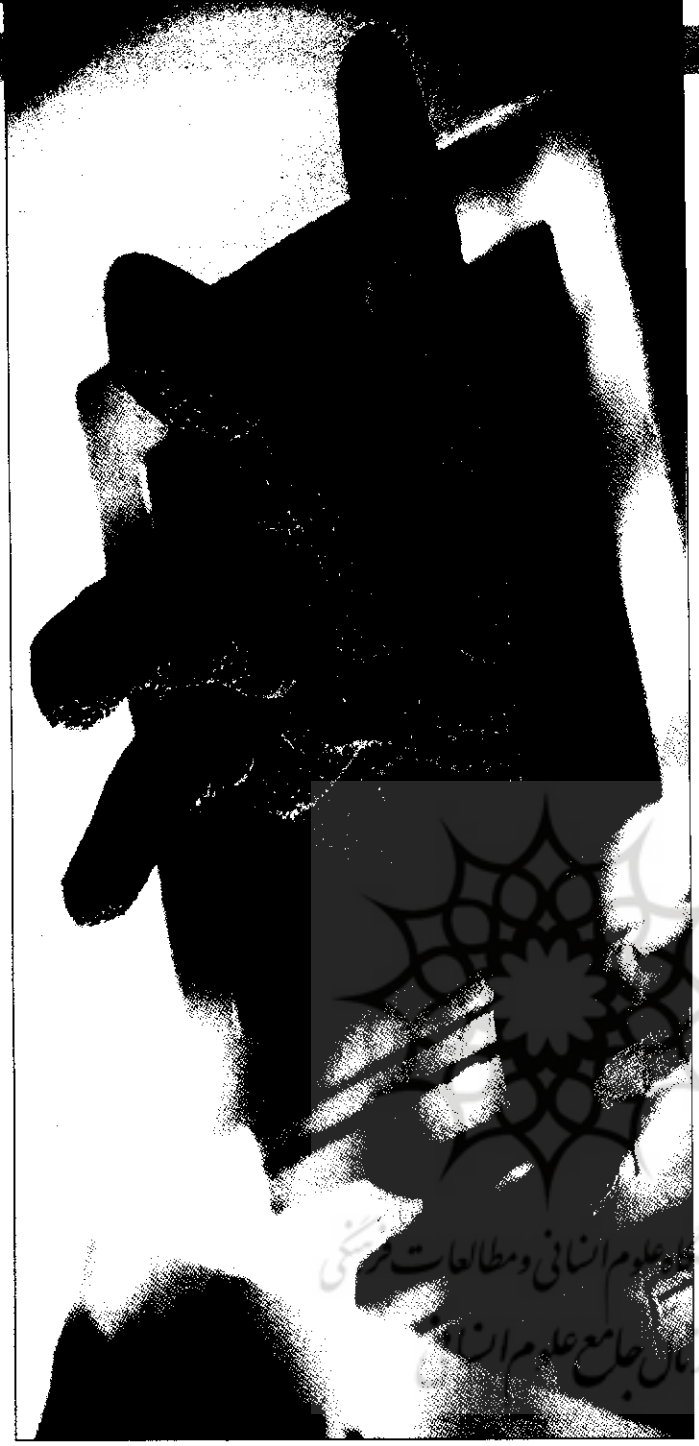


بررسی جرایم کامپیوتری

رادیو، در مدت ۳۸ سال در دسترس ۵۰ میلیون مخاطب قرار گرفت ؛ کامپیوتر، در مدت ۱۶ سال در دسترس ۵۰ میلیون کاربر قرار گرفت ؛ اینترنت، در مدت ۴ سال، در دسترس ۵۰ میلیون کاربر قرار گرفت. کافی است نگاهی به اطراف خودمان بیندازیم. اولین موضوعی که مشاهده خواهیم کرد، انقلاب تکنولوژیکی است که در جامعه در حال وقوع است. در طی ۵ سال آینده کامپیوتر با اتصالات اینترنتی فراگیر، به همان اندازه که امروزه تلفن برای مأموران تحقیق و بازجویان مهم است، از اهمیت ویژه‌ای برخوردار خواهد بود. زیرا کامپیوتر و اتصالات اینترنتی آن، جرایمی را به دنبال می‌آورد که به جرایم کامپیوتری معروف است. ولی به راستی مفهوم جرم کامپیوتری در پرونده‌های روزانه بازجویان کیفری چیست ؟

در این مقاله سعی کرده‌ایم که جرم کامپیوتری را مورد بحث و بررسی قرار دهیم تا بدین وسیله به قانونگذاران و مجریان قانون در پرداختن به نیاز روزافزون برای سرویسهای اجرای قانون کمک بکنیم.

