نشریه علمی "شهر تاب آور"
سال دوم، شماره ۱، بهار ۱۳۹۹، ص ۱۱-۱

تحلیل فضایی وقوع جرم کلاهبرداری مالی شهروندان در فضای مجازی شهر تهران

محمدرضا پورغلامی سروندانی[1*]، وحید بارانی پسیان[2]، سیدعلی عبادی‌نژاد[3]

۱- استادیار، ۲- استادیار، ۳- دانشیار، دانشگاه علوم انتظامی امین

(دریافت: ۹۸/۰۳/۰۱، پذیرش: ۹۸/۰۷/۲۰)

چکیده

راهبرد مدیریت جغرافیای جرایم فضای مجازی، تضمین استمرار موفقیت سازمان و جلوگیری از پیشامدی ناگهانی و غافلگیرانه از طریق انتخاب راهبردهای مناسب در برابر دگرگونی‌های محیطی است. برای رویارویی با تبعات ناشی از ظهور فناوری‌های نوین اطلاعاتی، سازمان‌های پلیسی ناگزیرند طیفی از گزینه‌های راهبردی جغرافیایی را انتخاب کنند که در میانهٔ دو وضعیت ادامهٔ وضع موجود و ایجاد تغییر و توسعه قرار دارند. باید توجه داشت که مولفه های جرم شناسی کلاهبرداری فیزیکی با جرم کلاهبرداری فضای مجازی بسیار متفاوت بوده و قانونگذار نیز در کیفرشناسی این نوع جرایم عکس العمل جزیی را از خود نشان داده است. یکی از مشکلات اساسی در خصوص رسیدگی به این نوع جرائم ارتباط موضوع ویژگی های فضایی وقوع این نوع جرم است که موارد صلاحیت‌های قضایی و پلیسی را در پی دارد. هدف این مقاله تحلیل فضایی وقوع جرم کلاهبرداری مالی شهروندان در فضای مجازی شهر تهران است. روش تحقیق این مقاله توصیفی- تحلیلی می‌باشد و ازجامعه آماری تمام شمار ازپرونده‌های برداشت غیرمجاز از حساب‌های بانکی در فضای مجازی در سال ۹۵ در شهر تهران استفاده شده است. در تجزیه و تحلیل اطلاعات این پژوهش از روش‌های آماری- گرافیکی در قالب سیستم اطلاعات جغرافیایی بهره گرفته شده است. در این پژوهش از آزمون مرکز متوسط، بیضی انحراف معیار، آزمون خوشه‌بندی انجام گرفته است. نتایج نشان داد که جرم کلاهبرداری مالی در فضای مجازی با جهت شرقی- غربی در مناطق که بیشترین تمرکز فعالیت‌های اقتصادی را دارد، مشاهده شده است. دو عامل مهم فضایی یعنی تراکم جمعیت و مراکز اقتصادی، از مهم‌ترین عوامل مهم کانون‌های این نوع جرم محسوب شده‌اند.

کلیدواژه‌ها: محل وقوع جرم، جرم کلاهبرداری مالی، شهروندان، فضای مجازی، تهران

۱. مقدمه

افزایش میزان جرائم اینترنتی با ویژگی‌های متنوع آن، موجب نگرانی بوده است. جرائم اینترنتی یک اصطلاح است که گستره وسیعی از فعالیت‌های جنایی با استفاده از رایانه را پوشش می‌دهد. جرائم اینترنتی به اعمال جنایی با استفاده از فضای سایبری در رسانه‌های ارتباطی اشاره دارد. اکثر کشورها به‌طور کامل با زیرساخت‌های قانونی برای رسیدگی به جرائم سایبری مجهز نیستند [۱]. درعین‌حال، مجرمین کلاهبردار، به‌طور مداوم در جستجوی فرصتی برای دریافت مشخصات امنیتی از کارت‌های اعتباری و سایر اطلاعات شخصی مانند آدرس‌های پست الکترونیکی و تاریخ تولد اشخاص هستند تا بتوانند فهرست‌های اسپم ایمیل را در بسیاری از بازارهای سیاه الکترونیکی بفروشند. تجارت الکترونیک، منطقه‌ای است، که برای جرائم، کلاهبرداری و اقدامات جعلی آماده شده است [۲]. محققین مطالعاتی را انجام دادند که به چگونگی و چرایی پیدایش، کیفیت و نحوه پراکندگی اعمال و رفتارهای مجرمانه در محدوده جغرافیایی شهر موردبررسی قرار دادند که توانسته است به کمک نمایش فضایی اعمال مجرمانه و تلفیقی اطلاعات با داده‌های فضایی جرایم و شاخص‌های اجتماعی،اقتصادی مجرم و ویژگی‌های محل سکونت او، امکان شناسایی کانون‌های جرم خیز و پیش‌بینی محل‌های احتمالی وقوع ناهنجاری در محدوده شهر فراهم می‌شود [۳].

متأسفانه میزان ناهنجاری در حوزه‌های شهری بیش از نقاط دیگر کشور است. برابر آمار ارائه‌شده از سوی پلیس فتا، درصد زیادی از جرائم اینترنتی، در اشکال جرائم فضای مجازی در کشور را به خود اختصاص داده است. طی ۶ سال گذشته به ۱۲۰ هزار فقره پرونده توسط پلیس رسیدگی شده و بیش از ۸۶٪ پرونده‌ها در حوزه جرایم سایبری کشف و بیش از ۷۰ هزار مجرم سایبری دستگیر که ۷۷٪ آقایان و ۳۳٪ خانم‌ها بوده‌اند. بیشترین جرایم سایبری به ترتیب مربوط به تهران بزرگ، خراسان‌رضوی، فارس و اصفهان و کمترین جرایم نیز در استان‌های یزد، لرستان، ایلام، کهکیلویه و بویراحمد و جزیره کیش اتفاق افتاده است [۴].

با توجه به آمارهای ذکرشده توسط رییس پلیس تولید و

* نویسنده پاسخگو: rezamrps@yahoo.com

تبادل اطلاعات ناجا (فتا) بزرگترین تهدید جرایم در حوزه فضای مجازی در شهر تهران برداشت‌های مالی غیرمجاز می‌باشد. شهر تهران به دلیل شرایط خاص فضایی و جغرافیایی دارای بالاترین آمار جرائم در بین شهرهای کشور دارا است. با بررسی‌های به‌عمل آمده، برای رسیدگی به وقوع جرم کلاهبرداری مالی شهروندان در فضای مجازی، تحقیقی تاکنون در مورد تحلیل فضایی از داده‌های این نوع جرم را انجام نگرفته است. بنابراین، تجزیه وتحلیل‌های فضایی محل وقوع جرم در این نوع جرائم و تحلیل روند مکان جرایم برداشت غیرمجاز از حساب بانکی به ماموریت‌ها پلیس فتا کمک شایانی خواهد کرد. لازم به ذکر است برای کشف این نوع جرم بایستی در آزمایشگاه‌هایی موسوم به (ادله دیجیتال) مطالعه ومورد بررسی قرار گیرد. در این مقوله به‌واسطه بدیع بودن نوع مسئله و موضوع، محققین ضمن بررسی اشکال ماهوی و شکلی این نوع جرائم، به دنبال پاسخ به این پرسش اصلی هستندکه؛ جغرافیای جرم کلاهبرداری مالی در فضای مجازی در محدوده منطقه ۲۲گانه شهر تهران چگونه است؟

۲. روش تحقیق

این پژوهش از لحاظ جهت‌گیری‌های پژوهش کاربردی، از لحاظ هدف پژوهش، توصیفی- تحلیلی می‌باشد. همچنین این پژوهش از روش اسنادی برای جمع‌آوری اطلاعات استفاده نموده است. جامعه آماری به‌صورت تمام‌شمار می‌باشد که در این پژوهش ۳۰۰ پرونده مربوط به جرایم برداشت غیرمجاز از حساب‌های بانکی در فضای مجازی در سال ۹۵ در مناطق ۲۲گانه شهر تهران می‌باشد این داده‌ها از سوی نیروی انتظامی اخذ گردیده است. در تجزیه‌وتحلیل اطلاعات این پژوهش از روش‌های آماری- گرافیکی در قالب سیستم اطلاعات جغرافیایی بهره گرفته شده است. مهمترین آزمون‌های مورد استفاده در این پژوهش عبارتند از:

۲-۱. مرکز متوسط[1]:

مرکز متوسط را می‌توان به‌عنوان معیاری تقریبی برای مقایسهٔ توزیع فضایی انواع گوناگون جرم یا برای بررسی وقوع یک نوع جرم خاص، در دوره‌های زمانی مختلف به‌کار گرفت. خروجی این ابزار تحلیلی یک لایه جدید خواهد بود که در آن نقطه میانگین مرکزی وجود دارد. اگر هنگام ورود داده‌های این تحلیل فیلد موردی در نظر گرفته شود، در آن صورت لایه ایجاد شده دارای بیش ازیک نقطه میانگین مرکزی خواهد بود، که تعداد آن‌ها متناسب با تعداد طبقات موجود در فیلد مورد خواهد بود.

