مقاله پژوهشی

بررسی عوامل موثر بر جرم یابی کلاهبرداری در فضای سایبر[1]

مهدی نظری منظم[2]، عبدالله مجیدی[3]، عبدالله هندیانی[4]، حسین وفادار[5]

تاریخ دریافت:۹۸/۰۴/۱۵ تاریخ پذیرش:۹۸/۰۶/۰۵

چکیده

زمینه و هدف: جرم کلاه‌برداری سایبری یکی از مهم‌ترین جرایم علیه اموال و مالکیت می‌باشد که درفضای سایبری صورت می گیرد. این فضا با وجود مزایای فراوانش، به دلیل ویژگی‌هایی مانند امکان تحصیل هویت‌های گوناگون، گمنامی و سهولت انجام اعمال مختلف، موجب مهاجرت بسیاری از جرایم به آن شده است که کلاه‌برداری یکی از این جرایم است و مسؤلیت ناجا به عنوان متولی برقراری نظم و امنیت در فضای واقعی و مجازی را دشوار می سازد. هدف اصلی این مقاله، تبیین شیوه‌های موثر در کشف جرم کلاه‌برداری سایبری و نحوهٔ جرم‌یابی آن است.

روش شناسی: نوع تحقیق کاربردی بوده و روش تحقیق کمی و از نوع توصیفی- پیمایشی می‌باشد. جامعهٔ آماری این تحقیق را کلیه کارشناسان و متخصصان حوزه پی‌جویی جرائم رایانه‌ای پلیس فتای ناجا در سال ۱۳۹۷ به تعداد ۸۰ نفر تشکیل می‌دهند که به دلیل محدود بودن جامعه آماری کلیه افراد جامعه به شیوهٔ تمام شماری انتخاب و مورد ارزیابی قرار گرفتند. ابزار گردآوری داده‌ها، پرسش‌نامهٔ محقق‌ساخته است. پایایی پرسش‌نامه از طریق آزمون آلفای کرونباخ ۸۶/. محاسبه گردید.

یافته‌ها و نتایج: نتایج این پژوهش نشان می‌دهد که همکاری پلیس با مقامات قضایی، تجهیزات مدرن، علم و آگاهی از علوم رایانه‌ای توسط کارآگاهان سایبری و...در کشف جرم کلاه‌برداری سایبری تأثیر دارد. در بررسی عوامل موثر بر جرم‌یابی کلاهبرداری در فضای سایبر۱۷ عامل شناسایی شده‌اند که در بررسی دقیق‌تر مشخص می‌شود " استفاده مجرمین از فیلترشکن " با بار عاملی ۸۲۹/. در رتبه اول، " استفاده مجرمین از شبکه‌های تاریک " با بار عاملی ۸۱۶/. در رتبه دوم و " روش‌های نوین شناسایی IP توسط نیروهای پلیس " با بار عاملی ۸۱۱/. در رتبه سوم قرار دارند .

واژه‌های کلیدی: کلاه‌برداری، پلیس، جرم‌یابی، فضای سایبری، امنیت

---

۱. این مقاله مستخرج از رساله دکتری با عنوان «طراحی الگوی جرم یابی کلاهبرداری در فضای سایبری» می باشد.

۲. دانشجوی دکتری جرم یابی دانشگاه علوم انتظامی امین و عضو پیوسته انجمن علمی پژوهشهای انتظامی ایران.

۳. دانشیار مدیریت دانشگاه علوم انتظامی امین و عضو پیوسته انجمن علمی پژوهشهای انتظامی ایران، نویسنده مسئول، drmajidi@yahoo.com

۴. دانشیار گروه مدیریت راهبردی دانشگاه علوم انتظامی امین و عضو پیوسته انجمن علمی پژوهشهای انتظامی ایران

۵. دانشیار گروه کشف جرایم دانشگاه علوم انتظامی امین و عضو پیوسته انجمن علمی پژوهشهای انتظامی ایران

مقدمه

سال‌های واپسین هزاره دوم، برای بشر، سال های سرنوشت سازی بود. توسعه فناوری وهمچنین پیشرفتهای چشم گیر درتبادل اطلاعات وداده ها ازیک سو وگشوده شدن اینترنت(که بدوا یک شبکه خصوصی ومحرمانه تبادل اطلاعات محسوب می شدوآرپانت[1] نام داشت)به روی عموم ازسوی دیگر،به همراه توسعه کمی وکیفی رایانه های شخصی[2]، منجر به افزایش تصاعدی تعداد کاربران این شبکه جهانی گردید.(زندی، ۱۳۸۹: ۱۹) افزایش چشم گیر سوء استفاده های کامپیوتری وبالا بودن حجم خسارات و زیان های وارده و از سویی دیگرنیاز به پیچیدگی خاص درتدوین قوانین واجرای مجازات باتوجه به فراملی بودن ماهیت این جرایم و... موجب گردید تا افراد مختلف ازجمله جرم شناسان،حقوقدانان و متخصصان کامپیوتر به مطالعه و بررسی همه جانبه این پدیده روی آورند (صبح خیز،۱۳۹۴: ۵) ویژگی های خاص فضای جدید ازقبیل گمنامی وسهولت ارتکاب جرایم مختلف،باعث بروز جرایم نوینی شده که قابل مقایسه با هیچ یک از جرایم کلاسیک نبوده و چه بسا از نظر دامنه تاثیر، خطرناک تر هم باشند.کلاهبرداری سایبری یکی از مهم ترین این جرایم است باتوجه به روند رو به رشد وقوع کلاهبرداری سایبری به دلیل ماهیت و ویژگی های فضای مجازی و نقش ناجا در جرم یابی جرایم در فضای سایبر، این مقاله با هدف شناخت و تبیین شیوه های ارتکاب کلاهبرداری سایبری و و عوامل موثر بروقوع این نوع جرایم است. در واقع این پژوهش به دنبال پاسخ به این سؤال اساسی است که عوامل موثر بر جرم یابی کلاهبرداری در فضای مجازی کدامند؟ بر این اساس، هدف اصلی این پژوهش عبارت است از: شناخت و تبیین شیوه ها و علل ارتکاب جرم کلاهبرداری سایبری. اهداف فرعی نیز عبارتند از: شناسایی و ارایه عوامل و مولفه‌های اثرگذار در

1.Arpanent
2.Personal computer

جرائم کلاهبرداری رایانه ای؛ ارائه راهکار مناسب به منظور پیشگیری و مقابله با جرایم رایانه ای.

هرچند ازتصویب قانون جرایم رایانه ای مدت زیادی نمی گذرد، با این حال دربرخی ازمنابع ومتون مطالبی مرتبط با موضوع این تحقیق مورد بررسی قرار گرفت که بشرح ذیل ارائه می گردد.

پژوهشگران	موضوع تحقیق	توضیحات	یافته های تحقیق
زیبر، اولریش ترجمه: نوری،محمد علی وهمکاران	جرایم رایانه ای	کتاب	جرایم رایانه ای اثراولریش زیبر،حقوقدان برجسته آلمانی ازجمله کتاب های پایه این رشته حقوق کیفری است.موضوعات این کتاب عبارتند از :مقدمه وظهور خطر جدید، پدیده جرم رایانه ای ،محدوده تاثیرات و تحولات آینده جرایم رایانه ای،مسایل حقوقی مربوط به جرم رایانه ای،اقدامات امنیتی کاربران رایانه،تعقیب جرایم رایانه ای،ضرورت تحقیقات فعالیت وهمکاری بین المللی
جلالی فراهانی،امیر حسین	درآمدی برآیین دادرسی کیفری جرایم سایبری	کتاب	صلاحیت کیفری درفضای سایبر،استنادپذیری ادله الکترونیکی درامورکیفری،صلاحیت کیفری درفضای سایبر، صلاحیت سرزمینی،صلاحیت فراسرزمینی،مانع صلاحیت کیفری به همراه قوانین مرتبط با جرایم رانه ای ازمباحث مهم این کتاب می باشد.
پرویزی، رضا	پی جویی جرایم رایانه ای	کتاب	این کتاب یکی ازمهم ترین منابع موجود درخصوص پی جویی جرایم سایبری می باشدکه در پنج فصل شامل: آشنایی با سیستم های عامل و شبکه های رایانه ای ،تعریف وسابقه پیدایش جرایم رایانه ای ،نقش پلیس درمبارزه باجرام رایانه ای ،بررسی صحنه جرم الکترونیکی ونرم افزارهای مورداستفاده پلیس دربررسی جرایم سایبری می باشد.
حاجی ده آبادی،احمد وسلیمی،احسان	اصول جرم انگاری درفضای سایبر(بارویکرد انتقادی به قانون جرایم رایانه ای)	مقاله علمی پژوهشی	این مقاله جرم انگاری بی ضابطه وگسترده در قوانین کیفری را موجبات بروز آثارو تبعات سوء تورم کیفری دانسته و جرم انگاری در فضای سایبری را هنگامی صحیح وقابل پذیرش می داند که برمبنای اصولی چون ضرورت و مشروعیت انجام شود وتناسب دقیقی بین رفتارمجرمانه و نوع مجازات داشته باشد.

