تحقیقات جرایم رایانه‌ای در ایالات متحده:

قدرت دانش گذشته برای مقابله با آینده

چکیده

در حال حاضر بسیاری از جرایم سنتی با کمک و یاری استفاده از رایانه‌ها و شبکه قابل رسیدگی است و قبلا هرگز تصور نمی‌شد به دلیل قابلیت‌های باور نکردنی سیستم‌های اطلاعاتی تخلفات قابل پیگیری باشد. جرایم رایانه‌ای نیاز به اجرای قانون در تحقیقات دارند و به‌طورکلی جنایات خاص برای موفقیت در شناسایی، دستگیری و کمک به تعقیب موفقیت‌آمیز مجرمان به تلاش زیادی نیاز دارند. در متن زیر، یافته‌های پژوهش در حوزه‌ی سنتی تحقیقات جنایی آمریکا خلاصه شده است. شابهت‌ها و تفاوت‌ها بین جرم و جنایت سنتی و کامپیوتری و تحقیقات پس از آن ارائه شده است و مفاهیم به‌دست آمده بحث شده است. پیشنهادهای عملی مانند چگونگی تحقیق نیروها در جرم و جنایت رایانه‌ای آمریکا می‌تواند اهداف مورد نظر خود را در نتیجه‌گیری از طریق یک مثال فرضی از یک واحد داده تخصصی برآورده کند. امید است که دانش گذشته بتواند با جذب جریان مشاهدات جنایت مربوط به رایانه برای اطلاع‌رسانی و هدایت تحقیقات پلیس در آینده مورد استفاده قرار گیرد.

کلمات کلیدی: جرم‌وجنایت رایانه‌ای، تحقیقات، پلیس، اجرای قانون، اینترنت، فن‌آوری بالا، عدالت

معرفی

تحقیقات جنایی یک موضوع مطالعه یکسان برای دانشگاهیان و پزشکان است و به‌عنوان "روند قانونی جمع‌آوری شواهد جرم که در حال ارتکاب است » تعریف می‌شود (براون، 2001: 3). که به‌دنبال شناسایی حقایق مرتبط با چگونگی و چرایی جرم و جنایت رخ داده است و در جهت ایجاد موردی است که ممکن است منجر ایفای جرم شده است. بسیاری از مطالعات تحقیقاتی به‌دنبال تعیین بهترین راه هستند تا فرایند تحقیقاتی بتواند راحت‌تر اداره شود. هدف اساسی از این مطالعات فعال کردن پلیس است تا اعمال خود را در برابر پس‌زمینه این یافته‌ها منعکس کنند و پس از آن پیاده‌سازی تغییرات مثبت و برجسته عملیات، روزبه‌روز بهبود یابد. شیوه‌های تحقیق در طول سال‌ها با توجه به تغییرات حساب در اجتماع، سیاست، اقتصادی و دامنه علمی اصلاح و تصفیه شده است. این شیوه «علم» به یک فعالیت که القا شده است عمدتا به‌عنوان 'هنر' در نظر گرفته می‌شود (بوریج، 1957)، و در نتیجه فرآیند تحقیقاتی افزایش یافته است.

در درج قانون خود، Tarde Gabriel ([1890] 1903) اظهار داشت که صور جدید رفتار مجرمانه از طریق درج پرورش شیوه‌های جدید بر روی آنهایی که سنتی هستند، اغلب از طریق فن‌آوری پیشرفت یا نوآوری انجام می‌گیرد. با توجه به رشد نمایی اطلاعات فن‌آوری در جامعه مدرن، بسیاری از جرایم سنتی درحال‌حاضر با کمک و یاری رایانه‌ها و شبکه پشتیبانی می‌شود و پیش از جرم و جنایت هرگز تصور نمی‌کردند که سیستم‌های اطلاعاتی قابلیت‌های باور نکردنی داشته باشند. جرایم رایانه‌ای[1] نیاز به اجرای قانون خواهند داشت و به‌طورکلی جنایات خاص برای موفقیت در شناسایی، دستگیری و کمک به تعقیب موفقیت‌آمیز مجرمان به تلاش زیادی نیاز دارند.

به‌منظور توسعه استراتژی صدا در این زمینه، یادگیری تحقیقات گذشته در این منطقه از تحقیقات بسیار مهم است و به‌عنوان سمبلی برای سازمان‌های اعمال قانون این سیاست تلقی می‌شود. در متن زیر، خلاصه‌ای از دو مطالعه‌ی مهم در تحقیقات سنتی امریکا به‌منظور ارائه یک موقعیت تاریخی و تطبیقی بیان شده است. سپس، شباهت‌ها و تفاوت بین

[1] تمرکز این مقاله بر تحقیقات زیر است: 1) جنایات سنتی که در آن کامپیوتر به شیوه‌ای فرعی استفاده شده است و 2) جنایات غیرسنتی و یا با تکنولوژی بالا که در آن کامپیوتر ابزار اولیه و یا مخزن مدارک مربوط به یک جرم و جنایت است.

تحقیقات جرایم سنتی و رایانه‌ای آورده شده است، و مفاهیم منتج از بحث عبارتند از: نقش اولین پاسخ افسر و محقق؛ اطلاعات، ابزار دقیق، مصاحبه؛ جمع‌آوری شواهد و پردازش؛ مسائل اداری و قضایی؛ استراتژی واکنش و فعال؛ و استفاده از تحقیقات نمادین است. درحال‌حاضر برخی پیشنهادات عملگرا مانند چگونگی تحقیق نیروهای وظیفه در جرایم رایانه‌ای باید ایجاد شود و به‌شایستگی در جهت تحقق اهداف مدیریت شود. که از طریق یک مثال فرضی از یک واحد تخصصی ارائه شده است.

تحقیق ابتدایی در تحقیقات

مطالعه Rand در تحقیقات جنایی

در سال 1970، شرکت Rand در ایالات متحده (US) یک مطالعه از تحقیقات جنایی در سراسر کشور توسط بخش‌های اجرای قانون با بیش از 150 افسر قسم خورده و یا خدمت جمعیت بیش از 100.000 انجام گرفت. از طریق تجزیه‌وتحلیل سازمان‌های مختلف با فلسفه تحقیقی متفاوت، مقایسه با آمار رسمی جرایم برای تعیین اثربخشی تحقیق و بازنگری دقیق مطالعات انجام شده پرونده ، درکی از چگونگی سازمان‌های مدیریت و سازماندهی تحقیقات بدست آمد. چهار نتیجه اصلی مطرح شده:

1. راه‌حل پرونده: تعیین مهم‌ترین راه‌حل پرونده، اطلاعات به‌دست آمده توسط قربانی برای افسر بود (Grenwood، Chaiken، و Petersilia، 1977). همچنین کشف شد که پیگیری تحقیقات تا حد زیادی بی اثر بودند. به‌طورخاص، درصورتی که قربانی قادر به ارائه اطلاعات شناسایی مجرم نباشد، بعید نبود که موجب دلهره شود. اهمیت این افسر، نیاز به پرسنل گشت را که به‌خوبی آموزش دیده باشند پررنگ‌تر کرده است، که پس از آن قادر به بستن بسیاری از پرونده‌ها به‌جای واگذاری آنها به شخص دیگری هستند (نگاه کنید به، block و Weidman، 1975؛ Greenberg، Elliot، Kraft، و Protor، 1977). به‌عنوان یک نتیجه، این اجازه می‌دهد تا نیروهای تحقیقی تخصصی برای رسیدگی به آن دسته از حوادثی که کاملا نیاز به توانایی‌های تخصصی دارد اندازه قابل کنترل از پرونده را حفظ کنند.

2. اثر تحقیقاتی: تفاوت در سازمان تحقیق، آموزش، نیروی انسانی، حجم کار و روش انجام با نرخ جرایم، دستگیری، و یا نرخ رسیدگی متناسب نیست.

3. پردازش شواهد فیزیکی: درحالی‌که بخش‌های اجرای قانون مقدار زیادی از شواهد فیزیکی را جمع‌آوری می‌کنند، که بیشتر آن‌ها در پردازش شیوه‌ای موثر هستند. به این ترتیب، سیاست پیشنهادی، درگیر تخصیص منابع بیشتر به پردازش شواهد جمع‌آوری می‌شود، که در نتیجه تاثیر مثبتی بر حل جرایم دارد.

