بررسی شیوه‌های پیشگیری از جرایم سایبری؛ مبتنی بر فناوری اطلاعات

تاریخ دریافت: ۹۲/۱۲/۰۵ تاریخ پذیرش: ۹۳/۰۵/۲۵

از صفحهٔ ۹۹ تا ۱۲۰

غلامرضا شاه محمدی[۱]، منصور تاهو[۲]

چکیده

فضای مجازی با وجود مزایای فراوانش، به دلیل ویژگی هایی مانند امکان تحصیل هویت های گوناگون، گمنامی و سهولت انجام اعمال مختلف، موجب مهاجرت بسیاری از جرایم به آن شده است و مسؤلیت ناجا را که متولی برقراری نظم و امنیت است، دشوار می سازد. هدف اصلی این مقاله، تبیین شیوه های ارتکاب جرایم سایبری و نحوهٔ پیشگیری از آن است. این تحقیق از نظر نوع و هدف، کاربردی و از نظر روش‌های کمی گردآوری داده‌ها توصیفی- پیمایشی است. جامعهٔ آماری این تحقیق را کلیه کارشناسان و متخصصان و صاحب نظران حوزهٔ فناوری اطلاعات، معاونت پیشگیری پلیس فتای ناجا و قم در سال ۱۳۹۱ تشکیل می‌دهند که به دلیل محدود بودن جامعه آماری کلیه افراد جامعه به شیوهٔ تمام شماری انتخاب و مورد ارزیابی قرار گرفتند. ابزار گردآوری داده ها، پرسش نامهٔ محقق ساخته است. نتایج این پژوهش نشان می دهد که شیوه‌های مبتنی بر فناوری اطلاعات شامل ردیابی هویت مجازی مهاجمان، گشت فضای مجازی و کنترل و نظارت بر فضای مجازی، جمع آوری ادلهٔ الکترونیکی جرم و مستند سازی صحنهٔ جرم در پیشگیری از جرایم سایبر تأثیر دارد.

کلید واژه‌ها

جرایم سایبری، فضای مجازی، پیشگیری، فناوری اطلاعات، ادلهٔ جرم، پیشگیری از جرایم سایبری

۱- استادیار فناوری اطلاعات و ارتباطات دانشگاه علوم انتظامی(نویسنده مسؤل: Shah_mohammadi@yahoo.com).

۲- دانشجوی کارشناسی ارشد فرماندهی و مدیریت دانشگاه علوم انتظامی امین.

مقدمه

فناوری اطلاعات تحولات شگرفی در روند فعالیت جامعهٔ بشری به وجود آورده است، به گونه ای که زندگی امروزی بدون استفاده از این فناوری با دشواری های فراوانی مواجه است. رایانه ها با توجه به قابلیت های بسیار زیاد مانند دقت بالا، سرعت زیاد، قابلیت ذخیره سازی حجم زیاد اطلاعات، تبادل سریع اطلاعات، دسترسی آسان و محاسن بی شمار دیگر، امکانات زیادی را برای بشر به ارمغان آورده است. از منظر دیگر با گسترش اینترنت و ظهور فضای مجازی، به دلیل ویژگی های خاص این فضا مانند امکان تحصیل هویت‌های گوناگون، گمنامی و سهولت انجام اعمال مختلف، ضمن مهاجرت بسیاری از جرایم از فضای فیزیکی به فضای مجازی موجب بروز جرایم نوینی نیز شده است که قابل مقایسه با هیچ یک از جرایم موجود کلاسیک نبوده و چه بسا از نظر دامنه تأثیر، خطرناک‌تر باشد.

توسعه فناوری های نوین هر روز ابعاد جدیدتری پیدا می کند و در حال در هم نوردیدن و حضور فعال در تمامی زمینه ها و حوزه های بشری است. همین گستردگی و توسعهٔ فراگیر آن موجب شده تا بسیاری از ابعاد آن ناشناخته بوده و محل مناسبی برای مجرمان در اجرای عملیات مجرمانهٔ آنها باشد. فضای سایبر در کنار برخورداری از مزایا و آثار مثبت فراوان، منشاء تهدیدهایی جدی برای کلیهٔ افراد، سازمان ها و کشورهای جهان از توسعه یافته و غیر توسعه یافته شده است(جلالی، ۱۳۹۱: ۷).

با توجه به گسترش استفاده از فناوری اطلاعات و انجام بسیاری از امور سازمان ها و افراد در فضای مجازی و در واقع رواج استفاده از اینترنت، گرایش و تمایل به انجام جرم در این محیط نیز به دلایل مختلف افزایش می یابد. بسیاری از افرادی که در محیط های واقعی به دلایل متعدد از جمله شرم و حیا، و ترس از برخورد پلیس و دلایل دیگر اقدام به انجام ارتکاب عمل مجرمانه نمی کنند، در این فضا به دلیل ویژگی های فضای مجازی تمایل به ارتکاب جرم پیدا می کنند. با توجه به این موارد و عدم وجود محدودیت مکانی و زمانی (فضای مجازی محدود به زمان و مکان نیست و محدودیت های انجام جرم در محیط فیزیکی را ندارد)، تمایل به ارتکاب جرم در این فضا به سرعت درحال افزایش است. برابر آمار موجود از سال ۸۹ تا نیمهٔ اول سال

۹۲، آمار جرایم سایبری در ایران به سرعت در حال افزایش است (پلیس فتا، ۱۳۹۲). باتوجه به روند رو به رشد وقوع جرایم سایبری به دلیل ماهیت و ویژگی های فضای مجازی و نقش ناجا در پیشگیری از وقوع جرایم در فضای فیزیکی و مجازی، این مقاله با هدف تبیین شیوه های ارتکاب جرایم سایبری و نحوهٔ پیشگیری از آن مبتنی بر فناوری اطلاعات انجام می شود. در واقع این پژوهش به دنبال پاسخ به این سؤال اساسی است که شیوه‌های جرایم سایبری کدام اند؟ و چگونگی می توان باز آنها پیشگیری کرد؟

پیشینه تحقیق

بررسی های انجام شده نشان داد هیچ پژوهشی به طور مستقیم به موضوع این تحقیق نپرداخته است ولی تحقیقاتی که به جرایم رایانه ای پرداخته اند عبارت‌اند از:

شیرزاد(۱۳۷۶) در تحقیق خود با عنوان «بررسی جرایم رایانه ای در قلمرو حقوق کیفری ایران و حقوق بین الملل»، به بررسی ابعاد کیفری جرایم رایانه ای پرداخته است. در اولین گام برای شناسایی مصادیق و نمونه های عینی «بزهکاری پیشرفته به شبکه های اطلاعاتی و رایانه ای به خصوص «اینترنت» گام برداشته است و نحوهٔ عمل بزهکاران را در این وادی به نظاره گذاشته است. برای شناخت دقیق موضوع به بیان انواع جرایم رایانه ای براساس اصل قانونی بودن و همچنین به برخورد با جرایم رایانه ای در حقوق ایران و حقوق بین المللی پرداخته است.

