درآمدی بر تروریسم سایبری

هدف از این نوشته، آشنایی مقدماتی با تروریسم سایبری به عنوان گروهی از جرایم زیر گروه جرایم سایبری است. طبعاً آنچه در این متن ذکر می‌شود صرفاً جنبه طرح مسئله دارد و قصد ورود به جزئیات را ندارد. این مقاله توسط محمدحسین دزیانی نوشته شده‌است

۱- حملات سایبری به گروه یا تعداد زیادی از اعمال ارتکابی از سوی هکرها اطلاق می‌شود که بعضاً با خشونت یا آثار شدید همراه است. البته حملات سایبری یا به عبارت دیگر حملات هکری می‌تواند رویکردهای مجرمانه متفاوتی داشته‌باشد. گاه این حملات مقدماتی است و برای کسب اطلاعات و داده‌ها جهت ارتکاب جرایم سایبری صورت می‌گیرد و گاه این حملات مستقیماً در چارچوب یک توصیف جزایی سایبری صورت می‌گیرد. بهر حال حملات هکری یا حملات سایبری عنوان عامی است که بر مصادیق متعدد اطلاق می‌شود و دسته‌ای از این مصادیق را تروریسم سایبری می‌نامند.

شناخت حملات هکری به عنوان مبنای حملات اختصاصی امری ضروری است. از این رو برای شناخت تروریسم سایبری باید با تاریخچه و تحول و عمل حملات سایبری، مرتکبین و اشخاص یا شرکتهای موضوع جرم تروریسم سایبری و روش مبارزه و پیشگیری عام آشنا شد.

۲- حملات سایبری از سوی افرادی به نام معترضین سایبری صورت می‌گیرد و به فعل آنها اعتراض سایبری (پروتست) می‌گویند. تروریست‌های سایبری در زمره معترضین سایبری هستند.

۳- حملات سایبری حسب آمار، در سالهای اخیر دو برابر شده به گونه‌ای که این میزان در سال ۲۰۰۱ به حدود ۵۰ هزار حمله می‌رسد که هر حمله خود شامل آسیب به چند عدد یا چند هزار کامپیوتر است.

۴- حملات سطوح شامل سطوح مختلفی می‌شوند: از صرف حملات اطلاعاتی (برای موارد آسیب پذیر توسط افراد مترصد این حملات)، تا حملات خطرناک و شدید (مخاطرات امنیتی شدید).

۵- چهل درصد حملات علیه سازمانهای خاص یا شبکه‌های شرکت‌های خاص انجام شده است (مثل حمله به تلکام بریتانیا به دلیل خدمات رسانی به تل‌آویو...) برخی شرکتها حملات شدیدی را تجربه کرده‌اند (از نوع حملات اضطراری).

۶- ریشه حملات در کجاست؟ آمارها و کشفیات مراجع اختصاصی نشان می‌دهد حملات از آمریکا علیه کره جنوبی، چین، آلمان و فرانسه صورت گرفته و بالعکس. برخی حملات نیز از اسرائیل به هنگ کنگ، تایلند، کره‌جنوبی، فرانسه و ترکیه و بالعکس صورت گرفته است.

۷- نوعی از حملات از طریق ایمیل‌های آلوده صورت می‌گیرد. میزان ایمیل‌های ویروسی و آلوده روبه افزایش است. در سال ۱۹۹۹ از هر یک‌هزار و ۴۰۰ ایمیل یکی ویروس بود اما در سال ۲۰۰۱ از هر ۳۰۰ ایمیل یکی ویروس بوده است. پیش بینی شده در سال ۲۰۱۵ از هر ۴ ایمیل، ۳ تا ویروسی باشد.

۸- آلودگی ویروسی صرفاً از راه ایمیل نیست. آلودگی ویروسی کامپیوترها کلاً رو به افزایش است. در ۱۹۹۶ از هر یک‌هزار کامپیوتر تعداد ۱۰ تا کامپیوتر آلوده شده اما در سال قبل از هر یک‌هزار کامپیوتر، ۱۰۰ کامپیوتر آلوده شده‌اند. بخشی از این آلودگی ناشی از حملات تروریستی سایبری است.

حملات ویروسی گاه از طریق نرم افزار رایگان

محقق می‌شود گاه از طریق ضمیمه ایمیل (code red) که ۳۹۵ هزار میزبان و کامپیوتر را آلوده کرد و سرعت نفوذ آن به گونه‌ای بود که پس از ۱۳ ساعت کل کامپیوترهای هدف را آلوده کرد). ویروس‌های جدید در ظرف ۱۵ دقیقه تا نهایت یک ساعت تعداد زیادی کامپیوتر را آلوده می‌کنند و ویروسهای کوچک در عرض ۳۰ ثانیه این کار را می‌کنند.

۹- علت افزایش حملات ویروسی، افزایش آسیب‌پذیری در سیستم‌ها است. به خاطرداشته باشیم همه سیستم‌ها و ... اعم از مایکرو سافت، لینوکس و ... آسیب پذیرند. همین نکته موجب پیدایش دو رویکرد یکسال شده: افزایش حملات اطلاعاتی= افزایش جنگ اطلاعاتی (دفاع اطلاعاتی).