تعریف اصطلاحات:

اصطلاحات گوناگونی برای تعریف جرم کامپیوتری مورد استفاده (و سوء استفاده) قرار می‌گیرد. ما در این مقاله، جرم کامپیوتری را بدین صورت تعریف می‌کنیم: « یک جرم کیفری که با ظهور تکنولوژی کامپیوتر ایجاد شده یا امکان آن به وجود آمده است. یا به عبارت دیگر، یک جرم سنتی که با استفاده از کامپیوتر به گونه‌ای تغییر شکل یافته که مأموران برای رسیدگی به این جرم، نیازمند یک فهم ابتدایی از کامپیوتر هستند. »

این تعریف، دو مجموعه متمایز را شامل می‌شود: الف ـ جرم کامپیوتر[۲] ب ـ جرم مربوط به کامپیوتر[۳]

الف جرم کامپیوتری: متضمن استفاده از کامپیوتر به عنوان ابزار اصلی جرم است که معمولاً شامل این موارد می‌شود: ۱ـ استفاده، دسترسی یا صدمه غیرمجاز به یک سیستم کامپیوتری ؛ ۲ـ دریافت، کپی کردن، تغییر، حذف یا تخریب غیرمجاز اطلاعات، نرم افزارها یا برنامه‌های کامپیوتری ؛ ۳ـ اختلال در سیستمها و یا ممانعت غیرمجاز کاربران از دستیابی به خدمات مجاز کامپیوتری ؛ ۴ـ وارد کردن غیرمجاز یک ویروس کامپیوتری به هر کامپیوتر یا سیستم ؛ ۵ـ استفاده غیرمجاز از نام دامنه اینترنت شخصی دیگر

ب ـ جرم مربوط به کامپیوتر: متضمن استفاده از کامپیوتر، برای ارتکاب یک جرم و یا استفاده از آن به عنوان یک منبع از مدارک مرتبط با جرم است. به طور کلی، این جرم مشتمل بر جرایم سنتی است که به وسیله تکنولوژی کامپیوتری تغییر شکل یافته‌اند ؛ مانند: ۱ـ اسناد جعلی به وجود آمده به وسیله کامپیوتر ؛ ۲ـ تهدید به واسطه کامپیوتر ؛ ۳ـ استفاده و جمع آوری تصاویر مربوط به هرزه‌نگاری (Pornography) کامپیوتری ؛ ۴ـ هر جرمی که در آن اسناد یا مدارک در یک کامپیوتر ذخیره می‌شود ؛ مانند اسناد مربوط به توزیع مواد مخدر، قمار یا اختلاس.

جرم مربوط به کامپیوتر می‌تواند متضمن استفاده از اینترنت برای تسهیل جرایمی مانند جرایم زیر باشد:

۱ـ تقلب در حراج (مزایده) اینترنتی (به طور عمده سرقتها) ؛ ۲ـ تهدیدهای کیفری ؛ ۳ـ تعقیب ایذایی کامپیوتری ؛[۴] ۴ـ تهدید یا مزاحمت برای پست

الکترونیکی ؛ ۵ـ توزیع برهنه نمایی بچه‌ها ؛[۵] ۶ـ بازی قمار در شبکه ؛ ۷ـ معاملات متقلبانه به وسیله کارت اعتباری ؛ ۸ـ تقاضای متقلبانه برای کالاها یا خدمات ؛ ۹ـ سرقت کد شناسایی.

اهمیت شناخت این دو طبقه متمایز، که هر یک نیازمند سطوح متفاوتی از مهارت در بازجویی و رسیدگی هستند، ضروری است. به ویژه، جرایم کامپیوتری که نسبت به جرایم مربوط به کامپیوتر نیازمند سطح بسیار بالاتری از دانش فنی است. در این مقاله، ما به بررسیهای ویژه‌ای در مورد با این دو گروه خواهیم پرداخت.

رسیدگی به جرم کامپیوتری:

بسیاری از افراد، جرم کامپیوتری را به صورت بسیار مضیقی تعریف کرده و آن را تنها موضوعات پیچیده و ویژه کامپیوتر، مانند هک یا جرایم می‌دانند که نیازمند یک بررسی قضائی کامپیوتری هستند. این تعریف از دو جهت اشتباه بزرگی به حساب می‌آید ؛ اول اینکه این تعریف آنچه را که در واقع جرایمی بسیار پیچیده هستند، بیش از اندازه ساده کرده است ؛ ثانیاً اینکه دشواری رسیدگی به جرایم نسبتاً ساده را چند برابر جلوه می‌دهد. در سطح ملّی، مراجع اجرای قانون باید بدانند که بسیاری از قالبهای ساده سرقت و کلاهبرداری، در صورت استفاده از یک کامپیوتر برای ارتکاب جرم، جرایم کامپیوتری محسوب می‌شوند. ممکن است که یک سرقت ساده و دارای ابعاد کوچک به نظر برسد ؛ به گونه‌ای که حتی در بسیاری از موارد گزارش نمی‌شود، ولی در واقع، یک جرم بزرگ با خسارتی سنگین می‌باشد.