تحیری(۱۳۸۴) نیز به دسترسی غیرمجاز به سیستم های رایانه ای در حقوق ایران و اسناد بین المللی پرداخته است. در این پژوهش در بخش نخست به صورت کلی و جامع به جرم دسترسی غیرمجاز و طرفین آن و در بخش دوم به پاسخ ها در برابر دسترسی غیرمجاز می پردازد.

محمدی (۱۳۷۸) در طرح تحقیقی خود با عنوان «شناخت کلی جرایم رایانه ای و شیوه های مبارزه با آن» که به سفارش ناجا انجام شده، توجه عمده معطوف به جایگاه ویژهٔ ناجا در مقابله با جرایم، رایانه ای و نگاه به موضوع از این منظر خاص است و موضوع شناخت و پیشگیری را به عنوان هدف اصلی قرار داده است که در نخستین اقدام در جهت تحقیق اولین مرحله از مقابلهٔ نیروی انتظامی با جرایم رایانه‌ای به شمار می‌آید.

جلالی فراهانی(۱۳۸۴) در مقالهٔ خود ضمن مرور جرایم سایبری و پیشگیری وضعی از جرم، پیشگیری وضعی از جرایم سایبری را در قالب تدابیر محدود کننده یا سلب کنندهٔ دسترسی، تدابیر نظارتی، تدابیر صدور مجوز و ابزار ناشناس کننده و رمزگذاری مطرح می کند.

جلالی(۱۳۸۹) در مقالهٔ خود با عنوان «نظارت همگانی عامل پیشگیری جرایم در فضای مجازی» به ابعاد مختلف نظارت همگانی پلیس و سازمان مجازی پلیس در فضای مجازی به عنوان یکی از عوامل مؤثر پیشگیری از جرایم در فضای مجازی پرداخته است. هرچند که نظرات خوبی در این مقاله مطرح شده است؛ لیکن این نظرات اعتبارسنجی نشده است.

مالمیر و همکار(۱۳۸۹) نیز در مقالهٔ خود با عنوان «پیشگیری از بزه‌دیدگی سایبری» به بررسی بزه دیدگی ناشی از جرایم سایبری و راه های پیشگیری از آن پرداخته اند. در این تحقیق بر مبنای نظریهٔ سبک زندگی روزمره به بررسی دلایل بزه‌دیدگی سایبری پرداخته است و سه رکن اصلی بزه دیدگی سایبری را ۱- مجرم تحریک شده(کسی که به اندازهٔ کافی برای ارتکاب جرم برانگیخته شده باشد)؛ ۲- هدف مناسب (باید دارای ارزش، سکون، دید و دسترسی باشد) و ۳- فقدان محافظ توانا(محافظانی که از تحقق جرم در زمان فعالیت های روزمرهٔ مردم که هر روز نیز تکرار می‌شوند، جلوگیری کنند) می‌داند. پس از تحلیل انطباق نظریهٔ سبک زندگی با بزه دیدگان سایبری مشخص شد تنها یکی از سه رکن اصلی در تحقق بزه دیدگی سایبری نقش عمده بازی می‌کند و آن فقدان حفاظت است.

مبانی نظری تحقیق

اینترنت به حق یکی از مظاهر فناوری اطلاعات است که با پیدایش و گسترش رایانه‌های شخصی و امکانات وسیع ارتباطات راه دور شبکه ای و مخابراتی به منصهٔ ظهور رسید. اینترنت را نمی توان تنها یک شبکهٔ رایانه ای یا مجموعه ای از شبکه‌های رایانه ای متصل به هم تلقی کرد. در واقع به اینترنت باید به عنوان منبع عظیمی از اطلاعات قابل استفاده نگاه شود. با توجه به قابلیت های بسیار بالای این شبکه که مجموعهٔ جهان را به یک شهر کوچک تبدیل کرده و از لحاظ دسترسی به

نقاط و اطلاعات جای جای این دنیا با فشردن یک کلید امکان پذیر شده؛ امکان ارتکاب جرایم متعدد و مختلف چه از لحاظ جرایم سنتی و چه خلق جرایم بسیار جدید و بی سابقه را برای مجرمان به وجود آورده است(دزیانی، ۱۳۸۹).

شبکهٔ جهانی اینترنت یکی از مظاهر فناوری اطلاعات، زیربنا و شاهراه بسیاری از تخلفات و جرایم جدید رایانه ای است. طبیعت جرایم و سوء استفاده های ارتکابی در فضای مجازی هیچ گاه در دنیای حقیقی دیده نشده است و دولت ها در تلاش هستند تا سیاست های حقوقی جدیدی را برای مهار کردن این جرایم تدوین کنند. امنیت ناکافی فناوری همراه با طبیعت مجازی آن فرصت بسیار مناسبی را در اختیار افراد شرور قرار می دهد. در دنیای امروزی اینترنت به دلیل عدم توجه به امنیت در سال های اخیر، جعل هویت فرد، ورود حساب بانکی دیگری و ارتکاب جرایم دیگر به راحتی انجام پذیر است. کلاهبرداری برخط، انتشار عکس های خصوصی افراد و هک، تنها برخی از نمونه های جرایم رایانه ای هستند که هر روز در حجم وسیعی انجام می‌شوند. ضرر و زیان مالی ایجاد شده توسط جرایم سایبری خیلی زیاد است. تنها در سال ۲۰۰۳ میلادی خرابی های ایجاد شده توسط نرم افزارهای مخرب بالغ بر ۱۷میلیون دلار بوده است. با اندکی تخمین، برای اولین بار بیشتر از تجارت غیرقانونی داروها، درآمدها از جرایم سایبری از۱۰۰میلیون دلار در سال ۲۰۰۷ فراتر رفته است. تقریبا ۶۰ درصد تجار در ایالت متحدهٔ آمریکا باور دارند که جرایم سایبری برای آنها از جرایم فیزیکی پر هزینه تر هستند. این تخمین ها به طور واضح اهمیت حفاظت ساختار زیر بنایی اطلاعات را نشان می دهد(گرکی، ۱۳۸۹ : ۱۸).

فضای سایبر (مجازی): واژهٔ سایبر را به مجازی[1] ترجمه کرده اند. این واژه از لغت سکاندار[2] یا راهنما گرفته شده است و نخستین بار توسط ویلیام گیبسون نویسندهٔ داستان های علمی- تخیلی در کتاب نورومنسر[3] به کار برده شد. سایبر پیشوندی است برای توصیف یک شخص، یک شیء، یک ایده یا یک فضا که مربوط به دنیای رایانه و اطلاعات است. در طی توسعهٔ اینترنت واژه های ترکیبی بسیاری از این کلمهٔ

1- Virtual
2- Sculls
3- Neuromancer

سایبر همچون فضای سایبر، شهروند سایبر و پول سایبر به وجود آمده است (حسنوی و فرسایی، ۱۳۷۹: ۱۵۰). فضای مجازی عبارت است از مجموعهٔ ارتباطات درونی انسان ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی. به تعبیر دیگر، فضای مجازی فضایی است که در آن فعالیت های مختلف در ابعاد داده‌ورزی و اطلاع رسانی، ارتباطات و ارائه خدمات، مدیریت و کنترل از طریق ساز و کارهای الکترونیکی و مجازی صورت می‌پذیرد(صدری و کروبی، ۱۳۸۴: ۵۸). فناوری ارتباط راه دور اساس فضای مجازی را تشکیل می دهد. هر چند برخی از این فناوری‌ها مانند تلگراف و تلفن در اوایل قرن نوزده اختراع شد اما همه گیر و ارزان شدن این فناوری ها و بالا رفتن توان فنی آنها که شرط اصلی ظهور فضای مجازی است در چند سال اخیر اتفاق افتاده است(شریفی هولاسو، ۱۳۸۷: ۵۲).

