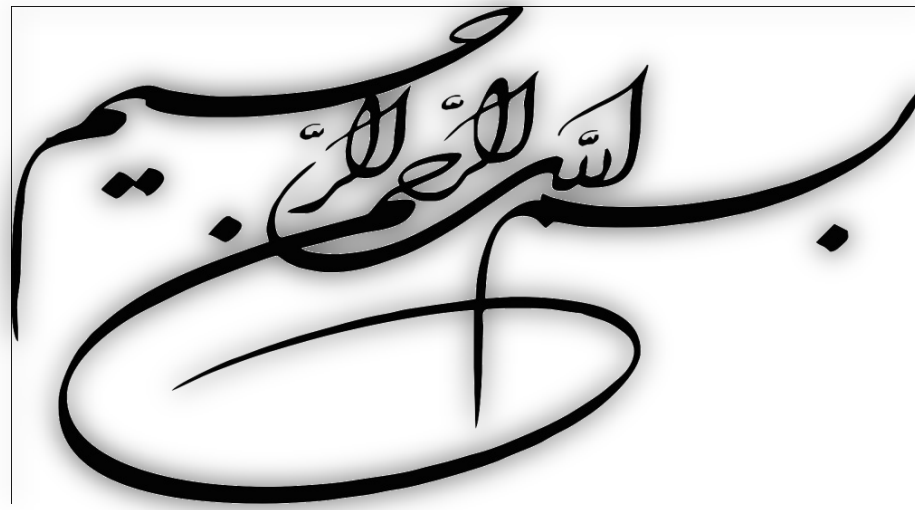




امنیت در فضای سایبری

ارائه: پیام کریم آبادی

امنیت



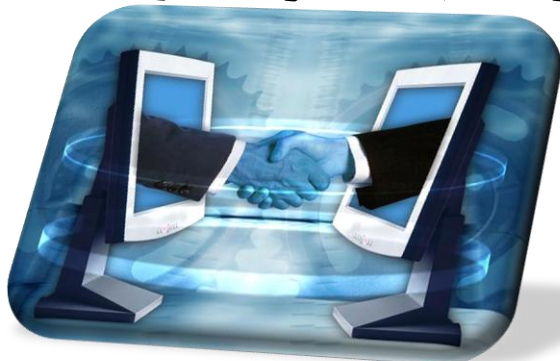
امنیت، یکی از اصلی‌ترین نیازهای بشری در تمامی اعصار و قرون بوده است و در آینده نیز خواهد بود. در عین پایداری اصل نیاز به امنیت، آنچه در بررسی‌های امنیتی اهمیت دارد، مصداق‌های مربوط به امنیت است. در این تردیدی نیست که همگان نیازمند امنیت هستند، اما در اینکه مصداق ناامنی چیست؟ بحث و گفت‌وگو فراوان است و قابل دقت آنکه منابع تهدید کننده امنیت براساس شرایط و ساختاری مختلف، دگرگون شده و مصداق‌ها تابعی از شرایط زمانی و مکانی هستند. هرچند که جنگ از قدیمی‌ترین منابع تهدیدکننده امنیت در طول تاریخ بوده، ولی 100 سال پیش، از جنگ‌های الکترونیک خبری نبود و 20 سال پیش کسی از امنیت فضای سایبر و مجازی سخنی نمی‌راند، ولی اکنون امنیت فضای مجازی به جزئی جدا نشدنی از امنیت بین‌المللی تبدیل شده است.[4]

فضای سایبری؟؟؟

فضای سایبر یا همان سایبر اسپیس (Cyberspace) عبارتی است که در دنیای اینترنت ، رسانه و ارتباطات بسیار شنیده می شود.[4]

فضای سایبر در معنا به مجموعه هایی از ارتباطات درونی انسان ها از طریق کامپیوتر و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود.