رجبی،ابراهیم	جرم شناختی فضای اینترنت	مقاله علمی پژوهشی	به نظرمولف آگاهی ازپی آمدهای استفاده ازاینترنت ودرنظرگرفتن راهبردهای مناسب برای استفاده درست وپیش گیری ازاثرات احتمالی منفی آن،اهمیت اساسی دارد.براساس یافته های این تحقیق: اینترنت علاوه بر دستاوردهای مثبت وانکارناپذیر دارای پیامدهای نامطلوبی ازجمله اعتیاداینترنتی،انحرافات جنسی،وسلطه فرهنگی به همراه دارد .که باید موردتوجه والدین و برنامه ریزان قرار گیرد.
افتخارجهرمی، گودرز، اسلامی، ابراهیم	نحوه اعمال صلاحیت دادگاه ها دررسیدگی به جرایم فضای مجازی	فصلنامه علمی پژوهشی	یکی ازمهمترین پرسش هایی که این مقاله درپی پاسخگویی به آن است این است که درهنگام ارتکاب یک جرم سایبری صلاحیت محکمه رسیدگی کننده را با استناد به کدام یک ازاصول حقوقی آیین دادرسی کیفری باید شناخت.وهمچنین درصورت بروزتعارض درمیان صلاحیت های متفاوت دادگاه ها اصول حاکم براساس کدام موازین قانونی می باشد.
رضوی،محمد	جرایم سایبری ونقش پلیس درپیشگیری ازاین جرایم وکشف آن ها	مقاله علمی پژوهشی	در این مقاله به چالش های نوین جرایم سایبری درحوزه پیشگیری وکشف جرم پرداخته شده و آموزش های تخصصی و جامع در خصوص رایانه واینترنت را جهت نیروهای پلیس پیشنهاد می نماید.
وروایی،اکبر میرزکی، سید شمس الدین	بررسی عوامل موثر برکشف جرم کلاهبرداری رایانه ای پلیس آگاهی تهران ۱۳۸۶-۱۳۸۷	مقاله علمی ترویجی	این مقاله مبارزه با جرایم سایبری خصوصا کلاهبرداری رایانه ای را نیازمند تدابیر وراهکارهای نوینی دانسته است وتوانمندی کارآگاهان وتجهیزات سازمانی وارتقاء دانش فنی ماموران پی جویی را بر عملکرد بهتر ماموران در کشف جرم کلاهبرداری رایانه ای موثر دانسته است .
شایگان،محمد رسول وسروستانی ثابت، محمد امین	راهکارهای مقابله با کلاهبرداری رایانه ای درحقوق کیفری ایران	مقاله علمی ترویجی	حفاظت فیزیکی ،حفاظت کارکنان، حفاظت ارتباطات وحفاظت اطلاعات ،نظارت مستمر ودائمی سازمان ها بر سیستم های رایانه ای ،ایجادفرهنگ بهره گیری از رایانه و آگاه ساختن افراد را از راهکارهای موثردرمقابله با جرایم رایانه ای دانسته است.

جلالی فراهانی،امیرحسین، منفرد، محبوبه	حمایت قانونی ازآسیب دیدگان سایبری	مقاله علمی پژوهشی	مولفین جبران زیان های ناشی ازبی نظمی های قانونی را یکی ازدستاوردهای برقراری نظم درجامعه دانسته ووظیفه قانونگذار را وضع قوانین،ایجاد سازوکارهاوپیش بینی قواعد لازم درجهت حمایت ازبزه دیده گان سایبری دانسته است ودراین راه شناسایی تهدیدها وآسیب های پیش رو واستفاده ازتدابیر پیشگیرانه را ازوظایف قانونگذار دانسته است.
شهبازی نیا، مرتضی، عبدالهی، محبوبه	دلیل الکترونیک درنظام ادله اثبات دعوا	مقاله علمی پژوهشی	دراین مقاله مولفین ابتدا به تعریف دلایل پرداخته وبه تفاوت ادله سنتی با ادله الکترونیک اشاره کرده ، سپس به بررسی ادله الکترونیک وارزش اثباتی آن می پردازد.ومعتقد است می توان با استفاده از روش های فنی ارزش ادله الکترونیک را درحد ادله سنتی جهت ارائه دردادگاه ارتقاء داد.

مبانی نظری

-**تعریف جرم**: جرم و جنایت یک پدیده ی پیچیده ی اجتماعی، اقتصادی، فرهنگی، محیطی و روانی است که حقوق اشخاص و جامعه را در معرض خطر جدی قرار داده است. مطابق ماده ۲ قانون مجازات اسلامی"هر رفتاری اعم از فعل یا ترک فعل که در قانون برای آن مجازات تعین شده است ؛جرم محسوب می شود ."و مقابله با جرم ، به دلیل آثار مخرب آنها در روابط اجتماعی و زندگی آحاد مردم ، به عنوان یکی از وظایف اساسی حکومت ها و دولت ها درآمده است(انصاری،۱۳۹۱: ۵)

- **جرایم رایانه ای:** سیر تحول تاریخی جرایم رایانه ای را از زمان پیدایش رایانه تا اوایل هزاره سوم به سه نسل می توان طبقه بندی کرد.(نجفی علمی،۱۳۹۳: ۶) ۱- نسل جرایم رایانه ای کلاسیک،۲-نسل جرایم علیه داده ها،۳-نسل جرایم سایبری : اولین نسل این گونه جرایم که تا اواخر دهه ۸۰ میلادی ادامه داشته و سیر پیدایش و تکمیل خود را طی نموده است تحت عنوان جرایم رایانه ای کلاسیک بروز کرد که بیشتر شامل جعل رایانه ای و کپی برداری از برنامه ها و کلاهبرداری بود. با گسترش

فناوری اطلاعات در دهه ۹۰ میلادی ؛جرایم نسل دوم تحت عنوان جرایم علیه داده‌ها که اغلب به صورت حذف، تخریب، مختل نمودن و جعل داده ها بود ؛ جلوه بیشتری پیدا نمود. در اواسط دهه ۱۹۹۰ میلادی نسل جدیدی از تکنولوژی کامپیوتر (که در واقع باید آن را ماحصل تکنولوژی ارتباطی و اطلاعاتی نامید) تجلی پیدا کرد. کامپیوترها در یک روند تکاملی بسیار سریع، به سیستم های کامپیوتری متشکل از چندین وسیله کامپیوتری که قابلیت ارتباط بین سیستم‌ها و شبکه‌های بین المللی را داشتند، تبدیل شدند.(صبح خیز،همان، ۱۶)

- **جرم یابی**[1]**:** هیئت جرم یابی آمریکا ، جرم یابی را رشته حرفه ای و علمی مدیریت تشخیص، تعیین، تمایز (تفرد) و ارزیابی ادله مادی با استفاده از علوم فیزیکی و طبیعی در موضوعات علوم حقوقی تعریف کرده است(موذن زادگان و حمیدزاده ،۱۳۹۲: ۱۰۰) درتعریفی دیگر جرم یابی را: علمی که درباره کاربرد علوم مادی در کشف جرایم و شناسایی مجرمان و اثبات جرم بحث کرده و به سه شاخه پلیس علمی (کشف علمی جرایم)، پزشکی قانونی و روان شناسی تقسیم می شود.

- **پلیس فتا ضابط دادگستری در فضای سایبر**: قوه قضائیه مسلما بدون وجود بازوی اجرایی نمی تواند اقتدار خود را به کرسی بنشاند . محاکم قضائی نیز اعم از دادسراها و دادگاه ها قبل از وقوع جرم تا پس از اجرای مجازات وظایفی بر عهده دارند که باید با توسل به بازوی اجرایی خود که پلیس می باشد آن ها را انجام دهند که این بازوی اجرایی تحت عنوان ضابطین قضایی یا ضابطین دادگستری شناخته می شوندمقنن در قانون آیین دادرسی کیفری جدید مواد ۲۸تا ۶۳ را حسب مورد جایگزین مواد ۱۵ تا ۲۵ قانون سابق آیین دادرسی کیفری و مواد ۳، ۱۲، ۱۵و ۳۹ قانون تشکیل دادگاه های عمومی و انقلاب نموده است (سلیمی و بخشی زاده اهری ، ۱۳۹۳: ۳۹) پلیس به عنوان

1. Criminalistics

بازوی اجرایی قوه قضائیه به سبب ارتباط و تعاملی که با شهروندان دارد همواره در اجرای وظیفه ذاتی خود می بایست ضمن آگاهی از قوانین موضوعه در تحصیل دلایل علیه متهم در جمع آوری دلایل له او نیز تلاش و دقت لازم را داشته باشند . لازم به ذکر است در این تحقیق پلیس فتا به عنوان ضابط قوه قضائیه و پلیس تخصصی در مقابله با جرایم ارتکابی درفضای سایبر می باشد.