بنیان فضای مجازی که بر استفاده از شبکهٔ جهانی وب به منزلهٔ یکی از فضاهای قدرتمند حاضر در فضای واقعی مجازی استوار است، کاربردی وسیع یافته و به علت سهولت استفاده، باعث جذب بسیاری از محققان شده است. مهم ترین ویژگی‌های فضای مجازی عبارت‌اند از: ۱- هزینه پایین ورود، ۲- گمنامی(ابراهیم پور، ۳:۱۳۹۰)، ۳- نامتقارن بودن در آسیب‌پذیری (درگاهی و همکاران، ۱۳۸۶)، ۴- جهانی و فرامرزی بودن، ۵- دسترسی دائم و آسان به آخرین اطلاعات، ۶- جذابیت و تنوع، ۷- عدم وابستگی به زمان و مکان خاص(عاملی (الف)، ۱۳۹۰)، ۸- چند رسانه ای بودن (عاملی (ب)، ۱۳۹۰)، ۹- سهولت تعامل و تبادل اطلاعات با دیگران و ۱۰- سرعت بالای تبادل اطلاعات و امکانات قابل توجه اینترنت برای افراد جامعه (ابراهیم پور، ۱۳۹۰ :۳).

جرم سایبری و ویژگی های آن: جرم سایبری، یکی از اصطلاحاتی است که بر استفاده از فناوری رایانه در پرداختن به یک فعالیت غیر قانونی دلالت دارد. جرم فناوری های پیشرفته[1] و جرم عصر اطلاعات[2] نیز همین پدیده را توصیف می‌کند. اغلب جرایم سایبری که تا به حال شاهد آنها بوده ایم چیزی نیست جز مهاجرت

1- High Tech Crime .
2- Information Age Crime .

جرایم از دنیای واقعی به فضای اینترنت. امروزه جرایم سایبری با سرعت نگران کننده‌ای، بدون کنترل رو به تکثیر و افزایش است و به عنوان فعالیت های به واسطهٔ رایانه که هم غیر قانونی و هم نامشروع هستند، می توانند از طریق شبکه های الکترونیک جهانی هدایت شوند(هیل[1]، ۲۰۰۲). جرم سایبری را هر جرمی می‌دانند که شامل رایانه ها و شبکه ها باشد، ولو آنکه خیلی متکی به رایانه نباشد(کسی[2]، ۲۰۰۰: ۸). در حالی که برخی جرم سایبری را جرایمی می دانند که دسته های مختلفی از جرایم را در فضای سایبر و شبکهٔ جهانی اینترنت در بر می‌گیرند و شامل جرایم ارتکابی به کمک رایانه و جرایم متمرکز بر رایانه نیز نامیده می شود(فرنل، ۲۲:۲۰۰۲).

جرایم سایبری، ویژگی های متمایزی نسبت به جرایم کلاسیک دارند؛ زیرا ماهیت این گونه جرایم به دلیل فناوری پیچیده و بالا، خصوصیات منحصر به فردی دارند مانند شیوهٔ ارتکاب آسان، خسارات و ضررهای هنگفت با حداقل منابع و هزینه، عدم حضور فیزیکی در محل ارتکاب جرم، عدم شناسایی جرایم در بعضی موارد، خصوصیت فراملی، وسعت و دامنهٔ وسیع جرم. برخی از ویژگی‌های جرایم سایبری عبارت‌اند از:

- **خصوصیات مرتکبان جرایم سایبر**: مرتکبان جرایم سایبری شامل طیف گسترده ای از افراد هستند. نوجوانان، دانشجویان، کارمندان ناراضی، خلافکاران و تروریست های بین المللی و غیره که منحنی سنی مجرمان رایانه ای، سنی بین ۱۰ تا ۶۰ سال را نشان می‌دهد و دامنهٔ مهارت آنان از تازه کار تا حرفه ای گسترده است. بسته به نوع جرم، گاه آشنایی کمی با رایانه کافی است و گاه نیازمند تخصص در سطح بالا است (سازمان ملل، ۱۳۷۶: ۲۴).

- **عدم تخمین میزان دقیق جرایم ارتکابی:** جرایم سایبری می‌تواند توسط هر کسی در هر نقطه از دنیا به وقوع بپیوندد و با آنکه آمار تحقیقات به عمل آمده نشان از روند رو به رشد جرایم رایانه ای دارد و لیکن تعداد آمار موجود نمی تواند ما را به

1- Hale
2- Casey

نتیجه گیری مطلوب رهنمون سازد؛ چه بسا این آمار منعکس کنندهٔ تعداد جرایم مکشوفه هستند و نه تعداد جرایم واقعی. انجمن بین المللی حقوق جزا بر پایهٔ گزارش‌های دریافتی از کشورهای عضو اعلام داشته که تنها ۵ درصد جرایم سایبری به مقامات مجری قانون گزارش شده اند (سازمان ملل، ۱۳۷۶: ۲۲).

- **حجم و وسعت ضرر و خسارت وارده:** مرتکبان با کمترین سرمایه و هزینه (یک رایانه شخصی) می توانند با ورود به شبکهٔ اطلاعاتی و نفوذ در آن خسارات هنگفتی وارد نمایند، سهولت ارتکاب با حجم زیاد موضوعات مطروحه، سرعت عملکرد رایانه، عدم نیاز به تخصص خاص یا بالا، عدم نیاز حضور فیزیکی مرتکب در محل و... همگی موجب شده تا حجم صدمات و خسارات وارده افزون گشته و گاه به چندین هزار برابر جرایم معمولی برسد. وسعت خسارات وارد ناشی از یک نفوذ غیرقانونی یا گسترش ویروس در اینترنت می تواند در کسر ثانیه صدها هزار استفاده کننده در سراسر جهان را متحمل خسارت کند.

- **خصوصیت فراملی و بین المللی جرایم سایبری:** به دلیل فراملی بودن ماهیت جرایم رایانه ای این گونه جرایم را باید جرایم بدون مرز نامید. جرایم رایانه ای به دلیل ماهیت و فناوری خاص، اختصاص به محیط فیزیکی معین و محدودی ندارد و به راحتی در مقیاس بین المللی قابل تحقق است.

مصادیق جرایم فضای سایبر

- **کلاهبرداری کارت اعتباری**: شایع‌ترین جرمی که در سال‌های اخیر در فضای سایبر گزارش شده کلاهبرداری کارت اعتباری است. دزدی و سوء استفاده از کارت‌های اعتباری[1] بی حد و حصر است. عوامل بی شماری از جمله: وسوسه، دسترسی آسان و عدم لزوم مهارت های فنی خاص برای موفقیت در این جرم، از دلایل ارتکاب به این جرم است.