4. نظم و دقت تحقیقاتی: به‌طورکلی محققان در سند کردن همه‌ی مدارک حقایق مهم که توانایی دادستان برای به‌دست آوردن مناسب‌ترین تصمیمات را تقویت می‌کند، شکست می‌خورند. ناتمامیت در اسناد و مدارک، که استدلال شده بود، ممکن است به افزایش تعداد ناکامی‌ها در پرونده کمک کند و یک تضعیف در درخواست تجدیدنظر دادستان ایجاد کند (Greenwood و همکارانش 1977). این نقص در ثبت جامعیت ضروری است.

مطالعه PERF در بررسی دزدی و سرقت

در یک مطالعه مهم توسط John Eck تحت نظارت انجمن تحقیقات پلیس رهبری (PERF)، بیش از 3360 سرقت و 320 تحقیقات سرقت در طی یک دوره دو ساله در سه حوزه قضایی: Dekalb County، گرجستان؛ سن پترزبورگ، فلوریدا؛ و ویچیتا، کانزاس تجزیه تحلیل شد. مطالعه PERF از پژوهش‌های پیشین توسط RAND که در آن به‌جای موارد دستگیری بر کل فرایند تحقیقاتی متمرکز بود متفاوت است. به‌این ترتیب، Eck قادر به تعیین تاثیر یک میزبان از متغیرها که نتیجه را با درجه‌ی نامتناسبی تحت تاثیر قرار می‌دهد شد.

یافته‌های اولیه که در آن هر دو کارآگاهان و ماموران گشت به اندازه یکسان در حل پرونده‌ها کمک می‌کردند، زیانی بود یکی را بر دیگری ترجیح می‌داد (Eck، 1983). این تحقیق همچنین نشان داد که افراد در هر دو موقعیت باید کمتر بر اطلاعات ارائه شده توسط قربانی متکی باشند و در زمینه کاوش مربوط به این حادثه فعال‌تر باشند (Eck ،

1983). عمل رأی‌گیری و استفاده از خبرچینان به‌عنوان تکنیک مهمی برای افزایش اثربخشی تحقیقات تأکید شد. به‌نظر می‌رسد که بسیاری از اطلاعات قربانیان جرایم در پاسخ اولیه به پلیس، بی‌ثمر هستند. زمانی که دیگر منابع مورد مشورت قرار گرفتند، بااین‌حال، اطلاعات بسیار مفیدتر کشف شدند.

ضرورت حساسیت به قربانیان نیز توسط Eck تاکید شده است، که بی‌ثمری نسبی اظهارات قربانی در طول تحقیقات بعدی را نشان می‌دهد. شواهد فیزیکی برای اثبات هویت موجود و نه به‌عنوان وسیله‌ای برای شناسایی مظنون که قبلا ناشناخته بود بیشتر مفید واقع می‌شود (Sanders، 1977؛ Wilson، 1976). همکاری، تبادل اطلاعات و مدیریت اطلاعات در میان ادارات پلیس نیز به‌عنوان عوامل کلیدی در موفقیت‌آمیز بودن تحقیقات مورد ستایش قرار گرفته است (Eck ، 1983).

یکی از توصیه‌های عملی ناشی از مطالعه Eck طبقه‌بندی موارد مربوط به سه گروه است - کسانی که می‌توانند حل شوند، کسانی حل شده هستند و کسانی که ممکن است از طریق برخی از تلاش‌ها حل شوند(Brown، 2001). این سیستم تریاژ برای کمک به پرسنل اجرای قانون در تصمیم‌گیری هدف ابداع شد. از طریق فرم غربالگری، تحقیقات می‌تواند با هدفمندی و شیوه‌ای آگاهانه پس از تعیین حضور عوامل خاص که به احتمال زیاد منجر به حادثه شده است ادامه یابد. علاوه‌براین، این روش به قانون اجازه می‌دهد تا تلاش‌های خود را به سمت گروه کوچکی از مجرمین یا مجرمان حرفه‌ای، که مرتکب اکثریت جنایات جدی می‌شوند سوق دهد (Wolfgang، Figlio، و Sellin، 1972). Eck احساس کرد که این تغییرات توصیه شده یک راه طولانی در پالایش فرآیند و بهبود ابزار و میزان موفقیت آن است.

از این دو تحقیق فشرده در ایالات متحده، برخی درس‌های مهم می‌توان آموخت. نخست، نقش افسر پاسخ در تحقیقات بسیار مهم است و اغلب اطلاعات ارائه شده به او و یا تصمیم‌گیری او در حل یک پرونده مهم است. علاوه‌براین، به‌نظر می‌رسد که گسترش وسعت تحقیقات از طریق بررسی راه‌های دیگر کسب اطلاعات ممکن است منجر به اثبات ارزش، که می‌تواند در این روش به دست آید شود. تخصیص منابع فقط به مواردی که احتمال زیادی برای حل شدن دارند،

استراتژی عاقلانه دیگری است که گروه اجرای قانون می‌تواند به‌دست گیرد. در نهایت، نظم و دقت در پرونده‌سازی اسناد و مدارک مهم است و احتمال محکومیت و تحت پیگرد قانونی قرار گرفتن را افزایش می‌دهد.

تفاوت تعاریف

همانطور که گفته شد، شیوه‌های تحقیقی برای هر دو جنایات سنتی و جرایم رایانه‌ای اشکال بسیار توسعه یافته‌ای به خود گرفته است. در بسیاری از جهات تنها به‌دلیل روند بازگشتی ذاتی در اصلاح جنایات سنتی از طریق نوآوری و یا فن‌آوری توسعه مشابه است (Tarde،]1890 [1903). بااین‌حال، تفاوت‌های حیاتی در وجود فرآیند تحقیقاتی وجود دارد و این باید برای رسیدگی بهتر جرایم رایانه‌ای جایگزین شود. این تفاوت‌ها تا حد زیادی توسط تفاوت تعریف آن نشان داده شدند.

جنایات سنتی به‌طورکلی مربوط به جرائم شخصی و یا اموالی هستند که اجرای قانون همچنان برای مبارزه با آن قرن‌ها ادامه دارد مانند 1 : جرایم گزارش FBI در آمریکا.

جنایات غیرسنتی، برای اهداف کار فعلی، شامل کسانی است که با رایانه درگیر هستند. این تاریخچه یک مقدار متناسب از توجه نسبی به جنایات سنتی را علی‌رغم وخامت و آسیب اساسی آنها بیان می‌کند (Braitewaite، 1985؛ Hinduja، 2004؛ Newman و Clarke، 2003؛ Parker، 1976؛ Rosoff، Pontell، و Tillman، 2002؛ Webster، 1980). علاوه‌براین، آنها واکنش و بار عاطفی یکسانی از مردم آمریکا و نظام سیاسی در انجام جنایات شخصی که پلیس تا حد زیادی کار می‌کند می‌بینند (Benson، Cullen، و Maakestad، 1990؛ Cullen ، Link، و Polanzi، 1982). از آنجا که این اشخاص به‌طور قابل توجهی سیاست‌ها و اقدامات عدالت کیفری آمریکا را تحت تاثیر سیستم قرار می‌دهند، در نتیجه یک مقدار نسبتا کمی از تلاش‌ها و منابع برای جرایم رایانه‌ای اختصاص می‌یابد. جرایم رایانه‌ای به‌عنوان، هر عمل غیرقانونی جهت ترویج و یا با بهره‌گیری از یک رایانه تعریف شده است، که آیا رایانه یک شی از یک جرم است، یک ابزار مورد استفاده برای ارتکاب جرم است و یا یک مخزن از شواهد مربوط به یک جرم است (Royal Canadian Mounted Police، 2000). برخی از مهم‌ترین انواع برجسته شامل تقلب تجارت

الکترونیک، قاچاق پورنوگرافی کودکان، دزدی نرم‌افزار و نقض امنیت شبکه می‌باشد. مشکلات تحقیق هنگامی که در تلاش برای مقابله با جرایم رایانه‌ای به‌دلیل کلی طبیعت و پیشرفت ان هستیم معرفی می‌شود، این واقعیت است که می‌تواند تقریبا بلافاصله رخ دهد و به‌دلیل مشاهده، تشخیص، و یا توالی آن سیار دشوار است (Leibowitz، 1999؛ سازمان ملل متحد، 1994؛ Wittes، 1994). این مشکلات توسط گمنامی نسبی توسط اینترنت و همچنین محدودیت جغرافیایی و فیزیکی در فضای مجازی فراهم شده است، که هر دو تشخیص جنایتکاران را که قادر به استفاده از یک استخر تقریبا بی حدوحصر قربانیان هستند دشوار می‌کند.

