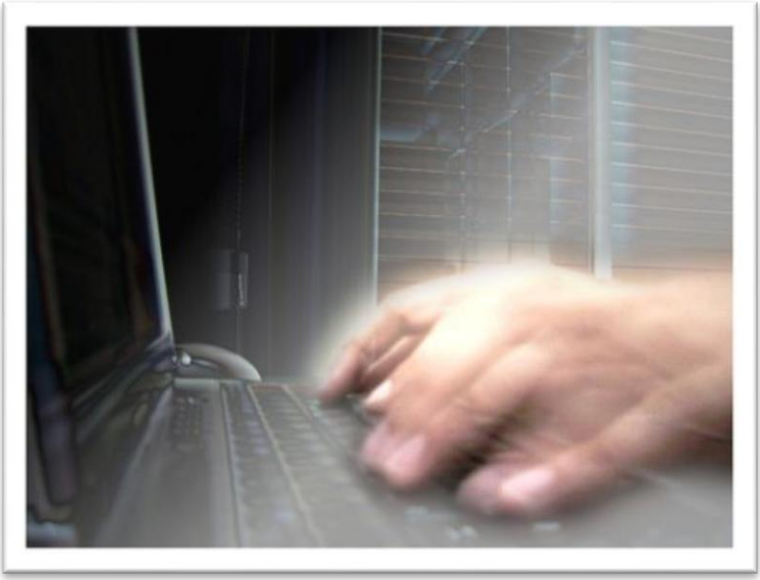
بدون شک هزینه جنگ فیزیکی از جنگ سایبر بیشتر است و این خصوصیت بارز فضای سایبر است که عوامل و عناصر آن سهل الوصول‌تر و ارزان‌تر هستند.

۷- 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.

❖ ابزارها و سلاح های جنگ سایبر

سلاح جنگ سایبر را تلفیقی از دانش و تجهیزات تشکیل می دهد. دانش تخصصی بالاترین اثر را دارد ولی بدون شک ابزار نیز نقش کلیدی خواهد داشت.



دسته بندی سلاح های سایبری به شرح ذیل می باشد:

۱- ابزارهای شناسائی

عموم سلاح‌های شناسائی در خود فضای سایبر یا اینترنت وجود دارند. نمونه‌های کلی این ابزارها در ادامه آورده شده است:

- موتورهای جستجوی دامنه‌ها
- ثبات دامنه اینترنتی
- ثبات آدرس اینترنتی

- تکنیک‌های ردیابی[۱]
- ابزارهای شناسائی DNS
- ابزارهای شناسائی شبکه و همبندی آن
- ابزارهای متفرقه

۲- ابزارهای وارسی

با سلاح‌های وارسی می توان سامانه های زنده و فعال[۲] و قابل دسترسی از طریق اینترنت[۳] را مشخص نمود. نمونه‌های کلی این ابزارها شامل موارد زیر می باشد:

- انواع جاروب کننده‌ها[۴]
- انواع وارسی کننده‌های پورت‌های TCP و UDP

۳- ابزارهای کنکاش

---

[۱] Trace Routing

[۲] alive

[۳] Internet Reachable

[۴] Sweep

سلاح‌های کنکاشگر عموماً درون سیستم‌های عامل حضور دارند. این ابزارها مبادرت به بیرون کشیدن اطلاعات خاص سیستم عامل ها و شبکه‌ها، نظیر عناصر کاربری و تولیدات نرم‌افزاری می‌نمایند.

٤- ابزارهای نفوذ

این ابزارها شامل موارد ذیل می گردد:

- ابزارهای صرفاً سایبری
- سلاح‌های فیزیکی/سایبری. مانند امواج کوتاه و بلند دستکاری شده، موسوم به بمب الکترونیکی[۱]

٥- ابزارهای ارتقاء مزایا

[۱] E-Bomb

این ابزارها شامل موارد ذیل می گردد:

- روش‌ها و ابزارهای تزریق
- متدهای فریبکارانه[1]
- استراق سمع

٦- سلاح‌های پنهان

این ابزارها شامل موارد ذیل می گردد:

- انواع اسب‌های تروآ
- انواع ویروس‌ها و کرم‌ها
- نقاط پنهان در سیستم‌های عامل

۷- جنگ افزارهای حملات DoS

در استفاده از این نوع روش ها جنبه در دسترس بودن هدف مورد تهدید قرار می گیرد. این حملات بعنوان ابزار برای دیگر سناریو های جنگی نیز مورد استفاده قرار می گیرند.

[1] Art of Deception

آیا میدانید در فضای جنگ سایبری می توان مدیریت شبکه سازمان شما را در اختیار گرفت و یا آن را مختل و یا فلج نمود؟