- **فضای سایبر(فضای مجازی):** سایبر در لغت به معنای مجاز است. اما امروزه فضای سایبر عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. به نظر می رسد بکارگیری این اصطلاح در این زمینه وبرای ارجاع به امور فنی به آن رنگ و بویی صرفا فنی و مکانیکی داده باشد. ملاحظه دقیق‌تر این اصطلاح نشان می‌دهد که این واقعیت، وجوه و جنبه های متنوعی از جمله خصلت های روانشناختی قابل توجه نیز دارد .واژه سایبردرزبان فارسی به معنای مجازی ترجمه شده است اما واقعیت این است که این فضا مجازی نیست چون تاثیر آن برفضای واقعی قابل رویت می باشد. واژه سایبر از لغت یونانی کیبرنتس به معنی سکاندار یا راهنما مشتق شده است. نخستین بار اصطلاح "سایبرنتیک" توسط ریاضیدانی به نام نوربرت وینر در کتابی با عنوان "سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین" در سال ۱۹۴۸ بکار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم ها در سیستم‌های انسانی، ماشینی و کامپیوتر ها است .در سال۱۹۸۴ نیز یک نویسنده علمی- تخیلی به نام ویلیام گیبسون واژه سایبررا به اسپیس چسباند تاشبکه های کامپیوتری دنیای آن لاین را نشان دهد وازآن زمان فضای سایبر مترادف با دنیای کامپیوترها وشبکه اینترنت قرار گرفت.

-**کلاهبرداری سایبری**: ازسوی کمیته تخصصی شورای اروپادرزمینه جرایم کامپیوتری درخصوص کلاهبرداری کامپیوتری تعریفی بدین شرح ارائه شده است: واردکردن،تغییر،محویاموقوف سازی داده های کامپیوتری یابرنامه های کامپیوتری

یادیگرمداخلات درپردازش داده هاکه برنتیجه پردازش داده ها اثربگذارد و موجب ضررهای اقتصادی یاهرتصرفی دراموال شخصی دیگر به قصدتحصیل منفعت اقتصادی غیرقانونی برای خودیادیگری شود.(راه حل جایگزین:باقصدمحروم کردن غیرقانونی آن شخص ازاموالش) .(نجفی علمی،۱۳۹۳: ۲۸)

- **مجرمین سایبری:** تاریخ نشان داده است که جرایم کامپیوتری توسط طیف وسیعی از افراد انجام می‌گیرند. دانشجویان، افراد تازه‌کار، تروریست‌ها و اعضای شبکه‌های سازمان یافته،کارمندان ناراضی نمونه‌هایی از این دست هستند.(شایگان و ثابت سروستانی، ۱۳۸۸: ۲۵) آنچه که آنها را از یکدیگر متمایز می‌کند، ماهیت جرم ارتکابی است. شخصی که بدون اهداف مجرمانه در یک شبکه فعال است با کارمندان یک سازمان مالی که طرح‌های کلاهبردارانه را اجرا می‌کند بسیار متفاوت است. مجرمان کامپیوتری به طبقات مختلف تقسیم می‌شوند. این طبقه بندی ممکن است براساس اهداف این افراد صورت گیرد آنچه در زیر می‌آید، یک طبقه بندی از مجرمان مجازی است.

-**کودکان و بزرگسالان ٦ تا ١٨ ساله**: دلیل ساده ارتکاب جرم از سوی این گروه، تمایل به کنجکاوی و کشف چیزهاست. دلیل منطقی دیگر می‌تواند اثبات خود در میان گروه همسالان بوده و دلایل دیگر نیز می‌تواند ریشه‌های روانشناسی داشته باشد.

-**هکرهای سازمان یافته:** این نوع از هکرها معمولاً برای برخی از اهداف، با یکدیگر همکاری می‌کنند. دلیل آن ممکن است تأمین تعصبات سیاسی، ساختارگرایی و ... باشد. گفته می‌شود که پاکستانی‌ها از بهترین هکرهای دنیا هستند. آنها معمولاً سایت‌های دولت هند را با اهداف سیاسی هک می‌کنند. .(مقیمی،۱۳۹۴: ۱۳۲)

-**هکرهای حرفه‌ای**: این هکرها با هدف کسب پول اقدام به رفتارهای مجرمانه می‌کنند و معمولاً برای کسب اطلاعات موثق، قابل اعتماد و ارزشمند، استخدام

می‌شوند. همچنین آنها برای هک کردن عمدی سیستم‌ها به کار گرفته می‌شوند. تا نفوذهای ایمنی توسط آنها یافت شوند.(مقیمی،۱۳۹۴: ۱۳۲)

-**کارمندان ناراضی**: این گروه شامل کارکنانی هستند که توسط کارفرما اخراج شده یا از کار خود ناراضی هستند. در اقداماتی تلافی جویانه، آنها یک سیستم کارفرما را هک می کنند. .(شایگان و ثابت سروستانی، ۱۳۸۸: ۲۵)

سطح مهارت‌های مجرمان کامپیوتری، موضوعی بحث برانگیز بوده است. برخی ادعا می کنند که سطح مهارت نشان دهنده شاخصی از جرم کامپیوتری نیست. در حالی که دیگران معتقدند، مجرمان بالقوه کامپیوتر، با هوش، مشتاق و با انگیزه هستند که به راحتی چالش‌های تکنولوژی را می‌پذیرند. ویژگی‌هایی که برای بسیاری از افراد یک آرزو به حساب می‌آید. .(مقیمی،۱۳۹۴: ۱۳۲)

ابعاد جرم کلاهبرداری سایبری : ارتکاب کلاهبرداری سایبری تاثیر زیادی بر زیر ساخت های حیاتی و اداری کشور بر جا خواهد گذارد و با زیرسئوال بردن توانمندی های نظام قضایی و پلیس فتا عملا منجر به کم اعتبارشدن دستگاه عدالت کیفری خواهد شد این

جرم و پیچیدگی های خاص کشف آن به طرز ویران کننده ایی زندگی بسیاری از مالباختگان را مورد هجوم قرار داده و دربرخی مواقع به قتل مالباختگان منجر شده است. (نتزگر و موراسی،۲۰۰۸: ۱۲۷)

جدول ۱: ابعاد جرم کلاهبرداری سایبری

	زمینه ساز	تسریع ساز	تکمیل کننده
عوامل اجتماعی و اقتصادی	۱-ناکارآمد جلوه دادن نظام بانکی کشور ۲-گسترش احساس نارضایتی مردم از نظام اقتصادی حاکم بر بانک ها ۳-گسترش و نا امیدی مردم ازسرمایه گذاری دربانک های داخلی ۴-گسترش فقرو بیکاری ۵-افزایش جرایم درحوزه مالی ۶-برآورده نشدن مطالبات مردم از نظام قضایی و پلیس فتا ۷-عدم دسترسی به فرصت های جدید توسط مردم و نسل جوان تحصیل کرده ۸-احساس نا امنی در مردم	۱-فعالیت گسترده شبکه های کلاهبرداری در سطح بین المللی ۲-فعالیت گسترده کشورهای حامی مجرمین و کلاهبرداران سایبری ۳-فعالیت گسترده باندهای زیر زمینی و کلاهبرداران سایبری ۴-گسترش و پیشرفت شگردهای مجرمین و کلاهبرداران سایبری ۵-فعالیت گسترده شبکه های رایانه ای مخالف نظام از طریق ارسال ویروس و .... ۶-فقر و ضعف مالی ناشی از تحریم ۷-افزایش قشرجوان و تحصیل کرده بیکار	۱-فعالیت گسترده شبکه های اجتماعی غیرمجاز ۲-عدم توجه به ارتقاء سیستم های ایمنی توسط مسولین و مدیران بانک ها ۳-ضعف قوانین حاکم بر کلاهبرداری سایبری درسطح ملی ۴-ضعف پلیس فتا به لحاظ عده و عده در تقابل با افزایش حجم عظیم و ناگهانی کاربران رایانه ای ۵-سهل انگاری یا سوء نیت برخی از کارکنان بانک ها یا کارمندان شرکت ها در حفظ ۶-پایین بودن سواد رایانه ای مردم
عوامل فرهنگی	۱-گسترش فساد ۲-کم رنگ شدن ارزش های دینی و مذهبی ۳-تضعیف ارزش های ملی ۴-تغییر ذائقه رفتاری مردم خصوصا نسل جوان	۱-رواج ابتذال در کشور ۲-گسترش فرهنگ مصرف گرایی توسط کشورهای غربی ۳-گسترش فرهنگ سکولار و اسلام آمریکایی درکشور ۴-تغییر در ذائقه رفتاری مردم از طریق رسانه	۱-کم توجهی به امور فرهنگی در جامعه ۲-بی توجهی خانواده ها به تربیت دینی فرزندان ۳-دور شدن جوانان از ارزش های فرهنگی و ملی اسلامی ایرانی
عوامل سیاسی	۱-بدبین شدن مردم به نظام اقتصادی داخلی ۲-تخریب چهره سیاسی و اقتصادی کشور	۱-تلاش کلاهبرداران سایبری بین المللی در حمله به زیر ساخت های مالی کشور ۲-تلاش گروه های معارض و تبهکار	۱-ضعف سیستم های نظارتی ، دینی و همکاری برخی از کارمندان با مجرمین ۲-ضعف سیستم های امنیتی بانکی ۳-پرداخت امکانات نا مناسب و بی

	۳-تضعیف نظام بانکی و عدم اعتماد مردم به سرمایه گذاری در بانک های داخلی	بین المللی در ضربه زدن به اقتصاد کشور ۳-تبلیغات حرفه ای بانک های خارجی در خصوص ایمنی نظام بانکی خود و تبلیغ درخصوص تشویق سرمایه داران به سپرده گذاری در بانک های خارجی	توجهی به حقوق سپرده گذاران توسط بانک های داخلی

مستندات قانونی جرم کلاهبرداری: پلیس فتا در مقابله با کلاهبرداری سایبری با الهام گرفتن از روح حاکم بر قوانین و مستندات قانونی موجود در قانون جرایم رایانه ای عمل می نماید که این مستندات به شرح جدول ذیل ارائه می گردد.