نرم‌افزار و فرمت جرایم رایانه‌ای

بسیاری از جنبه‌های مربوط به تحقیقات لزوما دخیل هستند که با توجه به شیوه‌های سنتی باید با تفاوت ذاتی در جبران جرایم رایانه‌ای اصلاح ، تقویت و یا حتی بازسازی شوند. درحالی‌که هیچ نوشدارویی قابل اجرا وجود ندارد، به‌نظر می‌رسد که اعتراف و انطباق نکات زیر در نتیجه اثر تحقیق بیشتر زمانی در پرداختن به فن‌آوری بالای تخلف است. قبل از ادامه، باید گفت که این کار به‌طور خاص بر تحقیقات جرایم رایانه‌ای است، برخی از نمونه‌های جرم یقه سفید است که می‌تواند از طریق استفاده از رایانه در سیستم‌های ارائه شده برای حمایت از اظهارات رخ دهد.

نقش افسر اول-در پاسخ

همانطور که قبلا گفته شد، یکی از مهم‌ترین یافته در مطالعه RAND نگرانی در مورد نقش افسران گشت است که برای اولین‌بار به صحنه جرم می‌رسند. پیشنهاد شده است که اولین پاسخ‌دهندگان مسئولیت تحقیقاتی اضافی برای کاهش حجم فشار ناشی از تحقیق تخصصی دارند و به‌دلیل حضور اولیه در صحنه، اغلب آنها اطلاعات را برای استفاده در کشف علت استفاده می‌کنند (نگاه کنید به مثال، Block و Weidman، 1975؛ Greenberg و همکارانش، 1977). با گسترش روز افزون، نقش مامور اول پاسخ در اجرای قانون در جرایم رایانه‌ای به دلیل انتقادات وارده و شواهد در ارتباط با جرایم رایانه‌ای اغلب در طبیعت نامشهود است. اقدامات احتیاطی خاصی باید انجام شود تا اطمینان

حاصل شود که داده ذخیره شده بر روی یک سیستم و یا بر روی رسانه‌های جداشدنی اصلاح و یا حذف شده است که عمدا به‌طور تصادفی است (Lyman، 2002؛ Parker، 1976). حتی بستن ساده یک رایانه می‌تواند آخرین تغییرات و یا آخرین دسترسی‌ها را در فایل‌های سیستم خاص، که به معرفی پرسش مرتبط با یکپارچگی داده می‌پردازند تغییر دهد. در مجموع، جهت جلوگیری از آسیب‌پذیری در پرونده دادستانی و دفاع به‌اندازه کافی در برابر هر گونه چالش مرتبط، مراقبت باید توسط اولین پاسخ‌دهندگان در جستجو و تشنج تجهیزات کامپیوتری اعمال شود.

برخی از تشابهات موضوع در دست، مجموعه‌ای از مو، مایعات بدن و نمونه لباس که از آن DNA استخراج شده است، را به تصویر می‌کشد. آنها هیچ استفاده‌ی آشکاری از جزیه‌وتحلیل جرم‌شناسی متخصص ندارند و در نتیجه پزشکی قانونی اهمیت آنها را تعیین می‌کند. هنگامی که دانش به دست آمده از این نمونه‌ها با پرسنل آموزش دیده مستدل و اثبات می‌شود، تحقیقات و تلاش در جهت دستیابی به همراه عدالت است. در یک حالت مشابه، مهارت‌های تخصصی باید به افسران اولین-پاسخ آموزش داده شود که ممکن است با شواهد فن‌آوری که ممکن است موجب تجزیه‌وتحلیل بیشتر شود روبرو شوند اما پزشکی قانونی محققین رایانه‌ای ممکن است در نقل و انتقال بانکی یک پرونده بسیار مهم باشد.

نقش محقق

پژوهش Greenwood و همکارانش (1977) اظهار داشت که بیش از 50٪ جنایات سنتی خیابان بر اساس اطلاعات ارائه شده به کمک سوالات افسر از قربانی حل شده است و در مواردی که اطلاعات ناقص و یا غیر قابل استفاده توسط یک قربانی ارائه شده است، بسیاری از آنها از طریق تلاش‌های تحقیقی حل شده است. سایر تحقیقات نیز نشان می‌دهد که از طریق تلاش پلیس برای کمک به دلهره مجرم پس از ارتکاب جرم موفقیت کمی به دست آمده است (Block و Bell، 1976؛ Skogan و Antunes، 1979). در واقع، Skogan و Antunes (1979: 223) به‌طورخاص اظهار داشتند که "کار پیگیری تحقیق، جمع‌آوری شواهد فیزیکی و گریزاندن جنایتکاران از طریق کار پلیسی، نقش نسبتا بی‌اهمیتی در شناسایی و توقیف مجرمان بازی می‌کند.

بااین‌حال، نقش محقق در پرونده‌های جرایم رایانه‌ای بسیار مهم‌تر از پاسخ افسر، قربانیان، یا شهود است که به او ارائه شده است. با توجه به ماهیت تکنیک‌های مرتبط با جرایم رایانه‌ای و حتی خود قربانی واقعی، تلاش زیادی صرف شناسایی حقایق مدارک، تفسیر سرنخ و جمع‌آوری داده‌ها علیه مظنون می‌شود. که علاوه‌براین، مطالعه PERF توصیه می‌کند که افسران شاهدان را از طریق غربال‌گری در یک محله و در یک روش مشابه در زمینه سازمانی که در آن جرایم رایانه‌ای رخ داده است بدست آورند.. دامنه‌ی این تحقیقات را می‌توان گسترش داد و با افراد دیگری که ممکن است اطلاعات کیفی مربوط به ارائه فشار، خواسته‌ها، محدودیت‌ها، انگیزه‌ها و توجیهات بر رفتار داشته باشند مصاحبه کرد. براین‌اساس، حس چگونگی شکل‌گیری سازمان و رفتار ممکن است به درستی به‌دست آید و درنتیجه می‌تواند به محقق در درک بهتر محرک‌های ممکن برای کمیسیون جرایم کمک کند.

اطلاعات، ابزار دقیق، و مصاحبه

Ohara (1980) نوشته است که سه جزء تحقیقات جنایی وجود دارد: اطلاعات، ابزار دقیق و مصاحبه. درحالی‌که فن‌آوری و تکنیک ممکن است تغییر کند، این اصول در طول زمان و در نتیجه تعیین ارزش باقی بماند.

اطلاعات به‌سادگی به این واقعیت اشاره دارد که تحقیقات جنایی حول جمع‌آوری، سازماندهی و تفسیر مستقیم داده و یا حاشیه مربوط به پرونده می‌چرخد. دومی، ابزار دقیق مربوط به علم پزشکی قانونی و تکنیک‌های خاص حل جرایم است. به‌عنوان مثال، پیشرفت‌های فن‌آوری مانند بیومتریک، تحلیل DNA [۲] و پردازش داده‌ها/ویدیو به‌منظور افزایش دقت اجرای قانون در موارد بانکی ادامه خواهد داشت. سومی، مصاحبه شامل فرآیند درخواست و استخراج قانونی اطلاعات از افرادی است که در مورد شرایط یک جرم آگاه هستند.

این سه اصل که در تحقیقات جرائم سنتی در ایالات متحده یک نسبتا روش درست است، بوده - و ادامه خواهد داشت . بااین‌حال، کاربرد آنها در جرایم رایانه‌ای کمتر روشن و به ظاهر متنوع است. تجمع اطلاعات همچنان به‌عنوان "نان و

[2] هر چند خارج از محدوده این مقاله است، اما جالب است که به بررسی چگونگی تخصص DNA در جمع‌آوری شواهد و تحلیل‌های مهاجرت به سازمان پلیس، و اینکه آیا توسعه بخش تخصصی می‌تواند به عنوان یک الگوی آموزنده برای خدمت به تخصص کامپیوتری پزشکی قانونی قرار گیرد می‌پردازد.

