گونه شناسی باندهای جرم و فساد در فضای مجازی

دکتر طلعت اله یاری[1] و سجّاد مجیدی پرست[2]

چکیده:

بیان مسئله: *توسعه پدیده جهانی فناوری اطلاعات و ارتباطات، تحولی شگرف در ابعاد مختلف 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 فرصت های جنایی بدل گشته است. این ویژگی توسط مجرمان مجازی مورد سوء استفاده قرار گرفته و شکل گیری گروه های فساد و جرم در این فضا را به دنبال داشته است.*

روش پژوهش: *مقاله حاضر به شناخت و طبقه بندی جرائم مجازی سازمان یافته و موانعی که باعث عدم شناخت این جرائم می باشند را به روش کتابخانه ای مورد تحلیل و بررسی قرار داده است.*

یافته ها: *سه دسته از گروه های جرائم سازمان یافته که از پیشرفت تکنولوژی های ارتباطی و اطلاعاتی به منظور نقض کنترل های نظم بخش و قانونی بهره می برند عبارتند از: ۱) گروه های جرائم سازمان یافته سنتی که از تکنولوژی های ارتباطی و اطلاعاتی استفاده می کنند تا فعالیت های مجرمانه خود را تسهیل کنند. ۲) گروه های سازمان یافته مجازی مجرمانه که به طور اختصاصی به صورت آنلاین عمل می کنند. ۳) دسته سوم، از فعالیت هایی تشکیل شده است که مقصود و هدف از آن به خطر انداختن درستی، مقبولیت و اعتماد به رایانه ها و سیستم هایی است که به اینترنت متصل می شوند و اطلاعات بر روی آنها پردازش می شود.*

نتایج: *در پایان با توجه به شناخت حاصل شده به منظور کاهش آسیب های ناشی از باندهای جرم و فساد پیشنهاد می شود که بهترین شیوه در جلوگیری از وقوع جرائم رایانه ای، آموزش عموم جامعه از یک سو و ایجاد پلیس سایبر و تقویت آن به منظور گشت زنی در فضای مجازی از سویی دیگر می تواند به افزایش امنیت در این عرصه کمک شایان توجهی نماید.*

کلمات کلیدی: فضای مجازی، گروه سازمان یافته مجرمانه، جرائم رایانه ای، فناوری اطلاعات

---

۱. استادیار گروه مددکاری اجتماعی، دانشکده علوم اجتماعی، دانشگاه علامه طباطبایی، تهران، ایران
پست الکترونیک: Siba345@yahoo.com
۲. دانشجوی کارشناسی ارشد مددکاری اجتماعی، دانشگاه علامه طباطبایی، تهران، ایران
پست الکترونیک: Majidisajjad@gmail.com

Typology of Organized Crime Groups in Cyberspace

Talat Allahyari[1], Ph.D. and Sajjad Majidi Parast[2]

Abstract:

Objectives: *Global development of information and communication technology have created impressive changes in all aspects of economic, social, cultural, security and political life. This cyberspace is growing due to proliferation of many unknown components for people that increase opportunities for criminals. This property has been exploited by cyber criminal and it causes the formation of organized crime groups in cyberspace.*

Method: *This article is recognizing and categorizing crime groups in cyberspace with research library method.*

Findings: *Three categories of organized groups that exploit advances in information and communications technologies (ICT) to infringe legal and regulatory controls are: (1) traditional organized criminal groups which make use of ICT to enhance their terrestrial criminal activities. (2) Organized cybercriminal groups which operate exclusively online. and (3) The third category comprises those activities where the intention is to compromise the integrity, availability and confidentiality of the computers and systems connected to the internet and the data being processed on them, such as hacking and the distribution of viruses.*

Results: *The results show that the best way to prevent cybercrime is educating people and in the other hand we should create cyber police to patrol in cyberspace to increase security.*

Key Words: Cyberspace, Organized Crime Groups, Cybercrime, Information Technology.

---

1. Assistant professor of Allameh Tabatabaii University, school of social sciences, Tehran, Iran.
E_mail: Siba345@yahoo.com
2. M.A. student of social work, Allameh Tabatabaii University, Tehran, Iran,
E_mail: Majidisajjad@gmail.com

مقدمه:

توسعه پدیده جهانی فناوری اطلاعات و ارتباطات، تحولی شگرف در ابعاد مختلف حیات اقتصادی، اجتماعی، فرهنگی، امنیتی و سیاسی ایجاد نموده است. انقلاب الکترونیک تبدیل به مهم ترین پدیده تعیین کننده معاصر شده است. روزانه ده ها هزار رایانه ورود خود را به دنیای جدید اعلام می کنند. این گستره بیکران از یک سو فرصت های بی نظیری را فراهم ساخته و از سوی دیگر تهدیدهای جدی را متوجه بخش اعظم ساختارهای اجتماعی ساخته است(جوان جعفری، ۱۳۸۹: ۲). این ویژگی های دوگانه را در بسیاری از نوآوری ها و ابداعات بشری از جمله انقلاب صنعتی می توان مشاهده کرد. اما به نظر می رسد اَبَرساختار فناوری اطلاعات، دنیای جدیدی را خلق کرده است، دنیایی مملو از نوآوری ها و پیچیدگی ها که قاعده و نُرم پذیرفته شده ای ندارد (Grareth, et.al, 2005).