ما در اینجا به بررسی مهمترین مسائل مطرح در حوزه جرایم کامپیوتری خواهیم پرداخت. روشن است که این موضوعات، فقط به صورت محدودی در این مقاله قابل بررسی هستند. ولی تحقیقات و اطلاعات روز افزونی در مورد تمامی این عناوین وجود دارد که به طور مسلم مبنای حرکت آینده مجریان قانون قرار خواهند گرفت.

الف ـ ساختار سازمانی[۶]:

۱ـ مسؤولیت بازجویی: اغلب در درون یک مؤسسه، در مورد مسؤولیت رسیدگی به جرایم کامپیوتری سردرگمی وجود دارد. رسیدگی به جرایم کامپیوتری، نیازمند مهارتهای تخصصی در سطح بالا است ؛ در حالی که جرایم مربوط به کامپیوتر، به طور حتم نیازمند این دسته از مهارتها نیست. بنابراین، در خصوص برخورد با جرایم کامپیوتری پیچیده، پرورش افراد متخصص ضروری است. اما در خصوص جرایم سنتی که تنها به وسیله تکنولوژی تسهیل می‌شوند، به طور کلی مسؤولیت واحدهایی که از قدیم به این گونه جرایم رسیدگی کرده‌اند، باید همچنان باقی بماند.

وجه تمایز این دو گروه، در ضرورت تأمین آموزش برای تمام بازجویانی است که با مدارک کامپیوتری در ارتباط هستند ؛ تا بدان وسیله، مسؤولیتهای خود را به بهترین وجه انجام دهند.

۲ـ تخصیص منابع: بسیاری از نمایندگیهای بزرگ پلیس، روش کلی خود را در پرداختن به جرایم کامپیوتری تفکیک کرده‌اند. با این حال، اغلب برای کسب موفقیت در این ناحیه و نیز درک صحیح مسأله و تأثیر آن، یک روش یکسان مورد نیاز است. این روش، شامل شناسایی استعدادها، تقسیم منابع، تجهیزات تخصصی و اجتناب از دوباره کاری و تکرار است. به عبارت دیگر، در حالی که بسیاری از جرایم مربوط به کامپیوتر باید به صورت غیرمتمرکز باقی بمانند. جرایم کامپیوتری پیچیده و رسیدگیهای قضائی باید در درون واحدی که از دسترسی فوری یک محیط آزمایشگاهی کامپیوتری برخوردار است، متمرکز شوند.

۳ـ گزارش جرایم اینترنتی: قربانیان معمولاً جرایم اینترنتی را به نمایندگی پلیس محلی خود گزارش می‌دهند، ولی برخی از این ادارات، قربانی را به اداره پلیس محل اقامت احتمالی مظنون ارجاع می‌دهند. هر چند این امر ممکن است از نظر مراجع اجرای قانون امری منطقی به حساب آید، اما احتمال دارد برای یک قربانی موضوعی کاملاً ناامید کننده باشد و نیز مشکلات بزرگی را برای اداره، اداره ارجاع شده که ممکن است فاصله زیادی تا محل قربانی داشته باشد به همراه بیاورد. شاید راه حل بهتر این باشد که یک سیاست هماهنگ و استاندارد در سطح ملی به وجود بیاید و اداره محلی را ملزم کنیم که گزارش اولیه جرم را از قربانی دریافت کند و آن را به اداره حوزه قضائی صلاحیت دار بفرستد. در این صورت، خدمت به قربانی بهتر انجام می‌شود و اداره دور افتاده مربوط این امر را نوعی تأیید در مورد هویت و ادعای قربانی محسوب خواهد کرد.

۴ـ صلاحیت قضائی بین المللی[۷]: کنترل کمی بر اینترنت وجود دارد و استفاده از آن در میان کشورها فاقد هر گونه مرزی است. موضوع تعیین مرجع صلاحیت دار قضائی، با توجه به این واقعیت که مجرمین غیرقانونی خود را بدون ترس از شناسایی و با آسودگی خاطر در خانه‌های خود انجام می‌دهند)، پیچیده‌تر می‌شود.