جدول ۲: مستندات قانونی جرم یابی کلاهبرداری در فضای سایبری درقانون جرایم رایانه ای

فصول	مواد قانونی	مباحث
	ماده ۱۳ قانون جرایم رایانه ای	تعریف کلاهبرداری رایانه ای
جمع آوری ادله الکترونیک	ماده ۳۲و۳۳ (نگهداری داده ها)	نگهداری داد ه های ترافیک را حداقل تا شش ماه پس از ایجاد اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک
	ماده ۳۴ (حفظ فوری داده ها)	حفظ داد ه های رایانه ای ذخیره شده برای تحقیق یا دادرسی خطر آسیب دیدن یا تغییر یا از بین رفتن داد ه ها
	ماده۳۵ (ارائه داده ها)	در اختیار قرار دادن داده های حفاظت شده به ضابطان برابر دستور قضایی
	مواد ۳۹ تا ۴۷ (تفتیش و توقیف دادها)	تفتیش و توقیف داد ها و سامانه های رایانه ای و مخابراتی و رعایت تناسب، نوع، اهمیت و نقش آن ها در ارتکاب جرم، به روش هایی از قبیل چاپ داد ها، کپی برداری یا تصویربرداری
	ماده ۴۸ (شنود محتوا)	شنود محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه ای یا مخابراتی و دسترسی به محتوای ارتباطات غیرعمومی ذخیر هشده، نظیر پست الکترونیکی یا پیامک

استناد پذیری	ماده ۴۹(حفظ صحت داده ها)	حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی جمع آوری شده مطابق آئین نامه
سایر	ماده ۵۲ (رسیدگی به جرایم رایانه ای)	سامانه رایانه ای یا مخابراتی به عنوان وسیله ارتکاب جرم باشد و در قانون جرایم رایانه ای مجازات پیش بینی نشده باشد مطابق قوانین جزائی عمل خواهد شد
		در مواردی که برای رسیدگی به جرایم رایان های مقررات خاصی از جهت آئین دادرسی پیش بینی نشده است طبق مقررات قانون آئین دادرسی کیفری اقدام خواهد شد.

روش های ارتکاب کلاهبرداری سایبری در سطح ملی و بین الملل

۱-روش های ارتکاب کلاهبرداری سایبری در سطح بین الملل :

حال پس از مشخص شدن ماهیت این جرم نوبت به بررسی و شناسایی انواع کلاهبرداری رایانه ای و شیوه های مختلف ارتکاب این جرم می رسد که در ادامه به عمده‌ترین آنها اشاره شده است.

۱-۱-کلاهبرداری از طریق بازاریابی شبکه ای در اینترنت : بازاریابی شبکه‌ای در سال ۱۹۲۱ توسط یک کلاهبردار آمریکایی به نام پونزی ابداع گردید و در محافل آکادمیک اقتصادی آن زمان به طرح پونزی یا توطئه هرمی مشهور گشت .و در حوزه رشته بازاریابی با عنوان بازاریابی چند لایه از آن نام برده شده است. طرفداران بازاریابی چند لایه معتقد بودند که این شیوه آرزوی دیرینه ارتباط بدون واسطه تولیدکننده با مصرف‌کننده را تا حدودی برآورد کرده است. اما چندی نگذشت که تعدادی سودجو با استفاده از این روش اقدام به کلاهبرداری‌های کلان کردند و این شیوه مطرود گردید. اما با پیدایش شبکه‌های بین‌المللی مثل اینترنت مجرمان یقه سفید و کلاهبرداران حرفه‌ای در سطحی گسترده‌تر اقدامات خود را از سر گرفتند و شیوه مذکور به کلاهبرداری شبکه‌ای معروف گردید.

۱-۲-کلاهبرداری از طریق اعلام برنده شدن در قرعه‌کشی یا لاتاری: این شیوه نیز معمولا از طریق ارسال نامه الکترونیکی انجام می‌شود که در آن کلاهبردار با دادن خبرهای کذب مبنی بر برنده شدن در قرعه‌کشی اینترنتی و ارسال مدارک جعلی وسوسه قربانی را برانگیخته و جهت ارسال جایزه تقاضای مبلغی پول به عنوان حق بیمه و یا هزینه ارسال جایزه می‌نماید و بدین‌صورت اقدام به کلاهبرداری می‌نماید. در بررسی و تحلیل پست الکترونیک دو بحث عمده و بزرگ وجود دارد که بحث اول تحقیقات جنایی و بحث دوم ادله اثبات کیفری است.

۱-۳-کلاهبرداری در معاملات آنلاین[1]**:**کلاهبرداری آنلاین یک مشکل جهانی است. میلیون ها نفر از افراد در سراسر جهان قربانی این جرم شده و میلیون ها دلار خسارت مالی به بار آورده است. برابر گزارش سازمان (ACCC) استرالیا سال ۲۰۱۵ این نوع از کلاهبرداری خسارتی حدود ۸۲ میلیون دلار در این کشور به جا گذاشته است که این قسمت بسیار ناچیزی از خسارت واقعی از این طریق می باشد . (کراس، ۲۰۱۶: ۳) حدود ۳۵ میلیون نفر در آمریکا معاملات آنلاین را تجربه کردهاند و اکثر آنان از این نوع معامله راضی هستند اما از هر ۱۰ مورد معامله ۴ مورد آن با مشکلاتی همراه بوده است. معمولاً در این نوع معاملات خریداران ثمن معامله را از طریق چک و بوسیله پست برای فروشنده ارسال می کنند و فروشنده پس از دریافت پول مبیع را برای خریدار ارسال می نماید. یکی از مهم ترین مشکلات پیش آمده برای خریداران، عدم ارسال کالا و یا ارسال کالایی متفاوت از کالاهای معرفی شده در اینترنت یا دریافت کالای معیوب می باشد. برگشت خوردن چک خریداران نیز از مشکلاتی است که فروشندگان با آن مواجه هستند.

1. Online Auction Fraud

۱-٤-کلاهبرداری از طریق ارسال نامه های الکترونیکی(معروف به کلاهبرداری ٤١٩): این شیوه ابتدا توسط کلاهبرداران نیجریه‌ای مورد استفاده قرار گرفت و به نامه‌های الکترونیکی نیجریه‌ای معروف است. این جرم حداقل از سال ۱۹۸۹ در دولت های نیجریه درجریان بوده است که بخاطر بند مربوط به قانون کیفری نیجریه به کلاهبرداری ۴۱۹ معروف شده است. (نتزگر و موراسی،۱۳۹۴: ۱۲۴)در این روش کلاهبردار با ارسال یک نامه الکترونیکی به پست الکترونیکی قربانی خود را فردی ثروتمند از خانواده هیئت حاکمه کشور نیجریه معرفی می‌نماید که بدلیل برخی محدودیت‌ها قادر به خارج نمودن دارایی‌اش از کشور نیجریه به نام خود و خانواده‌اش نمی‌باشد. او از دریافت‌کننده نامه تقاضا می‌کند مشخصات هویتی و شماه حساب ارزی خود را برای نقل و انتقال پول در اختیارش بگذارد و در عوض ۲۵٪ از کل مبلغ جابجا شده را بعنوان پاداش دریافت کند. (نتزگر و موراسی،۱۳۹۴: ۱۲۵) بدین‌ترتیب کلاهبردار پس از دریافت پول متواری می‌شود و به سراغ قربانیان بعدی می‌رود .

۱-۵-کلاهبرداری از طریق فیشینگ [1] : امروزه از مهم ترین چالش های موجود در اینترنت، خطر حملات فیشینگ و کلاهبرداری های اینترنتی است. این حملات تنها در آمریکا، سالیانه چندین میلیارد دلار خسارت به بار می آورد. از این رو، پژوهشگران تلاش های زیادی در جهت شناسایی و مقابله با این گونه حملات داشته اند(کمالی زاده و شاه محمدی،۱۳۹۵: ۹)فیشینگ درحال حاضریکی ازمهمترین جرایم درفضای سایبری است.(هادیانفر، ۱۳۹۴) عبارت فیشینگ برای توصیف نوعی ازجرم که باتلاش فریبکارانه برای بدست آوردن اطلاعات حساس شناخته می شود استفاده می شود ازقبیل رمزهای عبور باتظاهرکردن به عنوان فرد طرف مقابل یابنگاه اقتصادی قابل اعتماد(برای مثال موسسه مالی)دریک جامعه الکترونیکی رسمی. مهاجمان ممکن است

1- Phishing

با ارسال یک ایمیل با ظاهری قابل قبول و از یک شرکت معتبر کارت اعتباری و یا موسسات مالی، از شما درخواست اطلاعات مالی را نموده و اغلب عنوان نمایند که یک مشکل خاص ایجاد شده است و ما در صدد رفع آن می‌باشیم. پس از پاسخ کاربران به اطلاعات درخواستی، مهاجمان از اطلاعات اخذ شده به منظور دستیابی به سایر اطلاعات مالی و بانکی استفاده می‌نمایند.لازم به توضیح است که انواع مختلفی از کلاهبرداری درفضای سایبر وجود دارد که در این قسمت به مهمترین روش های ارتکاب آن اشاره شده است.