کره" در تحقیقات جرایم غیرسنتی ادامه خواهد داشت. در واقع، مهارت محقق اگر اطلاعات او برای حرکت در جهت حل پرونده در طول این دوره از تحقیق و بررسی کافی نباشد تا حد زیادی نامربوط است. به‌طورمشابه، حتی ماهرترین محقق نیز اگر اطلاعات جمع‌آوری‌شده در طول دوره ناقص باشد و یا به‌طورکلی قابل اعمال نباشد به مشکلاتی برخورد خواهد کرد. با در نظر گرفتن این مسئله در ذهن، ابزار دقیق و مصاحبه - که به سادگی روش‌های دیگری برای جمع‌آوری اطلاعات هستند - باید به شیوه‌ای کاملا متفاوت اجرا شوند.

ابزار دقیق در رسیدگی به جرائم مالی مرتبط در درجه اول شامل سیستم‌های کامپیوتری در سراسر ردیابی و تجزیه‌وتحلیل سوابق و سیاهه‌های مربوط به تعیین اختلاف و یا بی‌نظمی است. به‌عنوان مثال، پول‌شویی با استفاده از رایانه مربوط به روند پنهان کردن منبع پول به دست آمده به طور غیرقانونی و اغلب شامل ایجاد، ساخت و یا تغییر اسناد با ایجاد یک دنباله مشروع و تاریخ است (Lyman، 2002). موسسات مالی فرض به حفظ سوابق دقیق تمام معاملات، مبادلات ارز، و حمل‌ونقل بین‌المللی از وجوه بیش از یک مقدار مشخصی دارند. علاوه‌براین، قانون محرمانه بودن بانک از 1970 نیاز به این نهادها برای حفظ سوابق در درجه بالایی از سودمندی در جنایی، مالیات و مقررات و اقدامات، و اجازه وزارت خزانه‌داری به نیاز به گزارش فعالیت‌های مالی مشکوک که ممکن است به نقض قانون مربوط شود دارد (دفتر ارزیابی فناوری، 1995).

مثال دیگر اهمیت ابزار دقیق در هنگام برخورد با تخلف مربوط به رایانه است. قبل از رشد نمایی اینترنت، بررسی تقلب کارت اعتباری اغلب با شناسایی دقیق توسط شاهدان و جمع‌آوری و شناسایی شواهد فیزیکی محکوم همراه بود. هنگامی که یک مجرم نسبت به خرید از طریق استفاده از یک کارت اعتباری جعلی برای پرداخت اقدام می‌کند، کارمندان فروش و کارکنان آموزش دیده فروشگاه با دقت جزئیات فیزیکی و رفتاری عاملان را برای کمک به تحقیقات مشاهده و به خاطر می سپارند. فریفتن مجرم با در اختیار داشتن کالای تقلبی نیز آسان‌تر از خرید در یک مکان فیزیکی ساخته شده است. در نهایت، دست خط نمونه به دست آمده هنگامی که کالا امضا شد، و اثر انگشت دست چپ در صحنه جرم، به‌عنوان همخوانی شواهد استفاده می‌شود. بااین‌حال، با ظهور و رشد تجارت الکترونیکی، نقش کمکی شهود و مدارک فیزیکی منابع اطلاعات قبلی (و به شدت قوی) درحال‌حاضر تا حد زیادی از بین برده شده است.

ترکیب عوارض بین اداری و قضایی، کمبود دسترس منابع تحقیقاتی، و این واقعیت که این جنایات در چنین شیوه‌ی نامحدود و غیرقابل تنظیم در فضای مجازی رخ می‌دهد، مشکل است. محققان جرایم رایانه‌ای باید به دنبال راه‌های دیگری از پرس‌وجو و یادگیری با استناد به بازیابی اطلاعات از این منابع باشند. سومین جزء - مصاحبه - به نظر می‌رسد کمتر به عنوان یک روش برجسته مستقیم برای بررسی جرایم رایانه‌ای قرار گرد، عمدتا به این دلیل که قربانی اغلب غافل است (یا بلافاصله یا حتی برای مدت زیادی) که جرم اتفاق افتاده است و آسیب منجر شده است (Parker، 1976؛ Webster، 1980). استفاده از اطلاعات در حل این موارد و گاهی اوقات تنها شناسایی از طریق داده موجود بر روی یک سیستم کامپیوتری مفید است و اغلب تنها نقش قربانی را در این تحقیقات، گزارش جرم و جنایت و دسترسی به ماشین آلات ذخیره‌سازی داده‌ها بازی می‌کند. علاوه‌براین، شواهد در جرایم رایانه‌ای نسبتا نادر است چون این جرائم تمایل به رخ دادن در پشت درهای بسته دارد (Rosoff و همکارانش، 2002). تنها شاهدان در اغلب موارد کسانی هستند که مرتکب جنایات صورت فردی و یا جمعی شده‌اند بنابراین روش‌های دیگری برای جمع‌آوری اطلاعات باید استفاده شود (Lyman، 2002).

پس از آن، مصاحبه، ممکن است مطلوبیت غیرمستقیم برای محقق فراهم کند - مانند بینش به انگیزه و احتمالا تکنیکهای خاص استخدام، به خصوص اگر مجرم بود. انگیزه برای جرایمی مانند اختلاس (انحراف مسیر منابع مالی از یک کارفرما توسط کارمند - اغلب از طریق استفاده از سیستم‌های کامپیوتری رخ می‌دهد (Lyman، 2002؛ Rosoff و همکارانش، 2002)، برای مثال، ممکن است از متغیرهای سازمانی - مانند فشار سرپرستان یا مدیران برای نشان دادن بهره وری یا اثربخشی، و یا از یک "فرهنگ رقابت که نفوذ شرکت را نشان می‌دهد استفاده کنند (Coleman و Ramos، 1998). همچنین ممکن است ساقه از متغیرهای سطح فردی مانند یک شخصیت که با تنبلی، تمایلات کینه توز، تمایل به قدرت ساختگی و یا یک ناتوانی در مقابله با استرس به شیوه‌ای طرفدار اجتماعی ناشی شود (Krause، 2002). همکاران یک مظنون احتمالی ممکن است اطلاعات مفید ثانویه در این زمینه ارائه دهند، درحالی‌که ترسیم قابلیت‌های فردی (و روش‌های بالقوه‌ی استفاده شده) برای دور زدن کنترل دسترسی به ارتکاب جرم است.

وظیفه‌ی این محقق ارزیابی زنده ماندن از بازخورد شفاهی است و به دنبال آن ممکن است شواهد قوی که تاثیر اساسی در کشف در دادگاه قانون دارد ارائه شود.

جمع‌آوری شواهد و در حال پردازش

از نظر مسائل مدارک، تحقیقات مقدماتی راهبردهای مرتبط با جرایم رایانه‌ای باید به‌عنوان نوعی از جرایم باشد. بخش اجرای قانون رویه مورد نیاز برای جمع‌آوری شواهد را دارد که باید دنبال شود، اما باید به برخی از پیچیدگی‌های خاص جرایم رایانه‌ای بومی باید توجه کرد. به‌عنوان مثال، Lyman (2002) به پیچیدگی ارتباط با شواهد ملموس و صحنه‌های واقعی مورد بررسی اشاره کرده است. به‌این‌ترتیب، نشان می‌دهد که محقق تا آنجا که ممکن است در مورد قربانی و مظنون یک پرونده یاد می‌گیرد. هر چند تاثیر آن منحصر به فرد نیست، برجستگی متغیرهای درک در سطح فردی به‌عنوان شکلی از جرایم پیش‌بینی می‌شود. علاوه بر این، تجزیه‌وتحلیل دقیق سیاهه‌های مربوط، سوابق و اسناد مربوط به تراکنش‌های غیر قانونی یا عمل باید (Lyman، 2002) انجام گیرد. جمع‌آوری و استفاده از شواهد فیزیکی به عنوان مستند حیاتی است (Eck، 1983) و درحالی‌که این روش در جرایم رایانه‌ای بررسی شود بسیار زمانبر استخواهد بود اما اغلب سرنخ کلیدی است که می‌تواند به یک دلهره منجر شود.

شیوه‌ای که در شواهد پرونده‌های جرایم رایانه‌ای وجود دارد یک چالش قابل‌توجه برای اجرای قانون باقی مانده است. اطلاعات خاص مربوط به سیستم‌های کامپیوتری که نیاز به تشنج جستجو دارد ممکن است در حکم جزئیات تایید شود، و همچنین به‌طوری‌که دادستان بتواند هر گونه چالش مدارک آورده شده برای دفاع مقابله کارکنان را بپذیرد. استانداردهای تحقیقی سازگار و پروتکل‌های جرایم رایانه‌ای هنوز بصورتی پایدار و محکم در اکثر ادارات پلیس اجرا نمی‌شود و این می‌تواند به شواهدی منجر شود که تلقی ناروایی از شواهد دارند که در غیر این صورت ممکن است به یک اعتقاد (Webster، Lyman 1980، 2002) منجر شود.