به منظور برخورد با این واقعیت، قواعدی باید به وجود آید تا مسؤولیت رسیدگی به جرایم مطرح در سطح بین المللی را به هم مربوط سازد. این امر مستلزم وجود توانایی تبادل فوری مدارک است تا بدین وسیله تعقیب مظنونین در جرایم کامپیوتری ارتکاب یافته در دیگر کشورها، تسهیل گردد.

ب ـ اقدامات لازم برای مبارزه

۱ـ دسترسی به تکنولوژی: همزمان با پیچیدگی روزافزون نرم‌افزار و سخت افزارهای کامپیوتری، مجریان قانون باید بازرسان جریان کامپیوتری خود را به تکنولوژی لازم برای رسیدگی به جرایم پیچیده کامپیوتری مجهز نمایند. همچنین به صورت عملی باید به هر مأموری که برای اجرای رسیدگیهای کیفری تعیین می‌شود یک کامپیوتر با دسترسی به اینترنت واگذار گردد. در دو مورد مذکور آموزش مستمر در زمینه استفاده صحیح از این وسیله امری کاملاً ضروری است.

۲ـ حمایت از علوم قضائی کامپیوتری[۸]: نیاز به حمایت از علوم قضائی کامپیوتر در حال افزایش است. واقعیت این است که بسیاری از جرایم کامپیوتری، هم بر کامپیوتر و هم بر اینترنت از خود «ردپاهایی»[۹] بر جای می‌گذارند. توانایی استخراج آن اطلاعات و ارایه آنها در دادگاه به صورت موثق، یکی از مهمترین تقاضاهای روزافزون در زمینه تکنولوژی کامپیوتر است. همچنین، این توانایی باید با کارهای سنتی دادگاهی و قضائی تلفیق و تکمیل گردد.

سرمایه گذاری خاص دولت در زمینه جرایم کامپیوتری و وجود استانداردها در این ناحیه، امری ضروری خواهد بود که در آن آموزش کارکنان قضائی در زمینه کامپیوتر از ارزش بالایی برخوردار است.

۳ـ آموزش: حتی رسیدگی به عادی‌ترین جرایم کامپیوتر نیز نیازمند مهارتها و منابعی است که از مهارتها و منابع لازم برای مأموران رسیدگی به جرایم مربوط به خطوط تلفن پا را فراتر می‌گذارد.

جرایمی که متضمن استفاده از اینترنت است (از آن جایی که مجرمین تکنولوژی مربوط را می‌آموزند و توسط مجرمین دیگر اینترنتی مورد آموزش قرار می‌گیرند)، هر روز رایجتر می‌شود. به طور کلی، مأموران اجرای قانون، به دلیل کمبود آموزش مدونه و رسمی در زمینه کشف و رسیدگی و تعقیب این نوع از جرایم متضرر می‌شوند.

سطوح دقیق آموزشی، بر حسب سطح «سواد کامپیوتری» هر اداره متفاوت خواهد بود. با این حال، آموزش را باید با اعضای جدید آغاز کرد و آن را به وسیله مدارس تبلیغاتی و ضمن خدمت یک مؤسسه ادامه داد. این آموزش شامل موارد زیر می‌شود:

تشریح موقعیت مدارک مبتنی بر کامپیوتر، استفاده از اینترنت به عنوان یک ابزار رسیدگی، کسب اطلاعات مشترکان از تأمین کنندگان خدمت اینترنتی (۱۰)، کسب مجوزهای جستجو برای جرایم مرتبط با کامپیوتر و روشهای مناسب برای ضبط و ذخیره مدارک موجود در کامپیوتر، ایجاد یک برنامه درسی برای این گونه کلاسها و برنامه‌های آموزش کارآموزان، یک بخش از این طرح خواهد بود که ادارات پلیس را از رسیدگی به جرایم کامپیوتری ـ در حال حاضر و در آینده ـ ورزیده و ماهر خواهد نمود.

بسیاری از دادیاران و دادستانها نیز، همچون همتایان خود در بخش پلیس و کلانتری، برای پرداختن به تعقیب مجرمینی که از اینترنت یا کامپیوتر به عنوان ابزار ارتکاب جرایم استفاده می‌کنند، با کمبود آموزش و تخصص مواجه هستند. دادستانها، اغلب مایل هستند تا با نمونه‌های آشنای پرونده‌ها سروکار داشته باشند و از ورود به زمینه‌های ناآشنا و بیگانه اجتناب کنند؛ ولی اگر در صدد برخورد مؤثر

با این جرایم هستند، باید از یک دانش تجربی در خصوص رسیدگیهای کامپیوتری و اینترنتی برخوردار شوند.