۲- روش های ارتکاب کلاهبرداری سایبری در سطح ملی:

در سطح کشورمان کلاهبرداری های سایبری در شهرهای مختلف و به روش های گوناگون ارتکاب می یابد که در ذیل به چند روش از کلاهبرداری های موجود در پلیس فتا اشاره می گردد.

جدول۳: انواع روش های رایج کلاهبرداری های سایبری در کشور

نوع جرم کلاهبرداری سایبری	نحوه ارتکاب جرم	محل ارتکاب
کلاهبرداری های کاریابی اینترنتی	راه اندازی سایت ها و موسسات مجازی غیرقانونی کاریابی + جلب اعتماد طعمه های خود+اخذ شماره حساب و مشخصات و ربودن وجه	خراسان جنوبی
فروش بلیط اینترنتی شگرد کلاهبرداری از مسافران نوروزی	برپایی سایت های جعلی مهمترین شگرد مجرمانه کلاهبرداران است + سرقت اطلاعات کارت های بانکی+ برداشت از حساب مسافران	تهران
دام فیشرها برای سرقت اطلاعات بانکی کاربران به مناسبت روز پدر	کاربران با توجه به محدودیت های زمانی و مکانی اقدام به خرید آنلاین و ارسال کادو به آدرس پدر خود می نمایند. که در این بین کلاهبرداران سایبری با تشکیل فروشگاه های تقلبی پول را گرفته و اقدام به کلاهبرداری می نمایند.	تهران
ایمیل های کلاهبردارانه تبریک روز معلم در کمین معلمان	ارسال یک بدافزار در قالب فایل پیوست تبریک روز معلم+این فایل پیوست می تواند حاوی کیلاگر و یا بدافزار دسکتاپ فیشینگ باشد که در این صورت به محض نفوذ به سیستم قربانی، مجرم می تواند به اطلاعات بسیار مهمی از قربانی دست پیدا کند. اطلاعاتی مثل رمز های بانکی، رمز های ورود به حساب های کاربری	تهران

بیماریهای خاص ترفند جدید کلاهبرداران سایبری	مجرمان سایبری در ترفندی جدید با ارسال ایمیل و اینکه آنها بیماران کلیوی، قلبی هستند ویا کودکان آنها دارای بیماری خاص (دیالیز، تالاسمی و هموفیلی) هستند از کار افتاده هستند و توانایی کار ندارند و از نظر اقتصادی دچار مشکل هستند + و با کمک چند خیر اقدام به تاسیس فروشگاه اینترنتی کرده اند و خرید از آنها باعث می گردد تا مشکلات اقتصادی آنها کاهش یافته و هزینه های درمانی خود یا نزدیکانشان را در آورند +پس از خرید یا اجناس تقلبی می فرستند و یا اصلا اقلامی نمی فرستند و از کاربران کلاهبرداری می کنند. حتی برخی از درگاههای بانکی متصل به این فروشگاهها فیشینگ می باشد و کاربران را فریب داده و اطلاعات حساب کاربران را به سرقت می برند.	تهران
کلاهبرداری از طریق خرید هدیه روز معلم	کلاهبرداران فضای سایبر با در پیش بودن روز معلم و ایجاد شور و شوق دانش آموزان و دانشجویان جهت هر چه باشکوه تر برگزار کردن این مراسم،و نظر به اینکه بازار خرید های اینترنتی و کادوهایی که به این منظور در سایت های فروشگاهی ارائه می شود بسیار داغ تر از قبل خواهد شد ، برخی از کلاهبرداران فضای سایبر با طراحی سایت های جعلی که از نظر ظاهری دارای شباهت بسیار زیادی با سایت اصلی می باشد اقدام به سرقت اطلاعات مهم بانکی کاربران می کنند .	تهران
حذف شدگان یارانه برای ثبت نام در دام کلاهبرداران سایبری می افتند.	سایتwww.yaraneh10.ir توسط وزارت تعاون،کار و رفاه اجتماعی برای ثبت نام حذف شدگان معرفی شده که کلاهبرداران سایبری شبیه آنرا تعبیه نمودند و اقدام به سرقت اطلاعات بانکی ثبت نام کنندگان نمودند.	تهران
دایر کردن سایت‌های همسریابی	گروه‌های منحرف و غیراخلاقی به بهانه آسان‌سازی ازدواج و همسریابی، اقدام به فریب افراد و سرقت اطلاعات شخصی و خصوصی آنان +هنگام دریافت حق عضویت کاربران را به صفحات فیشینگ راهنمایی کرده و اطلاعات بانکی آنها را سرقت می کنندهمسریابی زنان را شناسائی و پس از کلاهبرداری میلیونی از طعمه هایش ناپدید شد، گفت: هر چند این مجرم دستگیر و تحویل مراجع قانونی گردید، اما آسیبی روحی و استرسی که این زنان و خانواده آنها در این ماجرا دید به این زودی‌های پاک نخواهد شد.	مازندران و....
کلاهبرداری با تبلیغ فروش خودروی ارزان	کلاهبرداری به شیوه تبلیغ فروش ماشین به قیمت ارزان، در یکی از سایت های معتبر تبلیغی با عنوان فروش پژو پارس به مبلغ ۲۹ میلیون تومان مشاهده کردم و چون ارزان قیمت بود اقدام به تماس با فروشنده کردم پس از واریز مبلغی از	خراسان جنوبی

	پول وقتی بار دیگر برای هماهنگی با فروشنده تماس گرفتم پاسخ نداد و من هم به سایت مربوط مراجعه و مشاهده کردم آگهی فروش ماشین حذف شده است.	
کلاهبرداری از طریق شبکه اجتماعی بی تالک	جوان ۳۰ ساله شیرازی با ارائه مرجوعه قضائی مدعی شد از طریق شبکه اجتماعی بی تالک با دختری آشنا می شود که خانواده اش در ایران نبوده وپیش دایی اش زندگی می کندو... پس از مدتی دوستی اینترنتی قرار می شود مراسم خواستگاری با حضور خانواده ها در شیراز جنبه رسمی به خود بگیرد. وی افزود: روز مراسم خواستگاری دختر مورد نظر با ارسال پیامی ادعا می کند خودرو عمویش در جاده خراب شده و برای تسویه حساب تعمیرگاه به مبلغ شش میلیون ریال نیازمند است جوان نیز مبلغ خواسته شده را واریز می نماید اما پس از آن تنها پل ارتباطی آنها که شبکه اجتماعی بی تالک بوده است، توسط خانم جوان مسدود می گردد.(ضمنا متهم پس از دستگیری انگیزه خود را سرگرمی اعلام نموده و جالب آنکه مردی ۲۹ ساله بوده و به این روش کلاهبرداری می کرده است.)	فارس

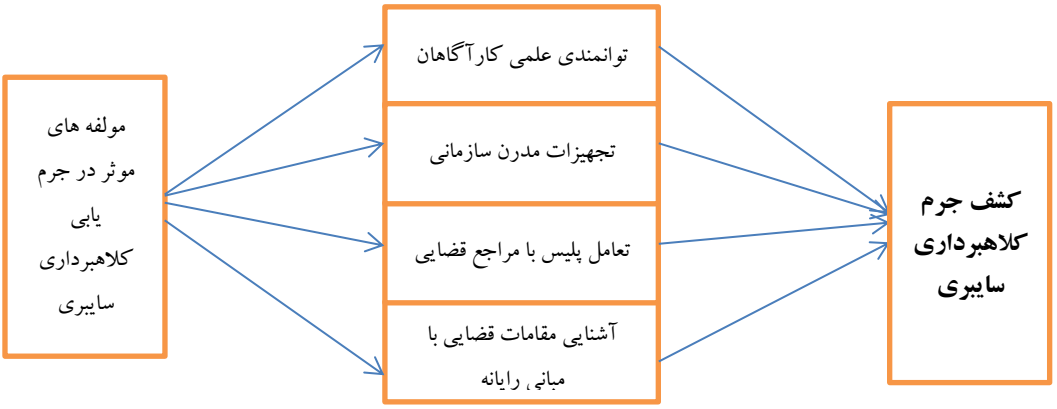
فرضیه های تحقیق :

۱-میزان توانمندی علمی کارآگاهان در جرم یابی کلاهبرداری سایبری تاثیر دارد.

۲- میزان تجهیزات سازمانی کارآگاهان در جرم یابی کلاهبرداری سایبری تاثیر دارد.