۱۰- میزان حملات تروریستی معمولی، کم است زیرا علیه اهداف فیزیکی ارتکاب می‌یابند اما بالعکس حملات تروریستی سایبری، زیاد است دلایل آن نیز واضح است: آسیب‌پذیری‌ها در فضای سایبری بسیار زیاد، ارتکاب جرم بسیار آسان، دست‌یابی به اهداف خیلی راحت‌تر، بحران‌های بین‌المللی رو به افزایش و ... است.

۱۱- باید بین حملات اعتراضی / تروریستی و حملات معمولی که توسط سازمان‌های مجرمان سازمان یافته یا اشخاصی برای دسترسی به شماره‌های کارت‌های اعتباری، دسترسی به سیستم‌های مالی و بانکی، مداخله در مبادلات مالی و ... تفاوت قایل شد.

۱۲- حمله‌کنندگان اعتراضی / تروریستی حسب منطقه، کشور، موضوع مورد حمله و ... دسته‌بندی می‌شوند. گروههای عمده این حمله‌کنندگان عبارتند از:

الف - گروههای Israeli -pro

(طرفدار اسرائیل):

این‌ها به وب سایت‌های حامی سازمانهای به زعم آنان تروریستی مانند حماس و حزب‌ا... حمله می‌کنند.

ب- گروههای pro - Palestinian

(طرفدار فلسطین):

این گروهها شامل گروههایی مانند یونیتی، المهاجرون در لندن و ... می‌شود که به وب سایتها واهداف دیجیتالی اسرائیل و ... حمله می‌کنند.

پ-هیپی‌های الکترونیک

(Electro hippies): افرادی که علیه وب سایتهای اسرائیل فعالیت می‌کنند و به سیاست‌های رژیم اشغالگر قدس مانند سیاست‌های شارون و ... اعتراض می‌کنند.

ت- گروههای طرفدار بن لادن مانند القاعده الیانس آن لاین و ... که به طرفداری از بن لادن علیه وب سایتهای آمریکایی فعالیت می‌کنند. این گروهها گاه در خاورمیانه مرکزیت و سکنی دارند مانند گروههای معترض کشمیری و یا force-G در پاکستان.

ث- گروههای خارج از خاورمیانه و آسیا مانند اولد اصلاحی در سوئیس که مورد استفاده القاعده می‌باشند.

ج- گروه چچنی Chechnya)) علیه روسیه و ...

۱۳- برخی گروهها را بعنوان گروههای ضدتروریستی طبقه بندی می‌کنند که البته این طبقه‌بندی، متفق فیه نیست و حسب سیاست خارجی کشورها شاید در زمره گروههای تروریستی جای گیرند مانند:

الف - yihat (هکرهای اطلاعاتی جدید مخالف تروریسم) که علیه منابع مالی تروریست‌ها فعالیت می‌کنند مانند حمله هکری این گروه به دو بانک در خاورمیانه که حساب‌های بن لادن در آن بوده است.

ب- مخالفین وب سایتهای حامی طالبان و بن لادن. و ...

۱۴- مشکل کشورها در مبارزه و به عبارت دیگر در جنگ اطلاعاتی محدود به یک یا دو مشکل نیست. مثلاً یکی از این مشکلات استفاده از زبان محلی و قومی برای اعضا و فعالیت آن گروه در سایت مربوطه خود است که اگر با این زبان آشنایی وجود نداشته باشد مشکل جدی ایجاد می‌کند.

۱۵- با تذکر مجدد این نکته که مفهوم تروریسم سایبری حسب کشور مورد نظر تفاوت می‌یابد و اگر به زعم کشوری، عملی برابر و مساوی با تروریسم سایبری است در کشور دیگر آن عمل جنگ سایبری یا دفاع سایبری است به جا و لازم است به اقدامات ضد تروریستی یا دفاعی اشاره شود:

الف - استفاده از ضد ویروس و جدار آتش.

ب- برنامه Infragard مورد استفاده اف بی آی.

ج- سیستم FAA (سیستم امنیت گشت هوایی).

د- ISACS در صنایع و ...

■ طرح بحث

با نکات کلی که در ۱۵ شماره بالا مرور کردیم حال برخی نکات به عنوان شروع بحث جزایی تروریسم سایبری قابل ذکر است:

الف - تروریسم سایبری با تروریسم معمولی به گونه و به صورت تطبیقی چه وجوه اشتراک و افتراقی دارند؟

ب- سیر تحول تروریسم سایبری؟

پ-تمایز و تفاوت مخالفین با حکومت داخل، مخالفین با حکومت دیگر، مخالفین دارای مرام و ایدئولوژی خاص، تروریست‌های بی‌هدف (کور) و ...؟

برای شناخت تروریسم سایبری باید با تاریخچه و تحول و عمل حملات سایبری، مرتکبین و اشخاص یا شرکتهای موضوع جرم تروریسم سایبری و روش مبارزه و پیشگیری عام آشنا شد

ت-مفهوم تروریسم سایبری: تروریسم سایبری آیا مفهوماً جرم واحد است یا مفهومی است که بر مصادیق مجرمانه متعدد اطلاق می‌شود؟

ت- چگونگی تروریسم سایبری و دفاع سایبری (یا تعبیر درست‌تر جنگ سایبری) در وجوه عمومی و خصوصی و نیز در وجوه کشوری یا عقیدتی / مرامیس؟

ج - اقدامات جهت مبارزه و پیشگیری؟

و ...

حال با این مختصر می‌توان به بحث تروریسم سایبری وارد شد که ان‌شاءا... درمجالی جداگانه، چنین خواهد شد.