ج ـ قوانین و مقررات:

۱ـ حفظ و نگهداری سوابق اجرایی: هیچ گونه تمهیداتی وجود ندارد که تأمین کنندگان خدمات اینترنتی را ملزم به حفظ و نگهداری اطلاعات استاندارد شده کند. شیوه تأمین کنندگان خدمات اینترنتی، نگهداری از اسناد و سوابق متفاوت است. برخی از مجریان خدمات پست الکترونیک بی نام مدعی هستند که هیچ گونه سوابقی را نگه نمی دارند. فقدان سوابق و دیگر اطلاعات، موجب ناتوانی در هر گونه رسیدگی اینترنتی شده است. نوشتن یک قانون در سطح حکومت ضروری است تا به واسطه الزاماتی برای نگهداری سوابق و دیگر اطلاعات کاری به وجود آید.

۲ـ جستجوی ریشه ارتباطات: قانونی باید تصویب شود که به واسطه آن مراجع اجرای قانون مجاز به ریشه یابی ارتباطات در خصوص رفتارهای مجرمانه باشند. این قانون، تأمین کنندگان خدمات اینترنتی را ملزم خواهد کرد که اطلاعات تبادلی مربوط به ارتباطات مشتریان خود را برای مدت زمان قابل توجهی نگهداری کنند تا بدین وسیله، مراجع اجرای قانون قادر به انجام رسیدگیهای خود باشند. این قانون، همچنین باید تأمین کنندگان خدمات اینترنتی را از بستن حساب ممنوع کند و نیز مانع از آن شود که تأمین کننده این خدمات، مشترک را در خصوص تصمیم مراجع قانون برای کسب اطلاعات مشترک آگاه سازد.

۳ـ استانداردهای ملی برای ارایه گزارش: به منظور ثبت و ضبط دقیق جرایم کامپیوتری، باید استانداردهایی برای گزارش جرم در سطح ملی تدوین گردد. به عنوان مثال، این موضوع که آیا جرمی جزو جرایم کامپیوتری است یا جزو جرایم مربوط به کامپیوتر، نیازمند تدوین گزارشهای استانداردی در زمینه جرایم هست. سپس اطلاعات باید تحت استانداردهای ملی گزارش جرم برای ارایه گزارش قرار بگیرد.

د ـ برنامه های مربوط به پیشگیری:

ما باید گامهایی را در جهت جلوگیری از وقوع جرایم کامپیوتری برداریم. بسیاری از تأمین کنندگان اینترنت و نیز بازرگانانی که به ارایه خدمات به وسیله اینترنت می پردازند، با تمام وجود به دنبال راههایی برای ایمنی معاملات تجاری بر روی شبکه هستند. با این حال، باید تلاشهایی نیز در خصوص آموزش مردم صورت گیرد تا بدین وسیله افراد با آموختن روشهای ویژه، از دسترس مرتکبان جرم اینترنتی مصون بمانند. این آموزش، در مورد والدین ۴۰ میلیون کودک که احتمال دارد تا سال ۲۰۰۲ به استفاده از اینترنت مشغول باشند، از اهمیت ویژه‌ای برخوردار است. در بیشتر خانواده ها، دانش کامپیوتر و توانایی استفاده ماهرانه از کامپیوتر به وسیله اتاقهای چت و سایتها به فرزندان مربوط می شود.

بسیاری از والدین حتی حاضر نیستند که به بچه های خود اجازه دهند به تنهایی به مغازه بروند یا بدون نظارت بزرگتر در یک پارک بازی کنند. اما در عین حال، اکثر والدین نسبت به خطرات موجود در کامپیوتر بی اعتنا هستند و برای ایمن نگهداشتن خانواده ها و بچه های خود از متجاوزان کامپیوتری از دانش کافی برخوردار نیستند.

ما برای شناسایی الگوهای متجاوزان کامپیوتری و ارایه برنامه های پیشگیری در خصوص سوء استفاده از اینترنت نیازمند همکاری هستیم. در این کوشش، ما باید با همکاران واقعی خود، همچون مدارس، همکاری کنیم.

(همکاری مدارس در این زمینه، بدین صورت است که به والدین و فرزندان آنها آموزشهای لازم را در خصوص کلاهبرداری اینترنتی، سرقت هویت، سوء استفاده جنسی و هرزه نگاری ارایه نمایند). برای والدین باید کلاسهای آموزشی کوتاه در خصوص استفاده ابتدایی از اینترنت فراهم گردد.

همچنین باید آموزش لازم به والدین داده شود تا برای جلوگیری از استفاده مخرب از کامپیوتر کنترلهایی را به وجود آورند. فرزندان نیز باید در خصوص موارد زیر آموزش ببینند:

۱ـ خطرات ناشی از مبادله اطلاعات شخصی؛

۲ـ دیدار با افراد به وسیله اینترنت؛

۳ـ گفتگوی اتاق چت که ممکن است امنیت شخصی، اخلاقیات و ارزشهای خانوادگی آنها را به خطر بیندازد؛

۴ـ فرزندان و والدین باید بدانند که در صورت وقوع جرایم، چگونه آنها را شناسایی کنند و چه موقع و به چه کسی باید وقوع یک حادثه را گزارش دهند.

هـ ـ توصیه ها و پیشنهادات

۱ـ در خصوص جرایمی که به واسطه تکنولوژی تغییر شکل یافته اند یا تنها مستلزم استفاده از یک کامپیوتر هستند (جرم مربوط به کامپیوتر)، مسؤولیت بازرسانی که به طور سنتی به رسیدگی به این جرایم می پردازند، همچنان باید باقی بماند.

۲ـ جرایم پیچیده تر کامپیوتری (جرایم کامپیوتری) باید در درون یک اداره متمرکز شوند و مأموران رسیدگی به این جرایم به منظور اجرای رسیدگیهای قضائی کامپیوتری باید از دسترسی فوری به یک محیط آزمایشگاهی کامپیوتری برخوردار باشند.

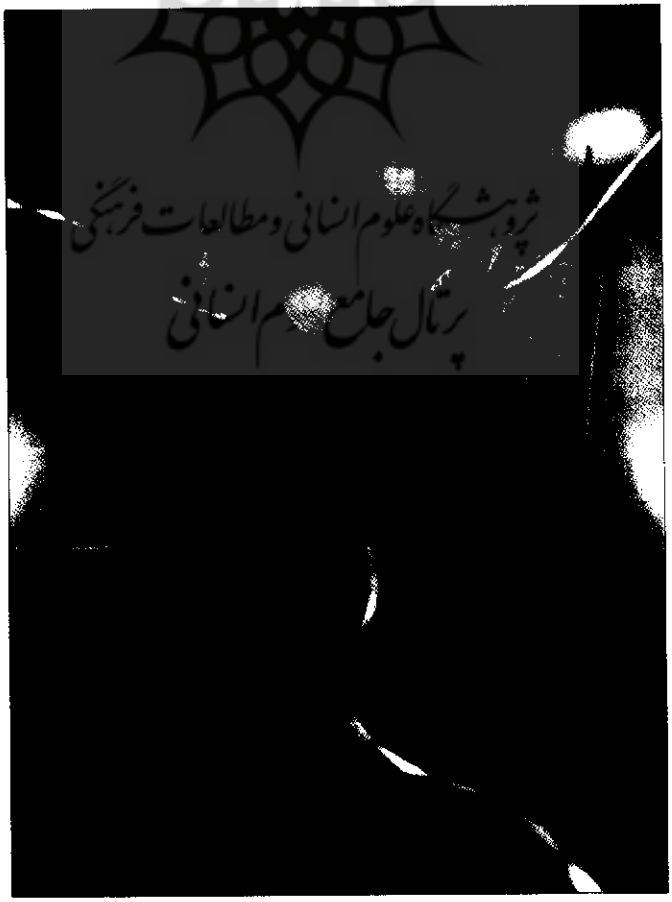
۳ـ همزمان با رشد و تکامل جرم کامپیوتری، لازم است که مراجع اجرای قانون، به ایجاد روابط کاری مستحکم با همتایان خود در بخش خصوصی بپردازند تا بدین وسیله، جرایم مربوط به مصالح دو طرفه را به طور مشترک مورد رسیدگی قرار دهند.

۴ـ اداره‌ای که قربانی جرم مربوط به اینترنت با آن تماس برقرار نموده‌اند، باید به جای ارجاع قربانی به اداره دیگر، گزارش رسیدگی مقدماتی را تکمیل نماید.

۶ـ به منظور ثبت و ضبط اطلاعات مربوط به جرایم کامپیوتری، استانداردهای ملی برای گزارش جرم باید به صورت هماهنگ و پیشرفته درآید.

۷ـ به منظور هماهنگی مسؤولیت رسیدگی به جرایم در سطح بین المللی، باید قواعدی به وجود بیاید.

۸ـ قانونی باید تصویب شود که تضمین کند که تأمین کنندگان خدمات اینترنتی سوابق معاملاتی خود را حفظ و نگهداری کنند. همچنین این قانون باید موجب افزایش قدرت مراجع اجرای قانون در خصوص ردیابی به ریشه اطلاعات گردد.



۹ـ مراجع اجرای قانون باید رهبری ترویج اطلاعات مربوط به پیشگیری از جرایم کامپیوتری را در راستای آموزش عمومی بر عهده بگیرند.

سخنرانی دادستان ایالات متحده در نخستین گردهمایی سالیانه محرمانگی، سیاست و امنیت کامپیوتری

اظهارات جان اشکرافت دادستان ایالت متحده:

دغدغه هایی که موجب حضور در این گردهمایی شده است، یعنی امنیت کامپیوتری و دارائیهای اطلاعاتی، برای همه ما اهمیت اساسی دارد. تا چند سال پیش چنین کنفرانسهایی به ندرت برگزار می شد. «کرمها و ویروسها»، در متون زیست شناسی تعریف می شد نه در گزارشهای پلیسی ارتباطی و زیربنایی و میلیاردها دلار خسارت را ذهن متبادر می کند. اینترنت نیز مانند تکنولوژیهای انقلابی پیش از خود، ظرفیتهای فوق العاده‌ای را هم برای پیشرفت و هم برای سوء استفاده دربر دارد.

حمله به شبکه ها، کلاهبرداریها، سرقت برنامه ها، جاسوسی گروهی و خرید و فروش غیرقانونی هرزه نگاری کودکان، فقط بخشی از جرایمی هستند که اینترنت موجب تسهیل آنها شده است. اگر چه ارقام دقیقی از خسارات ناشی از جرایم کامپیوتری در آمریکا در دسترس نیست، اما این خسارات سالانه میلیاردها دلار برآورد می شوند و برخلاف جریان سنتی تر، تحقیق و تعقیب جرایم کامپیوتری امری مشکل می باشد؛ زیرا:

اولاً: اینترنت می تواند موجب عدم شناسایی شود در اینترنت، ایجاد یک هویت موهوم برای یک مجرم جهت ارتکاب کلاهبرداری، اخاذی و جرایم دیگر، کاری آسان است. از آنجا که بسیاری از جرایم کامپیوتری از جمله خرید و فروش برنامه های سرقت شده یا هرزه نگاری کودکان را می توان در روی شبکه (به صورت Onlne) مرتکب شد، این عدم شناسایی به صورت عمده‌ای می تواند تحقیق و تعقیب را پیچیده نماید.

ثانیاً: ماهیت بدون مرز اینترنت، این مشکلات را وخیمتر می کند. اگر یک مجرم در هر نقطه دنیا فقط به یک کامپیوتر شخصی مجهز به مودم وصل باشد، می تواند علیه افراد و تجارتها در سطح جهان مرتکب جرم شود.

ثالثاً: قدرت فوق العاده کامپیوترهای امروزی یک مجرم کامپیوتری را قادر می سازد تا خسارتهای وحشتناکی به بار آورد؛ خسارتهایی به مراتب بیش از آنچه یک شخص معمولی می توانست در جرایم سنتی موجب شود. برای مثال، یک مجرم زبده کامپیوتری می تواند ویروسی منتشر کند یا یک حمله رد سرویس انجام دهد که صدها هزار کاربر کامپیوتری یا زیر ساختهای حیاتی ـ مانند شبکه های قدرت ـ را در برگیرد.

علاوه بر آن، ما فقط با تهدیدهای فنی مواجه نیستیم. حتی اگر ما بتوانیم تمامی تکنولوژی را کنترل کنیم، بعد انسانی جرایم کامپیوتری تهدیدات خاص خود را در پی دارد. متأسفانه در میان بسیاری از افراد ـ به خصوص جوانان ـ این سوء برداشت وجود دارد که میزان جرایمی که بر روی شبکه (به صورت Online) ارتکاب می یابند، از جرایم سنتی تر کمتر است. وزارت دادگستری تمامی تلاش خود را صرف مقابله با این تهدیدات می نماید.

۱ـ ما آموزش دادیاران و عوامل مربوط به این بخش را به صورت چشمگیری افزایش داده ایم؛ بخشی از شاخه جنایی وزارت دادگستری، یعنی بخش جرایم کامپیوتری و مالکیت معنوی، به مبارزه با جرایم کامپیوتری اختصاص دارد. علاوه بر آن، FBL در شانزده منطقه مرکزی کشور، گروههای ویژه جرایم کامپیوتری جهت تحقیق و تعقیب این جرایم تأسیس کرده است.

در واشنگتن، «مرکز ملی حمایت از زیرساختها»[11] به عنوان یک «اتاق پایاپای برای اطلاعات»[12] و تخصص مربوط به جرایم کامپیوتری عمل می کند و هر منطقه قضائی فدرال، از جمله منطقه مونتانا (Montana)، حداقل دارای یک معاون دادستان ایالات متحده و یک مدیر کامپیوتر و مخابرات است که در خصوص چگونگی تحقیق و تعقیب جرایم کامپیوتری آموزش ویژه دیده اند.