۳- میزان تعامل پلیس با مقام های قضایی در جرم یابی کلاهبرداری سایبری سایبری تاثیر دارد. ۴- میزان آشنایی مقامات قضایی با مبانی فنی وحقوقی جرایم کلاهبرداری سایبری جرم یابی کلاهبرداری سایبری تاثیردارد.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی



نمودار ۱ مدل مفهومی تحقیق

روش شناسی تحقیق

تحقیق حاضر از آنجا که به تبیین شیوه های کلاهبرداری سایبری می پردازد، از نوع توصیفی – پیمایشی است و از آنجا که به جرم یابی کلاهبرداری سایبری می پردازد، از نوع کاربردی است. جامعهٔ آماری تحقیق شامل کلیهٔ کارشناسان خبره در مورد جرایم سایبری در شهر تهران است که تعداد آنان ۷۰ نفر هستند و به صورت تمام شمار عمل شده است. گرد آوری اطلاعات به دو صورت کتابخانه ای و میدانی انجام شده است. ابزار سنجش پژوهش حاضر پرسش نامهٔ محقق ساخته است که برای سنجش نظرهای افراد مطابق با طیف لیکرت مورد بحث و بررسی قرار گرفت. زمان اجرای تحقیق در سال ۱۳۹۵ در شهر تهران است. درتنظیم پرسش نامه نظرات کارشناسان و متخصصان مورد نظر لحاظ و در نتیجه پرسش نامهٔ نهایی تهیه و توزیع شد و برای آزمون پایایی پرسش نامه از روش محاسبه آلفای کرونباخ استفاده شده است که نتیجه به دست آمده نشان داد پایایی کل پرسشنامه ۸۶/. می باشد.

یافته های تحقیق

بعد از تجزیه وتحلیل داده ها نتایج این تجزیه و تحلیل مورد تعبیر و تفسیر قرار گرفته است. اطلاعات لازم برای پژوهش حاضر از پرسشنامه ای که اطلاعات آن مورد آزمون قرار گرفته بود، جمع آوری شد. این اطلاعات در محیط نرم افزاری SPSS با اعمال آزمون های آماری مناسب با توجه به فرضیات پژوهش، تجزیه وتحلیل گردید ونتایج در دو بخش اطلاعات توصیفی و آزمون فرضیات ارائه شد.

الف-عوامل موثر در بعد کلان

در بررسی عوامل موثر در بعد خرد ۴ عامل توانمندی کارآگاهان، تجهیزات سازمانی، تعامل پلیس با مقامات قضایی و آشنایی مقامات قضایی با مبانی فنی و حقوقی جرایم رایانه ای شناسایی شده اند که هر یک از عوامل بصورت مجزا مورد بررسی قرار گرفته اند و نتایج آن به شرح زیر ارائه می گردد:

جدول٤: بررسی تاثیر میزان توانمندی کارآگاهان

متغیر	میانگین Mean	(sd)	سطح معنی‌داری (sig)	t	Mean difference
توانمندی کاراگاهان	۴,۵۲	۰/۵۲	۰/۰۰۱	۲۴,۸۷	۱,۵۲

با توجه به میانگین (۴,۵۲) و آماره آزمون، از آنجایی که T محاسبه شده (۲۴,۸۷) از T جدول (۱,۶۵) بزرگ‌تر است، بنابراین می‌توان با اطمینان ۹۵ درصد بیان کرد میزان توانمندی علمی کارآگاهان در جرم یابی سایبری تاثیر دارد.

جدول٥: بررسی تاثیر میزان تجهیزات

متغیر	میانگین Mean	(sd)	سطح معنی‌داری (sig)	t	Mean difference
تجهیزات سازمانی	۴,۶۰	۰/۵۱	۰/۰۰۱	۲۶,۶۵	۱,۶۰

با توجه به میانگین (۴,۶۰) و آماره آزمون، از آنجایی که T محاسبه شده (۲۶,۶۵) از T جدول (۱,۶۵) بزرگ‌تر است. بنابراین می‌توان با اطمینان ۹۵ درصد بیان کرد میزان تجهیزات سازمانی کارآگاهان در جرم یابی سایبری تاثیر دارد.

جدول٦: بررسی تاثیر میزان تعامل پلیس با مقامات قضایی

متغیر	میانگین Mean	(sd)	سطح معنی‌داری (sig)	t	Mean difference
تعامل پلیس با مقامات قضایی	۴,۲۹	۰/۵۱	۰/۰۰۱	۲۱,۷۹	۱,۲۹

با توجه به میانگین (۴,۲۹) و آماره آزمون، از آنجایی که T محاسبه شده (۲۱,۷۹) از T جدول (۱,۶۵) بزرگ‌تر است، بنابراین می‌توان با اطمینان ۹۵ درصد بیان کرد ،میزان تعامل پلیس با مقام های قضایی در جرم یابی سایبری تاثیر دارد.

جدول۷: بررسی تاثیر میزان آشنایی مقامات قضایی با مبانی فنی و حقوقی

متغیر	میانگین Mean	(sd)	سطح معنی‌داری (sig)	t	Mean difference
آشنایی مقامات قضایی با مبانی فنی و حقوقی	۴,۴۵	۰/۵۰	۰/۰۰۱	۲۵,۱۱	۱,۴۵

با توجه به میانگین (۴,۴۵) و آماره آزمون، از آنجایی که T محاسبه شده (۲۵,۱۱) از T جدول (۱,۶۵) بزرگ‌تر است، فرض محقق تایید می‌گردد. بنابراین می‌توان با اطمینان ۹۵ درصد بیان کرد ،میزان آشنایی مقامات قضایی با مبانی فنی وحقوقی کلاهبرداری سایبری در جرم یابی کلاهبرداری سایبری تاثیردارد.

ب- عوامل موثر در بعد خرد

در بررسی عوامل کلان از آزمون kmo و بارتلت استفاده شده است، در این بخش تاثیر هریک از عامل های خرد مشخص و به شرح جدول زیر ارائه شده است:

جدول۸: بررسی تاثیر میزان عوامل خرد

مقدار آزمون KMO	مقدار آزمون بارتلت	سطح معناداری	درجه آزادی	مقدار واریمکس
/۸۴۱	۱۲۴۱/۸۳	/۰۰۰	۱۶	/۶۹

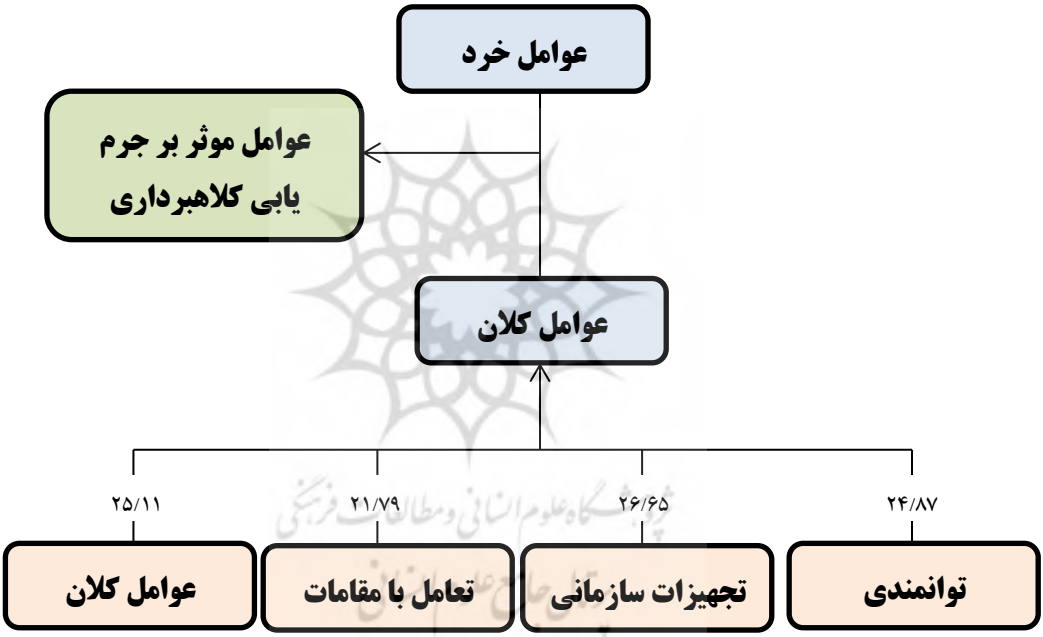
با توجه به مقدار آزمون kmo که ۸۴۱/. و بارتلت که ۱۲۴۱/۸۳ و سطح معناداری ۰۰۰/. می توان با اطمینان ۹۵ درصد بیان کرد رتبه بندی روش های موثر معتبر بوده و روش های مورد نظر ۶۹/. درصد از واریانس کل را تبیین می کند که برای رتبه بندی این روش ها باید به جدول بعد و مقدار ضریب بارعاملی مراجعه کرد :