مثال: یک سیستم آنلاین نمونه ای از فضای سایبر است که کاربران آن می توانند از طریق **ایمیل** و... با یکدیگر ارتباط برقرار کنند. بر خلاف فضای واقعی ، در فضای سایبر نیاز به جابجایی های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می گیرد.[3]

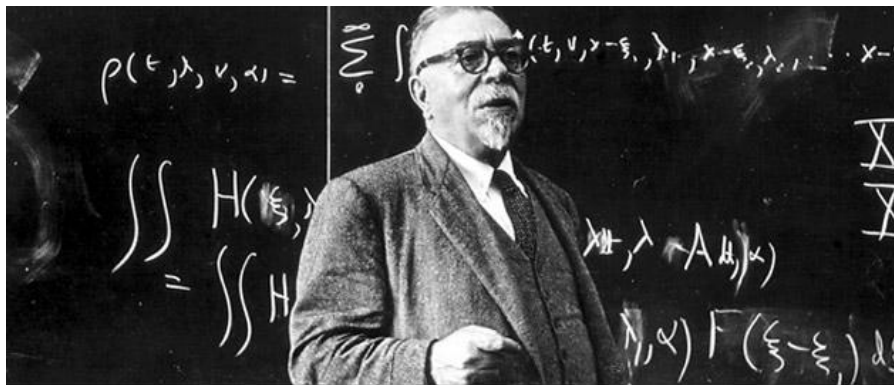


تاریخچه فضای سایبری

➤ مشتق شده از لغت یونانی **Kybernetes** به معنی سکاندار یا راهنما مشتق شده است [4]

➤ استفاده شده توسط نوربرت وینر در سال 1948

➤ *Cybernetics: Or Control and Communication in the Animal and the Machine*

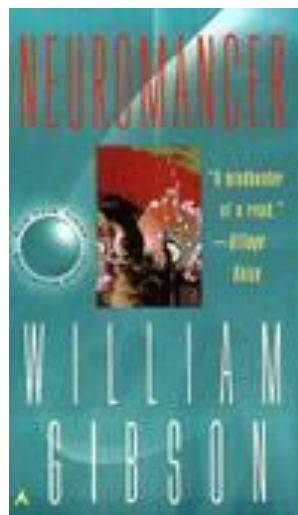


تاریخچه واژه فضای سایبری

◀ نویسنده داستان‌های علمی تخیلی: ویلیام گیbson [4]



◀ 1984: نورومنسر



واژه Cyber

سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است. در طی توسعه اینترنت واژه های ترکیبی بسیاری از این کلمه سایبر بوجود آمده است که به تعدادی از آنها اشاره می کنیم [2]

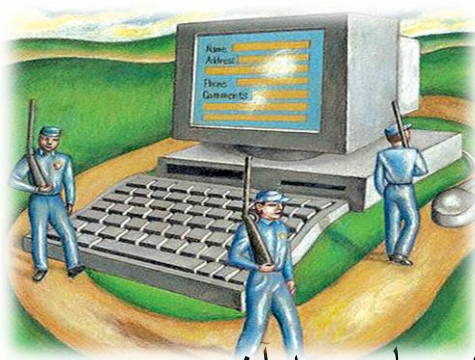
فضای سایبر Cyberspace، شهروند سایبر Cybercitizen، پول سایبر Cybercash، فرهنگ سایبر Cyberculture، راهنمای فضای سایبر CyberCoach، تجارت سایبر Cyberbussiness، کانال سایبر Cyberchannel و ...





شروع مطالعات در زمینه علم سایبری

- این عدم جابجایی فیزیکی، محققان را واداشت که به مطالعه بررسی شباهت‌های فضای سایبر با حالت‌های نا هشیاری، بخصوص حالت‌های ذهنی‌ای که در رویا ها ظاهر می‌شوند، بپردازند. [4]
- آنان با الهام از گفته‌های یکی از رهبران بزرگ "ذن" به نام چانگ تزو Chuang Tzu برای تحقیقات خود در زمینه کشف شباهت‌هایی بین فضای سایبر و رویا بهره جسته اند. گفته می‌شود که:
- "چانگ تزو شبی در خواب می‌بیند که یک پروانه شده است. وقتی بیدار می‌شود با خود می‌اندیشد: آیا من مردی هستم که خواب می‌بیند پروانه شده است، یا اینکه پروانه ای هستم که اکنون خواب می‌بیند یک "مرد" شده است."