۲-۲. بیضی انحراف معیار[2]:

توزیع بسیاری از پدیده‌های جغرافیایی در فضا به‌گونه‌ای هستند که ممکن است جهت دار بوده و نتوان آن‌ها را با دایره نشان داد. در این موارد می‌توان با محاسبه واریانس محورهایXو Y به‌طور جداگانه و مستقل روند و جهت توزیع پدیده‌ها درفضا را نشان داد. روشی که معمولاً برای اندازه‌گیری روند در مجموعه‌ای از نقاط یا نواحی به‌کار گرفته می‌شود، محاسبه فاصله استاندارد در جهت X و Y به‌طور جداگانه می‌باشد. این دو مقدار محورهای بیضی که توزیع جهت دارعوارض را در بر می‌گیرد، بیضی انحراف استاندارد نامیده می‌شود. زیرا در این روش انحراف استاندارد مختصات X و Y ازمیانگین مرکزی برای تعیین محورهای بیضی محاسبه می شوند. بیضی انحراف استاندارد این امکان را می‌دهد که اگر توزیع عوارض در فضا از الگوی جهت داری برخوردار باشند آن را شناسایی نماید.

۲-۳. آزمون خوشه‌بندی

آزمون خوشه‌بندی، اولین گام برای شناسایی کانون جرم خیز است. چند روش برای آزمون خوشه‌بندی در توزیع بزهکاری قابل استفاده است. اکثر این روش برای آزمون خوشه‌بندی در توزیع بزهکاری قابل استفاده است. اکثر این روش‌ها در برگیرنده اصل اولیه آزمون فرضیه و آمار کلاسیک است، که درآن فرض می‌شود؛ توزیع بزهکاری از نظر فضایی کاملاً تصادفی است. با درنظر گرفتن فرض توزیع فضایی کاملاً تصادفی به‌عنوان فرضیه صفر، می‌توان توزیع جرایم را در سطح معناداری با فرضیه صفر مقایسه نمود، تا اعتبار آن قبول یا رد شود. "میانگین نزدیکترین همسایه[3]" از جمله آزمون‌های خوشه‌بندی است. در آزمون شاخص نزدیکترین همسایه، فرض صفر (H_0) یعنی توزیع داده‌ها در فضا از الگوی خاصی تبعیت نمی‌کند، و فرض مقابل ۱ (H_1) توزیع داده‌ها در فضا از الگوی خاصی تبعیت می‌کند، تعریف می‌شود. این روش را هنگامی می توان به‌کار گرفت که کاربر به داده‌هایی دسترسی دارد که هرنقطه به یک جرم منفرد مربوط است. اگر نتیجه آزمون، شاخص نزدیک‌ترین همسایه برابر یک باشد، داده‌های بزهکاری به‌صورت تصادفی توزیع شده‌اند. اگر نتیجه کوچکتر از یک باشد، بیانگر خوشه‌ای بودن داده‌های مجرمانه است و اگر شاخص نزدیکترین همسایه بزرگتر از یک باشد، نشان‌دهنده الگوی توزیع یکنواخت داده‌های مجرمانه است.

۳. تحلیل فضایی

تحلیل فضایی، جغرافیا را از یک علم معلومات عمومی به علم

[1]. Mean Center

[2] .Standard Deviation Ellipse

[3] . Average Nearest Neighbor

استخراج دانش علمی و کاربردی تبدیل کرد. اکنون بیشتر مسائل فضایی انسان را تحلیل فضایی پاسخگو است. دراین زمینه، ساختار پراکندگی‌ها شناسایی می‌شود و علت آن‌ها با استفاده از روابط فضایی استدلال می‌شود. با استفاده از داده‌های اندازه‌گیری محدود برای همه نقاط زمین، از طریق فرایند درون‌یابی، داده مورد اطمینان و قابل استفاده به‌دست می‌آید. مهمترین کاربرد چنین نگرشی در برنامه‌ریزی فضایی یا آمایش سرزمین است که کلید اصلی همه فعالیت‌های انسان برروی زمین و استفاده از پراکندگی‌ها یعنی توان زمین است. فقط با استفاده از این توان تحلیل فضایی، می‌توان رابطه منطقی بین پراکندگی جمعیت انسانی ومنابع محیط برقرار کرد [۵].

۳-۱. دیدگاه در مورد فضای مجازی

دیدگاه‌های عمومی و علمی در مورد جرائم رایانه‌ای در دهه ۱۹۸۰ میلادی به‌گونه‌ای بنیادین تغییر یافت و مشخص گردید که جرم رایانه‌ای محدود به جرائم اقتصادی نبوده و سایر زمینه‌هایی را که جنبه اقتصادی نیز ندارد، مانند دست‌کاری رایانه‌ای و تجاوز به حریم زندگی دیگران را نیز در بر می‌گیرد [۳]. اصطلاح "فضای مجازی" توسط "ویلیام گیبسون[۱]" در رمانی تحت عنوان "نئورومانسر[۲]" ساخته شد. همان‌طور که توسط گیبسون به تصویر کشیده شد، فضای سایبر یک محیط مصنوعی است که تجربه‌های حس واقعی سه‌بعدی را فراهم می‌کند، امکان روابط صمیمیت بین افراد در مکان‌های دور را فراهم می‌کند. درحالی‌که بسیاری معتقدند که ظهور اینترنت یک رویداد کاملاً مثبت بوده است، دیگران احساس می‌کنند که یک فضای تاریک در فضای مجازی وجود دارد. این دیدگاه دوم استدلال می‌کند که وقتی افراد از فناوری بیش‌ازحد استفاده می‌کنند و ارتباط مستقیم با دیگر انسان‌ها را از بین می‌برند، خطر از بین رفتن جهان گسترده‌تر وجود دارد. نتیجه این می‌شود که با توجه به تنوع و فراوانی اطلاعات در فضای مجازی باعث می‌شود که هزینه اجتماعات در فضای مجازی در مقایسه با هزینه اجتماعات دنیای واقعی کاهش یابد. اینترنت توانایی افراد را برای کنترل زندگی خود افزایش می‌دهد. درعین‌حال، فردی می‌تواند از طریق هک کردن، اخاذی، گسترش ویروس، فرستادن پیام‌های عظیم ایمیل اسپم، فروش پورنوگرافی دائماً برنامه‌های امنیتی را مورد سوءاستفاده قرار دهد [۲].

۴. تئوری فعالیت‌های روزمره

تئوری فعالیت روزمره (RAT[۳]) نشان می‌دهد که برای رخداد جرم، سه عنصر اساسی- انگیزه مجرم، هدف مناسب و عدم وجود محافظ ماهر- در یک تقاطع زمان و مکان باید باشد. تئوری RAT نشان می‌دهد که افراد تمایل به ارتکاب جرائم دارند و فعالیت‌های سازمانی را در فضایی که توسط انسان ایجادشده، را به انحراف سوق دهند. کوهن و فلسون[۴] تغییرات در میزان جرم در سطح کلان را درنتیجه بیشتر افراد به نیروی کار پیوند می‌دهد، که باعث افزایش مواجهه با مجرمان با انگیزه شده است. همچنین ادعا شده است که افزایش تولید و استفاده گسترده از کالاهای قابل‌حمل باعث افزایش میزان جرم در سال‌های اخیر شده است. علاوه براین، گرابوسکی[۵] ادعا می‌کند که جرائم اینترنتی مانند "شراب قدیمی در بطری‌های جدید است[۶]"، که نشان می‌دهد که فناوری رایانه صرفاً تسهیل یا فراهم کردن وسایلی است که می‌توانند جرائم سنتی را مرتکب شوند. این استدلال، این ایده را مطرح می‌کند که جرائم اینترنتی، جرائم جنایی جدید نیستند، بلکه مشابه با آن‌هایی است که همیشه قبل از توسعه فنّاوری وجود داشته است [۶].

