گونه شناسی باندهای جرم و فساد در فضای مجازی

طلعت اله‌یاری*

سجّاد مجیدی پرست**

تاریخ دریافت: ۹۳/۳/۲۵

تاریخ پذیرش: ۹۳/۶/۱۵

چکیده

توسعه پدیده جهانی فناوری اطلاعات و ارتباطات، تحولی شگرف در ابعاد گوناگون حیات اقتصادی، اجتماعی، فرهنگی، امنیتی و سیاسی ایجاد نموده است. این گسترش رو به رشد فضای مجازی با توجه به ناشناخته بودن بسیاری از اجزای آن برای عامه مردم به عاملی برای افزایش فرصت‌های جنایی بدل گشته است. این ویژگی توسط مجرمان مجازی مورد سوء استفاده قرار گرفته و شکل‌گیری گروه‌های فساد و جرم در این فضا را به دنبال داشته است.

مقاله حاضر شناخت و طبقه بندی جرایم مجازی سازمان یافته و موانعی که باعث عدم شناخت این جرایم می‌باشند را به روش کتابخانه‌ای مورد تحلیل و بررسی قرار داده است.

* دانشیار مددکاری اجتماعی، دانشگاه علامه طباطبائی. allahyari@atu.ac.ir

** دانشجوی کارشناسی ارشد مددکاری اجتماعی، دانشگاه علامه طباطبائی. majidisajjad@gmail.com

سه دسته از گروه‌های جرایم سازمان یافته که از پیشرفت تکنولوژی‌های ارتباطی و اطلاعاتی به منظور نقض کنترل‌های نظم بخش و قانونی بهره می‌برند عبارتند از: ۱) گروه‌های جرایم سازمان یافته سنتی که از تکنولوژی‌های ارتباطی و اطلاعاتی استفاده می‌کنند تا فعالیت‌های مجرمانه خود را تسهیل کنند. ۲) گروه‌های سازمان یافته مجازی مجرمانه که به طور اختصاصی به صورت آنلاین عمل می‌کنند. ۳) دسته سوم، از فعالیت‌هایی تشکیل شده است که مقصود و هدف از آن به خطر انداختن درستی، مقبولیت و اعتماد به رایانه‌ها و سیستم‌هایی است که به‌اینترنت متصل می‌شوند و اطلاعات بر روی آنها پردازش می‌شود.

در پایان با توجه به شناخت حاصل شده به منظور کاهش آسیب‌های ناشی از باندهای جرم و فساد پیشنهاد می‌شود که بهترین شیوه در جلوگیری از وقوع جرایم رایانه‌ای، آموزش عموم جامعه از یک سو و ایجاد پلیس سایبر و تقویت آن به منظور گشت زنی در فضای مجازی از سویی دیگر می‌تواند به افزایش امنیت در این عرصه کمک شایان توجهی نماید.

واژه‌های کلیدی: *فضای مجازی، گروه سازمان یافته مجرمانه، جرایم رایانه‌ای، فناوری اطلاعات*

مقدمه

توسعه پدیده جهانی فناوری اطلاعات و ارتباطات، تحولی شگرف در ابعاد گوناگون حیات اقتصادی، اجتماعی، فرهنگی، امنیتی و سیاسی ایجاد نموده است. انقلاب الکترونیک تبدیل به مهم‌ترین پدیده تعیین کننده معاصر شده است. روزانه ده‌ها هزار رایانه ورود خود را به دنیای جدید اعلام می‌کنند. این گستره بیکران از یک سو فرصت‌های بی نظیری را فراهم ساخته و از سوی دیگر تهدیدهای جدی را متوجه بخش اعظم ساختارهای اجتماعی ساخته است (جوان جعفری، ۱۳۸۹: ۲). این ویژگی‌های دوگانه را در بسیاری از نوآوری‌ها و ابداعات بشری از جمله انقلاب صنعتی می‌توان مشاهده کرد. اما به نظر می‌رسد اَبَرساختار فناوری اطلاعات، دنیای جدیدی را خلق کرده است، دنیایی مملو از نوآوری‌ها و پیچیدگی‌ها که قاعده و نُرم پذیرفته شده‌ای ندارد (Grareth, et.al, ۲۰۰۵).

نکته مهم در ارتباط با جرایم سایبری ویژگی‌های انحصاری آنها در مقایسه با جرایم سنتی است. سرعت، کثرت، سهولت ارتکاب، ارزان بودن، بی مرز بودن، ناشناختگی، اتوماتیک بودن و... در جرایم دیجیتال موجب ظهور گونه‌ای متمایز از جرایم شده است. ویژگی‌های مذکور، سهولت سازماندهی و تهاجم از راه دور مجرمین سایبری از

یک سو و وابستگی روزافزون ساختارهای اقتصادی، صنعتی، خدماتی، امنیتی و سیاسی به فضای سایبر از سوی دیگر، جامعه بشری را با تهدیدهای جدی جدیدی مواجه ساخته است، به گونه‌ای که گزارشات رسمی‌سازمان ملل هیچ حوزه‌ای از زندگی بشری را فارغ از تهدیدات فضای مجازی نمی‌بیند (Kamal, ۲۰۰۵). این گسترش رو به رشد فضای مجازی با توجه به ناشناخته بودن بسیاری از اجزای آن برای عامه مردم به عاملی برای افزایش فرصت‌های جنایی بدل گشته است. این ویژگی توسط مجرمان مجازی مورد سوء استفاده قرار گرفته و شکل‌گیری گروه‌های فساد و جرم در این فضا را به دنبال داشته است.

از آنجایی که تعداد کاربران شبکه اینترنت در سطح جهان و در کشور ایران در حال افزایش است و کاربرد آن از حالت تجملاتی و لوکس به پدیده‌ای کاربردی و محسوس در زندگی روزمره تبدیل شده است، بسیاری از مجرمین نیز از فضای واقعی به فضای مجازی حرکت کرده‌اند و به دنبال آن گروه‌هایی با اهداف مجرمانه را نیز شکل داده‌اند. حضور این گروه‌های مجرمانه در این فضا سبب ایجاد آسیب‌های نوپدیدی شده است که شناخت، بررسی و مهندسی آن بر عهده متخصصین علوم گوناگون است که نقش متخصصین حوزه اجتماعی در کنترل و مهندسی این فضا می‌تواند کمک شایانی به شناخت این پدیده و کنترل آن بکند.