- **افترا و نشر اطلاعات از طریق پست الکترونیک:** پست الکترونیک مرسوم ترین و گسترده‌ترین سرویس اینترنت است و توسط آن علاوه بر فایل های متنی، صوت،

1- Carding

تصویر فایل‌های ویدئویی نیز به دیگر کاربران اینترنت قابل ارسال است. هر کاربر می‌تواند در شبکه‌های بین المللی از طریق یک آدرس پست الکترونیک مشخص شناخته شود که با دسترسی به رمز آن می توان به آسانی در آن تقلب کرد.

- **تطهیر پول نامشروع رایانه ای در فضای سایبر:** تطهیر پول نامشروع[1] از جرایم کلاسیک بوده که دارای سابقه و قدمت زیادی است و با فناوری رایانه و بسط شبکه‌های بین المللی، مصادیق جدید این جرم در فضای سایبر به کمک اینترنت، پست الکترونیک و شبکه‌های بین‌المللی ارتباطی صورت می پذیرد. نحوهٔ ارتکاب بدین نحو است که باندهای بزرگ نامشروع توسط نامهٔ الکترونیکی یا اینترنت بدون هیچ گونه اثر و نشانی درخواست ارسال مبالغی پول به حساب شخص معینی را (به وی) می‌کنند و در تقاضای خود نحوهٔ ارسال پول و دستمزد و مدت استرداد را بیان و در صورت قبول طرف، نوع و نحوهٔ تضمین‌های لازم را اعلام می دارند و اصولاً در زمان استرداد پول یک عنوان مشروع در تجارت الکترونیک را با منشا تجاری انتخاب و با هدف خود هماهنگ می‌کنند.

- **دسترسی غیر مجاز در محیط سایبر:** دسترسی غیر مجاز به داده ها یا سامانه‌های رایانه ای از جمله جرایمی است که در محیط سایبر به وقوع می پیوندد. دسترسی غیر مجاز را به عنوان جرمی مادر تلقی می‌کنند، زیرا دارای نقشی مؤثر در وقوع سایر جرایم سایبری است. در برخی موارد دسترسی غیر مجاز عامل تسهیل کننده در وقوع سایر جرایم سایبری و حتی جرایم سنتی است و در برخی موارد دیگر مقدمهٔ ارتکاب جرم تلقی می شود. از نظر میزان وقوع و میزان خسارت هم در سطح بالایی قرار دارد.

- **جمع آوری اطلاعات شخصی:** مجرمان اطلاعات شخصی افراد را از قبیل شماره کارت ملی، اطلاعات گواهینامه، شماره تلفن، آدرس شخصی و نظایر آن جمع آوری کرده و سپس آن را با قیمت مناسبی به فروش می رسانند. این اطلاعات توسط افراد مختلف به خصوص نفوذگرها به منظور شناسایی اطلاعات سری افراد استفاده می‌شود. یکی از کاربردهای بالقوهٔ این اطلاعات شخصی، دزدی شخصیت است. دزدی

1.Money Laundery

شخصیت می تواند یک مشکل اساسی برای بخش های قضایی باشد. افراد، اطلاعات دیگران را از روی اینترنت جمع آوری کرده و سپس خود را جای آنان معرفی می‌کنند (گرگی، ۱۳۸۹).

پیشگیری: لغت پیشگیری[1] در منابع فارسی به معنای رفع، جلوگیری، مانع شدن و از پیش مانع چیزی شدن (فرهنگ دهخدا) و در منابع دیگر نیز جلوگیری، دفع، صیانت، مانع شدن و جلو بستن تعریف شده است. اقدامات احتیاطی برای جلوگیری از اتفاقات بد و ناخواسته هم به معنای پیش دستی کردن، پیشی گرفتن و پیشگیری یا جلوگیری کردن، به جلو چیزی رفتن و هم به معنی آگاه کردن و هشدار دادن است (زینالی، ۱۳۸۱: ۹۹). پیشگیری، عبارت است از تمامی اقداماتی که از وقوع بزه جلوگیری می‌کند. به عقیده شرمن، هر رویدادی که انجام آن در یک معنای عام و نتیجه آن نشان دهد که از نرخ بزهکاری کاسته شده، می‌تواند پیشگیرانه قلمداد شود (نجفی ابرندآبادی، ۱۳۸۱: ۱۵۸).

پیشگیری از جرم: به لحاظ این‌که انسان دارای ابعاد گوناگون زیستی، روانی و اجتماعی است و احتمال ابتلای او به اختلال و ناهنجاری در هر یک از زمینه‌های مذکور وجود دارد؛ لذا به‌کار بردن روش‌های احتیاطی و کنترلی و انجام اقدامات پیشگیرانه درجلوگیری از ابتلای انسان به اختلال و ناهنجاری‌ها در هر یک از ابعاد فوق در حکم نوعی پیشگیری است. از طرفی در تعریف مفهومی، پیشگیری از جرم به مجموعه اقداماتی اطلاق می‌شود که برای جلوگیری از فعل و انفعال زیان‌آور محتمل برای فرد یا گروه و یا هر دو به عمل می‌آید. مثل پیشگیری از حوادث کار، جرایم جوانان و حوادث در جاده‌ها و ... (رجبی‌پور، ۱۳۸۲: ۱۵).

پیشگیری از منظر رویکرد: بر این اساس، پیشگیری بر دو نوع پیشگیری کیفری(از طریق سازوکارهای نظام عدالت کیفری) و غیر کیفری(از طریق سازوکارهای خارج از نظام عدالت کیفری) تقسیم می شود(عباچی، ۱۳۸۷). پیشگیری کیفری را می توان از یک منظر بر دو نوع، پیشگیری قضایی و پیشگیری انتظامی تفسیم کرد:

---

1 -Prevention

- **پیشگیری قضایی:** در پیشگیری قضایی سیاست پیشگیری از این منظر که دولت(دستگاه حاکم) به عنوان اولین نهاد در مقابل جرم و مجرم (بزهکار) قرار می‌گیرد و از طریق اعمال قانون و سیاست های تقنینی در مقابل بزهکار، به اصلاح آنان می‌پردازد، مورد توجه قرار می گیرد.

- **پیشگیری انتظامی:** در نقش اول پلیس به عنوان ضابط قوۀ قضائیه عهده دار امر پیشگیری انتظامی است و در چهارچوب سیاست های کیفری یا جنایی و تحت نظارت مقامات قضایی عمل می کند و در نقش دوم، پلیس به عنوان سازمان یا نهاد همچون سایر سازمان ها و دستگاه های دولتی و غیر دولتی اقداماتی را انجام می دهد که جلوۀ اقدامات اجتماعی پلیس یا فعالیت های جامعه محوری پلیس محسوب می‌شود (بیات و همکاران،۱۳۸۷: ۱۴۲).