۵. فسادهای مالی ناشی جرائم اینترنتی

از زمان ظهور اولین جرم فناوری اطلاعات تاکنون، تعدادی از اصطلاحات برای نامیدن این پدیده استفاده شده است. که بیشترین آن شامل جرائم کامپیوتری، جرائم اینترنتی، جرائم شبکه‌ای، جرائم اینترنتی و جرائم با فناوری بالا[۷] است. کلاهبرداری کامپیوتری یکی از سریع‌ترین شکل‌های جرم کامپیوتری است. جرایم اینترنتی در اصطلاح به جرایمی گفته می‌شود که در محیطی غیر فیزیکی علیه فناوری اطلاعات ارتکاب می‌یابند [۷]. با توجه به این‌که رایانه‌ها و سامانه‌های اطلاعاتی بخش مهمی از سازمان‌های امروز هستند، سوءاستفاده از سیستم اطلاعاتی بسیار افزایش یافته است. انواع مختلف جرائم اینترنتی می‌تواند توسط مدیران، کارکنان، مشتریان، گروه‌های ذینفع، هکرها و غیره انجام گیرد. کلاهبرداری در اینترنت توسط کاربران به‌عنوان یک نوع فساد در سازمان‌های امروز دیده می‌شود و می‌تواند دلایل مختلفی داشته باشد. فساد ریشه در شرایط فرهنگی، اقتصادی و سیاسی افراد درگیر آن دارد. زمانی در سطح سازمانی، مبارزه با فساد مؤثر خواهد بود که آن‌ها مملو از ارزش‌های اخلاقی باشد. سامانه‌های اطلاعات کامپیوتری ممکن است، برای توقف برخی از فعالیت‌های خود طراحی‌شده باشند. با این‌حال، این سامانه‌های اطلاعات جدید فروکش نمی‌شوند، بلکه

[1] . William Gibson
[2] . Neuromancer
[3] . Routine Activities Theory

[4] . Cohen and Felson
[5] . Grabosky
[۶] . معادل فارسی" حیوان چهارپایی است که تن پوش او را عوض کرده اند"
[7] . High-tech

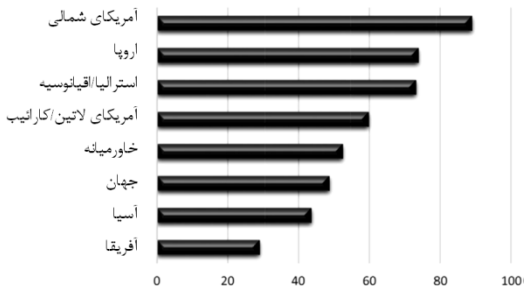
انگیزه اصلی برای درآمد اضافی در یک زمینه گسترده‌تر دلیل آن است. بنابراین، فساد مجبور است دوباره ظهور کند و این واقعیت است که IT (هنوز) نظارت بر تمام فعالیت‌های تمام کارکنان را ندارد. آن‌ها به‌اندازه کافی درآمد دارند تا زندگی کنند، اما می‌خواهند بیشتر درآمد کسب کنند؛ زیرا در موقعیتی قرار دارند که این کار را انجام دهند و به‌عنوان یک فعالیت طبیعی برای کسانی که در قدرت هستند دیده شود [۸]. واقعیت این است که ما هزینه واقعی جرائم اینترنتی را نمی‌دانیم. زیرا اطلاعات مربوطه را مخفی نگه می‌دارند. مطمئناً، ما هرگز نمی‌توانیم به‌حساب بانکی مجرمین دسترسی داشته باشیم. اما ما می‌دانیم که بیشتر درآمد جرائم سایبری، ماهیت مالی دارند و بانک‌های آمریکایی نشان نمی‌دهند که چقدر از آن‌ها مربوط به کلاهبرداری آنلاین است [۹].

۶. جغرافیای ترافیک اینترنت

دو دهه پیش، بری جیمز[1] (۱۹۹۶) اینترنت را "شهر مرزی غرب وحشی و بدون کلانتر" توصیف کرد و به مصرف‌کنندگان در مورد خدمات وب که عرضه سهام جعلی را ارائه می‌داد، هشدار داد و دیگر سهام‌های جعلی شامل معادن طلا، سنگ‌های قیمتی و حتی از دست دادن هویت از طریق آدرس ایمیل و کارت اعتباری. مسئله محتوای دیجیتالی و کالای تقلبی از طریق اینترنت، بیش از دو دهه با بخش‌های کلیدی شامل موسیقی، فیلم، نرم‌افزار و داروها مورد بررسی و مطالعه قرار گرفته است. اما، با ادامه رشد جهانی، دسترسی مصرف‌کننده به پهنای باند و استفاده از چندین دستگاه برای دسترسی به محتوای غیرقانونی دیجیتال رشد این نوع تجارت غیرقانونی را افزایش داد [۱۰]. برای نشان دادن پیشرفت سرقت اینترنتی، بیشترین سرقت مربوط به فیلم، در سال ۲۰۱۱، فست فایو[2] با حدود ۹/۲۶ میلیون دانلود از طریق سایت به‌صورت سیل‌آسا انجام شد. سارقان در دریای مجازی در سایت‌هایی چون بیت تورنت[3]، سایبر لوکرز[4] و مارکتزدارکنت[5] همچنان با استفاده از انواع سامانه‌های تخلف برای ارائه محتوای غیرقانونی دیجیتال و کالاهای تقلبی ادامه می‌دادند. در مبارزات با تخلفات اینترنتی، فروش داروهای تقلبی در اینترنت گزارش شده است، اما شرم‌آورترین تخلفات اینترنتی، در بازار آمازون دریک شبکه سیاه است که سایر کالاهای غیرقانونی مانند مواد مخدر و سلاح را به فروش می‌رساند. ارتباطات قابل توجهی بین نصب نرم‌افزار غیرقانونی و نرم‌افزارهای مخرب ایجاد شده است.

تحلیلگران ۴۳۰ میلیون بدافزار جدید در سال ۲۰۱۵ کشف کردند که ۳۶ درصد، نسبت به سال ۲۰۱۴ افزایش یافته است. اندازه جهان دیجیتال ازطریق محاسبه رشد نفوذ اینترنت، افزایش سرعت پهنای باند و تعداد دستگاه‌هایی که برای دسترسی به محتوای دیجیتالی استفاده می‌شود، اندازه‌گیری می‌شود. آمار جهانی اینترنت (۲۰۱۶) درصدی از کل جمعیت را با نرخ نفوذ اینترنت طبقه‌بندی نموده است.

شکل (۱) نرخ نفوذ واگرا را به‌صورت منطقه نشان می‌دهد. از ۲۷/۵ درصد در آفریقا به ۹/۸۶ درصد در آمریکای شمالی، و نرخ نفوذ اینترنت در سطح جهانی ۷/۴۸ درصد است که جمعیت جهانی آن به میزان ۷/۳۴ میلیارد دلار در سال ۲۰۱۶ است [۱۰].



شکل (۱): نمودار نرخ درصد نفوذ اینترنت در جهان بر اساس جغرافیای قاره‌ها

۷. موقعیت جغرافیایی IP کلاهبردارن در فضای مجازی

از ابزارهای مختلف ردیابی ایمیل ازجمله مسیر ردیابی:

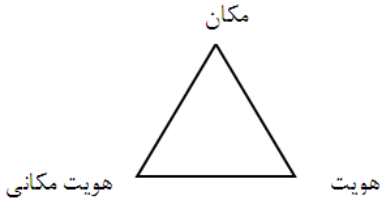
whatismyipadress.com, ip-adress.com and myaddr.com

استفاده و به شناسایی منشأ ایمیل‌های دریافت‌شده منجر شده است. تجزیه‌وتحلیل فارنزیک[6] از طریق آدرس‌های IP انجام تا منشأ ایمیل‌ها و موقعیت جغرافیایی مظنونین کلاهبرداری را شناسایی شود. همچنین تلاش زیادی برای ایجاد هرگونه ارتباط احتمالی بین دو یا چند مظنون مختلف (برای اطمینان از مشارکت شبکه‌های جنایی سازمان‌یافته) ایجاد شد. تجزیه‌وتحلیل نشان داد که ۵ نفر از ۱۰ مظنون از نیجریه، یکی در ایالات‌متحده، یکی در آفریقای جنوبی و دیگری مظنون در رومانی بودند. دو مظنون باقی‌مانده از سازوکار (استفاده از سرورهای پروکسی) برای مخفی کردن آدرس‌های IP خود برای جلوگیری از کشف استفاده کرده‌اند. تجزیه‌وتحلیل فارنزیک نشان داد که تمام ایمیل‌های سه نفر از مظنونین نیجریه، همان آدرس آی پی و همان ارائه‌دهنده خدمات اینترنت (ISP) واقع در شهر

[1] . Barry James
[2] . Fas`t Five
[3] . BitTorrents
[4] . Cyberlockers
[5] . Markets darknet
[6] . Forensic Analysis

ایبادان[1]، ایویو[2] در ایالت نیجریه است که توسط ردیابی ایمیل نشان داده شده است. دو مظنون دیگر نیجریه در شهر اوگان در ایبابوتا[3]، ایالت مرزی با ایویو قرار داشتند. به‌منظور اعتبارسنجی نتایج حاصل از تحلیل فارنزیک، تلاش شد تا آدرس ایمیل این کلاهبرداران مشکوک را دریافت کند [۱۱].