نکته ی مهم در ارتباط با جرایم سایبری ویژگی های 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 گونه ای متمایز از جرائم شده است. ویژگی های 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 گونه ای که گزارشات رسمی سازمان ملل هیچ حوزه ای از زندگی بشری را فارغ از تهدیدات فضای مجازی نمی بیند(Kamal, 2005). این گسترش رو به رشد فضای مجازی با توجه به ناشناخته بودن بسیاری از اجزای آن برای عامه مردم به عاملی برای افزایش فرصت های جنایی بدل گشته است. این ویژگی توسط مجرمان مجازی مورد سوء استفاده قرار گرفته و شکل گیری گروه های 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 پدیده ای کاربردی و محسوس در زندگی روزمره تبدیل شده است، بسیاری از مجرمین نیز از فضای واقعی به فضای مجازی حرکت کرده اند و به دنبال آن گروه هایی با اهداف مجرمانه را نیز شکل داده اند. حضور این گروه های مجرمانه در این فضا سبب ایجاد آسیب های نوپدیدی شده است که شناخت، بررسی و مهندسی آن بر عهده متخصصین علوم مختلف است که نقش متخصصین حوزه اجتماعی در کنترل و مهندسی این فضا می تواند کمک شایانی به شناخت این پدیده و کنترل آن بپردازد.

مقاله حاضر به شناخت و طبقه بندی جرائم مجازی سازمان یافته و موانعی که باعث عدم شناخت این جرائم می باشند را با روش کتابخانه ای مورد تحلیل و بررسی قرار می دهد.

طرح مساله:

فضای مجازی نوعی اجتماع و همسایگی بزرگی است که میلیون ها کامپیوتر و استفاده کنندگان آن را در سراسر جهان به هم پیوند می دهد. با غلبه ی اینترنت بر زندگی روزانه ی انسان ها، طبیعی به نظر می رسد که بسیاری از مشخصه های جامعه ی 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 مشاوره های پزشکی میان پزشکان و بیماران در اینترنت انجام می گیرد. 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 هویت های 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 می دارد، این مجال را فراهم می سازد 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 می نگرند، در حالی که آن فرد، شخصیت متمایزی را در این محیط از خود بروز می دهد و این اعتماد به بزه دیدگی آن شخص منجر خواهد شد(زررخ، ۱۳۹۰: ۱۳۷).

با توجه به اینکه جرائم در فضای مجازی، در اشکال مختلفی ارتکاب می یابند، لذا سخن گفتن در خصوص شرایط، ارکان و تقسیم بندی این جرائم، قدری مشکل به نظر می رسد. عدم ارائه آمار دقیق توسط نیروهای انتظامی و مراجع قضایی پیرامون جرائم مزبور، ناتوانی در خصوص ارائه ی تعریف صریح و روشن از ماهیت این جرائم 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 نمی خورد و شمار زیادی از آن ها نامکشوف محسوب می شوند. این مسئله یکی از معضلاتی است که متصدیان تحقیق در مرحله ی کشف و تعقیب جرائم مزبور با آن مواجه می باشند(خداقلی، ۱۳۸۳: ۳۵). از سوی دیگر پیوند و اتصال به شبکه ی جهانی اینترنت، به روشنی گویای این واقعیت است که ویرانگری و آسیب رسانی می تواند در یک لحظه، سراسر جهان را فراگیرد. سوء استفاده از فناوری های رایانه ای و اینترنتی می تواند امنیت ملی، آسایش عمومی و موجودیت یک جامعه را به مخاطره انداخته و تاثیرهای منفی بی شماری را بر زندگی افراد اجتماع تحمیل کند. همچنین با کمی دقت در این خصوص می توان به این نتیجه دست یافت که اغلب مرتکبان جرائم سایبری را جمعیت جوان تشکیل می دهند(آیکاو، ۱۳۸۳: ۵۵) که این مجرمان هم از ظرفیت جنایی بالایی برخوردارند و هم استعداد خوبی برای انطباق اجتماعی از خود نشان می دهند (جعفری، ۱۳۸۵: ۷۰).

با توجه به ابعاد گسترده و چند بُعدی این پدیده، نیازمند انجام پژوهش ها و بررسی هایی عمیق در خصوص نحوه ی شکل گیری، عملکرد و چگونگی مقابله با افراد و گروه های سازمان یافته در فضای مجازی می باشیم، که در این مقاله سعی شده است تا گونه شناسی[1] از باندهای جرم و فساد در فضای مجازی ارائه شود و در زمینه چگونگی کاهش این پدیده بررسی هایی انجام شود.