اهمیت امنیت در فضای سایبری

امنیت فضای سایبری به خاطر اتکای بیش از حد تمامی بازیگران سیاسی به آن، بی‌تردید مقوله‌ای استراتژیک قلمداد می‌شود و به همین دلیل است که در ارزیابی از تهدیدات امنیت ملی و بین‌المللی، مفهوم امنیتی فضای سایبری، وارد اسناد پایه‌ای امنیتی شده است. سندی که در اجلاس سران ناتو در 20 نوامبر 2010 (29/8/89) در لیسبون پرتغال به تصویب رسید، در این زمینه حائز اهمیت است. شایان ذکر است که ناتو از چندی پیش تعدادی از نخبگان امنیت ملی و سیاست خارجی را تحت رهبری «آلبرایت» وزیر خارجه پیشین آمریکا گردهم آورد تا به این سؤال پاسخ دهند که امنیت کشورهای عضو ناتو در آینده و دهه‌ای که در پیش است، چگونه و با تأثیر از چه منابعی مورد تهدید واقع می‌شود. [5]



جرائم سایبری

- تاریخچه جرائم سایبر

- در اواسط دهه ۹۰ با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، نسل سوم جرائم کامپیوتری، تحت عنوان جرائم سایبری (مجازی) یا جرائم در محیط سایبر شکل گرفته است. به این ترتیب جرائم اینترنتی را می‌توان مکمل جرائم کامپیوتری دانست، بخصوص اینکه جرائم نسل سوم کامپیوتری که به جرائم در محیط مجازی معروف است، غالبا از طریق این شبکه جهانی به وقوع می‌پیوندد. [1]



جرایم در سایبر سپیس

طبیعت این جرایم وسوءاستفاده‌های مرتکب شده در این دنیای مجازی جدید هیچ گاه در دنیای حقیقی دیده نشده است. امنیت نا کافی تکنولوژی همراه با طبیعت مجازی آن فرصت مناسبی را در اختیار افراد شرور قرار می‌دهد. نگران کننده‌ترین جنبه فضای سایبر انتشار سریع اطلاعات در آن می‌باشد، مثلاً در لحظه کوتاهی قسمتی از اطلاعاتی که می‌تواند بطور بالقوه مورد سوءاستفاده قرار گیرد کشف می‌شود. در فضای سایبر برای جستجو و پیدا کردن این جرایم مشکلات پیچیده تر می‌شود. در دنیای واقعی دزدی از بانک کاملاً مشخص است چرا که بعد از سرقت در خزانه بانک پولی موجود نیست. ولی در تکنولوژی کامپیوتری شدن یک خزانه می‌تواند بدون هیچ علامتی خالی شود.

برای **مثال** سارق می‌تواند یک کپی دیجیتال کامل از نرم افزار بگیرد و نرم افزار اصلی را همان طور که دقیقاً بوده باقی بگذارد. در فضای سایبر کپی عیناً اصل است با کمی کار روی سیستم، سارق می‌تواند امکان هرگونه تعقیب و بررسی مثل پاک کردن اثر انگشت تغییر دهد. [1]

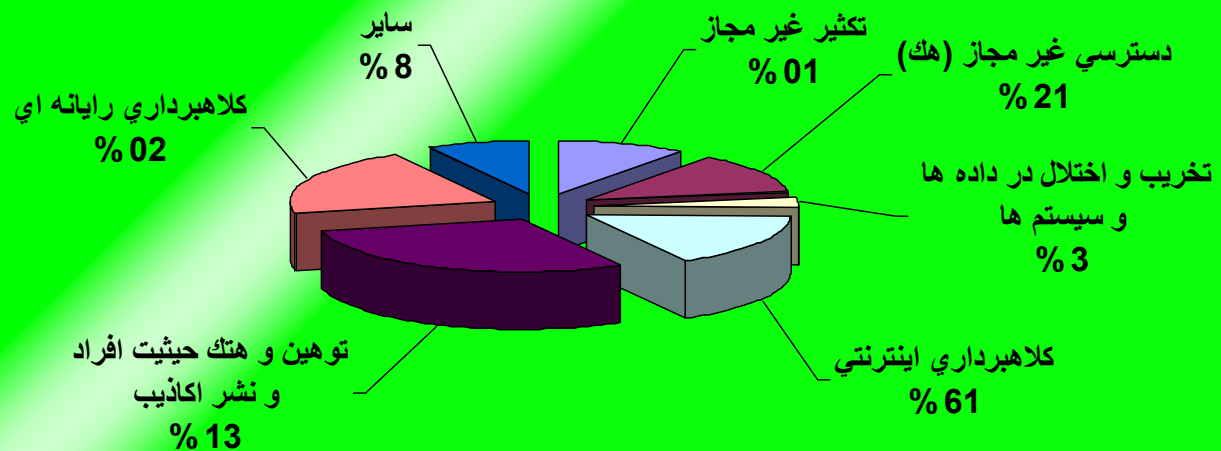
بررسی مصادیق و علل وقوع جرایم رایانه ای در ایران