در جغرافیای جرم فضای مجازی سه رکن اصلی باید مورد تاکید قرار گیرد که شامل هویت مکان جرم قربانی، مکان وقوع جرم، هویت مکانی بزهکار می‌باشد. این سه رکن را در قالب مثلث قابل (شکل۲) فهم می‌باشد:



شکل (۲): ارکان جغرافیای جرم فضای مجازی (محققین)

۸. پیشینه تحقیق

در مورد برداشت‌های غیرمجازی از حساب بانکی در قالب فیشینگ تحققیات گسترده‌ای صورت گرفته است. "هالام بیکر[4]" دریافتند که حملات فیشینگ و فارمینگ به‌طور فزاینده‌ای پیچیده شده‌اند و جلوگیری از اقدامات مجرمان اینترنتی باعث شده است که صنعت فناوری اطلاعات، موج جدیدی از اقدامات امنیتی را اتخاذ کند [۱۲]. نتایج" یوپ پیک ونالا[5]" [۶] نشان داد که افراد بیشتری از طریق سرقت، قربانی شدند. علاوه بر این، سطح آموزش، فعالیت‌های روزمره آنلاین و ترس از هویت سرقت قربانی، با هویت سرقت قربانی رابطه مثبت دارد."الرود و ژاو[6]" با ارائه دیدگاه یکپارچه از فیشینگ، یک طبقه‌بندی را پیشنهاد کردند که شامل فن‌های حمله، مقابله با اقدامات، محیط‌های هدفمند و رسانه‌های ارتباطی [۱۳] ". اراچالج و لاو[7]" دریافتند؛ خودکارآمدی، باعث می‌شود رفتارهای جلوگیری از تهدید فیشینگ را افزایش می‌دهد [۱۴]. نتایج توان‌بخش، دوستار و قیاسی"نشان داد که بین استانداردسازی بسترهای بانکداری الکترونیک و پیشگیری از فعالیت فیشینگ ارتباط معنی‌دار وجود دارد و همچنین، عدم آگاهی کاربران در خصوص فعالیت فیشینگ باعث ساده‌تر شدن کار فیشرها شده است [۱۵].

آرورا[8] جرائم اینترنتی را به جرائم علیه افراد، اموال، سازمان‌ها و دولت‌ها طبقه‌بندی نموده است [۱]. "ماسکون و همکاران[9]" آن‌ها به این نتیجه مهم دست یافتند که سوءاستفاده از اینترنت مسئله جاری است که برخی از موارد ازجمله در یک دانشگاه می‌تواند اتفاق افتد [۱۶]. برخی محققین درمورد کلاهبرداری با مخفی نمودن هویت خود به برداشت‌های غیرمجازی بانکی تحقیقاتی نمودند؛ نتایج "گالاکی وفوئی هون ناه[10]" نشان داد "پوشش ماسک" در فضای مجازی می‌تواند اضطراب را در فریب دادن دیگران کاهش دهد [۱۷]. یافته‌های آلیم وآنتوی باوسیکو[11] نشان داد، اساس مشکل کلاهبرداری دریeBay در ناتوانی ساختار پیشگیری از کلاهبرداری eBay در شناسایی معامله گران کلاهبردار با هویت گمنام است [۱۱]. در مطالعات "ماری هو و همکاران[12]" دریافتند؛ مردان تمایل دارند که باورهای خود کارآمدتری در فریب جنسیتی داشته باشند، و زنان به میزان موفقیت بیشتر در تشخیص اشتباه جنسیتی تمایل دارند [۱۸]. "جیمیسون وهمکاران[13]" دریافتند؛ اقدامات پیشگیرانه برای جلوگیری از جرائم هویتی انجام شود. همچنین باید قوانین مربوط به جرائم هویت جدیدی ایجاد شود [۱۹]. "سیمپسون[14]" نشان داد سرقت هویت در جرائم اینترنتی شتاب زیادی گرفته است. آن‌ها دریافتند که جعل هویت یک فرد یک موضوع مهم است، اما جعل هویت شرکت‌های بزرگ چندملیتی به موضوع دیگری تبدیل شده است [۲۰]. "بیکر" به این نتیجه رسید که بسیاری از شرکت‌های اینترنتی در طول سال‌های ۱۹۹۸ و ۱۹۹۹م در معرض فعالیت‌های فریبکارانه توسط افراد باهوش فاقد هویت بودند که منجر به کلاهبرداری شد. شرایط وعوام شکل‌گیری کلاهبرداری مالی در فضای مجازی از جذابیت‌های پژوهش برای محققین بود [۲]. "چاودری"[15] اظهار می دارد، سرقت دسترسی به رایانه‌ها و محتوای دیجیتالی آن‌ها، به‌منظور بازخرید آن‌ها به مصرف‌کنندگان یا سازمان‌ها، یکی از تهدیدهای پیشرو درزمینه جرائم اینترنتی محسوب می شود [۱۰]. وحدتی و یاسینی نتیجه گرفتند که دو گروه اصلی از عوامل مؤثر در کلاهبرداری در اینترنت وجود دارد که شامل: ۱- عوامل فردی و بین سازمانی، ۲- عوامل محیطی و خارجی [۸]. "هدایتی" به روشن شدن شرایط و عوامل ایجاد ضرر و زیان به افراد در فضای مجازی و جرائم رایانه‌ای که منشأ تمام موضوعات فضای مجازی است را

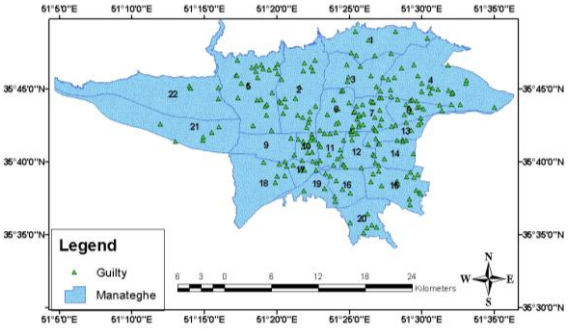
[1] . Ibadan,
[2] . Oyo
[3] . Ogun
[4] . Hallam-Baker
[5] . Yeop Paek & Nalla
[6] . Aleroud&Zhou
[7] . Arachchilage & Love
[8] . Arora
[9] . Maskun&et al
[10] . Galanxhi& Fui-Hoon Nah
[11] . Aleem & Antwi-Boasiako
[12] . Mary Ho& et al
[13] . Jamieson&et al
[14] . Simpson
[15] . Chaudhry

مورد بررسی قرارداد [۲۱]. "ریموندچاو[1]" دریافت که تمایل مجرمین مالی و جنایتکاران برای دست‌یابی به اطلاعات شخصی و محرمانه و به طبع آن تنوع جرائم فضای مجازی، افزایش‌یافته و حجم حملات نیز اجتناب‌ناپذیر شده است [۲۲]. یافته‌های "باوور و وان ایتن[2]" نشان داد که روابط بازار و غیر بازار در زیرساخت‌های اطلاعاتی،باعث افزایش انگیزش در ایجاد امنیت شده است [۲۳]." وکیلی"تاکید بر تدوین قوانین مدون جهت پیشگیری از وقوع جرائم اینترنتی دارد [۲۴]. "اوریولا[3]"در مورد کلاهبرداری نیجریه‌ای نشان داد که جامعه بین‌المللی باید به مقابله با چنین جرائمی کمک کند و باعث شفافیت سازوکار، آمادگی اجرای قانون، تشدید کمپین‌های روشنگری عمومی و رویکردهای فنّاورانه برای مقابله با پیش‌زمینه تهدید کلاهبرداری در اینترنت مورداستفاده قرار گیرد [۲۵]. "روضه‌ای، توان‌بخش و حسن‌زاده"به این نتایج دست یافته‌اند که شاخص‌های آموزش و آگاه‌سازی کاربران در خصوص کلاهبرداری اینترنتی، آموزش کاربران در خصوص خدمات بانکداری الکترونیکی توسط بانک‌ها و استفاده از نرم‌افزارهای امنیتی و ضد جاسوس‌افزارها توسط کاربران بیشترین تأثیر را در کاهش کلاهبرداری اینترنتی داشته‌اند [۱۵]. "وروایی و میرزکی" به این نتیجه دست یافتند که بخشی از شیوه‌های مقابله با جرایم کلاهبرداری، نیازمند ایجاد فرهنگ بهره‌گیری از رایانه و آگاه ساختن افراد و سازمان‌ها در مورد مخاطرات سامانه‌های رایانه‌ای است و نظارت دائمی سازمان‌ها، بر سامانه‌های رایانه‌ای و تدابیر امنیتی از قبیل حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و حفاظت اطلاعات در مقابله با کلاهبرداری رایانه‌ای از اهمیت ویژه‌ای برخوردار است [۲۶]. تحقیقات "مور[4]" منجر به توصیه‌های متعددی برای تغییرات سیاست برای بهبود امنیت سایبری مانند کاهش ویروس‌های مخرب از طریق سرویس‌دهندگان اینترنت با پاک‌سازی یارانه‌ای، افشای اجباری از تلفات کلاهبرداری و حوادث امنیتی، افشای اجباری در مورد حوادث سیستم کنترل و نفوذ و جمع‌آوری گزارش‌های جاسوسی فضای مجازی و ارائه آن‌ها به سازمان تجارت جهانی (WTO) شد [۹].

۹. یافته‌ها

۹-۱. تحلیل فضایی جرایم کلاهبـــرداری مـــالی در فضای مجازی در مناطق ۲۲گانه تهران

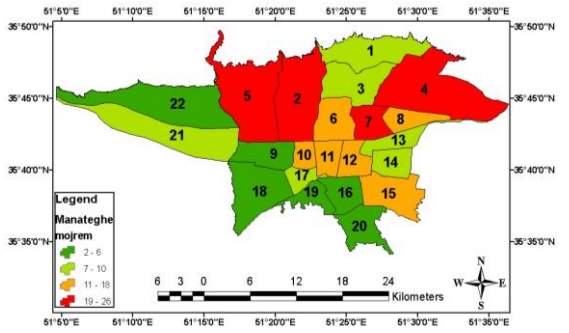
در شکل (۳)، استفاده از نرم‌افزار GIS توزیع نقاط جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران مشاهده شد. این نقشه نشان می‌دهد که بیشترین توزیع فضایی این نوع جرایم به ترتیب؛ در مناطق مرکزی، شرق و شمال شهر تهران مشاهده شده است. کمترین توزیع فضایی جرایم مذکور را در مناطق غرب وجنوب غرب مشاهده شده است.



شکل(۳): توزیع نقاط جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

۹-۲. توزیع مکانی–فضایی جرم کلاهبرداری مالی در فضای مجازی شهرتهران چگونه است؟

در شکل (۴)، پهنه‌بندی جرایم کلاهبرداری مالی در فضای مجازی، در مناطق ۲۲گانه شهرداری تهران مشاهده می‌شود. در این تصویر تعداد جرایم مذکور را با استفاده از رنگ طبقه شده است. در این تصویر بیشترین پهنه‌های جرایم کلاهبرداری در فضای مجازی در مناطق ۷، ۵، ۴ و ۲ مشاهده شده است و کمترین جرایم در مناطق ۹، ۱۶، ۱۹، ۱۸، ۲۰ و ۲۲ مشاهده شده است.

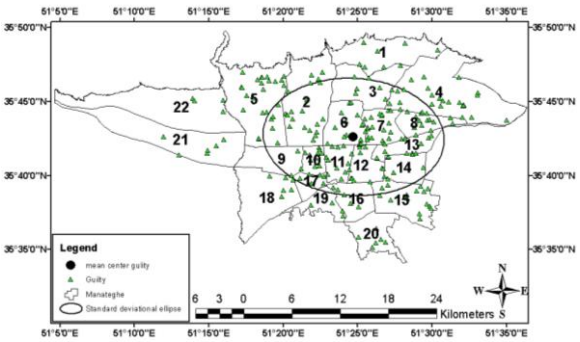


شکل (۴): پهنه‌بندی جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

در شکل (۵)، مرکز متوسط بیضی انحراف جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران مشاهده می‌شود. همان‌طور که در تصویر ملاحظه می‌شود مرکز متوسط بیضی انحراف جرایم کلاهبرداری مالی در فضای مجازی

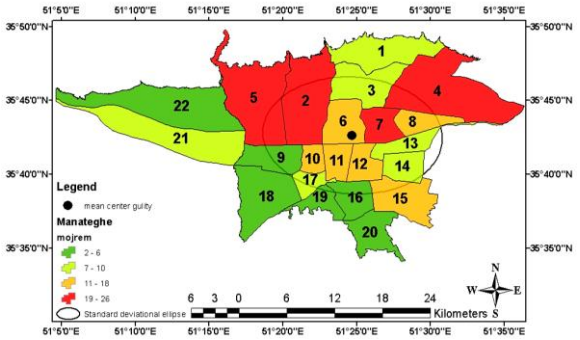
[1] . Raymond Choo
[2] . Bauer & van Eeten
[3] . Oriola
[4] . Moore

در منطقه ۶ شهرداری قرار گرفته است. بیضی انحراف معیار این نوع جرم در جهت شرقی- غربی در مرکز شهر تهران قرار دارد.



شکل (۵): مرکز متوسط و بیضی انحراف جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

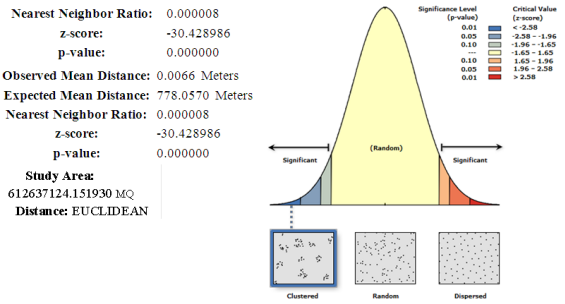
در شکل (۶)، به وضوح تطابق بین پهنه‌بندی بین جرایم کلاهبرداری مالی و مرکز متوسط و بیضی انحراف جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران مشاهده می‌شود. مرکز متوسط بیضی انحراف جرایم در این تصویر، بین مناطق ۷ و ۶ به‌صورت غربی- شرقی است که بیشترین تمرکزجرایم دیده می‌شود ونیز بین مناطق ۱۰،۱۱ و ۱۲ در قسمت جنوبی دیده می‌شود.



شکل (۶): تطابق مرکز متوسط و بیضی انحراف و پهنه‌بندی جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

۹-۳. شاخص میانگین نزدیکترین فواصل همسایگی (ANNI) جرایم کلاهبرداری مالی در فضای مجازی

در شکل (۷) شاخص میانگین نزدیکترین فواصل همسایگی (ANNI) جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران ملاحظه می گردد. در این بخش با استفاده از فاصله اقلیدسی[1] با استفاده از روش میانگین نزدیکترین فواصل همسایگی، مبین این واقعیت است که مقدار۳۰،۴۲۸۹۸۶- >Z و کوچکتر بودن این مقدار که دنباله توزیع Z در ناحیه سمت چپ قرار گرفته و آماره **p-value** صفر،نشان دهنده این است که الگوی جرایم کلاهبرداری مالی در فضای مجازی شهر تهران از الگوی خوشه‌ای با مقدار میانگین نزدیکترین همسایگی ۰/۰۰۰۰۰۸ برخوردار است. در واقع هر چه نمره Z عدد منفی بزرگ‌تری باشد، آزمون شاخص نزدیک‌ترین همسایگی را به‌کار گرفته است و می‌توان به درستی نتیجه آزمون شاخص نزدیک‌ترین همسایگی اطمینان کرد.



شکل (۷): شاخص میانگین نزدیکترین فواصل همسایگی (ANNI) جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

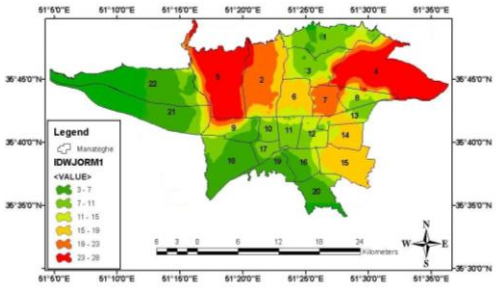
۹-۴. درون‌یابی[2] جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

روش درون‌یابی از جمله مدل‌های آماری است که برای پیش‌بینی مقادیر نامعلوم جرایم کلاهبرداری مالی در فضای مجازی به‌کار گرفته شده است. برای تخمین نقاط جرایم کلاهبرداری مالی در فضای مجازی مجهول، نمونه‌های اطراف باید مشارکت بیشتری نسبت به آنهایی که در فاصله دورتر قرار دارند، داشته باشند. در این مدل از فاصله به‌عنوان وزن متغیر معلوم در پیش‌بینی نقاط اندازه‌گیری نشده، استفاده نشده است. زیرا نقش متغیر جرم پیوسته در تاثیرگذاری با فاصله از مکان نقطه جرم مجهول، کاهش می‌یابد. بنابراین، هرچه فاصله داده معلوم ازنقطه مجهول افزایش یابد، وزن‌ها بر اساس فاصله کاهش خواهد یافت. مدل مورد استفاده موسوم به IDW می‌باشد. همان‌طور که در شکل (۸) ملاحظه می‌شود؛ جرایم کلاهبرداری مالی در فضای مجازی، به‌صورت پهنه‌های رستری همه مناطق ۲۲گانه شهر تهران را مورد پوشش قرار داده است. در این تصویر محدوده جرایم کلاهبرداری مالی در فضای مجازی ۲۳ تا ۲۸ بیشترین مساحت را در مناطق شهرداری ۲، ۴ و۶ به خود اختصاص داده است و در نهایت کمترین مساحت جرایم ۳ تا ۷ به‌صورت

[1] .Eucliden_Distance

[2] . Interpolation

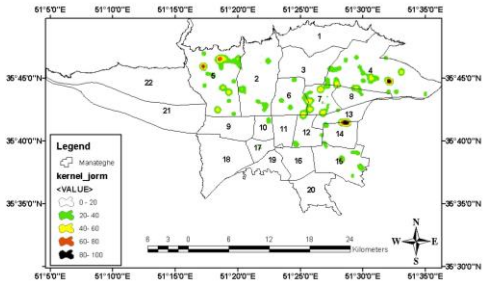
لکه‌های جرم خیز در مناطق ۱۸، ۱۹، ۲۰، ۲۱، ۲۲، ۱۶، ۱، ۳، ۷، و ۹ مشاهده شده است.



شکل (۸): درون‌یابی جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

۹-۵. توزیع فضایی جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهـران براسـاس تخمین تراکم کرنل

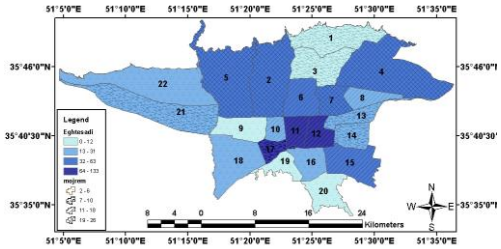
یکی از توابع‌های تحلیل فضایی به‌کار گرفته‌شده در این تحقیق تابع تراکم می‌باشد. در این تابع، تراکم جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران به تصویر کشیده شده است. در شکل (۹) یک پهنه و یک سطح هموار را با توجه به مساحت شهر و نوع متغیر یعنی جرایم کلاهبرداری مالی در فضای مجازی در سطح شهر تهران، به تصویر کشیده شده است. شکل (۹) توزیع فضایی جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران براساس تخمین تراکم کرنل به‌صورت نقشه دیده می‌شود. این نقشه نشان می‌دهد بین ۸۰ تا ۱۰۰ درصد تراکم جرم در واحد سطح (متر مربع) بالاترین تخمین را در مناطق ۱۳، ۱۴ و ۴ شهرداری شهر تهران بوده است. این نقشه صحت خوشه‌ای بودن جرایم سایبری را با توجه به تحلیل‌های خود همبستگی فضایی اثبات می‌کند. سپس منطقه ۵ و بعد مناطق ۶ و ۷ شهرداری شهر تهران به‌عنوان مناطق مستعد وحساس جرایم کلاهبرداری مالی در فضای مجازی محسوب می‌شوند. مابقی مناطق شهرداری شهر تهران از حساسیت کمتری نسبت به وقوع جرایم کلاهبرداری مالی در فضای مجازی برخوردار هستند.



شکل (۹): توزیع فضایی جرایم کلاهبرداری مالی در فضای مجازی در مناطق ۲۲گانه شهرداری تهران براساس تخمین تراکم کرنل

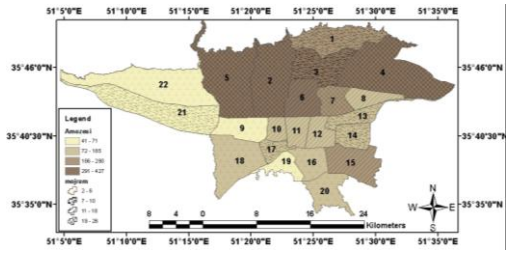
۱۰-۵. تحلیل نقشه های ترکیبی جرایم کلاهبرداری مالی در فضای مجازی

با استفاده از نقشه‌های ترکیبی جرم و عوامل مورد مطالعه چنین یافته‌ای به‌دست آمد؛ در شکل (۱۰) ارتباط بین جرم کلاهبرداری در فضای مجازی و فعالیت‌های اقتصادی، ملاحظه می‌شود که بیشترین تمرکز جرایم کلاهبرداری، ابتدا در مناطق ۲، ۴، ۵ و ۷ مشاهده شده است و این روند با جهت غربی- شرقی است. سپس در دو منطقه ۱۱ و ۱۲ مرکزی شهر و همچنین در منطقه ۱۵ در قسمت جنوب شرقی شهرداری تهران کشیده شده است. بیشترین پهنه‌های خدماتی و بازرگانی و به‌خصوص بازار، به وضوح با رخداد جرایم کلاهبرداری فضای مجازی منطبق است. در مناطق ۲، ۴، ۵ و ۷ بیشترین تمرکز فعالیت‌های تجاری در این منطقه وجود دارد. در مناطق ۱۱، ۱۲، ۱۵ و ۶ که بازار تهران به‌عنوان قلب فعالیت‌های تجاری و بازرگانی مشهور است، در این مناطق تمرکز دارند و این مناطق جزء دومین مناطق از نظر رخداد جرایم کلاهبرداری در فضای مجازی قلمداد شده است.



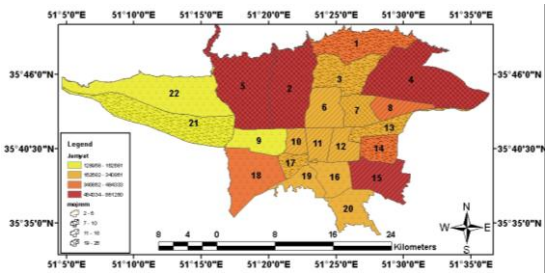
شکل (۱۰): نقشه متناظر پهنه‌های اقتصادی وجرم کلاهبرداری در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

در شکل (۱۱)، ارتباط بین پهنه‌های آموزشی و جرم کلاهبرداری در فضای مجازی شهرتهران مشاهده می‌شود. در تحلیل، نقشه پراکندگی پهنه‌های جرم کلاهبرداری با پهنه‌های آموزشی در مناطق ۲، ۴، ۵ و ۶ منطبق می‌باشد. در واقع این مناطق بیشترین تطبیق را پهنه‌های جرم دارند. پهنه‌های جرم با درجه کمترین، در مناطق ۹، ۱۹، ۲۱ و ۲۲ که از نظر فعالیت‌های آموزشی کمتری برخوردار هستند بیشتر دیده می‌شود.



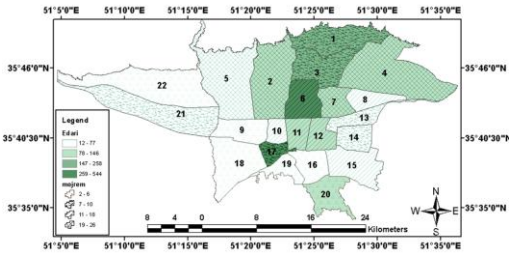
شکل (۱۱): نقشه متناظر پهنه‌های مراکزآموزشی وجرم کلاهبرداری در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

همان‌طور که در شکل (۱۲) مشاهده می‌شود؛ تمرکز جمعیت و جمعیت فعال به‌عنوان کانون‌های جاذب جهت جرم کلاهبرداری در فضای مجازی می‌باشد. بیشترین تمرکز مجرمان کلاهبرداری ابتدا در مناطق پرجمعیت (بیشترین) یعنی ۲، ۴ و ۵ است و سپس در مناطق ۱۵ در قسمت جنوب‌شرقی تهران و بعد در مناطق مرکزی شهر شامل مناطق ۶، ۷، ۸، ۱۰، ۱۱ و ۱۲ با جمعیت متوسط مشاهده شده است. اما در مناطق ۲۲، ۲۱ و ۹ که جزو کم جمعیت‌ترین مناطق شهر تهران محسوب می‌شود، تمرکز فعالیت‌های مجرمانه کلاهبرداری نیز کمتر مشاهده شده است. مناطق شهرداری ۱، ۱۴ و ۸ از نظر تعداد جمعیت در طبقه دوم (بیشتر) جمعیتی محسوب می‌شود. اما تعداد جرایم کلاهبرداری در این مناطق از تعداد کمتر و کمترین برخوردار هستند.



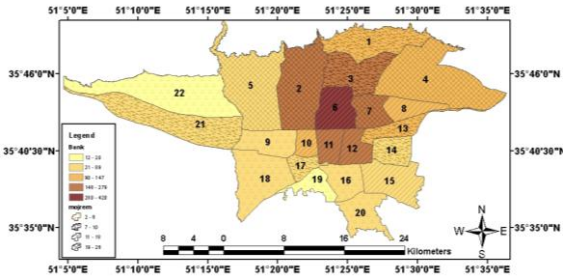
شکل (۱۲): نقشه متناظر پهنه‌های جمعیتی با کلاهبرداری در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

در شکل (۱۳) رابطه بین پهنه‌های اداری شهر تهران وجرم وضعیت، به‌گونه دیگری به چشم می‌خورد. اگر چه بیشترین پهنه‌های اداری، در مناطق ۱، ۳ و ۷ وجود دارد، اما پهنه‌های جرایم فقط با منطقه ۶ تطبیق دارد و مابقی مناطق دیگر شهرداری از چنین الگوهایی تبعیت نمی‌کند.



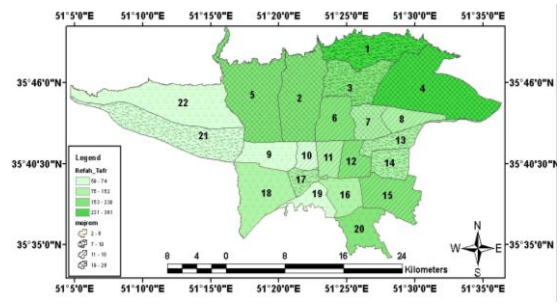
شکل (۱۳): نقشه متناظر پهنه‌های اداری وجرم کلاهبرداری در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

در شکل (۱۴)، ارتباط بین پهنه‌های موسسات مالی وبانک‌ها باجرم کلاهبرداری فضای مجازی را نشان می‌دهد. با توجه به این‌که، منطقه ۶ و سپس مناطق پیرامون (۲،۳،۷،۱۱،۱۲) بیشترین تعداد بانک‌ها مستقر می‌باشد، این مناطق به‌عنوان کانون‌های فعالیت‌های جرم کلاهبرداری محسوب شده‌اند. اما در سایر مناطق دیگر، به واسطه کم بودن شعب بانک‌ها، کمتر مورد توجه کلاهبرداران در فضای مجازی می‌باشد.



شکل (۱۴): نقشه متناظر پهنه‌های موسسات اعتباری بانک وجرم کلاهبرداری در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

در شکل (۱۵)، ارتباط بین جرم کلاهبرداری در فضای مجازی و مراکز رفاهی وتفریحی مشاهده می‌شود. منطقه ۴ و ۱ بیشترین مناطق رفاهی را به خود اختصاص داده است، ولی منطقه ۴ با مناطق جرم خیز متناظر می‌باشد. سپس مناطق ۵، ۲، ۶، ۱۲ و ۱۵ متناظر با پهنه‌های جرم خیز محسوب شده است.



شکل (۱۵): نقشه متناظر پهنه‌های رفاهی وجرم کلاهبرداری در فضای مجازی در مناطق ۲۲گانه شهرداری تهران

۱۰. نتیجه‌گیری

همان‌طورکه در پیشنیه بیان گردید؛ تاکنون هیچگونه پژوهشی درباره تفاوت‌های ناحیه‌ای درمورد جرم کلاهبرداری در فضای مجازی انجام نگرفته است. محققین تلاش کردند بر پایه داده‌های کمی، جرم کلاهبرداری مالی در فضای مجازی (استفاده از آمار فضایی)، به تحلیل داده‌های مکانی در شهرتهران بپردازند. نتایج این تحقیق نشان داد که هر فضایی از مناطق ۲۲گانه شهر تهران، دارای یک الگوی پراکندگی جرم است. علاوه برآن، نتایج نشان داد؛ این نوع جرم دارای تنوعی از رفتار فضایی درمیان متغییرها می‌باشد. هر چند ذات جرم کلاهبرداری مالی در فضای مجازی انجام می‌گیرد، اما این تحقیق نشان داد؛ این نوع جرایم نیز دارای فاصله، مکان و جهت در فضای جغرافیایی است. بر اساس نتایج این تحقیق می‌توان به پیش‌بینی، طراحی، سیاستگذاری و

سرانجام برنامه‌ریزی‌های مدون فضایی، به صورت علمی و دقیق اقدام کرد. نتایج نشان داد؛ یکی از عوامل بروز این نوع کلاهبرداری در فضای مجازی وجود مراکز اقتصادی است، چون گردش مالی واقتصادی زیادی دراین مناطق وجود دارد، مجرمین کلاهبردار این مناطق را به‌عنوان جولانگاه فعالیت‌های خود قلمداد می‌کنند.

عامل دیگر در رخداد این نوع جرم در نوع بافت جمعیتی جستجو کرد. مناطق ۱ و ۸ دارای بافت جمعیتی نوساز و در حال توسعه می‌باشد. ولی جمعیت مناطق ۱۴بیشتر از قشر نظامیان محسوب می‌شود، و آن هم به دلیل تعدد مراکز نظامی و به تبع آن تمرکز منازل مسکونی و متجمع‌های نظامی می‌باشد. بنابراین، به‌واسطه نظارت‌های امنیتی، و آموزش‌هایی که در این قشر جمعیتی وجود دارد، این نوع مناطق جمعیتی چندان مورد توجه کلاهبرداران برای انجام فعالیت‌های مجرمانه نیست. بین مراکز اداری، موسسات بانکی و مالی با پهنه‌های جرم کلاهبرداری ارتباطی دیده شد. علت این است که بخش عمده فعالیت‌های اداری در بستر بخش اقتصادی است و تمرکز زیاد بخش اقتصادی، باعث ایجاد کانون‌های هدف برای فعالیت‌های کلاهبرداری در فضای مجازی است.

باتوجه تحلیل‌های انجام‌شده برروی نقشه‌های ترکیبی، دو عامل مهم فضایی و مکانی را می‌توان در ایجاد مکان‌های جاذب برای کلاهبرداری درفضای مجازی، مد نظر قرار داد. تراکم جمعیت و تراکم مراکز اقتصادی، ازمهمترین عوامل مهم فضایی و مکانی محسوب شده‌اند. تراکم زیاد جمعیتی- اقتصادی و سطح بالای تحرک جمعیتی- اقتصادی و همچنین تمرکز فعالیت‌های تجاری، باعث شده است که برخی مناطق شهر تهران، تبدیل به مراکز پر جاذبه برای وقوع کلاهبرداری مجازی شود. با توجه به گسترش روزافزون فضای سایبری و گسترش تسهیلات اینترنتی از قبیل بانکداری الکترونیک و در نتیجه آن تعداد زیاد تراکنش‌های مالی، باعث گردیده، وسعت و تعداد کلاهبرداری در این مناطق به‌شدت افزایش یابد.