جدول۸: بررسی بارعاملی عوامل خرد

روش مورد استفاده	مقدار بار عاملی	رتبه
استفاده از فیلتر شکن	/۸۲۹	۱
استفاده از شبکه های تاریک	/۸۱۶	۲
روش های نوین شناسایی IP	/۸۱۱	۳
توانایی فنی و آزمایشگاهی نیروهای پلیس	/۸۰۹	۴
ضعف و خلاء های قانونی	/۸۰۲	۵
استفاده از تکنیک اختفا هویت	/۷۹۵	۶
استفاده از ظرفیت های بازارهای آنلاین و درج آگهی رایگان	/۷۷۴	۷
استفده از شناسایی شماره تماس	/۷۶۵	۸
دسترسی به ایمیل	/۷۵۹	۹
دسترسی به شمار ه حساب	/۷۵۲	۱۰
احراز هویت و شناسایی افراد در فضای سایبر	/۷۴۰	۱۱
امکانات و زیر ساخت های سازمانی	/۷۲۳	۱۲
دانش فنی مقامات قضایی	/۷۱۲	۱۳
هماهنگی بین دستگاه‌های ذی ربط	/۷۰۹	۱۴
میزان اشراف اطلاعاتی پلیس در فضای سایبر	/۷۰۶	۱۵
میزان دسترسی پلیس به بانک های اطلاعاتی	/۷۰۲	۱۶
رصد فضای مجازی توسط پلیس فتا	/۷	۱۷

در بررسی عوامل موثر بر جرم یابی کلاهبرداری در فضای سایبر ۱۷ عامل شناسایی شده اند که در بررسی دقیق تر مشخص می‌شود " استفاده مجرمین از فیلتر شکن " با بار عاملی ۸۲۹/. در رتبه اول، " استفاده مجرمین از شبکه های تاریک " با بار عاملی ۸۱۶/. در رتبه دوم و " روش های نوین شناسایی IP توسط نیروهای پلیس " با بار عاملی ۸۱۱/. در رتبه سوم قرار دارند .

مدل عوامل موثر بر جرم یابی کلاهبرداری سایبری



نمودار۲: شناسایی میزان عوامل تاثیرگذار

- میزان توانمندی علمی کارآگاهان در جرم یابی سایبری تاثیر دارد.
- میزان تجهیزات سازمانی کارآگاهان در جرم یابی سایبری تاثیر دارد.
- تعامل پلیس با مقام های قضایی در جرم یابی سایبری تاثیر دارد.

- آشنایی مقامات قضایی با مبانی فنی وحقوقی کلاهبرداری سایبری در جرم یابی کلاهبرداری سایبری تاثیردارد.
- در بررسی عوامل موثر بر جرم یابی کلاهبرداری در فضای سایبر ۱۷ عامل شناسایی شده اند که در بررسی دقیق تر مشخص می‌شود " استفاده مجرمین از فیلتر شکن " با بار عاملی ۸۲۹/. در رتبه اول، " استفاده مجرمین از شبکه های تاریک " با بار عاملی ۸۱۶/. در رتبه دوم و " روش های نوین شناسایی IP توسط نیروهای پلیس " با بار عاملی ۸۱۱/. در رتبه سوم قرار دارند .

نتیجه گیری

توانمندی کارآگاهان: میزان توانمندی کارآگاهان در جرم یابی کلاهبرداری سایبری تاثیر دارد تمایل روز افزون به استفاده از فناوریهای پیشرفته از جمله رایانه و اینترنت ، شرایط و بستر مساعدی برای ظهور اینگونه جرائم بوجود آورده است. از آنجا که این جرائم در فضای مجازی انجام می شوند و مانند سایر جرائم ملموس نیستند ، مراجع قضایی و انتظامی برای پیشگیری از وقوع این جرائم و کشف آنها با موانع و چالش های نوینی روبرو هستند.کشور ما به هیچکدام از کنوانسیون های بین المللی جرائم سایبری ملحق نشده است و این در حالیست که امروزه پلیس با استفاده از فن آوریهای نوینی که در عرصه نرم افزارهای تخصصی در اختیار دارد ، می تواند در پیشگیری از وقوع جرائم نقش موثری داشته باشند و از آنجا ئیکه مدتی است قانون جرائم سایبری به تصویب رسیده ، گام موثری در جهت پیشگیری از جرائم مرتبط برداشته شده است. با توجه به اینکه ارتکاب جرم در فضای مجازی عمدتا ادله الکترونیک می باشند ، ضرورت آموزش های تخصصی در حوزه رایانه و اینترنت به ماموران پلیس بیشتر آشکار شده و حائز اهمیت است. نتایج این بخش هم راستا با نتایج تحقیق وروایی و همکاران(۱۳۹۰) و پرویزی(۱۳۸۸) می باشد.

تجهیزات سازمانی: میزان تجهیزات سازمانی در جرم یابی کلاهبرداری سایبری تاثیر دارد. سوء استفاده از فن آوریهای سایبری و اینترنتی می تواند امنیت ملی ، آسایش عمومی و موجودیت یک جامعه را مخاطره انداخته و تاثیرهای منفی بیشماری را بر زندگی افراد تحمیل کند همچنین اغلب مرتکبین جرائم اینترنتی را جمعیت جوان تشکیل می دهند. امروزه شاهد آن هستیم که تعداد قابل توجهی از جرائم سنتی، همزمان با پیشرفت فن آوری اطلاعات و ارتباطات ، بشدت متحول شده و در سطح وسیعی صورت می گیرد.

با توسعه رسانه های الکترونیکی نیز، در کنار جرائم سنتی یاد شده فرصت های جدیدی برای بزهکاری فراهم شده است. اموری از قبیل حمله ویروس ها ، سرقت و سو استفاده از داده ها ، ورود غیر مجاز به سایت ها در زمره رفتارهای بزهکارانه تلقی می شوند که قابلیت ارتکاب در محیط خارج از رایانه را ندارند. از اینرو پیشرفت فن آوری رایانه ، شرایط و بستر مناسبی برای سرقت اطلاعات ، تکثیر نرم افزار های غیر مجاز ، تجاوز به حقوق مالکیت معنوی و تهاجم فرهنگی و کلاهبرداری سایبری را به دنبال خواهد داشت. با عنایت به اینکه افسران تحقیق با رسانه های اطلاعاتی ادله دیجیتال ، کد گذاری مدارک و... آشنایی کافی ندارند کشف جرم کلاهبرداری سایبری را با مشکلاتی روبرو کرده است. کنترل کامل یک برنامه و کشف و شناسایی داده های نامرئی و مخفی در رایانه ها به عنوان ادله دیجیتالی که برای اثبات جرم لازم است مستلزم آشنایی با روشها و شیوه های خاص پلیسی و وجود ابزار و تجهیزات تخصصی و نحوه استفاده از این تجهیزات می باشد. نتایج این بخش هم سو با نتایج بدست آمده توسط علیزاده(۱۳۹۶)، توانبخش (۱۳۹۶) و ایراتز و همکاران(۲۰۰۹) می باشد: افزایش بهره‌گیری از نظامهای نوین بانکی و بانکداری الکترونیک در کشور، کلاهبرداری در این سیستمها موضوعی است که عدم مقابله با آن می تواند هزینه های بسیاری برای

نظام بانکی و مشتریان بانکداری الکترونیک در پی داشته باشد. تقلب در سیستم بانکداری الکترونیکی نتیجه بی توجهی به برخی مشکلات امنیتی (از ضعف در سیستم‌های دسترسی تا کنترل‌های داخلی نامناسب) است. طبعا شناسایی عوامل موفقیت مقابله با تقلب می تواند برای توسعه دهندگان سیستم های بانکی در توسعه ضریب امنیتی این سیستمها بسیار مفید باشد.

آشنایی مقامات قضایی با مبانی فنی و حقوقی: میزان آشنایی مقامات قضایی با مبانی فنی و حقوقی در جرم یابی کلاهبرداری سایبری تاثیر دارد.یکی از چالش های مهم موجود در این حوزه نداشتن تخصص کافی مراجعی است که به تعقیب ، کشف ، و رسیدگی ماهوی به این جرائم می پردازیم این مسئله باعث می شود که تعقیب و کشف اینگونه جرائم با مشکل مواجه شده و دادگاهها نیز نتوانند بنحو شایسته به جرائم مزبور رسیدگی کنند. در خصوص تعقیب متهمان اینترنتی و بازجویی از آنها رویه یکسانی در کشورها به چشم نمی خورد فقدان همکاریهای متقابل نیز ملموس است با وجود اینکه جرائم اینترنتی در حال حاضر بخش عظیمی از جرائم ارتکابی را تشکیل می دهد در این خصوص تعریف قانونی واحدی به چشم نمی خورد. با توجه به ویژگی های خاص جرائم کلاهبرداری سایبری که ماهیت فرا ملی و فرا مرزی نیز دارند وجود یک بستر حقوقی و قوانین لازم در زمینه پی جویی ، تعقیب ، تحقیق و رسیدگی و همکاری و تعاون با جوامع بین المللی احساس می شود این نتایج همسو با نتایج تحقیقات حاجی ده آبادی و همکاران(۱۳۹۳)، افتخار جهرمی(۱۳۹۳)، پن، لی(۲۰۰۹) و اوقان(۲۰۰۹) می-باشد .