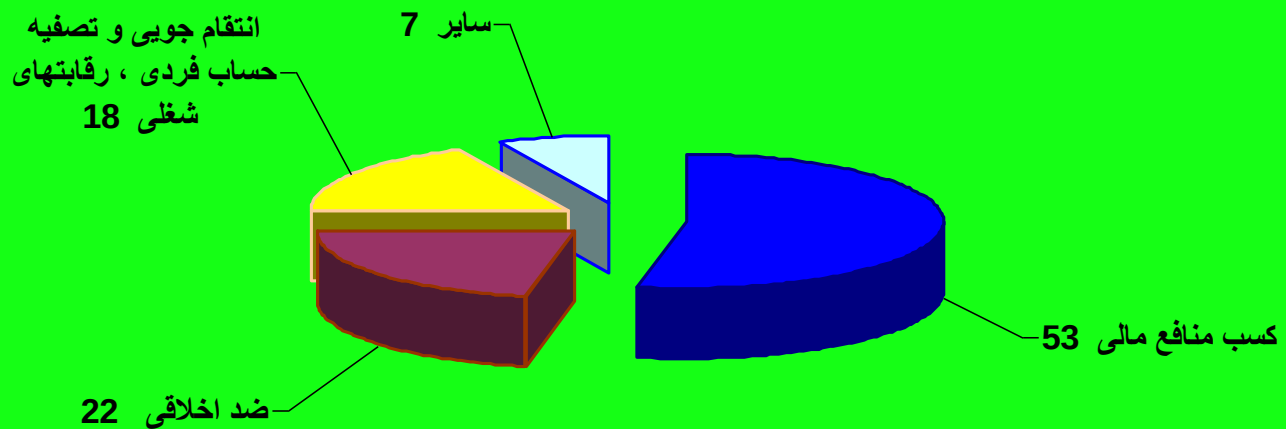
سیمای کلی جرایم رایانه ای



انواع جرایم گزارش شده در سال 1388



انگیزه در جرایم گزارش شده



جنگ نرم در فضای سایبری

در این جنگ جهانی نه از ارتش‌های کلاسیک خبری است نه از تسلیحات مرگبار. اینجا فقط رایانه است و کابل و ایده. [5]



Battlefield 3

نام جدیدترین بازی جنگی است که قرار است پاییز امسال به بازار عرضه شود. این بازی یک بازی تیراندازی از دید اول شخص است که از سوی شرکت EA Digital Illusions CE تولید و به وسیله شرکت Electronic Arts عرضه می‌شود. در این بازی شما نقش تفنگداران نیروی دریایی آمریکا را دارید که طبق معمول با نام عباراتی چون آزادی و مبارزه با تروریسم به کشورهای دیگر از جمله ایران حمله می‌کنید [4]



حملات مختلف در فضای سایبری

1. دستکاري يك ميليون آدرس سايت توسط هکرها
2. سرورهاي ناسا در معرض حملات سايبري
3. هکرها مرورگر مايکروسافت و اپل را از کار انداختند
4. افزايش بدافزارهاي مک در سال 2010



گزارش اختصاصی شرکت امنیتی Panda Security ، از وضعیت

جهانی امنیت اطلاعات در سال 1389

1. کرم رایانه ای استاکس نت، یک ویروس تمام عیار سیاسی

2. جنگ ها و درگیری های اینترنتی

3. تظاهرات و اعتراضات سازمان یافته اینترنتی

4. خطر شبکه های اجتماعی

5. ضدویروس های تقلبی



بر اساس اعلام شرکت امنیتی پاندا، "Mariposa" و "Bredolab" بزرگترین شبکه های مخربی بودند که در سال 1389 ردیابی و خنثی شده و تمام رهبران آن ها نیز با همکاری شرکت های امنیتی دستگیر شدند. این خبر خوبی برای دنیای امنیت رایانه ها بود چون در این دو شبکه بزرگ مخرب، بالغ بر 13 میلیون رایانه آلوده وجود داشت که تحت فرمان گروه های تبهکاری قرار داشتند.

علل وقوع جرایم رایانه ای



1- نا آشنایی کاربران با ویژگیهای فضای سایبر

2- بی توجهی و کم توجهی به امنیت فناوری اطلاعات

الف- کاربران منفرد

ب- موسسات و سازمانهای خصوصی و دولتی

3- افزایش میزان کاربری رایانه و بهره گیری از شبکه های رایانه ای

4- پیچیده تر شدن فعالیتهای متخلفین و مجرمین فضای سایبر

5- فقدان قوانین خاص جرایم رایانه ای

6- فقدان همکاریهای بین المللی در مقابله با جرایم رایانه ای

جلو گیری از به خطر افتادن اطلاعات فردی در فضای سایبری

- 1: کاربران برای افزایش ایمنی فضای سایبری می‌توانند بلوتوث گوشی خود را به گونه‌ای تنظیم کنند که برای دریافت فایل‌های ارسالی حداقل دوبار تایید بخواهد.
- 2: هنگام اتصال به اینترنت باید از جدیدترین و به‌روزترین نسخه‌های مرورگرهای وب استفاده شود، افزود: کاربران باید از آگهی‌های فریبنده پرهیز در این ارتباط پرهیز کنند.
- 3: هنگام خروج از ای‌میل از گزینه sign out استفاده کنند
- 4: استفاده از بازی‌های آنلاین در وب سایت‌ها خطرناک است و نرم افزار آلوده در این وب سایت می‌تواند اطلاعات رایانه کاربر را نیز آلوده به ویروس کند.
- 5: نهادها و سازمان‌های دولتی باید در استفاده از انواع مختلف فکس مودم‌ها نهایت دقت را داشته باشند، و قبل از استفاده از فکس مودم در نهادهای دولتی باید مدل آن از سازمان‌های امنیتی کشور استعلام شود و در صورت تایید مورد استفاده قرار گیرد. [3]



سیستم رمزنگاری RPK بر پایه کلید عمومی

بسیاری از سیستم‌ها اجازه می‌دهند که یکی از کلیدها (کلید عمومی) منتشر شود در حالی که دیگری (کلید خصوصی) توسط صاحبش حفظ می‌شود. فرستنده پیام، متن را با کلید عمومی گیرنده، کد می‌کند و گیرنده آن را با کلید اختصاصی خود رمزگشایی می‌کند به عبارتی تنها با کلید خصوصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد، یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی‌تواند از متن کد شده به متن اصلی دست یابد، بنابراین پیام کد شده برای هر گیرنده‌ای، به جز گیرنده مورد نظر فرستنده بی‌معنی خواهد بود. [2]



نتیجه گیری

هدف ما از این است که بتوانیم برای شبکه‌ها و محیط‌های اینترنتی خود امنیتی بوجود بیاوریم و از این جرایم جلوگیری کنیم که بهترین راه برای جلوگیری از وقوع اکثر جرایم رایانه‌ای یا غیر رایانه‌ای به آگاهی ما بستگی دارد. اگر تعداد بیشتری از مردم از اشکال و روش‌های فعلی جرایم سایبر آگاهی یابند، تعداد قربانیان کاهش خواهد یافت.

????????????!!!!!!!!!!!!

شاید زمانی نه چندان دور ما هم با این گفته چانگ تزو
Chuang Tzu هم کلام شویم ؛ آیا این ما هستیم که در فضای
سایبر به عنوان کاربر سیر می کنیم یا اینکه این فضای سایبر
است ، که به عنوان بخشی از برنامه های خود ما را تعریف می
کند ، کسی چه می داند؟



منابع

1. برومندباستانی «جرائم کامپیوتری و اینترنتی» انتشارات بهنامی، تهران، ۱۳۸۳
2. Gina.De.Angelis, Cyber Crimes, Chelsea House Publisher. ۲۰۰۰
3. دکتر ابراهیم حسن بیگی "حقوق و امنیت در فضای سایبر" موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار، تهران، ۱۳۸۴
4. <http://www.ictna.ir/security/archive/032297.html>
5. آموزش hack i.t. (کلوینسکی) مترجم الهام بشیری-تهران: بیشه ۱۳۸۹.