رسیدگی به حکم جنایات سنتی آشنا است و معمولا به گروه کاری در دادگاه محول می‌شود. با توجه به تازگی نسبی برنامه‌های کاربردی حکم بازرسی برای جرایم رایانه‌ای، برخی از ایالت‌ها به‌طورخاص قضاوت برای مقابله با این متخصص

را درخواست می‌کنند (کمیسیون دادستان کل تحقیقات نیوجرسی ، 2000). بااین‌حال، هنوز هم درخواست باید به شیوه‌ای ارائه شود که اجازه دهد تا درک مطلب به سهولت انجام گیرد. قاضی نباید با جزئیات فنی در ارتباط با بررسی گیج شود، اما باید تفاوت‌های ظریف را از آنچه که در آن درگیر است درک کند به‌طوری‌که دادگاه می‌تواند آگاهانه تصمیم بگیرد. هدف این است که به وضوح علت احتمالی وقوع جرایم مشخص شود و این موارد در حکم مربوط به جرایم شرح داده شده است. به‌همین ترتیب، اصطلاحات مخصوص فن‌آوری اغلب توسط قربانیان برقراری ارتباط ویژگی‌های قربانی و منابع احتمالی سرنخ‌های تحقیقی، و بسیاری از مأموران اجرای قانون که ممکن است قادر به درک کامل اطلاعات و جذب آن به‌طور مستقیم و یا اصلاح این تحقیقات نباشد مورد استفاده قرار گیرد (Lyman، 2002). بیشتر سازمانهای پلیس تکنسین استخدام هستند که می‌توانند به افسران یا کارآگاه در حفاظت مناسب، جمع‌آوری، پردازش و شواهد، و همچنین تفسیر و ارائه جزئیات کمیسیون فن‌آوری جرایم کمک کنند. وقتی شواهد مرتبط با جرم‌های رایانه‌ای کشف می‌شود، محافظان متعددی برای حفظ تداوم و یکپارچگی باید دست به کار شوند. توجه شدید باید به مشخصات داده در حکم بازرسی اعمال شود به‌طوری‌که تمام موارد به درستی و قانونی به دست آید. علاوه‌براین، آن‌ها قادر به حفاظت فیزیکی و رسانه‌های قابل‌حمل به دلیل ماهیت حساس بودن آن‌ها هستند. میدان‌های مغناطیسی و حتی الکتریسیته ساکن این پتانسیل را دارند که تجهیزات الکترونیکی خاص مانند دستگاه‌های ذخیره‌سازی داده‌ها و یا دیسک را غیرقابل استفاده و غیر قابل خواندن کنند. نقطه بحرانی دیگر این است که مظنونان یک پرونده باید از محیط محاسباتی به دلیل احتمال این که شواهد دیجیتال ممکن است تغییر و یا حذف شود محدود شوند (Lyman، 2002).

در این مرحله، تجزیه‌وتحلیل پزشکی قانونی از دیسک‌های سخت کامپیوتری در پرونده‌سازی علیه یک جنایتکار مشکوک ثابت شده است. این روش کسب شواهد، از لحاظ فنی پیچیده و پر زحمت است. در حالی که تعداد در حال افزایش است، اجرای قانون بسیاری از گروه‌ها فاقد تخصص برای انجام این تکنیک هستند و باید شرایط تجزیه‌وتحلیل قانونی خود را به سازمان‌های دیگر که لازمه‌ی پرسنل ماهر است ارائه کنند. متاسفانه، با افزایش مستمر جرایم رایانه‌ای و منابع محدود در دسترس برای اجرای قانون برای مقابله با جنایات سنتی اجازه دهید تا آنها در حجم کارهای عقب

افتاده ایجاد ور در اتاق انتظار شواهد تجزیه‌وتحلیل توسط یک تکنسین باشند (Bhaskar، 2006؛ Bogen و Dampier، 2004؛ Newville، 2001). مطابق با شهود، اولویت با پرونده‌های جرایم رایانه‌ای شامل آسیب جسمی بالقوه یا بالفعل به افراد است. بااین‌حال، حجم کارهای عقب افتاده همواره سازش تندی با عدالت به عاملان خدمت در سایر جرایم دارد و در نتیجه سیستم را تضعیف می‌کند.

درنهایت، مطالعه RAND (Greenwood و همکارانش، 1977) بر ضرورت اصلاح و بهینه‌سازی تلاش‌های پردازش شواهد مطالعه و PERF تأکید دارد (Eck، 1983) ابزار جمع‌آوری شواهد برجسته نیاز به تایید و تقویت پرونده در برابر یک مجرم مظنون و نه برای استفاده برای شناسایی یک مظنون دارد. این راهکارها برای کمک و پشتیبانی توسط پیشرفت‌های تکنولوژیک اخیر، مانند نرم‌افزار که می تواند صدها گیگابایت از داده‌های مالی الکترونیکی را به‌منظور ردیابی تناقضات مورد تجزیه‌وتحلیل قرار دهد و برنامه‌هایی که می‌تواند ورود به سیستم تجزیه فایل‌ها را در فعالیت‌های خاص مجرمین ردیابی کند پیشنهادی شده است. بدون شک، تجهیزات، پرسنل، و آموزش برای بهبود بیشتر بهره‌وری این فرآیند ضروری است.

صلاحیت

از آنجا که مرزهای ملی به‌طور موثر ناپدید می‌شوند توجه به بسیاری از جرایم رایانه‌ای، صلاحیت پیچیده دیگری است. درحالی‌که بررسی کامل مسائل قضایی کار فراتر از محدوده است و شایستگی اظهارنظر کشورها در جرم مدنی و کیفری متفاوت استانداردها، قانون اساسی و رویه، جمع‌آوری داده‌ها و حفظ شیوه و مدارک و عوامل حقوقی دیگر را دارد (Lyman، 2002). علاوه‌براین، اغلب به‌عنوان مسئولیت مبهم رسیدگی به یک جرم خاص و یا هر بررسی و یا چگونگی همکاری به بهترین وجه از طریق استرداد و کمک متقابل سیاست است. این بازی نه تنها در سطح بین‌المللی، بلکه در کشورهایی که چند بخش اجرای قانون دارند نقش دارد.

تحقیقات واکنشی و فعال

تمایز روشن دیگر بین تحقیقات واکنشی و فعال است (Lyman، 2002). به‌طورمستقیم، تحقیقات واکنشی تلاش برای حل مسائل جنایی است که درحال حاضر رخ داده است؛ که شایع‌ترین نوع هست. تحقیقات بلادرنگ، تلاش برای مقابله با جرایم قبل از قربانی شدن، به جای آسیب تحمیلی در فرد، یک شرکت، و یا جامعه است.اغلب در برنامه نویسی ابتکاری طراحی شده توسط سازمان‌های عدالت کیفری و نهادهای کمکی، مانند استراتژی پیشگیری از جرم موقعیتی جای دارد (Newman و Clarke، 2003). هنگامی که اجرای قانون قادر به پیش‌بینی ارتکاب جرائم خاص است، اغلب پرسنل برای بررسی و هدف قرار دادن منابع به سمت یک گروه شناخته شده از مجرمان و یا برای مقابله با نوع خاصی از جرایم اعزام می‌شوند. این نوع تحقیقات در درجه اول هوشمند است، که اهمیت جمع‌آوری و پاسخ مناسب به اطلاعات مفید از منابع زنده را نشان می‌دهد درحالی‌که به‌صورت همزمان حسابداری برای مسائل مربوط به آزادی‌های مدنی و قوانین مدارک در حال انجام است.

به‌عنوان‌مثال، نظارت بر بولتن تابلوها و اتاق‌های چت توسط محققان به تشخیص و هراس از کسانی که فاقد شرکت در جرایم جنسی علیه کودکان هستند کمک می‌کند (Meehan، Manes، Davis، Hale، و Shenoi، 2001؛ Mitchell، Wolak، و Finkelhor، 2005؛ Penna، Clark، و Mohay، 2005). علاوه‌براین، شرکت‌کنندگان در جوامع آنلاین به جلوگیری از جنایات با اطلاع‌رسانی مقامات در مورد رفتار مشکوک کمک می‌کنند، که پس از آن قادر به ارائه این اطلاعات برای محققان هستند. به‌عنوان مثال، خود پلیس در سایت‌های حراج اینترنت به شناسایی اقدام منجر به خریدوفروش تقلبی و اقلام جعلی می‌پردازد و به عاملان این گونه جنایات هشدار می‌دهد (Enos، 2000؛ Fusco، 1999). مشارکت در ایالات متحده بین بخش خصوصی و دولتی مربوط به اشتراک‌ذاری اطلاعات قربانی جرایم رایانه‌ای است که به اجرای قانون در تلاش تحقیقات کمک می‌کند.

تحقیقات نمادین

در نهایت، Brandl و Horvath (1991) کشف کردند که صرف تلاش با اجرای قانون از طریق شیوه‌های تحقیقی مثبت مرتبط به نرخ رضایت قربانی است. این است که، قربانیان بیشتری با پلیس هنگام بروز حوادث همکاری می‌کنند. این می‌تواند از طریق اعمال اثر انگشت، نمایش شات لیوان و سوال از شهود رخ دهد که در حقیقت اغلب به معنی داشتن یک تصویر رسانه‌ای به جای بررسی جرم است(Greenwood و همکارانش، 1977). که در مجموع بر اهمیت «نمادین» تحقیقات که در خدمت اهداف بیشتر برای «حل جرم» می‌افزاید (Greenwood و همکارانش، 1977). گسترش یافته‌های جرایم رایانه‌ای، به نظر می‌رسد که به‌منظور نشان دادن پلیس با انگیزه است که قادر به حل این جرائم غیرسنتی است و آنها باید در یک روش مشابه پاسخ دهند. در غیراین‌صورت، قربانیان فردی و سازمانی، ایمان خود برای اجرای قانون و کنترل جرایم و اعتمادبه‌نفس متزلزل در بازوی برجسته نظام عدالت کیفری را در برابر مشکلات بیشتر برای جامعه از دست خواهند داد (Webster، 1980). قربانیان نیز ممکن است در برابر گزارش مشکوک و یا تخلف واقعی انتخاب شوند و ممکن است تبدیل به بررسی و مجازات ستمکاران به یک شیوه‌ی غیر قانونی شوند (Johnston، 1996؛ Silke، 2001). اعتماد باید برای ایجاد و تداوم یک خط صریح و ثابت از ارتباط بین قربانیان و اجرای قانون ایجاد شود، به‌طوری‌که هر یک از طرفین بتواند در کمک به اهداف جمعی خود حرکت پیش‌دستانه انجام دهد و موجب ممانعت و پرداختن به جرایم رایانه‌ای شود.

نیروهای وظیفه‌ی تحقیق در جرایم رایانه‌ای

به‌عنوان منشاء جرایم رایانه‌ای در ایالات متحده اغلب به نقش قوانین ایالتی و بین المللی در بسیاری از موارد تحت فدرال حوزه قضایی باید اشاره کرد. همکاری فدرال با اجرای قانون محلی و دادستان برای به‌اشتراک گذاشتن اطلاعات و تلاش گروهی نشان دهنده‌ی مقابله با جرائم سنتی شامل مواد مخدر، سلاح، باندها[3] و غیره است (McGarrell و Schlegel، 1993؛ Einhorn -Russell، 2004). با گسترش بسیاری از محققان و دست اندرکاران باید اظهار

[3] وزارت دادگستری ایالات متحده آمریکا برنامه SEED و WEED دو نمونه هستند.

اهمیت تشکیل تیم قابل مقایسه برای مبارزه با جرایم رایانه‌ای با امید به نتایج مثبت مشابه را داشت (نگاه کنید به مثال، Conly و McEwen، 1990).

به‌تازگی تحقیقاتی برای تعیین چنین وظیفه‌ای انجام شده است که نیروها بهترین پاسخگویی را به نیازهای اجرای قانون، بخش خصوصی، و اعضای جامعه داشته باشند (Hinduja، 2004). این یافته‌ها برخی از بینش‌ها برای شکل‌گیری و سازمان دادن تیم را اختصاص داده‌اند. مهمتر از همه، به‌نظر می‌رسد که توابع تحقیقی باید در تلاش سازمان یافته و توجه به تجهیز پرسنل به اهداف خود باشند. ویژگی‌های سه حوزه باید جرایم رایانه‌ای را از یک واحد پلیس سنتی تشخیص دهند: استخدام، مربیگری و شیوه‌های ارتقاء مورد نیاز آموزش و برون سپاری به بخش خصوصی. در متن زیر، هر یک از این ویژگی‌ها در یک واحد جرایم رایانه‌ای فرضی شرح و بسط داده شده است.

استخدام، مربیگری، و توسعه

برای شروع، افرادی که به دنبال تبدیل شدن به بخشی از واحد هستند باید حداقل سه سال تجربه به عنوان مأموران اجرای قانون داشته باشند و از آشنایی با نقش خود را به‌عنوان یک عامل از دولت و همچنین بینش پویایی نظام عدالت کیفری ایالات متحده اطمینان داشته باشند. آنها همچنین باید توسط افسر نظارت خود از لحاظ فنی تایید شوند و در اختیار داشتن کیفیت شخصیت برای موفقیت به‌عنوان یک محقق مانند توجه به جزئیات، صبر، ارتباطات عالی مهارت‌ها و تمامیت ضروری است. استخدام جدید پس از آن با عنوان به‌دست آوردن تجربه در برخی از وظایف صورت می‌گیرد. به‌عنوان مثال، اعضای جدید واحد مسئول کمک به جانبازان با کسب، حفظ و تجزیه و تحلیل شواهد، پردازش برای دیدار با الزامات تیم تحت پیگرد قانونی، تکمیل و آرشیو گزارش برای اهداف جمع‌آوری داده‌ها و تلفن‌های متعدد و گفتگو چهره به چهره مربوط به حوادث خاص با قربانیان، شاهدان و آگاهان خواهند بود.

نکته کلیدی آغاز جدیدی است که به‌طورخاص به سرپرستی داده و نظارت یک محقق کهنه‌کار به جذب شدن او به واحد فرهنگ و بررسی پرونده‌های جرایم رایانه‌ای اختصاص خواهد یافت. این التزام، یک سال به طول می‌انجامد، پس از آن زمان اعضای جدید به بخش های خود اختصاص خواهند یافت. بررسی جرایم کمی پر خطر است - مانند تقلب

آنلاین در کارت اعتباری، تبلیغات گروه نفرت اینترنت، جعل و تقلب دیجیتال از چک و یا ارز کمتر از 1،000 دلار، نرم‌افزار دزدی دریایی و استفاده غیرمجاز از محاسبات جزئی منابع که می‌تواند موجی تزلزل شود. جانبازان باید بیشتر مراقب جرایم رایانه‌ای بالقوه یا بالفعل - مانند سایبر تروریسم، پورنوگرافی کودکان و شناسایی حلقه سرقت شود چرا که رسوخ شبکه باعث انکار در خدمات مقیاس بزرگ و یا آسیب اطلاعات، زیان‌های مالی سنگین به یک قربانی و تخلف با امکان روابط جرایم سازمان یافته می‌شود.

در مورد ارتقاء، شخص یک سلسله مراتبی معمولی را از طریق افسران پس از نشان دادن مهارت در سطح فعلی خود می‌پیماید. اگر یک محقق کارهای ستوده‌ای در نرخ دستگیری و نوع جنایات اختصاص داده نشان دهد، برای ارزیابی ارتقاء به سطح بعدی مورد آزمایش قرار می‌گیرد. افزایش مسئولیت خودمختاری با پاداش بیشتر مشروط به موفقیت در موقعیت جدید همراه استا. در نهایت خودمختاری بیشتر منجر به صدور آنی مجوز در انجام تحقیقات فعال برای کمیسیون جرایم رایانه‌ای قبل از رخ دادن آن می‌شود. با توجه به ماهیت جنجالی و پیامدهای استراتژی فعال حقوق بشر، تنها در دراز مدت، جانبازان در فراهم کردن آن بسیار ماهر خواهند بود[۴].

آموزش مورد نیاز

در طول دوره آزمایشی فوق، استخدام‌های جدید نیاز به شرکت در کارگاه‌های بسیاری برای تعمیق خود در مرکز آموزش با توجه به جنایات رایانه‌ای[۵] خواهد داشت. جلسات فنی- بر روی موضوعاتی مانند پروتکل‌های شبکه، سیستم عامل، طرح‌های رمزگذاری و تجزیه‌وتحلیل پزشکی قانونی -با قدردانی جلسات قانونی در موضوعاتی مانند نرم‌افزار و

[4] تحقیقات فعال، مجموعه‌های از تکنیک‌ها را که فعالان حقوق بشر و طرفداران حفظ حریم خصوصی، مانند کاوش در پایگاه داده، و کشف دانش و کمک‌های مالی و ایمنی و حفاظت طرفدار آن هستند معرفی می‌کند. ماهیت اخلاقی این تکنیک ادامه حکم بحث و نقض حقوق مدنی در همه هزینه‌ها از طریق سیاست و دستورالعمل رویه توسط سازمان‌ها برای محققان خود است (Brown، 2001)

[5] Hinduja (2004) از طریق یک نظرسنجی از سازمان‌های اجرای قانون دریافت که با ارائه گزینه‌هایی برای آموزش بیشتر پرسنل، یا تجهیزات، سازمان‌های اجرای قانون نیاز شدید به آموزش و منابع بالاتر مرتفع می‌گردد.

اجرای حکم جستجو در این موارد و اهمیت درستی حفظ و مستندسازی مدارک و حقایق[۶] تاکید خواهد کرد. در ایالات متحده، بسیاری از این کارگاه‌های آموزشی توسط نهادهای دولت فدرال بودجه سازمان یافته و بدون هیچ هزینه‌ای هستند[۷]. گواهی امتحانات نیز به اداره استخدام برای حصول اطمینان فرستاده می‌شود و می‌تواند آن را به‌طور عملی اعمال کند. چنین آموزش فشرده‌ای برای تجهیز بازرسان واحد به موقعیت خود ضروری است.

برون‌سپاری به بخش خصوصی

بحث قبلی به‌نظر می‌رسد بدون توجه به منابع محدود - زمان، پرسنل، تجهیزات و دانش - با اکثر بخش‌های اجرای قانون که به‌طور مستمر در حال مبارزه بودند است. براین‌اساس، فرض واحد مشارکت جرائم رایانه‌ای با توسعه بخش خصوصی برای کاهش ارتباط منابع ناکافی است. به‌عنوان مثال، فرض می‌شود که شرکت‌های آمریکایی می خواهند طوری عمل می‌کنند که نشان می‌دهد سرمایه‌گذاری در جامعه محلی برای حفظ اهداف و افزایش وفاداری مصرف‌کننده و دریافت معافیت‌های مالیاتی است. به این ترتیب، بسیاری از این شرکت‌ها می توانند تجهیزات مربوط به این واحد را در قالب سخت‌افزار، نرم‌افزار و لوازم جانبی برای رفع نیازهای اجرای قانون برای ابزار تحقیقی استفاده کنند. حتی زمان یک کارمند بخش خصوصی ممکن است غیر قابل قبول ارائه به سازمان اجرای قانون باشد اگر یک سوال فنی یا حقوقی مطرح شود که محققان قادر به پاسخ دادن و یا مشاوره به چگونگی ادامه نداشته باشند. یک تماس تلفنی ساده بین این اشخاص ممکن است بی‌اندازه به راه‌حل جرایم و تعقیب قانونی موفق سودمند باشد.

با توجه به جرائم رایانه‌ای، برخی معتقدند که فرآیند تحقیقاتی این جرائم باید بر عهده مسئولین این کار قرار گیرد. با توجه به تاریخچه قوانین موجود در این زمینه، خصوصی سازی تحقیقات به افراد اجازه می‌دهد تا بر مسئولیت‌های خود تمرکز داشته باشند و از پراکندگی کارها می‌کاهد. به عنوان مثال، آزانس کاراگاه‌ی در سال 1852 (Kuykendall, 1986; Lyman, 2002) متشکل از مناطق آمریکا در قرن 18 و 19 ایجاد شد. قوانین موجود در این آژانس، بیشتر

---

[6] Hinduja (2004) کشف کرد که بیشترین نیاز آموزشی در زمینه جستجو و آموزش و جمع‌آوری شواهد و پردازش است. که اهمیت جمع‌آوری دانش و تجربه مربوط به جنبه‌های حقوقی تحقیقات جرایم رایانه‌ای بیش از نیاز برای به‌دست آوردن مهارت‌های فنی دیگر است.

[7] به‌عنوان مثال، مرکز جرایم ملی یقه سفید دارای کارگاه‌های آموزشی در پایه و پیشرفت تجزیه‌وتحلیل بازیابی اطلاعات در سراسر کشور در طول سال است.

مربوط به دولتﺂهای افغانستان، پاکستان و ایران است که در 11 سپتامبر 2001 نیز آمریکا مورد جمله تروریستی قرار گرفته است. در واقع، حکومت فدرال عمومی و خصوصی از واژه "self help" استفاده می‌کنند و از سیستم‌ها سرویس هایی به منظور راه‌اندازی ضدحمله استفاده می‌کنند (Schwartau, 1999). یکی از اولین احساسات به اشتراک کذاشته شده بین ملت‌ها، این است که افراد باید در اجرای قانون، از تمامی منابع خود استفاده کنند تا با شایستگی آن قوانین را به اجرا در بیاورند. هوش، از ابزارهای جرایم رایانه‌ای است که متاسفانه به درستی استفاده نمی‌شود (Schwartau, 1999).

صرف نظر از اثربخشی این اقدامات، هر دولتی باید برای رفتارهای مجرمانه، پیگرد قانونی داشته باشد. یکی از اغلب قوانین موجود در جامعه این است که هر نقض قانون برای دستیابی به عدالت نیست و همه نیز این جمله را قبول دارند. بنابراین نقض قوانین، به احتمال زیاد به دلیل سود شخصی و یا سود جمعی خواهد بود. با توجه به این نکته، به نظر می‌رسد که عاقلانه‌ترین کار، انجام وظایف ضروری و عدم انجام کارهای جنایی می‌باشد. در حقیقت، ممکن است انجام این کارها، ثمربخش بوده و موجب تسهیل امور گردد.

توجه داشته باشید که اگر شرکتی تاسیس گردد، باید برخی کارها برون سپاری گردند. بنابراین این امور باید از امنیت بالایی برخوردار باشند. زیرا برون سپاری کارها، امری بسیار مهم و قابل توجه است که باید به درستی مکان و افراد انجام کارها در بیرون از سازمان تعیین گردد. ممکن است گاها، خود شرکت توانایی انجام برخی از کارها را داشته باشد، اما به دلیل نداشتن منابع کافی مجبور به برون سپاری گردد که هزینه‌بر و زمان‌بر است ولی نتایج بهتری را خواهد داشت. با توجه به ماهیترسود دنیای کسب و کار، بسیاری از کسانی که در این زمینه ماهر هستند، در بخش‌های خصوصی دیگری هم به فعالیت مشغولند.علاوه بر این، در هر کسب وکاری، افراد تمایل دارند که کارگران ماهری را استخدام کنند. آنها همچنین در موقعیت‌های مختلف، از افراد مختلفی استفاده می‌کنند[8].

با ایجاد ساختاری در جامعه و شرکت، در قالب، مربی و ترویج شیوه‌های مورد نیاز آموزش و برون سپاری کارهای ضروری که در توان شرکت قرار ندارند، می‌توان بهترین نوع کسب و کار را ایجاد نمود که احتمال موفقیت در تمامی

[8] تاکید بر مطلوبیت یک کسب و کار خصوصی برای کمک به جنایات کامپیوتری انجام گرفته، منجر به رخداد تقلب در سیستم‌هایی نظیر ebay می‌گردد. اما همواره راهی برای شناسایی افراد خاطی وجود دارد که این افراد با آدرس خانه خود و یا سایر نشانی‌ها و رد پاها شناسایی می‌گردند.

کارهای آتی شرکت با این اوصاف بسیار بالا است. در هر زمانی ممکن است برخی از نتایج غیرمنتظره نیز به وجود بیاید که تلاش افراد حاضر در شرکت را تحت تاثیر قرار دهد که در این وضعیت‌ها، باید نقاط ضعف شرکت شناسایی شده و روند آسیب پذیری آن جبران گردد.با این حال به نظر می‌رسد، برای ارزیابی ئ آدرس دهی برخی مشکلات احتمالی رخ داده، باید نهایت دقت وجود داشته باشد.

بحث و نتیجه‌گیری

اجرای قانون باید به شیوه‌های مختلف، موجب بالا رفتن شایستگی افراد گردد و خوشبختانه تحقیقات تجربی نشان می‌دهد که روش‌های زیادی برای مقابله با جرم و جنایات به وجود آمده است. تمامی راه‌کارهای مقابله با این جرم و جنایات را می‌توان در آینده نیز مورد استفاده قرار داد و از آن ها می‌توان برای آموزش‌های آتی نیز استفاده کرد. تحقیقات در ایالات متحده آمریکا نشان می‌دهد که بهترین روش مقابله با جرم و جنایات، استفاده از خود افراد خاطی با ایجاد یک مدیریت تخصصی و مناسب است.

قبل از انجام روش‌های مقابله با این جرم و جنایات، باید تمامی انواع جرم‌ها و علت رخداد و تاریخچه آن‌ها بررسی گردند تا به راحتی بتوان در آینده با هر نوع جنایتی به مقابله پرداخت. جرایم رایانه‌ای در اثر گذر زمان در حال رشد است و ممکن است به شیوه‌های جدیدی رخ دهد و باید برای مقابله با آن‌ها، نهایت تلاش انجام گیرد. امید است با تحقیقات بیشتر بتوان دانشگاهیان را از این امر مهم آگاه نموده و برای مقابله با این عوامل تجهیز نمود.

References

Benson, M. L., Cullen, F., & Maakestad, W. (1990). Local prosecutors and corporate crime. Crime and Delinquency, 36, 356-372.

Bhaskar, R. (2006). State and local law enforcement is not ready for a cyber Katrina. Communications of the ACM, 49(2), 81-83.

Block, P., & Bell, J. (1976). Managing investigations: The Rochester system. Washington, D.C.: Police Foundation.

Block, P., & Weidman, D. (1975). Managing criminal investigations: Perspective package. Washington, DC: U.S. Government Printing Office.

Bogen, A. C., & Dampier, D. A. (2004). Knowledge discovery and experience modeling in computer forensics media analysis. ACM International Conference Proceeding Series, 90, 140-145.

Braithwaite, J. (1985). White-collar crime. Annual Review of Sociology, 1, 1- 25.

Brandl, S. G., & Horvath, F. (1991). Crime-victim evaluation of police investigative performance. Journal of Criminal Justice, 19(3), 293-305.

Brown, M. F. (2001). Criminal investigation: law and practice (2nd ed.). Boston: Butterworth-Heinemann.

Coleman, J. W., & Ramos, L. L. (1998). Subcultures and deviant behavior in the organizational context. Research in the Sociology of Organizations, 15,3-34.

Conly, C. H., & McEwen, J. T. (1990). Computer crim. U.S. Department of Justice. National Institute of Justice.

Cullen, F., Link, B., & Polanzi, C. (1982). The seriousness of crime revisited: Have attitudes towards white-collar crime changed? Criminology, 20, 83-102.

Eck, J. (1983). Solving crimes: The investigation of burglary and robbery. Washington, DC: Police Executive Research Forum.

Enos, L. (2000). Group takes aim at net auction pirates. Retrieved December 28, 2002, from http://www.newsfactor.com/perl/story/6077.html

Fusco, P. (1999). eBay confirms federal investigation. Retrieved December 29, 2002, from http://www.internetnews.com/ec-news/article.php/4_73961

Greenberg, B., Elliot, C. V., Kraft, L. P., & Proctor, H. S. (1977). Felony decision model: An analysis of investigative elements of information. Washington, DC: U.S. Government Printing Office.

Greenwood, P. W., Chaiken, J., & Petersilia, J. (1977). The criminal investigation process. Lexington, MA: D. C. Heath and Company.

Hinduja, S. (2004). Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams. Policing-an International Journal of Police Strategies & Management, 27(3), 341-357.

Johnston, L. (1996). What is vigilantism? British Journal of Criminology, 36(2), 220-236.

Krause, M. S. (2002). Contemporary White Collar Crime Research: A Survey of Findings Relevant to Personnel Security Research and Practice. The Personnel Security Managers' Research Program. Aug. 2002. Retrieved December 29, 2002, from http://www.navysecurity.navy.mil/White%20Collar%20Crime.pdf

Kuykendall, J. (1986). The municipal police detective: An historical analysis. Criminology, 24(1), 175-201.

Leibowitz, W. R. (1999). How law enforcement cracks cybercrimes. New York Law Journal, 5.

Lyman, M. D. (2002). Criminal investigation: the art and the science (3rd ed.). Upper Saddle River, N.J.: Prentice Hall.

McGarrell, E. F., & Schlegel, K. (1993). The implementation of federally funded multi jurisdictional task forces: Organizational structure and interagency relationships. Journal of Criminal Justice, 21(3), 231-244.

Meehan, A., Manes, G., Davis, L., Hale, J., & Shenoi, S. (2001). Packet Sniffing for Automated Chat Room Monitoring and Evidence Preservation. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 285-288.

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2005). Police Posing as Juveniles Online to Catch Sex Offenders: Is It Working? Sexual Abuse: A Journal of Research and Treatment, 17(3), 241-267.

New Jersey Attorney General Commission of Investigation. (2000). Computer crime: A joint report. State of New Jersey, Commission of Investigation and the Attorney General of New Jersey. Trenton, New Jersey. Retrieved December 29, 2002, from http://www.state.nj.us/sci/pdf/computer.pdf

Newman, G., & Clarke, R. V. (2003). Superhighway robbery: Preventing ecommerce crime. Portland, Oregon: Willan Publishing.

Newville, L. (2001). Cybercrime and the Courts: Investigating and Supervising the Information Age Offender. Federal Probation, 65(2), 11-20.

Office of Technology Assessment. (1995). Information technologies for control of money laundering. Washington, DC: U.S. Government Printing Office.

O'Hara, C. E., & O'Hara, G. L. (1980). Fundamentals of criminal investigation (5th ed.). Springfield, IL: Charles C. Thomas.

Parker, D. B. (1976). Crime by computer. New York: Charles Scribner's Sons.

Penna, L., Clark, A., & Mohay, G. (2005). Challenges of Automating the Detection of Pedophile Activity on the Internet. Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering, 206-222.

Rosoff, S. M., Pontell, H. M., & Tillman, R. (2002). Profit without honor: white-collar crime and the looting of America. Upper Saddle River, NJ: Prentice Hall.

Royal Canadian Mounted Police. (2000). Computer crime, can it affect you? Retrieved November 10, 1999, from http://www3.sk.sympatico.ca/rcmpccs/cpu-crim.html

Russell-Einhorn, M. L. (2004). Federal-Local Law Enforcement Collaboration in Investigating and Prosecuting Urban Crime, 1982-1999: Drugs, Weapons, and Gangs (No. NCJ 201782): National Institute of Justice.

Sanders, W. (1977). Detective work. New York: Free Press.

Schwartau, W. (1999). Cyber-vigilantes hunt down hackers. Retrieved December 20, 2003, from http://www.cnn.com/TECH/computing/9901/12/cybervigilantes.idg

Silke, A. (2001). Dealing with vigilantism: Issues and lessons for the police. Police Journal, 74(2), 120-133.

Skogan, W. G., & Antunes, G. E. (1979). Information, apprehension, and deterrence: Exploring the limits of police productivity. Journal of Criminal Justice, 7, 217-241.

Tarde, G. (Ed.). ([1890] 1903). Gabriel Tarde's laws of imitation. New York: Henry Holt.

United Nations. (1994). International Review of Criminal Policy - United Nations manual on the prevention and control of computer-related crime.

Retrieved June 20, 1999, from http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html

Webster, W. H. (1980). An Examination of FBI Theory and Methodology Regarding White-Collar Crime Investigation and Prevention. American Criminal Law Review, 17(3), 275-286.

Wilson, J. Q. (1976). The investigators: Managing FBI and narcotics agents. New York: Basic Books.

Wittes, B. (1994). Perils of policing the internet: Law enforcement lacks the tools needed to go after a new breed of online criminal. The Recorder. No. October 11.

Wolfgang, M. E., Figlio, R. M., & Sellin, T. (1972). Delinquency in a birth cohort. Chicago: University of Chicago Press.