پیشگیری مبتنی بر فناوری اطلاعات: فناوری اطلاعات تأثیرات اساسی و مثبتی در زندگی انسان ها داشته است و این قابلیت را دارد که در امر پیشگیری از جرم نیز مورد استفاده قرار گیرد. از آنجا که بهره برداری از فناوری اطلاعات در برخورد با جرایم سایبری باعث می شود که : ۱- ارتکاب جرم سخت شود، ۲- هزینۀ ارتکاب جرم به دلیل قابلیت پیگرد و دستگیری سارقان، افزایش یابد؛ ۳- مجرمان سایبری به طور مؤثرتر و سریع تر دستگیر شوند. بنابراین پیشگیری مبتنی بر فناوری اطلاعات، نوعی پیشگیری وضعی تلقی می‌شود. ردیابی هویت مجازی، گشت فضای مجازی، جمع آوری ادلۀ جرم و مستند سازی صحنه جرم از مصادیق پیشگیری وضعی تلقی می شوند. روش های مختلف پیشگیری مبتنی بر فناوری اطلاعات برای پیشگیری از جرایم سایبری تبیین می شود.

الف) ردیابی هویت مجازی: نشانی پروتکل اینترنت[1] یا نشانی هویت مجازی، عددی است که به هریک از دستگاه ها و رایانه‌های متصل به شبکۀ رایانه ای که بر مبنای نمایه TCP/IP از جمله اینترنت کار می‌کند، اختصاص داده می‌شود. پیام‌هایی که دیگر رایانه‌ها برای این رایانه می‌فرستند با این نشانه عددی همراه است و مسیریاب‌های شبکه آن را مانند نشانی گیرنده در نامه‌های پستی تعبیر می‌کنند، تا

1.Internet Protocol Address/ IP

بالاخره پیام به رابط شبکهٔ رایانه مورد نظر برسد. هر نشانی کامل، شامل یک پیشوند و یک پسوند است و طوری تخصیص داده می‌شوند که یکتا باشند، بنابراین ویژگی اول تضمین می‌شود. اگر دو رایانه به دو شبکهٔ مختلف متصل شده باشند، نشانی‌هایشان پیشوندهای متفاوت خواهند داشت، اما اگر دو رایانه به یک شبکه وصل باشند، نشانی‌هایشان دارای پسوندهای متفاوت خواهد بود.

ب) گشت فضای مجازی: یکی از شیوه های مبتنی بر فناوری اطلاعات برای پیشگیری از جرایم سایبری، گشت فضای مجازی است. گشت فضای مجازی با هدف کشف پیش دستانه جرایم رایانه ای انجام می شود. به عبارت دیگر گشت زنی در فضای سایبر به منظور پیشگیری از وقوع جرم یاکشف جرم انجام می‌گیرد. مراحل انجام گشت فضای مجازی عبارتند از:

انتخاب کلید واژه ها: با توجه به موضوع مورد نظر، کلید واژه هایی انتخاب می‌شوند که به ما در رابطه با آن موضوع یا مصداق کمک می کند تا به ادلهٔ جرم برسیم.

– **انتخاب موتور جستجو و انجام جستجو:** بعد از تعیین موضوع یا مصداق جرم و انتخاب کلید واژه ها، یکی از موتورهای جستجوی مطرح در فضای مجازی از جمله بینگ[1]، یاهو[2] و گوگل[3] انتخاب و کلید واژه ها مورد جستجو قرار می‌گیرد.

– **بررسی صفحات حاصل از جستجو:** بعد از انجام جستجو، صفحات حاصل از جستجومورد بررسی قرار می‌گیرد که در این فرایند، تک تک سایت ها، وبلاگ ها، پایگاه ها و گلوگاه های خبری به صورت دقیق بررسی می شود و در صورت وجود ادلهٔ جرم در صفحات، از طریق اطلاعات موجود در آنها از قبیل شماره تماس، پست الکترونیکی، اطلاعات آدرسی که بتواند در جهت رسیدن به صاحب اصلی وبلاگ یا وب سایت کمک کند، مستند می شود.

ج) کنترل و نظارت بر فضای مجازی: کنترل و نظارت مستلزم انجام نظارت بر فعالیت شبکه های ارتباطی، وب سایت ها، ارائه دهندگان خدمات اینترنت است. فعالیت های انجام شده در طی کنترل و نظارت عبارتند از :

---
1 - Bing
2 - Yahoo
3 - Google

- مراجعه به مراکز وب سایت ها، شبکه های ارتباطی و مراکز ارائه دهندهٔ خدمات اینترنت و میزبانی و کافی نت ها.
- بازرسی محتوای موجود در سامانه ها، شبکه ها و وب سایت ها و بررسی و تحلیل داده های ترافیکی جمع آوری شده توسط ارائه دهندگان خدمات اینترنت و همچنین استفاده از نرم افزارهای مرتبط.
- در صورت لزوم شنود با مجوز موبایل یا تلفن عوامل مرتبط با شبکه ها، وب سایت‌ها یا ارائه دهندگان دارای ادلهٔ مجرمانه.
- در صورت مواجه با مصادیق مجرمانه، انعکاس مصادیق جرم به مبادی ذی ربط.

د) جمع آوری ادلهٔ الکترونیکی جرم: اولین فردی که وارد صحنهٔ جرم می شود موظف به تشخیص، انتخاب، حفاظت، حمل و یا ذخیرهٔ مدرک الکترونیکی است. ممکن است که هر کدام از کارکنان دستور جمع آوری مدارک الکترونیکی را داده یا خود در جمع آوری مدارک مشارکت کنند. شاید لازم باشد مسؤلان آزمایشگاهی در صحنهٔ جرم به عنوان دستیار عمل کرده و در بررسی مدارک ایفای نقش کنند. در این بین وظیفهٔ مدیران این است که اطمینان حاصل کنند افراد تحت امر آنها به خوبی آموزش دیده و در برخورد با مدارک الکترونیکی به اندازهٔ کافی مجهز هستند(جوکز، ۱۴۰:۱۳۸۹). هر فرد مسؤل باید حساسیت و ماهیت مدارک الکترونیکی، شیوه هایی که برای انتخاب و حفاظت از آنها وجود دارد را درک کند. آیین دادرسی باید به گونه‌ای باشد که اجازه بررسی صحنهٔ جرم الکترونیکی را صادر کند. ادلهٔ الکترونیکی، داده‌ها و اطلاعاتی هستند که توسط ابزار الکترونیکی ذخیره یا انتقال داده می شوند و حائز اهمیت تخصصی هستند. همان طور که اثر انگشت یا DNA ادله ای مخفی هستند، مدرک الکترونیکی نیز همان حالت را دارد. مرحلهٔ جمع آوری شامل جستجو برای شناسایی، جمع آوری و مستند سازی مدرک الکترونیکی است.

هـ) مستندسازی صحنهٔ جرم: مستند سازی صحنهٔ جرم موجب ثبت آن واقعه در تاریخ برای همیشه خواهد شد. مستند سازی صحنه در جریان تحقیقات، فرآیندی ثابت و دائم است. ثبت صحیح محل و وضعیت رایانه ها، وسایل ذخیره، دیگر وسایل الکترونیکی و ادلهٔ قراردادی حائز اهمیت است. صحنهٔ جرم را باید همراه با جزییات آن مستند سازی کرد. صحنهٔ فیزیکی را مشاهده و مستند سازی می‌کنیم. وضعیت و محل سیستم رایانه ای از جمله وضعیت برق رایانه (روشن، خاموش یا در حال

استراحت) را مستند سازی کنیم. اکثر رایانه ها دارای چراغ وضعیت هستند که نشان می دهد رایانه روشن است، به همین صورت چنانچه صدای پنکه (فن رایانه) به گوش برسد، احتمالاً سیستم روشن است و به علاوه اگر سیستم رایانه گرم باشد ممکن است نشان دهندهٔ این باشد که دستگاه روشن بوده یا اینکه به تازگی خاموش شده است. قطعات الکترونیکی مربوطه را مشخص و مستند سازی کنیم که جمع آوری نخواهند شد.

صحنهٔ جرم در نفوذ غیر مجاز، شامل سیستم های رایانه ای میزبان، سرویس گیرنده مخابرات و رایانهٔ بزهکار است. ممکن است رایانهٔ میزبان در ایران و رایانهٔ بزهکار در ایالات متحده باشد و یا بالعکس. پراکندگی جغرافیایی صحنهٔ جرم بسیار زیاد و معمولاً دور از هم و در محدودهٔ مرزهای جغرافیایی کشورهای مختلف است. در جرم (نفوذ غیر مجاز) نیز آثار ادلهٔ شناسایی، جمع آوری و تجزیه و تحلیل می شود که اغلب شامل نشانی هویت مجازی[1]، نام کاربر، گذر واژه و ... است. در جرم قتل، پلیس برای شناسایی هویت مظنون، از مصاحبه و تحقیقات محلی، آثار انگشت و چهره نگاری استفاده می‌کند. در جرم نفوذ غیر مجاز پلیس برای شناسایی هویت مظنون از (IP مشخصات سیستم عامل و سخت افزار مظنون، شناسه، گذر واژه و فایل‌های نگهداری شده در مسیری که مظنون طی کرده و...) همچنین آثار انگشت و روش‌های شناسایی هویت معمول در کشف جرایم کلاسیک بهره می برد. برای بررسی صحنهٔ جرم نفوذ غیر مجاز و شناسایی و جمع آوری آثار و ادلهٔ جرم از سخت افزارها و عمدتاً نرم افزارهای تخصصی که بر اساس استانداردهای بین المللی تولید شده‌اند استفاده می‌شود(جوکز، ۱۳۸۹: ۱۶۰).

فرضیه‌های تحقیق

۱- پیشگیری مبتنی بر فناوری اطلاعات درکاهش ارتکاب جرایم سایبری تأثیر دارد.

۲- پیشگیری مبتنی بر ردیابی IP (مهاجم) در کاهش ارتکاب جرایم سایبری تأثیر دارد.

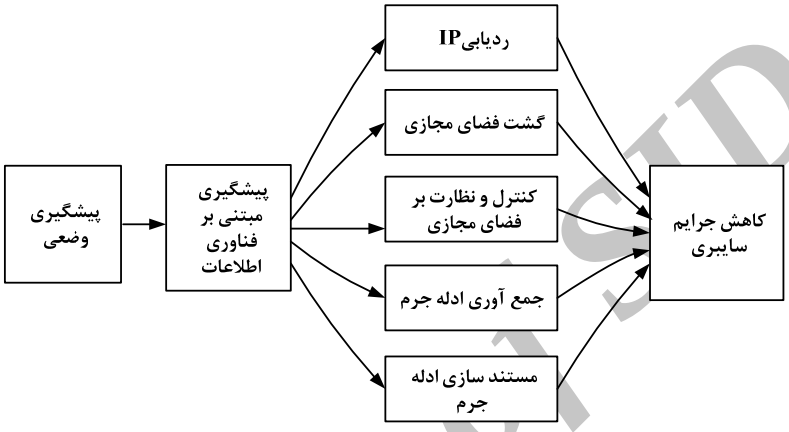
۳- پیشگیری مبتنی بر گشت و کنترل و نظارت فضای مجازی در کاهش ارتکاب جرایم سایبری تأثیر دارد.

---

1 - IP

۴- پیشگیری مبتنی بر جمع آوری ادلهٔ الکترونیکی جرم در محیط اینترنت درکاهش ارتکاب جرایم سایبری تأثیر دارد.

۵- پیشگیری مبتنی بر مستند سازی صحنه جرم درمحیط اینترنت در کاهش ارتکاب جرایم سایبری تأثیر دارد.



نمودار ۱ : مدل مفهومی تحقیق

روش شناسی تحقیق

تحقیق حاضر از آنجا که به تبیین شیوه های جرایم سایبری می پردازد، از نوع توصیفی - پیمایشی است و از آنجا که به پیشگیری از جرایم سایبری می پردازد، از نوع کاربردی است. جامعهٔ آماری تحقیق شامل کلیهٔ کارشناسان خبره در مورد جرایم سایبری در شهر تهران و قم است که تعداد آنان ۵۷ نفر هستند و به صورت تمام شمار عمل شده است. گرد آوری اطلاعات به دو روش 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 ۱۳۹۱ در شهر تهران و قم است. در تنظیم 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 محاسبهٔ ضریب آلفای کرونباخ استفاده شده است که نتیجهٔ به دست آمده (α =۰/۹۰۸) نشان داد که پرسش نامه طراحی شده از اعتبار کافی برای ارزیابی نقش و شاخص ها برخوردار است.

یافته های تحقیق

جدول ۱ : نتایج آزمونT تک نمونه برای پیشگیری مبتنی بر ردیابی IP مهاجم

عنوان	میانگین	تفاوت میانگین	dF	T	Sig
پیشگیری مبتنی بر ردیابی IP مهاجم	۴/۴۲	۰/۴۲	۵۶	۹/۴۶	۰/۰۰۲

مطابق جدول ۱، T حاصل از تجزیه و تحلیل داده‌ها بزرگ‌تر از T جدول(۱/۹۶) و از طرفی Sig= ۰/۰۰۲ است. بنابراین فرضیه اول تأیید می‌شود و نتیجه می‌گیریم رابطهٔ معناداری بین ردیابی IP مهاجم و کاهش ارتکاب جرایم سایبری در فضای مجازی وجود دارد. به عبارت دیگر ردیابی IP (مهاجم) در فضای مجازی بر میزان کاهش ارتکاب جرایم سایبری تأثیرگذار است.

جدول ۲: نتایج آزمونT تک نمونه برای پیشگیری مبتنی بر کنترل و نظارت بر فضای مجازی

عنوان	میانگین	تفاوت میانگین	dF	T	Sig
پیشگیری مبتنی بر کنترل و نظارت بر فضای مجازی	۴/۱۸	۰/۱۸	۵۶	۷/۸۶	۰/۰۰۲

مطابق جدول ۲، T حاصل از تجزیه و تحلیل داده ها بزرگ‌تر از T جدول(۱/۹۶) و از طرفی Sig= ۰/۰۰۲ است. بنابراین فرضیهٔ دوم تأیید می شود و نتیجه می‌گیریم رابطهٔ معناداری بین پیشگیری مبتنی بر کنترل و نظارت بر فضای مجازی وکاهش جرایم سایبری وجود دارد. به عبارت دیگر پیشگیری مبتنی بر کنترل و نظارت بر فضای مجازی بر کاهش جرایم سایبری مؤثر است.

جدول۳: نتایج آزمونT تک نمونه برای پیشگیری مبتنی بر گشت فضای مجازی

عنوان	میانگین	تفاوت میانگین	dF	T	Sig
پیشگیری مبتنی بر گشت فضای مجازی	۴/۰۴	۰/۰۴	۵۶	۵/۵۸	۰/۰۰۱

مطابق جدول ۳، T حاصل از تجزیه و تحلیل داده ها بزرگ‌تر از T جدول(۱/۹۶) و از طرفی Sig= ۰/۰۰۱ است. بنابراین فرضیهٔ سوم تأیید می شود و نتیجه می‌گیریم رابطهٔ معناداری بین پیشگیری مبتنی بر گشت فضای مجازی و کنترل (شناسایی) و کاهش ارتکاب جرایم سایبری وجود دارد. به عبارت دیگر پیشگیری مبتنی بر گشت فضای مجازی و کنترل (شناسایی) بر کاهش ارتکاب جرایم سایبری تأثیرگذار است.

جدول ۴: نتایج آزمونT تک نمونه برای پیشگیری مبتنی بر جمع آوری ادلهٔ الکترونیکی جرم

عنوان	میانگین	تفاوت میانگین	dF	T	Sig
پیشگیری مبتنی بر جمع آوری ادلهٔ الکترونیکی جرم در محیط اینترنت	۴/۲۸	۰/۲۸	۵۶	۴/۳۱	۰/۰۰۲

مطابق جدول ۴، T حاصل از تجزیه و تحلیل داده ها بزرگ‌تر از T جدول(۱/۹۶) و از طرفی Sig= ۰/۰۰۲ است. بنابراین فرضیه چهارم تأیید می‌شود و نتیجه می‌گیریم رابطهٔ معناداری بین پیشگیری مبتنی بر جمع آوری ادلهٔ الکترونیکی جرم در محیط اینترنت وکاهش ارتکاب جرایم سایبری وجود دارد.

جدول شماره۵: نتایج آزمونT تک نمونه برای پیشگیری مبتنی بر مستند سازی صحنهٔ جرم

عنوان	میانگین	تفاوت میانگین	dF	T	Sig
پیشگیری مبتنی بر مستند سازی صحنه جرم در محیط اینترنت	۴/۲۸	۰/۲۸	۵۶	۶/۴۳	۰/۰۰۲

مطابق جدول ۵، T حاصل از تجزیه و تحلیل داده ها بزرگ‌تر از T جدول(۱/۹۶) و از طرفی Sig= ۰/۰۰۲ است. بنابراین فرضیه پنجم تأیید می شود و نتیجه می‌گیریم رابطهٔ معنا داری بین پیشگیری مبتنی بر مستند سازی صحنهٔ جرم در محیط اینترنت وکاهش ارتکاب جرایم سایبری وجود دارد. به عبارت دیگر پیشگیری مبتنی بر مستند سازی صحنهٔ جرم در محیط اینترنت بر کاهش ارتکاب جرایم سایبری تأثیر دارد.

نتیجه‌گیری

فناوری اطلاعات این ظرفیت را دارد که در ابعاد مختلف پیشگیری وضعی از جرایم سایبری تأثیر گذار باشد. بنابراین از آنجا که استفاده از آن می تواند با ابزار کنترلی که فراهم می سازد از ارتکاب جرایم سایبری پیشگیری کند و با ابعاد نظارتی که دارد امکان شناسایی مجرمان سایبر را فراهم سازد. بنابراین زیر مجموعه پیشگیری وضعی تلقی می شود.

در این مقاله، ضمن بیان گسترش جرم در فضای مجازی به دلیل ویژگی های خاص آن، ابتدا به تبیین جرایم سایبر و ذکر نمونه هایی از آن پرداخته شد. آنگاه با

ارائه مفاهیم و دسته بندی پیشگیری از جرم، پیشگیری مبتنی بر فناوری اطلاعات به عنوان یک نوع پیشگیری وضعی مورد بررسی قرار گرفت. سپس راهکارهایی مبتنی بر فناوری اطلاعات شامل ردیابی هویت مجازی مهاجمین، گشت فضای مجازی، کنترل و نظارت بر فضای مجازی، جمع آوری ادلهٔ الکترونیکی جرم، مستند سازی صحنه جرم برای پیشگیری از جرایم سایبر احصاء شد. آنگاه با انتخاب جامعه کارشناسان مرتبط، و طراحی پرسش نامه بر مبنای راهکارهای احصاء شده، اعتبارسنجی راهکارها انجام شد. نتایج حاصل از تجزیه و تحلیل داده نشان داد که کلیهٔ فرضیه ها تأیید شدند. بنابراین پیشگیری مبتنی بر ردیابی نشانی هویت مجازی(مهاجم)، گشت فضای مجازی، کنترل و نظارت بر فضای مجازی و جمع آوری ادلهٔ الکترونیکی جرم در محیط اینترنت، مستند سازی صحنهٔ جرم در محیط اینترنت در کاهش ارتکاب جرایم سایبری تأثیر دارد.

مهم ترین نقش این تحقیق، احصای روش های پیشگیری از جرایم سایبری مبتنی بر فناوری اطلاعات و اعتبارسنجی روش ها از طریق اخذ نظر کارشناسان مرتبط است که در نوع خود بی نظیر می‌باشد. همان گونه که به تحقیقات مرتبط اشاره شد، با وجود ارائه پیشنهادهایی برای پیشگیری از جرایم سایبری، هیچ گونه اعتبارسنجی برای روش های پیشنهاد شده، انجام نشده است.

پیشنهادها

- از پیشگیری مبتنی بر ردیابی هویت مجازی برای ردیابی مهاجمان، مجرمان و کلاهبرداران فضای مجازی استفاده شود تا عرصهٔ فعالیت های مجرمانه برای آنها تنگ شود.

- با کنترل و نظارت بر فضای مجازی از طرق مختلف از جمله کنترل و نظارت بر ارائه دهندگان سرویس های اینترنتی و کنترل و نظارت بر شبکه های ارتباطی، از ارتکاب جرایم در این مراکز پیشگیری شود.

- با بهره گیری از گشت فضای مجازی هر گونه فعالیت و حرکت های مسئله دار شناسایی و مورد پیگیری قرار گیرد. انجام مؤثر این شیوه، منوط به طراحی و پیاده سازی نرم افزارهای مناسب برای خودکارسازی آن است.

- جمع آوری ادلهٔ الکترونیکی جرم در محیط اینترنت و کلیهٔ مکان هایی کـه جـرایم سایبری به وقوع می پیوندد، از بعد شناسایی اقدامات مجرمانهٔ مشابه آتی و شناسـایی مجرم یا ردپای او و بهره گیری از تجزیه و تحلیل‌هـای فنـی، بررسـی ادلـهٔ دیجیتـال حاصل از حفظ آثار و جمع‌آوری مدارک موجـود در صـحنهٔ جـرم درکـاهش ارتکـاب جرایم سایبری تأثیر گذار است.

- پیشگیری مبتنی بر مستند سازی صحنهٔ جرم در محیط اینترنـت از نظـر مـواردی مانند شناسایی اقـدامات مجرمانـهٔ مشـابه آتـی و ایجـاد بانـک اطلاعـاتی مجرمـان و شگردهای مجرمانهٔ فضای مجازی در کاهش ارتکاب جرایم سایبری تأثیر گذار است.

منابع

- ابراهیم پور کومله، سمیرا (۱۳۹۱). **آسیب های نوپدید شبکه هـای اجتمـاعی مجازی در کمین خانوادهٔ ایرانی**، نخستین کنگـرهٔ فضـای مجـازی و آسـیب هـای اجتماعی نوپدید.

- گرکی، مـارکو(۱۳۸۹). **جرایم سایبری: راهنمایی بـرای کشـورهای در حـال توسعه**، ترجمه: مرتضی اکبری، تهران: پلیس فضای تولید و تبادل اطلاعات(فتا).

- بیات، بهرام؛ شرافتی پور، جعفر و عبدی، نرگس (۱۳۸۷). **پیشگیری از جـرم بـا تکیه بر رویکرد اجتماع محور**، تهران: معاونت اجتماعی ناجا

- پلیس فتا (۱۳۹۲). **مجموعهٔ مستندات آمار جرایم فضای سایبر**، تهران: پلیس فتا.

- تحیری، فـرزاد (۱۳۸۴). **دسترسی غیرمجاز به سیسـتم هـای رایانـه ای در حقوق ایران و اسناد بین المللی**، پایان نامهٔ کارشناسی ارشد، دانشگاه مفید.

- جلالی فراهانی، امیرحسین (۱۳۸۴). پیشـگیری وضـعی از جـرایم سـایبر در پرتـو موازین حقوق بشر، **مجلهٔ فقه و اصول**، سال دوم، شمارهٔ ششم، صص ۱۶۱-۱۳۳.

- جلالی، علی اکبر (۱۳۸۹). نظارت همگانی عامل پیشگیری جرایم در فضای مجازی، **فصلنامهٔ کارآگاه**، شمارهٔ ۱۲، صص ۳۰-۶.

- جلالی، علی اکبـر(۱۳۹۱). رفتـار شناسـی مجرمـان در فضـای سـایبر، **فصـلنامهٔ**

کارآگاه، دورهٔ دوم، سال ششم، شمارهٔ ۲۱.

- جوکز، یونی و همکاران (۱۳۸۹). **جرم و اینترنت**، ترجمه: رسول نجار، تهران: دانشگاه علوم انتظامی امین.

- حسنوی، رضا و فرسایی، داریوش (۱۳۷۹). **فرهنگ تشریحی کامپیوتر ماکروسافت ۲۰۰۰**، تهران: انتشارات دانشیار.

- درگاهی، حسین و رضوی، سید منصور(۱۳۸۶). اعتیاد به اینترنت و عوامل مؤثر بر آن در ساکنان منطقه ۲ غرب تهران، **فصلنامهٔ پایش**، سال ششم، شمارهٔ سوم، صص ۲۷۲-۲۶۵.

- دزیانی، محمد حسن (۱۳۸۹). **جرایم سایبری**، تهران: روزنامهٔ رسمی جمهوری اسلامی ایران.

- رجبی پور، محمود(۱۳۸۲). راهبرد پیشگیری اجتماعی از جرم (تعامل پلیس و دانش آموزان)، **فصلنامهٔ دانش انتظامی**، سال پنجم، شمارهٔ سوم، صص ۳۲-۷.

- زینالی، حمزه (۱۳۸۱). پیشگیری از بزهکاری و مدیریت آن در پرتو قوانین و مقررات جاری ایران، **فصلنامهٔ رفاه اجتماعی**، سال دوم، شمارهٔ ششم، صص ۱۲۴-۹۷.

- سازمان ملل(۱۳۷۶). **نشریهٔ بین المللی سیاست جنایی (ش ۴۳ و ۱۹۹۴/۴۴)**، ترجمه: دبیرخانهٔ شورای انفورماتیک، تهران: سازمان برنامه و بودجه.

- شریفی هولاسو، اسماعیل (۱۳۸۷). **جامعه شناسی**، پایان نامهٔ کارشناسی ارشد، دانشگاه تربیت مدرس.

- شیرزاد نیک آبادی، کامران (۱۳۷۶). **بررسی جرایم رایانه ای در قلمرو حقوق کیفری ایران و حقوق بین الملل**، پایان نامهٔ کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران مرکزی – مرکز تحصیلات تکمیلی حقوق.

- صدری، سید محمدرضا و کروبی، محمد تقی (۱۳۸۴). **ابعاد حقوقی محیط سایبر در پرتو توسعه ملی**، تهران: نشر بقعه.

- عاملی، الف، سعید رضا (۱۳۹۰). دو جهانی شدن ها و جامعهٔ جهانی اضطراب، **فصلنامهٔ علوم اجتماعی**،سال یازدهم، شمارهٔ اول، صص ۱۴۳- ۱۷۴.

- عاملی، ب، سید سعیدرضا (۱۳۹۰). **رویکرد دو فضایی به آسیب ها، جرایم، قوانین و سیاست های فضای مجازی**، تهران: موسسهٔ انتشارات امیرکبیر.
- عباچی، مریم (۱۳۸۷). مبانی و مقدمات تدوین برنامه ملی پیشگیری از جرم در ایران، **فصلنامهٔ مطالعات پیشگیری از جرم**، تحقیقات کاربردی پلیس پیشگیری ناجا، سال سوم، شمارهٔ نهم، صص ۷۲-۲۳.
- محمدی(۱۳۷۸). **گزارش نهایی طرح شناخت کلی جرایم رایانه ای و شیوه‌های مبارزه با آن**، تهران: نیروی انتظامی جمهوری اسلامی ایران.
- مالمیر، محمود و زررخ، احسان (۱۳۸۹). پیشگیری از بزه دیدگی سایبری، **فصلنامهٔ مطالعات پیشگیری از جرم**، تحقیقات کاربردی پلیس پیشگیری ناجا، سال پنجم، شمارهٔ هفدهم.
- نجفی ابرندآبادی، علی حسین (۱۳۸۱). **تقریرات درس جرم‌شناسی**، تهران: مجتمع آموزش عالی دانشگاه تهران.
- هیل، کریس (۲۰۰۲)، **جرایم سایبری، حقایق و آمار و ارقام در خصوص این بی تکلیفی جهانی**، مجلد ۱۸، قابل دسترس در سایت
http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37.
- Casey, E. (2000). Digital evidence and computer crime. London: Academic Press.
- Furnell, S. (2002). Cybercrime: Vandalizing the information society. London: Addison Wesley.