۱۱. پیشنهادها

تجزیه‌وتحلیل فارنزیک که از طریق آدرس‌های IP انجام می‌گیرد، باعث می‌شود تا منشأ ایمیل‌ها و موقعیت جغرافیایی مظنونین کلاهبرداری را شناسایی شود. در واقع به هرگونه IP مشکوک باید حساس شد و سرورهایی که از پروکسی استفاده می‌نمایند را باید پس از کشف، مکانیسم خدمات‌دهی آنها را حذف نمود.

با توجه به جمعیت بالا و فعالیت زیاد اقتصادی در مناطقی مانند ۲، ۴ و ۵ که تراکنش‌های مالی زیادی هم صورت می‌گیرد موجب می‌شود تا وظایف نهادهای نظارتی نیز افزایش یابد. همان‌طور که در مبانی نظری نیز ذکر شد وابستگی مردم به اینترنت رشد یافته است، بنابراین، امکان هک شدن و سایر نقص‌های امنیتی به‌طور مرتب افزایش می‌یابد. با ملاحظه نقشه‌ها و پراکندگی جرایم کلاهبرداری در فضای مجازی بایستی تمرکز نظارت‌های امنیتی در این مناطق بیشتر گردد.

۱۲. منابع

1. B. Arora, “Exploring and analyzing Internet crimes and their behaviours. Perspectives in Science,” no. 8, 2016 .
2. C. Baker, “CRIME, Fraud and Deceit on the Internet: Is There Hyperreality in Cyberspace,” Critical Perspectives on Accounting. no. 13, 2002 .

۳. عبادی‌نژاد، سید علی، امینی، داود، مبانی جغرافیای انتظامی، سازمان تحقیقات و مطالعات ناجا، ۱۳۹۴.

۴. هادیان‌فر، سید کمال، نشست خبری با اصحاب رسانه، کد خبر ایرنا (6483126)82900640، مورخه۱۳۹۷/۲/۹، ۱۳۹۷.

۵. علیجانی، بهلول، تحلیل فضایی، نشریه تحلیل فضایی مخاطرات محیطی، سال دوم، شماره۳ ، ۱۳۹۴ .

6. S. Y. Paek and M. K. Nalla, “The relationship between receiving phishing attempt and identity theft victimization in South Korea,” International Journal of Law, Crime and Justice, no. 43, pp. 626-642, 2015.

۷. رضوی، محمد، جرایم سایبری و نقش پلیس در پشگیری از این جرایم و کشف آن‌ها، فصلنامه دانش انتظامی، دوره ۹، شماره ۱، ۱۳۸۶.

8. S. Vahdati and N. Yasini, “Factors affecting internet frauds in private sector: A case study in Cyberspace Surveillance and Scam Monitoring Agency of Iran,” Computers in Human Behavior, no. 51, 2015.
9. T. Moore, “The economics of cybersecurity: Principles and policy options. International Journal of Critical Infrastructure Protection3,” vol 3, no. 3-4, 2010.
10. P. E. Chaudhry, “The looming shadow of illicit trade on the internet,” Business Horizons, no. 13, 2016.
11. A. Aleem and A. Antwi-Boasiako, “Internet auction fraud: The evolving nature of online auctions criminality and the mitigating framework to address the threat,” International Journal of Law, Crime and Justice, no. 39, 2011.
12. P. Hallam-Baker, “Prevention strategies for the next wave of cyber crime,” Network Security, no. 10, 2005.
13. A. Aleroud and L. Zhou, “Phishing environments, techniques, and countermeasures: a survey,” Computers & Security, pp. 1-46, 2017.
14. N. A. G. Arachchilage and S. Love, “Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior,” no. 38, 2014.

۱۵. روضه‌ای، منصور، توان‌بخش، جعفر، حسن‌زاده، حمید، ابزارهای پیشگیری از جرائم نوظهور در فضای مجازی، فصلنامه علمی پژوهشی مطالعات امنیت اجتماعی، شماره ۵۰، تابستان ۱۳۹۶.

16. M. A. Manuputty, S. M. Noor, and J. Sumardi, "Cyber Security: Rule of Use Internet Safely? 13th International Educational Technology Conference," no. 103, pp. 255 – 261, 2013.

17. H. Galanxhi and F. Fui-Hoon Nah, "Deception in cyberspace: A comparison of text-only vs. avatar-supported medium," Int. J. Human-Computer Studies, no. 65, pp. 770–783, 2007.

18. S. Mary Ho, P. B. Lowry, M. Warkentin, Y. Yang, and J. M. Hollister, "Gender deception in asynchronous online communication: A path analysis," Information Processing and Management, pp. 1–21, 2016.

19. R. Jamieson, L. Pek Wee Land, D. Winchester, G. Stephens, A. Steel, A. Maurushat, and D. Sarre, "Addressing identity crime in crime management informationsystems: Definitions, classification, and empirics," Computer law & security review, no. 28, 2012.

20. P. Simpson, "Spoofed Identities: Virus, Spam or Scam?," Computer Fraud & Securit, no. 10, 2003.

۲۱. هدایتی، حمید، بررسی تجارت الکترونیک و جرم کلاهبرداری اینترنتی، پایان‌نامه کارشناسی ارشد، استاد راهنما: غلامرضا عبدلی، دانشگاه آزاد واحد شاهرود، ۱۳۹۳.

22. K. K. Raymond Choo, "The cyber threat landscape: Challenges and future research directions," Computers & security, no. 30, pp. 719 -731, 2011.

23. J. M. Bauer and M. J. G. Van Eeten, "Cybersecurity: Stakeholder incentives, externalities, and policy options. Telecommunications Policy," no. 33, 2009.

۲۴. وکیلی، شیدا، کلاهبرداری اینترنتی، کنفرانس جهانی روانشناسی و علوم تربیتی، حقوق و علوم اجتماعی در آغاز هزاره سوم، ۱۳۹۵.

25. T. A. Oriola, "Advance fee fraud on the Internet: Nigeria's regulatory response," Computer Law & Security Report, no. 21, 2005.

۲۶. ورواییی، اکبر، میرزکی، سید شمس‌الدین، بررسی عوامل مؤثر بر کشف جرم کلاهبرداری رایانه‌ای پلیس آگاهی تهران سال ۱۳۸۶-۱۳۸۷، فصلنامه کارآگاه، سال چهارم شماره ۱۴، بهار ۱۳۹۰.

Journal of Shahr-e-Tabavar
Vol. 2, No. 1, 2020, Serial No. 2

Spatial Analysis of of Financial Fraud Among Citizens in the Cyberspace of Tehran

M. R. Pourgholami Servandani*, V. Barani Pesyan, S. A. Ebadinejad

*Amin Police University

(Received: 22/05/2019, Accepted: 12/10/2019)

ABSTRACT

The goal of the geographic management of cyber crime is to ensure continuation of the police organization's accomlishments and achievments, and to prevent sudden and startling events by choosing appropriate strategies against environmental change. To confront the consequences of the emergence of new information technologies, police organizations have to choose a collection of strategic geographic options in the midst of two conditions of continuation the current state of affairs and the creation of change and development. It should be noted that the components of criminology of physical fraud are very different from cybercrime, and the legislator also has partial reaction in the penalization of these types of crimes. One of the main problems in dealing with these types of crimes is the spatial characteristics of the crime requiring legal and police jurisdiction. The purpose of this paper is the spatial analysis of criminality of citizens in the cyberspace of Tehran. The research method of this article is analytical-descriptive. This paper is based on the statistical community of all the number of unauthorized withdrawals from bank accounts in cyberspace in the year 1989 in Tehran. In the analysis of the information of this research, statistical-graphical methods have been used in the form of GIS. In this study, the mean center test, standard deviation ellipse, clustering test and spatial correlation analysis of the global Moran statistic have been performed. Results indicate that the crime of financial fraud in cyberspace was observed with an East-West orientation in the regions with the highest concentration of economic activity. Two important spatial factors, namely population density and economic centers, are among the most important factors in shaping the focal points of this type of crime.

Keywords: *Place of crime, crime of financial fraud, citizens, cyberspace, Tehran*

*Corresponding Author Email: rezamrps@yahoo.com