مقاله حاضر به شناخت و طبقه بندی جرایم مجازی سازمان یافته و موانعی که باعث عدم شناخت این جرایم می‌باشند را با روش کتابخانه‌ای مورد تحلیل و بررسی قرار می‌دهد.

طرح مسئله

فضای مجازی نوعی اجتماع و همسایگی بزرگی است که میلیون‌ها کامپیوتر و استفاده کنندگان آن را در سراسر جهان به هم پیوند می‌دهد. با غلبه اینترنت بر زندگی روزانه انسان‌ها، طبیعی به نظر می‌رسد که بسیاری از مشخصه‌های جامعه سنتی نیز به درون کشیده شوند و درآن جا شکل گیرند. امروزه، امور زیادی از قبیل خرید و فروش، تحصیل، مشاوره خانوادگی، ازدواج و حتی مشاوره‌های پزشکی میان پزشکان و بیماران در اینترنت انجام می‌گیرد. از این رو، هیچ جای تعجبی نیست که مجرمان اینترنتی در فضای مجازی مرتکب جرم شوند (کوثری،

۱۳۸۷: ۹۳). ویژگی خاص فضای سایبر از جمله امکان تحصیل هویت‌های گوناگون و نیز عدم برخورد فیزیکی و چهره به چهره با افراد دلیلی برای رفتارهای افراد نسبت به هم بر پایه شناخت آنها از ظاهر مجازی یکدیگر است. و از این رو برخی مزایای مواجهه حضوری که در فضای فیزیکی وجود دارد در فضای سایبر وجود نداشته است. از سوی دیگر ساختار فضای سایبر که ماهیت حقیقی افراد را در پس صفر و یک پنهان می‌دارد، این مجال را فراهم می‌سازد تا در پشت این ارقام که پنهان گر هویت ایشان است مرتکب اعمالی شوند که در فضای واقعی، بعید است دست به ارتکاب آنها بزنند. این ویژگی سبب شده تا افراد در این دو فضا دارای ماهیت متفاوتی باشند. از سوی برخی اشخاص با توجه به شناختی که از یک فرد در فضای واقعی دارند، با همان دید به وی در فضای سایبر می‌نگرند، در حالی که آن فرد، شخصیت متمایزی را در این محیط از خود بروز می‌دهد و این اعتماد به بزه دیدگی آن شخص منجر خواهد شد (زررخ، ۱۳۹۰: ۱۳۷).

با توجه به‌این که جرایم در فضای مجازی، در اشکال مختلفی ارتکاب می‌یابند، بناراین سخن گفتن در خصوص شرایط، ارکان و تقسیم‌بندی این جرایم، قدری مشکل به نظر می‌رسد. عدم ارائه آمار دقیق توسط نیروهای انتظامی و مراجع قضایی پیرامون جرایم مزبور، ناتوانی در خصوص ارائه تعریف صریح و روشن از ماهیت این جرایم را دو چندان کرده است. متاسفانه در حال حاضر، اطلاعات دقیق، مشخص و قابل اطمینانی در خصوص میزان و تاثیر جرایم سایبری، نه تنها در کشور، بلکه در سایر نقاط جهان نیز به چشم نمی‌خورد و شمار زیادی از آن‌ها نامکشوف محسوب می‌شوند. این مسئله یکی از معضلاتی است که متصدیان تحقیق در مرحله کشف و تعقیب جرایم مزبور با آن مواجه می‌باشند (خداقلی، ۱۳۸۳: ۳۵). از سوی دیگر پیوند و اتصال به شبکه جهانی اینترنت، به روشنی گویای این واقعیت است که ویرانگری و آسیب رسانی می‌تواند در یک لحظه، سراسر جهان را فراگیرد. سوء استفاده از فناوری‌های رایانه‌ای و اینترنتی می‌تواند امنیت ملی، آسایش عمومیو موجودیت یک جامعه را به مخاطره انداخته و تاثیرهای منفی بی‌شماری را بر زندگی افراد اجتماع تحمیل کند. همچنین با کمی‌دقت در این خصوص می‌توان به‌این نتیجه دست یافت که اغلب مرتکبان جرایم سایبری را جمعیت جوان تشکیل می‌دهند (آیکاو، ۱۳۸۳: ۵۵). که این مجرمان هم از ظرفیت جنایی بالایی برخوردارند و هم استعداد خوبی برای انطباق اجتماعی از خود نشان می‌دهند (جعفری، ۱۳۸۵: ۷۰).

با توجه به ابعاد گسترده و چند بُعدی این پدیده، نیازمند انجام پژوهش‌ها و بررسی‌هایی عمیق در خصوص نحوه شکل‌گیری، عملکرد و چگونگی مقابله با افراد و گروه‌های سازمان یافته در فضای مجازی می‌باشیم، که در این مقاله سعی شده است تا گونه شناسی[۱] از باندهای جرم و فساد در فضای مجازی ارائه شود و در زمینه کاهش این پدیده بررسی‌هایی انجام شود.

جرایم مجازی چیست؟

از لحاظ لغوی در فرهنگ‌های گوناگون سایبر به معنی مجازی و غیرملموس می‌باشد، محیطی است مجازی و غیر ملموس در فضای شبکه‌های بین‌المللی (این شبکه‌ها از طریق شاهراه‌های اطلاعاتی مثل اینترنت به هم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به طور کلی هر آنچه در کره خاکی به صورت فیزیکی ملموس وجود دارد (به صورت نوشته، تصویر، صوت، اسناد) در یک فضای مجازی به شکل دیجیتالی وجود داشته و قابل دسترس کاربران می‌باشند و به طریق رایانه، اجزا آن و شبکه‌های بین‌المللی به هم مرتبط می‌باشند (باستانی، ۱۳۸۳).

و در تعریفی دیگر محیط سایبر، به محیطی مجازی اطلاق می‌شود که اطلاعات در آن رد و بدل می‌گردند (پرویزی، ۱۳۸٤: ٤٦).

جرم عبارت دیگری است که در این فضا اتفاق می‌افتد، جرم را این گونه می‌توان تعریف کرد: فعل یا ترک فعلی که برای آن در قانون، مجازات تعیین شده است و جامعه با ابزار مجازات، آن را نکوهش می‌نماید (اردبیلی، ۱۳۸۰: ۱۲۰).

تعاریف بسیار گوناگونی در زمینه جرایم در فضای مجازی وجود دارد که به چند مورد می‌پردازیم. در تعریف جرم سایبری آمده است: جرم رایانه‌ای در بردارنده هر رفتار غیرقانونی است که رایانه یا شبکه به عنوان منبع، ابزار، هدف و مکان جرم مطرح می‌گردد (نورزاد، ۱۳۸۹: ۱۱٤). هر جرمی‌که دربردارنده رایانه‌ها و شبکه‌ها باشد جرم سایبری است، هر چند که خیلی متکی به رایانه نباشد (Casey, ۲۰۰۰: ۸). این درحالی است که عده‌ای جرایم سایبر

---

۱. Typology

را جرایمی‌می‌دانند که دسته‌های مختلفی از جرایم را در فضای سایبر و شبکه جهانی اینترنت در برمی‌گیرد و شامل جرایم ارتکابی به کمک رایانه و جرایم متمرکز بر رایانه نیز می‌شود (Furnell, ۲۰۰۲: ۲۲). در واقع جرایم سایبری در فضای سایبر که متشکل از شبکه‌هاست انجام می‌گیرد، لکن جرایم رایانه‌ای در فضایی گسترده‌تر که دربردارنده موارد خارج از شبکه‌ها به خصوص اینترنت می‌باشد، رخ می‌دهد.

جرایم مجازی با استفاده از خلاهای امنیتی موجود در فضای مجازی به ارتکاب جرایم دست می‌زنند بنابراین امنیت حالت فراغت نسبی از تهدید یا حمله و یا آمادگی برای رویارویی با هر تهدید و حمله را گویند (آشوری، ۱۳۸۷: ۳۸). براین اساس در واژه نامه وبستر[۲] امنیت به معنای کیفیت یا حالت امن بودن، رهایی از خطر، ترس و احساس نگرانی و تشویش می‌باشد. این تعبیر در دنیای الکترونیکی نیز صادق است اما افراد متخصص این زمینه را در حفظ و بقای ٤ اصل می‌دانند:

۱- محرمانگی: اطلاعات فقط و فقط بایستی توسط افراد مجاز قابل دسترس باشد.

۲- تمامیت: یک سیستم از عناصری متشکل است که در کنار هم برای رسیدن به هدفی یکسان همکاری دارند. حفظ تمامیت به معنای پیشگیری از بروز مشکل در این همکاری و پیوسته نگه داشتن عناصر یک سیستم می‌باشد.

۳- دسترس پذیری: اطلاعات بایستی به هنگام نیاز توسط افراد مجاز قابل دسترس باشد.

٤- عدم انکار: به هنگام انجام کاری و یا دریافت اطلاعات یا سرویسی، شخص انجام دهنده یا گیرنده نتواند آن را انکار کند (Stewart, ۲۰۰٤).

انواع گروه‌های جرایم سازمان یافته

جرایم مجازی می‌توانند از لحاظ فعالیت به سه دسته بزرگ تقسیم شوند و بدین گونه شرح داده می‌شوند:

---

۲. Webster

۱) گروه‌های جرایم سازمان یافته سنتی که از تکنولوژی‌های ارتباطی و اطلاعاتی استفاده می‌کنند تا فعالیت‌های مجرمانه خود را تسهیل کنند. در این دسته جرایم مجازی مرتبط با رایانه، مثل تقلب و سرقت، در جایی که رایانه‌ها به ابزارهایی برای عمل مجرمانه، دستکاری اطلاعات به منظور ارتکاب فعالیت‌های مجرمانه تبدیل می‌شوند.

۲) گروه‌های سازمان یافته مجازی مجرمانه که به طور اختصاصی به صورت آنلاین عمل می‌کنند. در این گروه جرایم مجازی مبنی بر محتوا مثل نقض قانون حق کپی و هرزه نگاری از کودکان است و رایانه‌ها و تکنولوژی‌های ارتباطی، توزیع این اطلاعات غیرقانونی را تسهیل می‌کند.

۳) دسته سوم، از فعالیت‌هایی تشکیل شده است که مقصود و هدف از آن به خطر انداختن درستی، مقبولیت و اعتماد به رایانه‌ها و سیستم‌هایی است که به‌اینترنت متصل می‌شوند و اطلاعات بر روی آنها پردازش می‌شود این فعالیت‌ها شامل هک کردن و ساخت ویروس‌هایی در فضای مجازی است (Walden ۲۰۰۳, ۲۹۵).

۱) گروه‌های جرایم سازمان یافته سنتی

دست یابی به سود مالی همواره یکی از نیرو محرکه‌های اصلی در شکل‌گیری گروه‌های جرایم سازمان یافته سنتی بوده است. از سوی دیگر جهانی سازی و گرایش به مهاجرت، مرزهای ملی را مبهم کرده است و شتاب در تغییر شکل جرایم آن‌ها را از پایگاه داخلی کشورها به خارج حرکت داده است.

مهاجرت در مقیاس بزرگی از کشورهای کمتر توسعه یافته به سمت کشورهای غربی در حال انجام است که برخی از افراد از جمله مهاجرین غیر قانونی بهترین طُعمه‌ها برای پیوستن به باندهای مجرمانه قومی – ملی می‌باشند. بنابراین گروه‌های کره‌ای، ویتنامی، چینی، روسیه‌ای (همان شوروی سابق)، کارائیبی و آمریکای جنوبی بهترین گروه‌های سازمان یافته در ایالات متحده، بریتانیا و اروپا می‌باشند (Singh, ۲۰۰۷: ۸۰).

برخلاف تلاش‌های دولتی در سرکوب فعالیت‌های جرایم سازمان یافته، این گروه‌های مجرمانه از قدرت تکنولوژی‌های ارتباطی و اطلاعاتی (ICT)[۳] به منظور تسهیل یا کمک به بالا بردن جرایم و پویایی در شناسایی

[۳]. Information Community Technology

شانس‌های جدید و راه‌هایی در غلبه بر اقدامات متقابل را به خوبی شناخته‌اند. آنها با تغییرات تکنولوژیک و قدرت تکنولوژی‌های ارتباطی و اطلاعاتی به منظور تسهیل فعالیت‌های مجرمانه دارای سود همچون قاچاق مواد مخدر، قاچاق انسان، قاچاق اطلاعات سری شرکت و اطلاعات هویتی، اخاذی، تقلب و کلاهبرداری آنلاین، پول شویی با استفاده از سیستم‌های پرداخت آنلاین، توزیع مواد غیرقانونی از طریق اینترنت و استفاده از اینترنت به عنوان بازار فروش غیرقانونی محصولات دارویی و داروهای تقلبی، خود را تطبیق داده‌اند (Raymond Choo, ۲۰۰۸: ۲۷۲).

اینترنت بازاری بزرگتر برای کسانی که به دنبال فروش اجناس تقلبی و دزدی شده هستند فراهم کرده است. داروهای تقلبی یکی از حوزه‌هایی است که رشدی خاص از طریق اینترنت را مشاهده کرده است یا بواسطه هزینه بالای داروهای تجویز شده، مشکل در بدست آوردن آنها، یا بواسطه خجالت بیمار در درخواست دارویی خاص است. اینترنت به متقلبین راهی آسان و ارزان به منظور تبلیغات، بازاریابی و توزیع محصولات پیشنهاد می‌کند و آن تجارتی پرسود برای موسسات تجاری مجرمان سازمان یافته فراهم کرده است. (UK OCTF, ۲۰۰۷: ۳٤)

مجرمان سازمان یافته به طور جدی و رو به افزایشی از پیشرفت‌های تکنولوژیک و به طور خاص رشد اینترنت به منظور توسعه جرایم جدید و تغییر روش‌های سنتی خود استفاده می‌کنند. آنها قصد، تصور و توانایی بهره بردن از ضعف امنیتی تکنولوژی اطلاعات و شناسایی شانس‌های جدید مجرمانه را به نمایش می‌کشند (SOCA, ۲۰۰٦: ۱). گروه‌های جرایم سنتی سازمان یافته به طور رو به افزایشی از هویت‌های غلط و دزدیده شده به منظور سرقت‌های مالی استفاده می‌کنند.

به طور کلی جرایم مرتبط با گروه‌های سازمان یافته شامل موارد زیر است:

- نفوذ به کامپیوتر و شبکه، از طریق هک و دسترسی غیرمجاز برای بدست آوردن اطلاعات حساس و مهم. برای مثال در ماه می‌سال ۲۰۰۷ اعضای گروه شش نفره‌ای به خاطر تبانی، کلاهبرداری، سرقت از بانک‌ها و پولشویی تحت تعقیب قرار گرفتند. کیفر خواستی تنظیم شد مبنی بر این که متهمان با استفاده از نرم افزار اسکن شبکه افراد و یا رایانه‌های موسسات مستقلی را که از امنیت بالایی برخوردار نبودند را شناسایی می‌کردند و به اطلاعات مالی اشخاص مثل شماره حساب، رمزهای عبور و حساب‌های اینترنتی بانکی را پیدا می‌نمودند و از اطلاعات بدست آمده به منظور سرقت از حساب‌های افراد استفاده می‌کردند. آنها پول را از حساب قربانی به حساب بانکی مورد کنترل خودشان ارسال می‌کردند و از آنجا به حساب اصلی خودشان انتقال می‌دادند.

• فیشینگ: کلاهبرداری، آنلاین و یا اینترنتی است که اغلب با استفاده از پیام‌های ناخواسته از سازمانی مشروع به منظور فریب افراد یا سازمان‌ها به منظور افشای مالی و یا اطلاعات هویت شخصی با هدف تسهیل جرایمی مانند کلاهبرداری، سرقت هویت و سرقت اطلاعات حساس و مهم (مانند اعتبار بانکی) انجام می‌شود. چندین پژوهشگر و شاغلین در حوزه امنیت به دخالت گروه‌های جرایم سازمان یافته در کلاهبرداری فیشینگ اشاره کرده‌اند. در سال‌های اخیر، پیام‌های فیشینگ به طور رو به افزایشی مدیران سطوح بالای سازمان یا اعضای گروه را مورد هدف قرار داده است – همچنین به عنوان فیشینگ نیزه یا صید نهنگ شناخته شده است.

• هرزنامه: پست الکترونیکی تجاری ناخواسته‌ای است که دریافت کننده را به خرید محصولات متقاعد می‌کند (به طور مثال سهام شرکت‌هایی که قیمت سهام‌شان دچار تورم شده است) در حقیقت آنها از تکنیک‌های بازاریابی فریبنده استفاده می‌کنند.

• ایجاد نرم افزارهای مخرب و انتشار آن: در گزارش اخیر ارزیابی تهدید بریتانیا به‌این موضوع اشاره می‌شود که جدیدترین نرم افزارهای مخرب به منظور سرقت اطلاعات مالی (مثل جزئیات کارت اعتباری، مشخصات حساب بانکی، رمزهای عبور و شماره‌های PIN) به عنوان راهی جدید در کلاهبرداری‌ها به شکلی متنوع طراحی شده است.

• کلاهبرداری‌ها و دزدی اینترنتی شامل کلاهبرداری از حراج‌های آنلاین، سرقت از طریق هویت و کارت اعتباری می‌باشد.

• سرقت هویت: گروه‌های جرایم سازمان یافته، از سرقت هویت برای پنهان کردن هویتشان به منظور گریز از آشکارسازی هویتی و حفاظت از دارایی‌هایشان از مصادره و توقیف استفاده می‌کنند. همچنین سرقت هویت به مجرمان این توانمندی را می‌دهد تا قابلیت انجام چندین کلاهبرداری و جرم را به صورت همزمان داشته باشند (SOCA, ۲۰۰۸:۹).

۲) گروه‌های جرایم مجازی سازمان یافته آنلاین

برخلاف همپوشانی‌های موجود بین گروه‌های جرایم سازمان یافته سنتی و گروه‌های آنلاین در فضای مجازی، این دو گروه از جرایم سازمان یافته را نباید با یکدیگر ترکیب کرد. همان گونه که ایوجین کسپراسکای[٤] بنیان گذار و مدیریت بخش پژوهش و توسعه آزمایشگاه روسی آنتی ویروس کسپراسکای مشاهده کرده است:

[٤]. Eugene Kaspersky

«مجرمان فناوری اطلاعات تنها افرادی هستند که فقط مغزهایشان را تغییر داده‌اند یا ذهنی منقطع دارند. به نظر می‌رسد که مجرمان سنتی به طور کامل از آنها دور هستند. مجرمان فناوری اطلاعات قربانیان خود را نمی‌بینند بنابراین انجام فعالیت‌های مجرمانه برای آنها ساده تر است چرا که آنها احساس نمی‌کنند دستشان در جیب شخصی دیگر است.»

فعالیت‌های گوناگون مجرمانه مستلزم ساختارهای سازمانی گوناگون و ساختار گروه جرایم مجازی سازمان یافته است. این فعالیت‌ها احتمالاً با ساختار سازمان که اعضا برای مدتی محدود از زمانِ ایجاد آن، برای هدایت وظیفه‌ای تعریف شده و معین یا تعیین وظایف و داشتن پیروزی، راه‌های مجزای خود را طی می‌کنند تشکیل شده است. گروه‌های جرایم مجازی سازمان یافته همچنین ساختاری قابل انعطاف، فراملی و علاقمند به داشتن اندازه‌های کوچکتر عضویت هستند. بِرنِر در ادامه این موضوع را توضیح می‌دهد:

قدرت بدنی در دنیای مجازی ناچیز است. یک هکر بر قدرت دفاعی قربانی خود غالب می‌شود نه بوسیله تلاش‌های ده یا بیست هکر بلکه با استفاده از تکنولوژی و تکنیک‌های خودکار که شخص را قادر می‌سازد تا از دفاع‌های الکترونیکی عبور کند. در دنیای مجازی قدرت، نرم افزار است نه تعداد افراد (Brenner, ۲۰۰٤).

حلقه‌های آنلاین پدوفیلیا

حلقه‌های آنلاین پدوفیلیا یکی از مصادیق جرایم آنلاین می‌باشد. ساختار توانمند اینترنت راه‌های جدیدی برای تجارت بهره کشی از کودکان را ایجاد کرده است که شامل آرایش کودکان و نمایش آن‌ها به صورت آنلاین به منظور ارتباط جنسی است. اینترنت به طور وسیعی با استفاده از اشتراک اطلاعات با دیگران، آرایش کودکان برای اهداف جنسی و تقویت بزرگسالان از طریق فلسفه تجاوز به کودکان را تسهیل کرده است.

دیوید هاینس[۵] یکی از مرتکبین به جنایتی است که عکس‌هایی از کودکان برای هرزه نگاری گرفته است و بر روی اینترنت قرار داده است – در بیست و چهار ساعت ابتدایی که او این اسناد را بارگذاری کرده است او را دستگیر کردند. او دیگر افراد پدوفیلیا را نیز ملاقات کرده بود. این گروه از افراد فکر می‌کردند که به خاطر ناشناس بودنشان در اینترنت هیچگاه شناخته نمی‌شوند بنابراین عکس‌های آشکار جنسی از کودکان را با یکدیگر معاوضه می‌نمودند و درباره آنها به گفتگو می‌نشستند. او فردی خجالتی و درون گرا شبیه به دیگر مجرمین در گفت و گوهای مجازی بود، که توانسته بود دوستانی فوری و سریع برای خود پیدا کند. مشکل اصلی تنها مبادله عکس‌ها، روش ارتباط افراد پدوفیلیا با یکدیگر و تقویت باورهای جنسی خودشان در زمینه کودکان نبود بلکه‌این واقعیت وحشتناک است که‌این کودکان به شکل و گونه‌ای در ارتباط با این چنین بزرگسالانی هستند (Adam, ۲۰۰۲: ۱٤۰).

دسترسی آسان بازار برای معامله کالاهای استثماری کودکان برای بدست آوردن سود مالی، مجرمان را برای ارتکاب جرایم استثمار کودکان به صورت آنلاین تحریک می‌کند. برای مثال، فردی در ایالات متحده در دادگاه‌ایالتی مورد اتهام قرار گرفت که بنا بر اظهارات "عکس‌هایی از بهره کشی جنسی کودکان نابالغ را در طی تابستان سال ۲۰۰۷ به نمایش گذاشته است". متهم بنا بر حکم دادگاه در ۲۹ آوریل سال ۲۰۰۸ محکوم شد. در رویدادی جدیدتر، ۹۰ نفر در دادگاه استرالیا برای دانلود تصاویر کودک آزاری در شبکه جهانی هرزه نگاری کودک محکوم شدند و تعقیب این افراد توسط تجسس جهانی به رهبری پلیس فدرال استرالیا به مدت ٦ ماه طول کشید.

گروه‌های جرایم سازمان یافته همچنین می‌توانند به صورت اشتراک خصوصی (تنها با دعوت) به اتاق‌های IRC که شامل توزیع بالایی از ویدئوهای کودک آزاری جنسی است وارد شوند. در این فضا افراد به فعالیت‌های تجاری جنسی مثل تولید و فروش کالاهای هرزه نگاری کودکان می‌پردازند (Harrison, ۲۰۰٦: ۳٦۸).

از دیگر تکنولوژی‌های ارتباطی مثل دارک‌نت[٦] (با شبکه‌های همتا به همتا مرتبط است) می‌توان به طور بالقوه‌ای بوسیله مجرمان مجازی برای تبلیغات، تصاویری از کودک آزاری، و یا از فایل‌های دیجیتال کپی رایت شده در حالتی امن به منظور اجتناب از پیگیری‌های قانونی استفاده نمود. شبکه‌های همتا به همتا همچنین می‌توانند بوسیله گروه‌های جرایم مجازی سازمان یافته به عنوان بازاری یکپارچه برای تصاویر آزار جنسی کودکان عمل کنند.

---

۵. David Hines
٦. Darknet

برای مثال در "عمل فشار بر گروه همتا" که به وسیله FBI در سال ۲۰۰۳ هدایت شد تصاویر دانلود شده از آزار جنسی کودکان از طریق شبکه‌های همتا به همتا انجام شده بود. یا در موردی جدیدتر، بیش از ۷۰۰ فرد مشکوک مرتبط با حلقه آنلاین پدوفیلیا که در چت روم‌های اینترنتی بریتانیا با نام "کودکان، نور زندگی ما هستند" عمل می‌کردند به صورت جهانی دستگیر شدند (UK CEOP, ۲۰۰۷).

با پیشرفت‌های انجام گرفته در تکنولوژی‌های ارتباطی، افزایش در راه‌هایی برای مجرمین جنسی کودکان و جرایم مجازی در بهره‌کشی آنلاین کودکان با ریسک پایین قابل ردیابی است. گمنامی در ارتباطات می‌تواند از طریق استفاده از "قرارداد گمنامی"[۷] اجازه دهد تا اطلاعات از طریق شبکه‌ای از سرورها حرکت کند. استفاده‌های دیگر از رمز گذاری به منظور پنهان کردن مسیر داده‌ها سبب از بین رفتن اجبار قانونی می‌شود (Marks, ۲۰۰۷).

مجرمان مجازی همچنین می‌توانند ارتباطات آنلاین، تصاویر دیجیتال (به طور مثال تصاویری که کاربران چت روم‌ها در قسمت پروفایل خود قرار می‌دهند) و فایل‌های ویدئویی را به وسیله استفاده از تعیین اعتبار رمز عبور، رمزگذاری و تکنیک‌های تندنویسی پنهان کنند. این موارد می‌تواند موانعی جدی در پیگیری قانونی و جست و جو در تلاش‌هایی برای مبارزه با آزار جنسی کودکان و دیگر فعالیت‌های بهره‌کشی کودکان باشد. (Raymond Choo, ۲۰۰۸: ۲۸۲)

۳) گروه‌های جرایم سازمان یافته مقابله با یکپارچگی رایانه‌ها

برای مجرمان یکپارچگی رایانه‌ها، فضای مجازی به افراد و شبکه‌های مجرمانه امکان محیط‌های ناموازی را پیشنهاد می‌دهد، به عبارت دیگر گمنامی، تحرک، دسترسی جغرافیایی و حوزه آسیب‌پذیری می‌تواند دامنه و مقیاس خساراتی را که ممکن است از حملات در برابر رایانه‌ها و اطلاعات اساسی ایجاد شود را افزایش می‌دهد. هنگامی که ویروسی ساخته می‌شود و شروع به تخریب سیستم می‌کند، در سیستم تجاری و بازرگانی، میلیون‌ها دلار از درآمد قطع می‌شود و یا اگر این تخریب از طریق فضای مجازی در سیستم‌های پزشکی اتفاق بیفتد جان انسان‌ها به

---

[۷]. Onion Router

خطر خواهد افتد. در جایی که چنین حملاتی مورد هدف قرار می‌گیرد تاثیر حملاتی این گونه در فضای مجازی بر زیر ساخت‌های ملی مثل سیستم‌های انرژی و یا شبکه حمل و نقل بسیار مشهود خواهد بود و پیامد آن به طور روشن مهم و نگران کننده خواهد بود. به طور مثال در سال ۲۰۰۳ بندر هوستون در ایالات متحده توقفی را بعد از حمله ویروسی به سیستم رایانه‌ای را تجربه کرد به طوری که عملیات و فعالیت‌های بندر به طور کامل متوقف شد و میزان خسارت بسیار بالایی را به همراه داشت.

به منظور مقابله با تهدیدات جرایم رایانه‌ای از این گروه و بالا بردن امنیت فضای مجازی، دولت‌ها به دنبال چارچوبی قانونی هستند که احتمال چنین حملاتی را کاهش دهد. این چارچوب باید به کارگزاران قانونی به طور کامل اجازه دهد تا به منظور رسیدگی و پیگرد قانونی اجازه فعالیت داشته باشند (Walden, ۲۰۰۵: ۵۲).

موانع موجود در تحلیل جرایم سازمان یافته مجازی

بدست آوردن آمار قابل اعتماد در زمینه جرایم مجازی و رایانه‌ای بسیار دشوار است (Smith et al, ۲۰۰٤). این موضوع در زمینه جرایم سازمان یافته با پیچیدگی‌های دو چندانی روبه رو است. از جمله مواردی که به‌این فقدان اطلاعات دامن می‌زند در ابتدا عدم گزارش قربانیان است. از آنجایی که در جرایم سازمان یافته بیشتر سازمان‌ها و شرکت‌ها مورد حمله قرار می‌گیرند این نهادها برای حفاظت از شهرت و نام تجاری خودشان گزارشی در این زمینه ارائه نمی‌دهند. پیماشی در ایالات متحده انجام شد و نشان داد که تنها ۳۰ درصد از پاسخگویانی که مورد تجاوز مجازی قرار گرفته بودند گزارشی را به نهادهای قانونی ارائه کرده‌اند.

دومین مانع فقدان تجربه و منابع کافی نهادهای قانونی به منظور مقابله با جرایم فضای مجازی است. این مانع دوم با مانع اول کاملاً در ارتباط است. زمانی که قربانیان پاسخ ضعیفی از نهادهای قانونی دریافت می‌کنند علاقه کمتری به گزارش این موارد خواهند داشت.

سوم، ثبت آمارهای مرتبط و مشترک با یکدیگر است. نهادهای قانونی اغلب در دسته بندی اطلاعات مرتبط با جرایم فضای مجازی شکست می‌خورند. بواسطه فقدان منابع و یا به واسطه پیچیدگی ثبت، ممکن است

رویدادهایی مثل ارتکاب به کلاهبرداری از طریق اینترنت در دو گروه دسته‌بندی شود. هم به عنوان جرمی‌در فضای مجازی و هم به عنوان جرمی‌در فضای واقعی. بنابراین آمارهایی این چنینی می‌توانند در دو منبع ثبت شوند که مشکلات بعدی در ارائه آمارها را به همراه خواهد داشت.

چهارم، سرشت فراملی جرایم فضای مجازی و مشکلات اداری قضایی مجرمان است. مقابله با جرایم فراملی نیاز به منابعی متمرکز است که پیگیری و تعقیب موفق مجرمان را به همراه داشته باشد (Sommer, ۲۰۰۰). در این رابطه می‌توان چنین مثالی را مطرح نمود که می‌توان فردی را تصور کرد که در نقطه دور افتاده‌ای از یک کشور آفریقایی، در اتاق کوچک خود نشسته و مدام با نفوذ در سیستم اطلاعات امنیتی وزارت دفاع آلمان، بدون آنکه کمترین اثری از خود بر جای بگذارد، به سرقت داده‌های حساس و کلیدی مبادرت می‌ورزد. این در حالی است که خودش هم نمی‌داند اطلاعات یاد شده در کجا قرار داردند. پس از این اطلاعات، احتمال دارد آن‌ها را به چندین کشور دیگر منتقل کند و این کشورها را نیز تحت تاثیر پیامدهای این امر قرار دهد. بر مبنای این واقعیت، چندین کشور در معرض ارتکاب چنین جرمی‌قرار می‌گیرند و احتمالاً ادعای خود را دایر بر صلاحیت رسیدگی به جرم مزبور، مطرح خواهند ساخت. با توجه به اولویتی که برای عناصر مراحل ارتکاب جرم قائل می‌شویم، کشورهای ذی نفع در چنین جرایمی، با اعلام این که حادثه مزبور در درون مرزهای آن اتفاق افتاده است، خود را محق می‌دانند در اجرای اصل صلاحیت سرزمینی، برای تعقیب و مجازات مرتکب جرم اقدام نمایند. این مسئله نوعی تعارض در صلاحیت دادگاه‌های کشورهای مزبور به وجود می‌آورد که‌این امر از مباحث مهم و اساسی در حوزه جرایم سایبری محسوب می‌شود (الماسی، ۱۳۸۲: ۲۲).

و در آخر، رایانه‌ها وقتی به طور مشخص شبکه هستند، امکان حذف همه اطلاعات پیش از تشکیل دادگاه چالش مهمی را برای فرد و نهادهای قانونی به منظور پیگیری و تعقیب ایجاد می‌کنند (Sommer, ۲۰۰۰).

بحث و نتیجه‌گیری

اینترنت یکی از مهم ترین وسایل ارتباط جمعی است که از دهه ۱۹۹۰ به‌این طرف به شدت رشد یافته است و ظرفیت و توانایی آن به عنوان یک عنصر اساسی ارتباطی و اطلاعاتی در عصر حاضر آشکار گردیده است (Currie, ۱۹۹۷). همچنین موضوعاتی چون جرم، مجرم و قربانی در هر جامعه از اهمیت خاصی برخوردار است، به طوری که توسط بسیاری از افراد به عنوان شاخص امنیت و یا عدم امنیت در جامعه به کار می‌رود (Hall, et al, ۱۹۷۸).

میل و اشتیاق به استفاده از رایانه و اینترنت و بهره‌مندی از مزایای آن، اگرچه زمینه مشارکت جوامع گوناگون در فناوری‌های پیشرفته را فراهم کرده، اما درعین‌حال، شرایط و بستر مساعدی نیز برای ظهور جرایم سایبری به وجود آورده است. تفاوت در استانداردهای موجود در فضای مجازی و فضای واقعی و عدم اجبارهای قانونی موجب شده است که برخی از مجرمان از رایانه و شبکه جهانی اینترنت به‌مثابه دامی برای اعمال مجرمانه خود و سوءاستفاده از دیگر کاربران که شاید اطلاعاتی کافی در زمینه امنیت و چگونگی حضور در این فضا را ندارند ایجاد کرده باشد و این غفلت کاربران (افراد یا سازمان‌ها) سبب شده است تا افراد با حضور در کنار یکدیگر گروه‌ها و باندهایی را به‌منظور کسب منافع اقتصادی بیشتر ایجاد کنند.

در فضای مجازی افراد و گروه‌های مجرمانه با تعاریف مرتبط با این زمینه و بافت شکل می‌گیرند که شناخت این فضا توسط متخصصین نیازی اساسی خواهد بود. پس از شناخت دقیق، عالمانه، جامع‌نگر و ارزیابی دقیق از نقطه‌ای که در آن قرار داریم می‌توانیم به مهندسی فضای مجازی توسط متخصصین در حوزه‌های گوناگون آسیب‌های موجود در این فضا را کاهش دهیم.

ازآنجایی‌که درزمینه فضای مجازی در کشور ما پدیده تاخر فرهنگی[۸] رخ‌داده است و تکنولوژی پیش از فرهنگ استفاده از آن در بین عامه مردم جای خود را بازکرده است امکان وقوع آسیب‌های گوناگون در بین افراد با ضریبی بسیار بالا افزایش پیداکرده است. پدیده تاخر فرهنگی در زمینه به‌کارگیری اینترنت و فضای مجازی اولویت آموزش افراد در زندگی روزمره و چگونگی بالا بردن ضریب امنیت در این فضا را می‌طلبد که به آموزشی صحیح ضریب نفوذ گروه‌های مجرمانه مجازی به اطلاعات و داده‌های شخصی افراد کاهش چشمگیری را نشان خواهد داد.

---

[۸]. Cultural Lag

پیشنهادها

۱- ازآنجاکه بسیاری از کاربران فضای مجازی آموزشی در زمینه رفتارهای پرخطری که منجر به آسیب دیدن در این فضا می‌شود را ندیده‌اند. آموزش همگانی به عامه مردم به‌منظور چگونگی استفاده از فضای مجازی و محفوظ ماندن از خطرهای نام‌برده شده ضروری به نظر می‌رسد.

۲- ارائه آموزش‌هایی خاص و فرآتر از آموزش عام به اشخاص و سازمان‌هایی که استفاده بیشتری از فضای مجازی دارند، چراکه این افراد بیشتر در معرض جرایم سایبری قرار دارند.

۳- ازآنجاکه یکی از راه‌های ورود و کاهش امنیت در فضای سایبر ارتباط با پایگاه‌های ضد اخلاقی و مبتذل است به‌منظور جلوگیری از ورود افراد به این بخش، سایت‌های مفید و درعین‌حال با جذابیت کافی طراحی و ایجاد کنیم.

٤- استفاده از نرم‌افزارها و سیستم‌های ایمنی و مناسب در رایانه‌های شخصی و سازمانی و به‌روزرسانی مداوم در مقابله با حملات افراد و گروه‌های مجرمانه.

۵- آموزش و به‌کارگیری نیروی انسانی متخصص درزمینه مقابله با جرایم رایانه‌ای در نیروی انتظامی.

٦- توسعه و حمایت همه‌جانبه از گشت زنی و مراقبت پلیس سبب می‌شود تا پلیس بتواند با استفاده از نرم‌افزارهای قدرتمندی که در اختیار دارد پیشگیری از وقوع جرم در فضای مجازی را کاهش می‌دهد.

۷- تعامل و همکاری مناسب میان شرکت‌های مخابراتی ارائه‌کننده خدمات اینترنت و پلیس در فرآیند پیشگیری می‌تواند کمک زیادی داشته باشد.

۸- پیش‌بینی مجازات سنگین برای افرادی که شبکه‌ها و باندهایی در حوزه جرایم فضای مجازی شکل می‌دهند به‌منظور بازداری و پیشگیری از وقوع جرم.

۹- انجام پژوهش‌هایی عمیق و به‌روز درزمینه چگونگی شکل‌گیری و عملکرد گروه‌های مجرمانه در فضای مجازی.

منابع

- آشوری، داریوش. (۱۳۸٦)، ***زبان‌باز، پژوهشی درباره زبان و مدرنیت***، تهران: نشر مرکز، چاپ دوم.
- آیکاو، دیوید جی. (۱۳۸۳)، ***راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای***، ترجمه: اکبر آسترکی، محمد صادق روزبهانی، تورج ریحانی و راحله الیاسی، تهران: معاونت پژوهش دانشگاه علوم انتظامی.
- اردبیلی، محمد علی. (۱۳۸۰)، ***حقوق جزای عمومی***، *چاپ دوم*، تهران: میزان، جلد۱.
- الماسی، نجاد علی. (۱۳۸۲)، ***حقوق بین المللی خصوصی***، چاپ اول، تهران: میزان.
- باستانی، برومند. (۱۳۸۳)، ***جرایم کامپیوتری و اینترنتی***، تهران: نشر بهنامی.
- پرویزی، رضا. (۱۳۸٤)، ***پی جویی جرایم رایانه‌ای***، تهران: جهان جام جم، چاپ اول.
- جعفری، مجتبی. (۱۳۸۵)، بزهکاری رایانه‌ای در رویارویی با حقوق جزای فرانسه، ***نشریه حقوقی گواه***، شماره ٦ و ۷.
- جوان جعفری، عبدالرضا.(۱۳۸۹)، جرایم سایبر و رویکرد افتراقی حقوق کیفری، ***مجله دانش و توسعه***، سال هفدهم، شماره ۳٤
- خداقلی، زهرا. (۱۳۸۳)، ***جرایم کامپیوتری***، چاپ اول، تهران: آریان.
- زررخ، احسان. (۱۳۹۰)، بزه دیده شناسی سایبری، ***فصلنامه مجلس و پژوهش***، سال ۱۷، شماره ٦٤.
- کوثری، مسعود و دیگران. (۱۳۸۷)، ***اینترنت و آسیب‌های اجتماعی (مجموعه مقالات)***، چاپ اول، تهران: سلمان.
- نورزاد، مجتبی. (۱۳۸۹)، ***جرایم اقتصادی در حقوق کیفری ایران***، تهران: جنگل.

- Adam, A (۲۰۰۲). ***Cyberstalking and Internet pornography: gender and the gaze.*** Ethics Inf Technol ٤ (۲).
- Brenner, S,W. (۲۰۰۲). ***Organized cybercrime? How cyberspace may affect the structure of criminal relationships***. North Carolina Journal of Law & Technology ٤ (۱).
- Casey, E. (۲۰۰۰). ***Digital Evidence and Computer Crime.*** London. Academic press.
- Currie, E. (۱۹۹۷). ***Market, Crime and Community: Toward a mid-Range Theory of post Industrial Violence***. Theoretical Criminology. ۱ (۲).

- Furnell, S. (۲۰۰۲). ***Cyber Crime: Vandalizing the Information Society*****,** London, Addison Wesley.
- Gareth Norris et.al (۲۰۰۵). ***Contemporary Comment: An Examination of Australian Internet Hate sites***. Bond University.
- Hall, S. Clarke, J. Critcher, C. Jefferson, T, and Roberts, B. (۱۹۷۸). ***Policing the Crisis, Mugging the State and Law and Orders***, London Macmillan.
- Harrison, C. (۲۰۰٦). ***Cyberspace and child abuse images: a feminist perspective***. Affiliate ۲۱ (٤).
- Kamal, Ahmad. (۲۰۰۵). ***The Law of Cyber_Space. An Invitation to the Table of Negotiations***. Published by United Nations Institute for Training and Research.
- Marks, P. (۲۰۰۷). ***How to leak a secret and not get caught***. New Sci ۲٥۸٦:۱۳
- Raymond Choo, K.K. (۲۰۰۸). ***Organised Crime Groups in Cyberspace: a Typology***. Trends Organ Crime. ۱۱.
- Serious Organised Crime Agency (SOCA) (۲۰۰٦). ***The United Kingdom threat assessment of serious organised crime***. Available at: (http://www.soca.gov.uk/assessPublications/downloads/threat_assess_ unclass_۲٥۰۷۰٦.pdf)
- Singh, S (۲۰۰۷). ***The risks to business presented by organised and economically motivated criminal enterprises***. J Financ Crime ۱٤ (۱).
- Smith, R., Grabosky, P. and Urbas, G. (۲۰۰٤). ***Cyber Criminals on Trial*****.** Cambridge, Cambridge University Press.
- Sommer, P. (۲۰۰۲). ***Evidence from Cyberspace: Downloads, Logs and Captures***. Computer and Telecommunications Law Review, ۸ (۲).
- Stewart, M James (۲۰۰٤). ***Security + Fast Pass***. Published by John Wiley & Sons
- United Kingdom Child Exploitation and Online Protection (UK CEOP) (۲۰۰۷). ***Global online child abuse network smashed—CEOP lead international operation into UK based paedophile ring***. Media release, ۱۸ June
- United Kingdom Organised Crime Task Force (UK OCTF) (۲۰۰۷). Annual report and threat assessment ۲۰۰۷: ***organised crime in Northern Ireland***. Available at:

(http://www.octf.gov.uk/index.cfm/section/publications/page/publicationList/viewArchives/true/category/٥)

- Walden, I. (۲۰۰۳). ***Computer Crime***. C. Reed and J. Angel (Eds), Computer Law, ۵th edition, Oxford University Press.
- Walden, I. (۲۰۰۵). ***Crime and Security in Cyberspace***. Cambridge Review of International Affairs, Volume ۱۸, Number