۲ـ ما با همتایان خارجی خود در اجرای قانون جهت مواجه با جهانی بودن جرایم کامپیوتری همکاری نموده ایم. جمعیتهایی مانند گروه هشت کشور صنعتی و شورای اروپا، ما را به ابزار بررسی و ایجاد راههای بهتر جهت تحقیق و تعقیب جرایم کامپیوتری که مرزها را در می نوردند، مجهز نموده اند.

۳ـ FBL با اجرای برنامه Ingragard مشارکتی منحصر به فرد میان وزارت دادگستری، تجارتخانه ها، مؤسسات دانشگاهی و عوامل حکومتی و محلی اجرای قانون، امنیت زیرساختهای حیاتی ایالات متحده را افزایش داده است.

در نهایت، ما مجرمان کامپیوتری را زندانی می کنیم. بازداشت و محکومیت تهیه کنندگان ویروس Melessa در ایالات متحده و ویروس Mafiaboy در کانادا، بیانگر توانایی ما در مورد برخورد با مرتکبان جرایم کامپیوتری است؛ حتی اگر این جرایم در سطح وسیع یا در خارج از مرزها ارتکاب یابند.

تجربه به ما نشان داده است که وقتی از یک بانک سرقت می شود، مسؤولین بانک به پلیس اطلاع می دهند؛ ولی هنگامی که اطلاعات ارزشمند تجاری از کامپیوترها به سرقت می رود، به ندرت قربانیان این جرایم مجریان قانون را از موضوع مطلع می سازند. این امر، دلایل متفاوتی می تواند داشته باشد؛ زیرا مدیران این بانکها تصور می کنند که کامپیوترهایشان از امنیت لازم برخوردار هستند، ولی چون چنین امنیتی ندارند، ممکن است به عدم اعتماد مشتری و زیانهای رقابتی منجر شود و یا این تحقیق و بازرسی، تجارت آنها را مختل سازد.

با این حال، می دانیم که شرکتی که جرایم کامپیوتری را به مجریان قانون گزارش نمی دهد، ممکن است خود را در موقعیتی بسیار بدتر از آنچه تصور می کرد بیابد. شرکتی که جرایم کامپیوتری را گزارش نمی کند، مجرم را در حمله دوباره آزاد می گذارد. اگر یک سارق کامپیوتری به شبکه شما نفوذ و شماره های کارت اعتباری را از پایگاههای اطلاعاتی شما سرقت کند و یا دارائیهای معنوی ارزشمندی از شما برباید، ممکن است راه میان بر جدیدی به شبکه شما ایجاد کرده باشد تا در صورتی که شما راه اصلی وی را مسدود کنید، از آن استفاده کند.

عدم گزارش جرایم کامپیوتری، همچنین انگیزه های جدیدی برای حملات مکرر علیه شما ایجاد می کند.

مجرمان کامپیوتری با یکدیگر در ارتباط هستند و در صورتی که شما گزارش نکنید، به عنوان یک قربانی سهل الوصول تلقی می شوید.

بنابراین، ما به تنهایی نمی توانیم این مشکل (جرایم کامپیوتری) را حل کنیم و احتیاج به کمک شما در گزارش جرایم داریم؛ چرا که ما به این امر واقف هستیم که میزان قابل توجهی از جرایم به طور کامل گزارش نمی شوند.

تجربه ما به شهروندانی که مرتکب جرایم را گزارش می کنند، تجربه‌ای فوق العاده بوده است و در نتیجه همکاری آنها، اخیراً گروهی از مظنونین به اخاذی و تجاوزهای کامپیوتری را دستگیر کردیم که علیه میشل بلومبرگ (Michael Bloomberg) و شرکت وی توسط افرادی در قزاقستان برنامه ریزی می شوند تا حدود زیادی اخبار مربوط به موفقیتها به گزارش منظم قربانیان بستگی داشته است.

منتخب از خبرنامه حقوق فناوری

پی نوشت:

1-Cyber Crime
2-Computer Crime
3-Computer_ Related Crime
4-Stalking
5-Child Pornography
6-Organizational Structure
7-International Jurisdiction
8-Forensic Computer Support
9-Foot Prints
10-Internet Service Providers(ISP)
11-FBL's National Infrastructure Protection Center
12-Clearin ghouse for Information and Expertise Relating Cubercrime

منابع:

http://www.neiassociates.org/cybercrime.htm
http://www.cybercrime gov/agcppsi.htm