جرائم مجازی چیست؟

از لحاظ لغوی در فرهنگ های مختلف سایبر به معنی مجازی و غیرملموس می باشد، محیطی است مجازی و غیر ملموس در فضای شبکه های بین المللی (این شبکه ها از طریق شاهراه های اطلاعاتی مثل اینترنت به هم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ ها، ملت ها، 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 می باشند و به طریق رایانه، اجزا آن و شبکه های بین المللی به هم مرتبط می باشند(باستانی، ۱۳۸۳).

و در تعریفی دیگر محیط سایبر، به محیطی مجازی اطلاق می شود که اطلاعات در آن رد و بدل می گردند (پرویزی، ۱۳۸۴: ۴۶).

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

تعاریف بسیار گوناگونی در زمینه جرائم در فضای مجازی وجود دارد که به چند مورد می پردازیم. در تعریف جرم سایبری آمده است: جرم رایانه ای در بردارنده هر رفتار غیرقانونی است که رایانه یا شبکه به عنوان منبع، ابزار، هدف و مکان جرم مطرح می گردد(نورزاد، ۱۳۸۹: ۱۱۴). هر جرمی که دربردارنده رایانه ها و شبکه ها باشد جرم سایبری است، هر چند که خیلی متکی به رایانه نباشد(Casey, 2000: 8). این درحالی است که عده ای جرائم سایبر را جرائمی می دانند که دسته های مختلفی از جرائم را در فضای سایبر و شبکه جهانی اینترنت در برمی گیرد و شامل جرائم ارتکابی به کمک رایانه و جرائم متمرکز بر رایانه نیز می شود(Furnell, 2002: 22). در واقع جرائم سایبری در فضای سایبر که متشکل از شبکه هاست انجام می گیرد، لکن جرائم رایانه ای در فضایی گسترده تر که دربردارنده موارد خارج از شبکه ها به خصوص اینترنت می باشد، رخ می دهد.

جرائم مجازی با استفاده از خلاهای امنیتی موجود در فضای مجازی به ارتکاب جرائم دست می زنند 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(Webster) امنیت به معنای کیفیت یا حالت امن بودن، رهایی از خطر، ترس و احساس نگرانی و تشویش می باشد. این تعبیر در دنیای الکترونیکی نیز صادق است اما افراد متخصص این زمینه را در حفظ و بقای ۴ اصل می دانند:

1.Typology

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 می باشد.

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

۴. عدم انکار: به هنگام انجام کاری و یا دریافت اطلاعات یا سرویسی، شخص انجام دهنده یا گیرنده نتواند آن را انکار کند (Stewart, 2004).

انواع گروه های جرائم سازمان یافته:

جرائم مجازی می توانند از لحاظ فعالیت به سه دسته بزرگ تقسیم شوند و بدین گونه شرح داده می شوند:

۱) گروه های جرائم سازمان یافته سنتی که از تکنولوژی های ارتباطی و اطلاعاتی استفاده می کنند تا فعالیت های مجرمانه خود را تسهیل کنند. در این دسته جرائم مجازی مرتبط با رایانه، مثل تقلب و سرقت، در جایی که رایانه ها به ابزارهایی برای عمل مجرمانه، دستکاری اطلاعات به منظور ارتکاب فعالیت های مجرمانه تبدیل می شوند.

۲) گروه های سازمان یافته مجازی مجرمانه که به طور اختصاصی به صورت آنلاین عمل می کنند. در این گروه جرائم مجازی مبنی بر محتوا مثل نقض قانون حق کپی و هرزه نگاری از کودکان است و رایانه ها و تکنولوژی های ارتباطی، توزیع این اطلاعات غیرقانونی را تسهیل می کند.

۳) دسته سوم، از فعالیت هایی تشکیل شده است که مقصود و هدف از آن به خطر انداختن درستی، مقبولیت و اعتماد به رایانه ها و سیستم هایی است که به اینترنت متصل می شوند و اطلاعات بر روی آنها پردازش می شود این فعالیت ها شامل هک کردن و ساخت ویروس هایی در فضای مجازی است(Walden 2003, 295).

۱) گروه های جرائم سازمان یافته سنتی:

دست یابی به سود مالی همواره یکی از نیرو محرکه های اصلی در شکل گیری گروه های جرائم 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 جرائم آن ها 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 طُعمه ها برای پیوستن به باندهای مجرمانه قومی _ ملی می باشند. بنابراین گروه های کره ای، ویتنامی، چینی، روسیه ای(همان شوروی سابق)، کارائیبی و آمریکای جنوبی بهترین گروه های سازمان یافته در ایالات متحده، بریتانیا و اروپا می باشند(Singh, 2007:80).

برخلاف تلاش های دولتی در سرکوب فعالیت های جرائم سازمان یافته، این گروه های مجرمانه از قدرت تکنولوژی های ارتباطی و اطلاعاتی (ICT[1]) به منظور تسهیل یا کمک به بالا بردن جرائم و پویایی در شناسایی شانس های جدید و راه هایی در غلبه بر اقدامات متقابل را به خوبی شناخته اند. آنها با تغییرات تکنولوژیک و قدرت تکنولوژی های ارتباطی و اطلاعاتی به منظور تسهیل فعالیت های مجرمانه ی 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 سیستم های 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 داده اند (Raymond Choo, 2008: 272).

اینترنت بازاری بزرگتر برای کسانی که به دنبال فروش اجناس تقلبی و دزدی شده هستند فراهم کرده است. داروهای تقلبی یکی از حوزه هایی است که رشدی خاص از طریق اینترنت را مشاهده کرده است یا بواسطه ی هزینه بالای داروهای تجویز شده، مشکل در بدست آوردن آنها، یا بواسطه ی خجالت بیمار در درخواست دارویی خاص است. اینترنت به متقلبین راهی آسان و ارزان به منظور تبلیغات، بازاریابی و توزیع محصولات پیشنهاد می کند و آن تجارتی پرسود برای موسسات تجاری مجرمان سازمان یافته فراهم کرده است(UK OCTF, 2007: 34).

مجرمان سازمان یافته به طور جدی و رو به افزایشی از پیشرفت های تکنولوژیک و به طور خاص رشد اینترنت به منظور توسعه جرائم جدید و تغییر روش های سنتی خود استفاده می کنند. آنها قصد، تصور و توانایی بهره بردن از ضعف امنیتی تکنولوژی اطلاعات و شناسایی شانس های جدید مجرمانه را به نمایش می کشند(SOCA, 2006:1). گروه های جرائم سنتی سازمان یافته به طور رو به افزایشی از هویت های غلط و دزدیده شده به منظور سرقت های مالی استفاده می کنند.

به طور کلی جرائم مرتبط با گروه های 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

1. Information Community Technology

ماه می سال ۲۰۰۷ اعضای گروه شش نفره ای به خاطر تبانی، کلاهبرداری، سرقت از بانک ها و پولشویی تحت تعقیب قرار گرفتند. کیفر خواستی تنظیم شد مبنی بر اینکه متهمان با استفاده از نرم افزار اسکن شبکه افراد و یا رایانه های موسسات مستقلی را که از امنیت بالایی برخوردار نبودند را شناسایی می کردند و به اطلاعات مالی اشخاص مثل شماره حساب، رمزهای عبور و حساب های اینترنتی بانکی را پیدا می نمودند و از اطلاعات بدست آمده به منظور سرقت از حساب های افراد استفاده می کردند. آنها پول را از حساب قربانی به حساب بانکی مورد کنترل خودشان ارسال می کردند و از آنجا به حساب اصلی خودشان انتقال می دادند.

- فیشینگ: کلاهبرداری آنلاین و یا اینترنتی است که اغلب با استفاده از پیام های ناخواسته از سازمانی مشروع به منظور فریب افراد یا سازمان ها به منظور افشای مالی و یا اطلاعات هویت شخصی با هدف تسهیل جرائمی مانند کلاهبرداری، سرقت هویت و سرقت اطلاعات حساس و مهم (مانند اعتبار بانکی) انجام می شود. چندین پژوهشگر و شاغلین در حوزه امنیت به دخالت گروه های جرائم سازمان یافته در کلاهبرداری فیشینگ اشاره کرده اند. در سال های اخیر، پیام های 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 ناخواسته ای است که دریافت کننده را به خرید محصولات متقاعد می کند (به طور مثال سهام شرکت هایی که قیمت سهامشان دچار تورم شده است) در حقیقت آنها از تکنیک های بازاریابی فریبنده استفاده می کنند.
- ایجاد نرم افزارهای مخرب و انتشار آن: در گزارش اخیر ارزیابی تهدید بریتانیا به این موضوع اشاره می شود که جدیدترین نرم افزارهای مخرب به منظور سرقت اطلاعات مالی (مثل جزئیات کارت اعتباری، مشخصات حساب بانکی، رمزهای عبور و شماره های PIN) به عنوان راهی جدید در کلاهبرداری ها به شکلی متنوع طراحی شده است.
- کلاهبرداری ها و دزدی اینترنتی شامل کلاهبرداری از حراج های آنلاین، سرقت از طریق هویت و کارت اعتباری می باشد.
- سرقت هویت: گروه های جرائم سازمان یافته، از سرقت هویت برای پنهان کردن هویتشان به منظور گریز از آشکارسازی هویتی و حفاظت از دارایی هایشان از مصادره و توقیف استفاده می کنند. همچنین سرقت هویت به مجرمان این توانمندی را می دهد تا قابلیت انجام چندین کلاهبرداری و جرم را به صورت همزمان داشته باشد(SOCA, 2008:9).

۲)گروه های جرائم مجازی سازمان یافته آنلاین:

برخلاف همپوشانی های موجود بین گروه های جرائم سازمان یافته سنتی و گروه های آنلاین در فضای مجازی، این دو گروه از جرائم سازمان یافته را نباید با یکدیگر ترکیب کرد. همان گونه که ایوجین کسپراسکای (Eugene Kaspersky) بنیان گذار و مدیریت بخش پژوهش و توسعه آزمایشگاه روسی آنتی ویروس کسپراسکای مشاهده کرده است:

«مجرمان فناوری اطلاعات تنها افرادی هستند که فقط مغزهایشان را تغییر داده اند یا ذهنی منقطع دارند. به نظر می رسد که مجرمان سنتی به طور کامل از آنها دور هستند. مجرمان فناوری اطلاعات قربانیان خود را نمی بینند بنابراین انجام فعالیت های مجرمانه برای آنها ساده تر است چرا که آنها احساس نمی کنند دستشان در جیب شخصی دیگر است.»

فعالیت های مختلف مجرمانه مستلزم ساختارهای سازمانی مختلف و ساختار گروه جرائم مجازی سازمان یافته است. این فعالیت ها احتمالاً با ساختار سازمان که اعضا برای مدتی محدود از زمان ایجاد آن برای هدایت وظیفه ای تعریف شده و معین یا تعیین وظایف و داشتن پیروزی، راه های مجزای خود را طی می کنند تشکیل شده است. گروه های جرائم مجازی سازمان یافته همچنین ساختاری قابل انعطاف، فراملی و علاقمند به داشتن اندازه های کوچکتر عضویت هستند. بِرنِر در ادامه این موضوع را توضیح می دهد:

قدرت بدنی در دنیای مجازی ناچیز است. یک هکر بر قدرت دفاعی قربانی خود غالب می شود نه بوسیله ی تلاش های ده یا بیست هکر بلکه با استفاده از تکنولوژی و تکنیک های خودکار که شخص را قادر می سازد تا از دفاع های الکترونیکی عبور کند. در دنیای مجازی قدرت، نرم افزار است نه تعداد افراد(Brenner, 2004).

حلقه های آنلاین پدوفیلیا

حلقه های آنلاین پدوفیلیا یکی از مصادیق جرائم آنلاین می باشد. ساختار توانمند اینترنت راه های جدیدی برای تجارت بهره کشی از کودکان را ایجاد کرده است که شامل آرایش کودکان و نمایش آن ها 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 (David Hines) یکی از مرتکبین به جنایتی است که عکس هایی 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 می کردند که به خاطر ناشناس بودنشان در اینترنت هیچگاه شناخته

نمی شوند بنابراین عکس های آشکار جنسی از کودکان را با یکدیگر معاوضه می نمودند و درباره ی آنها به گفتگو می نشستند. 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 عکس ها، روش ارتباط افراد پدوفیلیا با یکدیگر و تقویت باورهای جنسی خودشان در زمینه کودکان نبود بلکه این واقعیت وحشتناک است که این کودکان به شکل و گونه ای در ارتباط با این چنین بزرگسالانی هستند (Adam, 2002: 140).

دسترسی آسان بازار برای معامله کالاهای استثماری کودکان برای بدست آوردن سود مالی، مجرمان را برای ارتکاب جرائم استثمار کودکان به صورت آنلاین تحریک می کند. برای مثال، فردی در ایالات متحده در دادگاه ایالتی مورد اتهام قرار گرفت که بنا بر اظهارات "عکس هایی 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 ۶ ماه طول کشید.

گروه های جرائم سازمان یافته همچنین می توانند به صورت اشتراک خصوصی (تنها با دعوت) به اتاق های IRC که شامل توزیع بالایی از ویدئوهای کودک آزاری جنسی است وارد شوند. در این فضا افراد به فعالیت های تجاری جنسی مثل تولید و فروش کالاهای هرزه نگاری کودکان می پردازند(Harrison, 2006: 368) .

از دیگر تکنولوژی های ارتباطی مثل دارک نت[1] (با شبکه های همتا به همتا مرتبط است) می توان به طور بالقوه ای بوسیله ی مجرمان مجازی برای تبلیغات، تصاویری از کودک آزاری، و یا از فایل های دیجیتال کپی رایت شده در حالتی امن به منظور اجتناب از پیگیری های قانونی استفاده نمود. شبکه های همتا به همتا همچنین می توانند بوسیله ی گروه های جرائم مجازی سازمان یافته به عنوان بازاری یکپارچه برای تصاویر آزار جنسی کودکان عمل کنند. برای مثال در "عمل فشار بر گروه همتا" که به وسیله ی FBI در سال ۲۰۰۳ هدایت شد تصاویر دانلود شده از آزار جنسی کودکان از طریق شبکه های همتا به همتا انجام شده بود. یا در موردی جدیدتر، بیش از ۷۰۰ فرد مشکوک مرتبط با حلقه آنلاین پدوفیلیا که در چت روم های اینترنتی بریتانیا با نام "کودکان، نور زندگی ما هستند" عمل می کردند به صورت جهانی دستگیر شدند(UK CEOP, 2007).

با پیشرفت های انجام گرفته در تکنولوژی های ارتباطی، افزایش در راه هایی برای مجرمین جنسی کودکان و جرائم مجازی در

1. Darknet

بهره کشی آنلاین کودکان با ریسک پایین قابل ردیابی است. گمنامی در ارتباطات می تواند از طریق استفاده از " قرارداد گمنامی[1]" اجازه دهد تا اطلاعات از طریق شبکه ای از سرورها حرکت کند. استفاده های دیگر از رمز گذاری به منظور پنهان کردن مسیر داده ها سبب از بین رفتن اجبار قانونی می شود(Marks, 2007).

مجرمان مجازی همچنین می توانند ارتباطات آنلاین، تصاویر دیجیتال (به طور مثال تصاویری که کاربران چت روم ها در قسمت پروفایل خود قرار می دهند) و فایل های ویدئویی را بوسیله ی استفاده از تعیین اعتبار رمز عبور، رمزگذاری و تکنیک های تندنویسی پنهان کنند. این موارد می تواند موانعی جدی در پیگیری قانونی و جست و جو در تلاش هایی برای مبارزه با آزار جنسی کودکان و دیگر فعالیت های بهره کشی کودک باشد(Raymond Choo, 2008: 282).

۳) گروه های جرائم سازمان یافته مقابله با یکپارچگی رایانه ها:

برای مجرمان یکپارچگی رایانه ها، فضای مجازی به افراد و شبکه های مجرمانه امکان محیط های ناموازی را پیشنهاد می دهد، به عبارت دیگر گمنامی، تحرک، دسترسی جغرافیایی و حوزه آسیب پذیری می تواند دامنه و مقیاس خساراتی را که ممکن است از حملات در برابر رایانه ها و اطلاعات اساسی ایجاد شود را افزایش می دهد. هنگامی که ویروسی ساخته می شود و شروع به تخریب سیستم می کند، در سیستم تجاری و بازرگانی، میلیون ها دلار از درآمد قطع می شود و یا اگر این تخریب از طریق فضای مجازی در سیستم های پزشکی اتفاق بیفتد جان انسان ها به خطر خواهد افتد. در جایی که چنین حملاتی مورد هدف قرار می گیرد تاثیر حملاتی این گونه در فضای مجازی بر زیر ساخت های ملی مثل سیستم های 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 رایانه ای را تجربه کرد به طوری که عملیات و فعالیت های بندر به طور کامل متوقف شد و میزان خسارت بسیار بالایی را به همراه داشت.

به منظور مقابله با تهدیدات جرائم رایانه ای از این گروه و بالا بردن امنیت فضای مجازی، دولت ها به دنبال چهارچوبی قانونی هستند که احتمال چنین حملاتی را کاهش دهد. این چهارچوب باید به کارگزاران قانونی به طور کامل اجازه دهد تا به منظور رسیدگی و پیگرد قانونی اجازه فعالیت داشته باشند(Walden, 2005: 52).

1. Onion Router

موانع موجود در تحلیل جرائم سازمان یافته مجازی:

بدست آوردن آمار قابل اعتماد در زمینه جرائم مجازی و رایانه ای بسیار دشوار است(Smith et al, 2004). این موضوع در زمینه جرائم سازمان یافته با پیچیدگی های دو چندانی روبه رو است. از جمله مواردی که به این فقدان اطلاعات دامن می زند در ابتدا عدم گزارش قربانیان است. از آنجایی که در جرائم سازمان یافته بیشتر سازمان ها و شرکت ها مورد حمله قرار می گیرند این نهادها برای حفاظت از شهرت و نام تجاری خودشان گزارشی در این زمینه ارائه نمی دهند. 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 کرده اند.

دومین مانع فقدان تجربه و منابع کافی نهادهای قانونی به منظور مقابله با جرائم فضای مجازی است. این مانع دوم با مانع اول کاملاً در ارتباط است. زمانی که قربانیان پاسخ ضعیفی از نهادهای قانونی دریافت می کنند 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 جرائم فضای مجازی شکست می خورند. بواسطه ی فقدان منابع و یا به واسطه ی پیچیدگی ثبت، ممکن است رویدادهایی مثل ارتکاب به کلاهبرداری از طریق اینترنت در دو گروه دسته بندی شود. هم به عنوان جرمی در فضای مجازی و هم به عنوان جرمی در فضای واقعی. بنابراین آمارهایی این چنینی می توانند در دو منبع ثبت شوند که مشکلات بعدی در ارائه آمارها را به همراه خواهد داشت.

چهارم، سرشت فراملی جرائم فضای مجازی و مشکلات اداری قضایی مجرمان است. مقابله با جرائم فراملی نیاز به منابعی متمرکز است که پیگیری و تعقیب موفق مجرمان را به همراه داشته باشد(Sommer, 2000). در این رابطه می توان چنین مثالی را مطرح نمود که می توان فردی را تصور کرد که در نقطه ی دور افتاده ای 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 داده های حساس و کلیدی مبادرت می ورزد. این در حالی است که خودش هم نمی داند اطلاعات یاد شده در کجا قرار داردند. پس از این اطلاعات، احتمال دارد آن ها 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 جرمی قرار می گیرند 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 می شویم، کشورهای ذی نفع در چنین جرائمی، با اعلام اینکه حادثه ی مزبور در درون مرزهای آن اتفاق افتاده است، خود را محق می دانند در اجرای اصل صلاحیت سرزمینی، برای تعقیب و مجازات مرتکب جرم اقدام نمایند. این مسئله نوعی تعارض در صلاحیت دادگاه های کشورهای مزبور به وجود می آورد که این امر از مباحث مهم و اساسی در حوزه ی جرائم سایبری محسوب می شود(الماسی، ۱۳۸۲: ۲۲).

و در آخر، رایانه ها 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 می کنند(Sommer, 2000).

بحث و نتیجه گیری:

اینترنت یکی از مهم ترین وسایل ارتباط جمعی است که از دهه ی ۱۹۹۰ به این 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, 1997). 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 می رود(Hall, et al, 1978).

میل و اشتیاق به استفاده از رایانه و اینترنت و بهره مندی از مزایای آن، اگرچه زمینه ی مشارکت جوامع مختلف در فناوری های پیشرفته را فراهم کرده، اما در عین حال، شرایط و بستر مساعدی نیز برای ظهور جرائم 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 به مثابه ی دامی برای اعمال مجرمانه خود و سوء استفاده 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 سازمان ها) سبب شده است تا افراد با حضور در کنار یکدیگر گروه ها و باندهایی را به منظور کسب منافع اقتصادی بیشتر ایجاد کنند.

در فضای مجازی افراد و گروه های مجرمانه با تعاریف مرتبط با این زمینه و بافت شکل می گیرند که شناخت این فضا توسط متخصصین نیازی اساسی خواهد بود. پس از شناخت دقیق، عالمانه، جامع نگر و ارزیابی دقیق از نقطه ای که در آن قرار داریم می توانیم به مهندسی فضای مجازی توسط متخصصین در حوزه های مختلف آسیب های موجود در این فضا را کاهش دهیم.

از آنجایی که در زمینه فضای مجازی در کشور ما پدیده تاخر فرهنگی[1] رخ داده است و تکنولوژی پیش از فرهنگ استفاده از آن در بین عامه ی مردم جای خود را باز کرده است امکان وقوع آسیب های مختلف در بین افراد با ضریبی بسیار بالا افزایش پیدا کرده است. پدیده تاخر فرهنگی در زمینه به کارگیری اینترنت و فضای مجازی اولویت آموزش افراد در زندگی روزمره و چگونگی بالا بردن ضریب امنیت در این فضا را می طلبد که به آموزشی صحیح ضریب نفوذ گروه های مجرمانه مجازی به اطلاعات و داده های شخصی افراد کاهش چشمگیری را نشان خواهد داد.

1. Cultural Lag

پیشنهادات:

۱. از آنجا که بسیاری از کاربران فضای مجازی آموزشی در زمینه رفتارهای پرخطری که منجر به آسیب دیدن در این فضا می شود را ندیده اند. آموزش همگانی به عامه مردم به منظور چگونگی استفاده از فضای مجازی و محفوظ ماندن از خطرهای نام برده شده ضروری به نظر می رسد.

۲. ارائه آموزش هایی خاص و فراتر از آموزش عام به اشخاص و سازمان هایی که استفاده بیشتری از فضای مجازی دارند، چرا که این افراد بیشتر در معرض جرائم سایبری قرار دارند.

۳. از آنجا که یکی از راه های ورود و کاهش امنیت در فضای سایبر ارتباط با پایگاه های ضداخلاقی و مبتذل است به منظور جلوگیری از ورود افراد به این بخش، سایت های مفید و در عین حال با جذابیت کافی طراحی و ایجاد کنیم.

۴. استفاده از نرم افزارها و سیستم های ایمنی و مناسب در رایانه های شخصی و سازمانی و به روز رسانی مداوم در مقابله با حملات افراد و گروه های مجرمانه.

۵. آموزش و بکارگیری نیروی انسانی متخصص در زمینه مقابله با جرائم رایانه ای در نیروی انتظامی.

۶. توسعه و حمایت همه جانبه از گشت زنی و مراقبت پلیس سبب می شود تا پلیس بتواند با استفاده از نرم افزارهای قدرقتمندی که در اختیار دارد پیشگیری از وقوع جرم در فضای مجازی را کاهش می دهد.

۷. تعامل و همکاری مناسب میان شرکت های مخابراتی ارائه کننده خدمات اینترنت و پلیس در فرآیند پیشگیری می تواند کمک زیادی داشته باشد.

۸. پیش بینی مجازات سنگین برای افرادی که شبکه ها و باندهایی در حوزه جرائم فضای مجازی شکل می دهند به منظور بازداری و پیشگیری از وقوع جرم.

۹. انجام پژوهش هایی عمیق و به روز در زمینه چگونگی شکل گیری و عملکرد گروه های مجرمانه در فضای مجازی.

منابع:

۱. آشوری، داریوش (۱۳۸۶)، **زبان باز، پژوهشی درباره ی زبان و مدرنیت**، چاپ دوم، تهران: نشر مرکز.

۲. آیکاو، دیوید جی (۱۳۸۳)، **راهکارهای پیشگیری و مقابله با جرائم رایانه ای**، ترجمه: اکبر آسترکی، محمد صادق روزبهانی، تورج ریحانی و راحله الیاسی، تهران: معاونت پژوهش دانشگاه علوم انتظامی.

۳. اردبیلی، محمد علی (۱۳۸۰)، **حقوق جزای عمومی**، چاپ دوم، تهران: میزان، ج۱.

۴. الماسی، نجاد علی (۱۳۸۲)، **حقوق بین المللی خصوصی**، چاپ اول، تهران: میزان.

۵. باستانی، برومند (۱۳۸۳)، **جرائم کامپیوتری و اینترنتی**، تهران: نشر بهنامی.

۶. پرویزی، رضا (۱۳۸۴)، **پی جویی جرائم رایانه ای**، چاپ اول، تهران: جهان جام جم.

۵. جعفری، مجتبی (۱۳۸۵)، **بزهکاری رایانه ای در رویارویی با حقوق جزای فرانسه**، نشریه حقوقی گواه، شماره ۶ و ۷، بهار و تابستان.

۶. جوان جعفری، عبدالرضا (۱۳۸۹)، **جرایم سایبر و رویکرد افتراقی حقوق کیفری**، مجله دانش و توسعه، سال هفدهم، شماره ۳۴

۷. خداقلی، زهرا (۱۳۸۳)، **جرائم کامپیوتری**، چاپ اول، تهران: آریان.

۸. زررخ، احسان (۱۳۹۰)، **بزه دیده شناسی سایبری**، فصلنامه مجلس و پژوهش، سال ۱۷، شماره ۶۴.

۹. کوثری، مسعود و دیگران (۱۳۸۷)، **اینترنت و آسیب های اجتماعی (مجموعه مقالات)**، چاپ اول، تهران: سلمان.

۱۰. نورزاد، مجتبی(۱۳۸۹)، **جرائم اقتصادی در حقوق کیفری ایران**، تهران: جنگل.

11. Adam, A (2002). *Cyberstalking and Internet pornography: gender and the gaze*. Ethics Inf Technol 4 (2):133–42

12. Brenner, S,W. (2002). *Organized cybercrime? How cyberspace may affect the structure of criminal relationships*. North Carolina Journal of Law & Technology 4(1):1–50

13. Casey, E. (2000). *Digital Evidence and Computer Crime*. London. Academic press.

14. Currie, E. (1997). *Market, Crime and Community: Toward a mid-Range Theory of post Industrial Violence*. Theoretical Criminology. 1(2), 72-147

15. Furnell, S. (2002). *Cyber Crime: Vandalizing the Information Society,* London, Addison Wesley.

16. Gareth Norris et.al (2005). *Contemporary Comment: An Examination of Australian Internet Hate sites*. Bond University.

17. Hall, S. Clarke, J. Critcher, C. Jefferson, T, and Roberts, B. (1978). *Policing the Crisis, Mugging the State and Law and Orders*, London Macmillan.

18. Harrison, C. (2006). *Cyberspace and child abuse images: a feminist perspective*. Affiliate 21(4): 365–379

19. Kamal, Ahmad. (2005). *The Law of Cyber_Space. An Invitation to the Table of Negotiations*. Published by United Nations Institute for Training and Research.

20. Marks, P. (2007). *How to leak a secret and not get caught*. New Sci 2586:13

21. Raymond Choo, K.K. (2008). *Organised Crime Groups in Cyberspace: a Typology*. Trends Organ Crime. 11: 270_295

22. Serious Organised Crime Agency (SOCA) (2006). *The United Kingdom threat assessment of serious organised crime*. Available at: (http://www.soca.gov.uk/assessPublications/downloads/threat_assess_ unclass_250706.pdf)

23. Singh, S (2007). *The risks to business presented by organised and economically motivated criminal enterprises*. J Financ Crime 14(1):79–83

24. Sommer, P. (2002). *Evidence from Cyberspace: Downloads, Logs and Captures*. Computer and Telecommunications Law Review, 8(2).

25. Smith, R., Grabosky, P. and Urbas, G. (2004). *Cyber Criminals on Trial.* Cambridge, Cambridge University Press.

26. Stewart, M James (2004). *Security + Fast Pass*. Published by John Wiley & Sons

27. United Kingdom Child Exploitation and Online Protection (UK CEOP) (2007). *Global online child abuse network smashed—CEOP lead international operation into UK based paedophile ring*. Media release, 18 June

28. United Kingdom Organised Crime Task Force (UK OCTF) (2007). Annual report and threat assessment 2007: *organised crime in Northern Ireland*. Available at: (http://www.octf.gov.uk/index.cfm/section/publications/page/publicationList/viewArchives/true/ category/5)

29. Walden, I. (2003). *Computer Crime*. C. Reed and J. Angel (Eds), Computer Law, 5th edition, Oxford University Press.

30. Walden, I. (2005). *Crime and Security in Cyberspace*. Cambridge Review of International Affairs, Volume 18, Number 1