تعامل پلیس با مقامات قضایی: میزان تعامل پلیس با مقامات قضایی در جرم یابی کلاهبرداری سایبری تاثیر دارد. میل و اشتیاق به استفاده از رایانه و اینترنت و بهره مندی از مزایای آن اگر چه زمینه مشارکت جوامع مختلف در فن آوریهای پیشرفته را فراهم

مینماید در عین حال شرایط و بستر مساعدی برای ظهور جرائم سایبری را بوجود اورده است. فقدان توافق پیرامون تعریف قانونی واحد از جرائم اینترنتی، بالا بودن سرعت ارتکاب این جرائم ، فقدان رویه های مشخص پیرامون همکاریهای متقابل فی ما بین پلیس و قوه قضائیه و بالا بودن هزینه های کشف این جرائم مراجع ذیصلاح را با چالش هایی مواجه کرده است. امروزه به منظور پیشگیری از وقوع جرائم اینترنتی و مبارزه با آن می بایست با استفاده از نرم افزارهای قدرتمندی که در اختیار پلیس قرار داده می شود ، نقش موثری در پیشگیری از وقوع جرائم اینترنتی خواهد داشت. تعامل و همکاریهای مناسب میان قوه قضائیه و پلیس می تواند در فرایند پیشگیری بنحو شایسته ای مورد توجه قرار گیرد. دلایل ارتکاب جرم در فضای مجازی عمدتا الکترونیکی هستند. این دلایل در صورتی توان اثباتی دارند که نیروهای پلیس در مرحله کشف و جمع آوری آنها دستورات مناسب از مقامات قضایی را که نیازمند تعامل پلیس و قوه قضائیه می باشد بنحو احسن اجرا کنند. نتایج این بخش همسو با نتایج تحقیقات صبح خیز(۱۳۹۴) و فرجیها(۱۳۰۹۰) و پرویزی (۱۳۸۸) می باشد. مدیریت واحدهای جرم یابی را باید یکی از حوزه های بسیار مهم و در عین حال مغفول علوم جرم یابی دانست. نبود یک مدیریت اثربخش موجب پایین آمدن کیفیت ادله فیزیکی، به تأخیر افتادن فرایند بررسی های کارشناسی، به بن بست رسیدن برخی از پرونده های کیفری و نیز سرخوردگی کارکنان و از بین رفتن انگیزه کاری آنان خواهد شد. مدیریت اثربخش و کارآمد یک واحد جرم یابی نیازمند برخورداری از دانش و درکی عمیق نسبت به نقش آزمایش های علمی در فرایند کشف حقایق جنایی است. مدیران جرم یابی باید نسبت به تعهدات خود در برابر کنشگران این عرصه اعم از کارکنان و متخصصان، مدیران مافوق، پلیس، دادستان، قاضی، بزه دیده، متهم و مردم وفادار باشند. آنها ضمن در نظر

گرفتن تعهدات اخلاقی خود باید میان انتظارهای متفاوت کنشگران این حوزه و محدودیت های موجود در منابع و امکانات تعادل و توازن برقرار کنند.

در این مقاله، ضمن بیان انواع کلاهبرداری سایبری و روش های ارتکاب آن در سطح ملی و بین الملل در فضای سایبر به ذکر نمونه هایی از آن پرداخته شد.آنگاه با ارائه مفاهیم و دسته بندی های قانون جرایم رایانه ای مستندات مرتبط با کلاهبرداری مشخص شد.در ادامه راهکارهایی به منظور ارتقاء جرم یابی کلاهبرداری سایبری شامل میزان توانمندی علمی کارآگاهان ،میزان تجهیزات سازمانی کارآگاهان ، میزان تعامل پلیس با مقام های قضایی و میزان آشنایی مقامات قضایی با مبانی فنی وحقوقی جرایم کلاهبرداری سایبری به عنوان عوامل موثر در جرم یابی کلاهبرداری سایبری معرفی گردید. سپس با انتخاب جامعه کارشناسان مرتبط، و طراحی پرسش نامه بر مبنای راهکارهای احصاء شده، اعتبارسنجی راهکارهها انجام شد.نتایج حاصل از تجزیه و تحلیل داده نشان داد که کلیهٔ فرضیه ها تأیید شدند. مهم ترین نقش این تحقیق،احصای روش های مبتنی بر ارتقاء جرم یابی کلاهبرداری سایبری از طریق احصاء نظرات کارشناسان مرتبط با موضوع است که در نوع خود قابل توجه است.

سپاسگزاری:

نویسنده مسئول بر خود لازم می داند از اساتید محترم راهنما و مشاور رساله دکتری خود قدردانی نماید.

پیشنهادها:

۱- پلیس فتا با برگزاری دوره های حرفه ای و فنی بصورت کوتاه مدت در بدو خدمت و حین خدمت نسبت به ارتقاء سطح فنی و مهارتی کارآگاهان سایبری اقدام گردد.

۲- تعامل هرچه بیشتر پلیس با مراجع قضایی نقش موثر و قابل توجهی در جرم یابی کلاهبرداری در فضای سایبر دارد.

۳- تجهیزات سخت افزاری و نرم افزاری ویژه پلیس فتا باید به روز رسانی شده و در اختیار کارآگاهان فضای سایبری قرار گیرد. هرچند تحریم های ظالمانه علیه کشورمان چالشی پیش روی پلیس فتا در این حوزه خواهد بود.

۴- در چند سال گذشته عزم جزم قوه قضائیه در مقابله و مجازات مجرمین درفضای سایبر به وضوح نشان داده شده است اما نیاز امروز دادسرای جرایم رایانه ای تربیت قضات متخصص در امور رایانه ای می باشد . چرا که ضعف سیستم قضا در مباحث مذکور منجر به جمع آوری و ارائه ادله ضعیف به دادگاه و تضییع حقوق مجرمین و متهمین خواهد شد.

فهرست منابع

- انصاری،ولی ا... (۱۳۹۱) .کشف علمی جرائم، سازمان مطالعه وتدوین کتب علوم انسانی دانشگاه ها ، مرکز تحقیق و توسعه علوم انسانی
- هادیانفر، کمال (۱۳۹۴). جرم فیشینگ. بازیابی از سایت www.cyberpolice.ir/news/۷۵۸۲۱
- زندی، محمدرضا، (۱۳۸۹) تحقیقات مقدماتی درجرایم سایبری،چاپ اول،انتشارات جنگل
- سلیمی، صادق، بخشی زاده اهری ، امین ، تحلیل ماده به ماده قانون آیین دادرسی کیفری(۱۳۹۲)در مقایسه با قوانین سابق،چاپ دوم،انتشارات جاودانه جنگل، ۱۳۹۳،تهران،یک جلد،ص ۳۹
- صبح خیز ،رضا،(۱۳۹۴) بررسی تطبیقی جرایم سایبری در نظام حقوق بین الملل و نظام حقوقی ایران ،رضا ،کارشناسی ارشد حقوق بین الملل،دانشگاه آزاد اسلامی ،واحد مراغه

- کمالی زاده، سلمان و شاه محمدی، غلام رضا (۱۳۹۴) ارزیابی روش های شناسایی وب سایت فیشینگ،فصلنامه پژوهش های اطلاعاتی و جنایی،سال یازدهم ،شماره اول ،بهار ۹۵
- مقیمی،مهدی(۱۳۹۵) جرایم سایبری در اسناد بین الملل پایان نامه دکتری،دانشگاه شهید بهشتی،دانشکده حقوق ،مقطع دکتری حقوق جزا و جرم شناسی
- موذن زادگان، حسن علی، حمید زاده اربابی،نجف، کاربردانگشت نگاری در جرم یابی،تهران،نشر کارآگاه،دوره دوم،سال ششم ،شماره ۲۴،ص ۱۰۰
- مارسلا، آلبرت جی، مننذز،داگلاس،(۱۳۹۲) سایبر فارنزیک ،ترجمه امیر توکلی ،انتشارات حدیث کوثر، ۱۳۹۲، ص ۴۸۰
- نتزگر،مایکل و موراسی ،جرمی(۱۳۹۴)تحقیقات در جرایم با فناوری پیشرفته ،مترجم: مهدی جاوید، دانشگاه علوم انتظامی امین، معاونت پژوهش و فناوری
- نجفی علمی،مرتضی(۱۳۹۳)تقریرات درس تحقیقات جنایی درجرایم رایانه ای ، دانشگاه علوم انتظامی ،مقطع دکتری جرم یابی
- مجموعه قوانین :

۱- قانون تجارت الکترونیکی (مصوب ۱۳۸۲/۱۰/۲۹)

۲- قانون جرایم رایانه ای (مصوب ۱۳۸۸/۳/۲۰)

۳- آئین دادرسی کیفری ایران ،مصوب (۱۳۹۲)

۴- قانون مجازات اسلامی ایران،مصوب (۱۳۹۲)

- http://www.informatics.indiana.edu/markus/papers/aci.pdf
- ueti_Survey.pdfVisit the Taylor & Francis Web site at
- http://www.taylorandfrancis.com
- http://www.auerbach-publications.com
- http://www.nextgenss.com/papers/NISR-WP-phishing.pdf

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی