

توانمند سازی پلیس جهت امنیت در فضای مجازی

تاریخ پذیرش: ۹۵/۰۸/۰۲

تاریخ دریافت: ۹۵/۰۷/۱۳

قربانعلی حیدری منصورآباد^۱

مرتضی خلق نیک^۲

چکیده

امنیت به عنوان یکی از مهمترین پارامترهای ارزیابی یک جامعه شناخته میشود. در راستای ایجاد امنیت نقش پلیس بعنوان متولی نظم و امنیت در جامعه پررنگتر میشود. هدف اصلی در مقاله حاضر ارائه راهکار جهت توانمند سازی پلیس در فضای مجازی می باشد. در این مقاله ضمن بررسی نقش پلیس در توانمند سازی فضای مجازی با ارائه راهکارهایی جهت جلوگیری از آسیب های فضای مجازی میپردازیم در این تحقیق از روش پیمایشی استفاده شده است. جامعه آماری در این پژوهش دانشجویان می باشد. حجم نمونه ۱۰۰ نفر می باشد که برای انتخاب آنها از نمونه گیری تصادفی خوشه ای استفاده شده و با ابزار پرسشنامه اطلاعات جمع آوری گردید. نتایج نشان می دهد که بین فضای مجازی و آسیب های اجتماعی و همچنین وقوع وقوع جرم رابطه مستقیم وجود دارد.

کلید واژه: امنیت، فضای مجازی، آسیبهای اجتماعی، جرم

۱- رئیس دفتر تحقیقات کاربردی نیروی انتظامی استان کهگیلویه و بویراحمد(نویسنده مسئول)

۲- کارشناس ارشد برنامه ریزی شهری morteza.kholghnik@gmail.com

مقدمه

میل و اشتیاق به استفاده از رایانه و اینترنت و بهره مندی از مزایای، آن یک تمایل جهانی می باشد. این تمایل با سرعت قابل توجهی در حال افزایش است. اگر چه استفاده از اینترنت زمینه مشارکت جوامع را فراهم می سازد، اما در عین حال بدلیل ویژگی های خاص این فضا شرایط و بستر مساعدی برای ظهور آسیب های نوین را فراهم آورده است.

رشد بی سابقه و روز افزون فناوری اطلاعات و به تبع آن توسعه فضاهای مجازی افق جدیدی در مقابل دیدگان بشر امروز گشوده است و جامعه جدیدی به نام دنیای مجازی به وجود آمده است که همانند دنیای واقعی ویژگی و اقتضات یک جامعه را داراست.

گسترش فناوری اطلاعات و ارتباطات و دسترسی عموم مردم جامعه به اینترنت، باعث گردیده که این ابزار نه تنها در حد یک ابزار، نیازهای جامعه بشری را برطرف نماید؛ بلکه دنیای جدیدی به نام فضای سایبری را خلق نماید که با داشتن یک سلسله قابلیت های شگفت انگیز و منحصر به فرد بسیاری از موانع را نیز رفع گرداند. امروزه توسعه و گسترش علوم رایانه ای، گذشته از این که موجب بروز یک تحول یا انقلاب تکنولوژی در جهان گردید همزمان بستری مناسب برای جرایم سایبری شد.

شری تورکل در کتاب خود (زندگی بر صفحه نمایش، ۱۹۹۵: ۸۵) نشان می دهد که این کاربران نیستند که شیوه ی استفاده از فناوری جدید را انتخاب می کنند بلکه فناوری جدید شیوه ی خود را بر کاربران تحمیل می کند. مطالعات تورکل نشان می دهد ما در فضای مجازی وجوه جدیدی از خودمان را کشف می کنیم که در شرایط عینی به آن بی توجه هستیم. به اعتقاد تورکل، مهمترین تمایز فضای مجازی این است که شما می توانید ناشناس باقی بمانید، حتی می توانید جنسیت و سن خود را تغییر دهید.

بیان مساله

از ابتدای زندگی بشر امنیت یکی از دغدغه های اصلی انسان ها بوده است، امروزه با گسترش اینترنت و فضاهای شبکه ای در کشورمان لزوم امنیت برای فعالیت در این فضاهای مجازی بیش از پیش احساس می شود. برای ورود به دنیای مدرن و پیشرفت در همه زمینه ها ناگزیر از ورود به دنیای مجازی و استفاده از امکانات و قابلیت های این فضا می باشیم اما آنچه که در این میان حائز اهمیت می باشد تأمین امنیت می-

باشد. پلیس در هر جامعه، یکی از عناصر مهم و تاثیر گذار در تأمین امنیت است که به نظر می‌رسد که با وجود دنیای مجازی پلیس نیز وارد عرصه جدیدی از فعالیت های خود برای تأمین امنیت جامعه خواهد شد.

همگام با پیشرفت دنیای مجازی، جرم و بزهکاری نیز در این فضا توسعه یافته که عرصه را برای زندگی و کار در این فضا ناامن ساخته‌اند. همانطور که برای زندگی در دنیای واقعی امنیت یکی از ضرورت‌های زندگی بشمار می‌رود برای زندگی در فضای مجازی نیز نیازمند امنیت هستیم.

دامنه‌ی فعالیت پلیس سایبر، متناسب با گستره‌ی فضای سایبر، سرتاسر جهان است در صورتی که فعالیت پلیس‌های دنیای واقعی به یک منطقه‌ی جغرافیایی یعنی یک کشور محدود است.

اهمیت موضوع

در سال ۱۹۹۹، حدود ۲۶۰ میلیون نفر در سراسر جهان از اینترنت استفاده می کردند. در سال ۲۰۰۱ این تعداد به ۵۲۰ میلیون نفر رسید (Huey, ۲۰۰۲).

با توجه به اهمیت فضای مجازی در توسعه جوامع، در جامعه ما نیز در سال های اخیر به فن آوری اطلاعات و ارتباطات توجه زیادی شده است. ولی در این رابطه آسیب های جدی وجود دارد. کشور ما از نظر بهره مندی از اینترنت در بین ۱۸۷ کشور جهان رتبه ۱۸۷ را دارد که بر اساس طبقه بندی اتحادیه جهانی مخابرات جزء کشورهای متوسط به شمار می رود ۳۵ درصد استفاده کنندگان اینترنت را قشر جوان تشکیل می دهند و میانگین صرف شده برای اینترنت ۵۲ دقیقه در هفته است (صادقیان، ۱۳۸۴).

خسارت وارده در اثر جرایم فضای مجازی به مراتب گسترده تر و جبران ناپذیر تر در مقایسه با جرایم سنتی می باشد. در حال حاضر خسارت ناشی از جرم و جنایت کامپیوتری میلیاردها دلار در هر سال می باشد (Katyal, ۲۰۰۳).

گمنامی، بی چهرگی و بی نامی افراد در اینترنت نه تنها پیگرد قانونی جرم و مجرم را در فضای رایانه ای مشکل می سازد، بلکه زمینه گسترش آنها را نیز فراهم می آورد. عدم فشار های قانونی و حضور پلیس موجب می شود که عده ای از استفاده کنندگان اینترنت بر اساس هنجارهای لحظه ای عمل کنند. هنجارهای لحظه ای در واقع تفسیر دیگری از شرایط آنومیکی است که دورکیم از آن یاد می کند، شرایطی که می تواند زمینه ساز وقوع رفتارهای انحرافی و مجرمانه گردد. با توجه به اینکه تعریف واحد و مشخصی از جرایم اینترنتی وجود ندارد و تمایز میان طبیعی و انحرافی مبهم و

مخدوش است، واکنش‌های اجتماعی از جمله واکنش کسانی که قانون را به اجرا در می‌آورند، نامعلوم و نامشخص است. به عبارت دیگر، به نظر می‌رسد که سیستم‌های قانونی هنوز آمادگی برخورد با جرایمی را که در فضای رایانه‌ای اتفاق می‌افتد، ندارند (صادقی، ۱۳۸۷: ۹۴).

ویژگی‌های فضای مجازی همانند بی‌چهرگی و عدم کنترل در فضای سایبر و تفاوت زمانی و مکانی بین فضای آنلاین و آف‌لاین فضای مناسبی را برای مجرمان فراهم می‌سازد این مسئله کشف جرم و یافتن مجرمان را سخت‌تر میکند از طرف دیگر قوانین محکمی که این جرایم را کنترل کند بسیار محدود می‌باشد و یا با مشکل اجرایی برخورد می‌کند زیرا نمی‌توان از تعاریف قانون جرایم عادی و عمومی برای جرایم سایبر استفاده نمود و این امر کنترل جرایم سایبر را مشکل‌کرد و آنرا به مسئله‌ای بزرگ برای جامعه بشری تبدیل کرده است زیرا روزه روز بر میزان جرایم سایبر افزوده می‌شود و بسیاری از شبکه‌ها و افراد از تهدیدات مجرمان در امان نمی‌باشند.

در نتیجه برای مبارزه با جرایم سایبر، باید همگام با پیشرفت و توسعه کشور در زمینه فن‌آوری اطلاعات برای مبارزه با تهدیدات و خطرات ناشی از آن برنامه‌ریزی کرد و باید قوانین کیفری را بر اساس شرایط اقتصادی، فرهنگی، اجتماعی، سیاسی و حقوقی کشور به روز کرد تا مجرمان سایبر به راحتی از دست قانون نگریزند.

اهداف تحقیق:

ارتباط نقش پلیس در توانمندسازی فضای مجازی

ارتباط بین امنیت و میزان وقوع جرم

فرضیه‌های تحقیق

۱- به نظر می‌رسد بین فضای مجازی و میزان وقوع جرایم مجازی رابطه وجود دارد.

۲- به نظر می‌رسد بین فضای مجازی و آسیب‌های اجتماعی رابطه وجود دارد.

روش تحقیق

با توجه به موضوع مورد بررسی، روش انجام این تحقیق در بخش نظری، کتابخانه‌ای و در بخش عملی، پیمایشی می‌باشد. واحد تحلیل در این تحقیق، فرد است جامعه آماری در این تحقیق دانشجویان می‌باشد که با استفاده از فرمول کوکران ۱۰۰ نفر انتخاب شدند. بعد از مشخص شدن نمونه آماری برای انتخاب نمونه از جامعه آماری از روش خوشه استفاده شد.

تعریف مفاهیم

فضای سایبر

سایبر در زبان انگلیسی پیشوند و در زبان فارسی پسوندی است که به کلمات جدید و امروزی متصل می شود تا به آنها معنا و مفهوم دهد به گونه ای که مرتبط با فضای رایانه یا برخط باشد. در ترجمه فارسی این لغت معمولاً سه اصطلاح رایانه ای، سایبری و آنلاین به کار برده می شود؛ مثلاً دنیای مجازی آنلاین، بزه های رایانه ای یا سایبری یا پول رایانه ای» از حیث اصطلاحی فضای سایبر به مجموعه محیط‌هایی هم‌چون اینترنت گفته می‌شود که اشخاص در آنها از طریق رایانه‌هایی متصل به هم با یکدیگر ارتباط برقرار می‌کنند.» (پاکزاد، ۱۳۹۰: ۴۱).

در تعریف دیگر آمده که فضای سایبری عبارتست از محیط ساخته شده ذهنی، مصنوعی و مجازی یا فضای مفهومی که با کاربرد رایانه توسعه یافته است بنابراین فضای سایبر همان فضای بیکرانی است که از طریق اتصال شبکه های رایانه ای به وجود آمده است برخلاف فضای واقعی، در فضای سایبر نیاز به جابجایی فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یا حرکات ماوس صورت می گیرد. (پاکزاد، ۱۳۹۰: ۴۱).

جرایم رایانه ای و جرایم سایبری

نشانه‌گر فعالیت‌های غیرقانونی و خلافکارانه مبتنی بر رایانه‌های است که از (cybercrime) مفهوم جرم رایانه‌های طریق کاربرد شبکه جهانی آزاد و تکنولوژی اطلاعات و ارتباطات ناشی می‌شود. اینجرائم فقط رایانه را شامل نمی‌شود بلکه با فعالیتهایی مرتبط می‌شوند که از طریق تکنولوژی اطلاعات صورت می‌گیرند. (محسنی، ۱۳۸۶: ۲۲۳).

اینترنت در کنار کاربردهای فراوانی که دارد، دارای یک کاربرد و قابلیت اساسی است و آن ایجاد یک دنیای مجازی در کنار دنیای واقعی است و طبیعی است که یک سری جرایمی نیز در این محیط رخ می دهد. بنابراین جرایم سایبری را می توان زیر مجموعه ای از جرایم اینترنتی و به تبع آن زیر مجموعه ای از جرایم رایانه ای قلمداد کرد. نسل سوم جرایم رایانه ای را به طور خاص، جرایم سایبر نامیده اند.

البته به سبب آن که در حال حاضر اهم جرایم رایانه ای را جرایم سایبری تشکیل می دهند می توان آن را معادل جرایم رایانه ای در مفهوم عام قلمداد کرد. (جاوید نیا، ۱۳۸۷: ۱۲۸).

یک گونه شناسی از جرایم رایانه ای چهار نوع از جرایم رایانه ای را شناسایی می کند

گونه یکم: رایانه به عنوان هدف: این نوع جرم زمانی ارتکاب می یابد که آن عمل مانع کاربر قانونی از دریافت خدمات شود. این نوع از جرایم شامل سرقت اطلاعات، سرقت آثار ادبی و نیز شامل تخریب اطلاعات، داده ها یا اختلال در سیستم ها باشد.

گونه دوم: رایانه به عنوان ابزار جرم: مثلاً رایانه می تواند برای ارتکاب جرایمی مثل انتشار محتویات غیر قانونی، جرایم علیه اشخاص، جمع آوری اطلاعات سری و ... مورد استفاده قرار گیرد.

گونه سوم: رایانه برای تسهیل ارتکاب جرم: این رده از جرایم زمانی وقوع می یابد که در طرح یا رویداد مجرمانه از رایانه برای سهولت در ابقاء اثر دادو سندهای جنایی استفاده می شود. جرائمی مانند پول شویی و هرزه نگاری کودک نمونه هایی از این نوع جرایم هستند.

گونه چهارم: جرائم مربوط به حق تکثیر رایانه ای: این رده از جرائم حاوی مسائل مربوط به سرقت آثار ادبی یا هنری، مثل تخطی از حقوق کپی برداری نرم افزارهای رایانه ای و سوء استفاده های دیگر از خدمات الکترونیکی همچون سیستم تلفن است. برخی نیز برای جرم سایبری سه گونه پیش بینی کرده اند:

۱- رایانه به عنوان هدف یا موضوع جرم مانند سرقت اموال معنوی، سرقت اطلاعات تجاری، اخاذی اطلاعات

۲- رایانه به عنوان وسیله جرم مانند کلاهبرداری رایانه ای و پول شویی

۳- رایانه به عنوان مداخله گر در ارتکاب جرم. (پاکزاد، ۱۳۹۰: ۱۱۰).

انواع جرایم سایبر

هک و فعالیت های مرتبط با آن در تصور عمومی مردم و جوامع هک یا نفوذگری همان از میان رفتن یک وب سایت و اطلاعات موجود در آن است. هکرها خود دو نوع هستند:

۱- هکرها.

۲- کرکرها.

هکرها

کارهایی که هکرها انجام می دهند معمولاً از روی بدخواهی نیست. انگیزه بیشتر هکرها برای این کار، تمایل شدید به یادگیری نحوه کار سیستم رایانه، یافتن راهی برای ورود مخفیانه به آنها و پیدا کردن سوراخ های امنیتی این سیستم ها است. در

دهه ۱۹۷۰ واژه هکر به شخصی اطلاق می شد که در برنامه نویسی بسیار ماهر باشد. بعدها در دهه ۱۹۸۰ این واژه به معنی شخصی بود که در نفوذ به سیستم های جدید به صورت ناشناس تبحر داشته باشد. اما امروزه این واژه مفهوم یک جرم را می رساند.

کرکرها

کرکرها ، هکریایی بدخواه هستند . آنها به سیستم ها رخنه می کنند تا خرابکاری کنند، ویروس ها و کرم های رایانه ای را منتشر کنند ، فایل ها را پاک کنند یا بعضی انواع دیگر ویرانی را بار آورند . اختلاس ، کلاهبرداری یا جاسوسی صنعتی (سرقت و اطلاعات محرمانه یک شرکت) تنها بخش کوچکی از اهداف احتمالی کرکرها می باشد.

پرویزی عنوان می کند: " در هر جا که سیستم یا شبکه رایانه ای وجود داشته باشد ، هکرها نیز وجود خواهند داشت . شاید فقدان قوانین جزایی مرتبط با این جرایم و فقدان سیاست جزایی مناسب در یک جامعه و عدم توجه به اهمیت و امنیت سیستم ها و شبکه های رایانه ای و نادیده گرفتن اقدامات پیشگیرانه زمینه ساز رشد هکرها باشد . نفوذ گری به معنای خاص و قانونی آن ذاتاً جرایمی مثل ورود غیر مجاز و ورود به عنف امکان سنخیت بیشتری دارد". (طهماسبی، ۱۳۸۳: ۱۲۸).

فیشینگ

عبارت است از تلاش برای بدست آوردن اطلاعاتی مانند رمز عبور، شناسه عبور، جزئیات کارت اعتباری با جازدن خود به عنوان یک منبع قابل اعتماد. فیشینگ از طریق سرویس های پست الکترونیکی یا با وعده های دروغ انجام می گیرد یا با ایجاد برخی جذابیت ها کاربران اینترنتی را ترغیب می کنند اطلاعات خود را در سایت هایی که توسط کلاهبرداران ساخته شده است وارد کنند . این خلافکاران معمولاً وب سایت هایی طراحی میکنند که در کاربر احساس اعتماد و وارد شدن در یک سایت امن را می دهد و معمولاً هم موفق می شوند یعنی کاربر در دام آنها افتاده و اطلاعات خود را وارد می کند

ویروس های کامپیوتری

دسته ویروس های کامپیوتری (شامل ویروس ها ، کرم ها ، نرم افزارهای جاسوسی و ...) در حقیقت نرم افزارهایی هستند که خود را تکثیر و منتشر می کنند و کامپیوترهای موجود در یک شبکه را بدون اطلاع کاربران آلوده کرده و به آنها صدمه

می زند. ویروس ها از طریق فایل های سیستم یک شبکه کامپیوتری، اینترنت یا هر وسیله نقل و انتقال اطلاعات مانند فلش، سی دی و ... وارد کامپیوترهای دیگر می شوند.

ویروس های کامپیوتری کدهایی هستند که با هدف ضربه زدن به یک سیستم رایانه ای یا از بین بردن اطلاعات نوشته شده اند. نوشتن ویروس های کامپیوتری در همه جای دنیا یک جرم است به گونه ای که نویسنده ویروس در برابر تمام خسارت های وارده به همه کامپیوترهای آلوده شده مسئول است.

شنود غیر قانونی

شنود غیر قانونی از جمله جرایم مهم کامپیوتری است که به دلیل اهمیت آن در کنوانسیون اروپایی سایبر جرایم، توصیه نامه پدیده های الکترونیکی است که AIDP توصیه نامه، OECD اینترپل و ... ذکر شده است شنود معادل استراق سمع به صورت شنیداری و در مخابرات **Interception** با استراق سمع تفاوت دارد و (مکالمات تلفنی) صورت می گیرد. اما شنود کامپیوتری به صورت دسترسی به داده ها و توقف انتقال داده ها صورت می گیرد که خاص محیط سایبر است. (طهماسبی، ۱۳۸۳: ۸).

پورنوگرافی

«هر نمایشی که به واسطه آن یک کودک را واقعاً یا به طور شبیه سازی به فعالیت صریح جنسی یا هر نمایش» اعضای جنسی کودک تشویق می کند» (حسینی، ۱۳۸۳: ۱۰۱).

پورنوگرافی یا هرزه نگاری به کتاب ها، نشریات، فیلم ها و ... گفته می شود که بدون داشتن ارزش هنری، صرفاً به شرح و یا نمایش اعمال جنسی و یا افراد برهنه به گونه ای می پردازد که موجب تحریک جنسی شوند.

هرزه نگاری در بیشتر کشورها از جمله ایران ممنوع است. همچنین هرزه نگاری کودکان به موجب پروتکل کنوانسیون حقوق کودک منع شده است و بسیاری از کشورها از جمله ایران به این پروتکل پیوسته اند.

لاسر می گوید " اینترنت به خاطر داشتن سه ویژگی، مهمترین منبع اشاعه هرزه نگاری است. این سه ویژگی عبارتند از:

۱- قابلیت دسترسی آسان کاربران به آن

۲- توانایی پرداخت بهای آن در سایت هایی که استفاده از آنها مستلزم پرداخت پول است.

۳- ناشناس ماندن مصرف کنندگان آن. (پورخاتون، ۱۳۸۴: ۲۵).

کلاهبرداری رایانه ای

کلاهبرداری یکی از مهم ترین جرایم علیه اموال و مالکیت می باشد که برخی از آن به عنوان بحران قرن بیستم نام برده اند. کلاهبرداری رایانه ای همانند کلاهبرداری سنتی جرمی مقید به حصول نتیجه مجرمانه است و باید به واسطه سوء استفاده از رایانه از طریق افعالی نظیر ایجاد، محو، توقف داده و یا اختلال در سیستم رایانه ای، مال یا منفعت یا مزایای مالی عاید مرتکب شود. در حقوق کیفری رایانه ای همانند حقوق کیفری سنتی، سوءاستفاده از نرم افزارهای رایانه ای برای تحصیل مال یا منفعت یا مزایای مالی وجه تمایز بین کلاهبرداری رایانه ای از سایر جرایم مشابه است.

انتشار اسرار خصوصی و محتویات خانوادگی

هر کس به وسیله سیستم های رایانه ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، جرم شناخته می شود. (قانون جرایم رایانه ای، ماده ۱۷).

مبانی نظری تحقیق

تئوری آنومی دورکیم

مفهوم آنومی توسط جامعه شناسان متقدم به کار برده شد که توصیف کننده تغییرات در فرایندهای جامعه به وسیله انقلاب صنعتی بوده است. دورکیم برای اولین بار مفهوم آنومی را در تئوری های جامعه شناختی مطرح کرده است. دورکیم بیشترین بحث از این مفهوم را در کتاب خودکشی مطرح کرده است. همچنین در کتاب تقسیم کار در جامعه، دورکیم آنومی را به عنوان نتیجه ای از یک تقسیم کار غیر منصفانه در جوامع تعریف کرده است و چنین نابرابری را سبب انحلال و فقدان قوانین و هنجارها در جامعه معرفی می کند که در نتیجه، تضاد طبقاتی را در جامعه به دنبال دارد. در کتاب خودکشی، دورکیم آنومی را به عنوان نتیجه تغییر اقتصادی و اجتماعی سریع توصیف می کند که موجب وقوع نوعی از خودکشی آنومیک می شود.

دورکیم خصیصه ای چون بی سازمانی قاعده ای را شرایط آنومیک توصیف می کند و دقیقاً آنومی را به معنای بی هنجاری نمی داند و معتقد است که آنومی به یک موقعیت مرتبط با بی قاعدگی هنجاری نسبی اشاره دارد.

در مقایسه ویژگیهای اجتماعات به وسیله همبستگی مکانیکی، شهرهای بزرگ توسعه می یابند و شهرها کمتر ساختارمند و کمتر قاعده مند می شوند در این صورت از نظر دورکیم مردم در شرایط بی هنجاری نمی دانند چه توقعی داشته باشند و یا چگونه رفتار کنند. در تعدادی از مسائل اجتماعی که دورکیم در تغییرات سریع صنعتی شدن اروپا نام برده به عنوان تنظیمات قاعده ای ناکافی، که یکی از آنها خودکشی آنومیک می باشد. دورکیم معتقد است، وقتی که هنجارها و ارزشهای جامعه یا گروه باید دارای معنی بوده و خدماتی را برای افراد فراهم کنند در حالی که متوقف می شوند افراد به احساسی از انزوا و سردرگمی و ناامیدی می رسند و خودکشی آنومیک اتفاق می افتد. (سجادی، ۱۳۸۷: ۷۹).

آنومی برای دورکیم، معانی مشابه ای دارد که شکست در درونی کردن هنجارهای جامعه، عدم توانایی در سازگاری با هنجارهای در حال تغییر یا حتی تنش حاصل از تضاد در هنجارها.

از نظر دورکیم گرایشات اجتماعی جدید در جوامع شهری - صنعتی نتیجه تغییر هنجارها، اختلال و دست کم گرفتن کنترل اجتماعی فرد است. افزایش جمعیت، ایجاد شیوه های جدید زندگی و احتمالاً آزادی بیشتری به افراد داده می شود. اما همچنان احتمال رفتار منحرف بیشتر می شود. (روزبهانی، ۱۳۷۸: ۴۸).

صرف نظر از ویژگیهای فردی افراد همچون وجدان اخلاقی و اعتقادات شخصی، ویژگیهای دو فضا یعنی فضای سایبر و عالم واقع در قاعده مند سازی رفتار افراد تاثیر گذار می باشند و تاثیرات متفاوت بر جای می گذارند.

وجود پلیس و قوانین متقن در عالم واقع به عنوان عوامل کنترلی و بازدارنده عمل می کنند همچنین مقید بودن انسان در مکان و زمان در جهان واقعی و اینکه مهارتها و فعالیتهای انسان وابسته به مکان می باشند. هم اینکه افراد در زمان واقعی زندگی می کنند از دیگر ویژگیهای عالم واقع است که شرایط قاعده مند سازی افراد را موجب می شود و نیز تعامل چهره به چهره انسانها در جهان واقعی و یا شناخته شدن و ترس از طرد اجتماعی و تحت تعقیب قانون قرار گرفتن نیز از جمله عواملی است که افراد را به رعایت هنجارها سوق می دهد.

در نتیجه عواملی چون بی زمانی و بی مکانی در فضای سایبر و گمنامی و بی چهرگی و ناشناس ماندن و نبود نیروهای کنترل موجب وقوع شرایط آنومیک در این فضا می شوند.

از سویی دیگر، چون فضای سایبر متفاوت از عالم واقع می باشد پس هنجارها و قواعد حاکم بر آن نیز متفاوت با عالم واقع می باشد و کاربران در این فضا نیازمند یادگیری قواعد و هنجارهای حاکم بر آن می باشند در صورتی که کاربران بدون فراگیری قواعد و هنجارهای فضای سایبر و بدون فراگیری حقوق و تکالیف در فضای سایبر به یک کاربر حرفه ای تبدیل می شوند.

این موقعیت ها از نشانه های شرایط آنومیک در فضای سایبر می باشند. زیرا افراد باید ابتدا آموزش ببینند تا از فرصت ها و آزادی های این فضاء سوءاستفاده نکنند.

زمان و مکان از دیدگاه گیدنز

زمان و مکان در نظریه گیدنز، متغیرهای تعیین کننده ایاند. در جوامع ماقبل مدرن، زمان و مکان به نحو غیرقابل تفکیکی بر هم منطبق بودند. محاسبه ی زمان همانند اختراع خط، مربوط به جوامع کشاورزی است. محاسبه ی زمان با شاخص های اجتماعی-مکانی ورخدادهای منظم طبیعی امکان پذیر بود. همچنین محاسبه زمان با مکان در ارتباط بود و همی ن ارتباط، عدم یکنواختی و آشفتگی زمانی را نه تنها در میان ممالک گوناگون سبب می شد که در نقاط مختلف یک سرزمین نیز اختلاف زمانی وجود داشت. اختراع ساعت مکانیکی که سابقه ی آن به اواخر قرن هیجدهم برمی گردد به تفکیک زمان از مکان کمک کرد. این تفکیک که هنوز در سطح سازمانهای اجتماعی صورت نگرفته بود مصادف شد با گسترش مدرنیته. تقویم ها در سطح جهان یکدست و استاندارد شد و امروز شاهد به کارگیری سیستم زمانی واحد هستیم. اگر چه بسیاری از کشورها سال نوهای مختلف دارند اما همگی از چارچوب زمان یابی واحد پیروی می کنند.

می خواهم این ادعا را طرح کنم که اکثر اشکال مختلف نظریه های اجتماعی در توجه : «گیدنز اظهار میدارد جدی و کافی به زمانمند بودن رفتار اجتماعی و صفات فضایی آن ناکام مانده اند. در وهله اول، هیچ چیز مبتذلتر و غیر آموزشیتز از این ادعا نیست که بگوییم فعالیتهای اجتماعی در زمان و مکان رخ میدهند. نه زمان و نه مکان، هیچکدام در مرکز نظریه های اجتماعی قرار ندارند، بلکه به آنها صرفاً به مثابه محیط-هایی نگاه میشود که رفتارهای اجتماعی در آن به وقوع می پیوندند. نادیده گرفتن

مکان در نظریه‌پردازی‌های اجتماعی تاحدی ریشه در اشتیاق جامعه‌شناسان به دور کردن خود از انگ جبرگرایی جغرافیایی داشته است. حتی ورود اکولوژی به علوم اجتماعی نیز نتوانسته است کمک چندانی به موضوع کند، چون هم ویژگی‌های فضایی را با سایر ویژگی‌های جهان فیزیکی که می‌تواند زندگی اجتماعی را تحت‌تاثیر قرار دهد خلط کرده است و هم اینکه ویژگی‌های (افروغ، ۱۳۷۷: ۶۶) فضایی را به مثابه محیط فعالیت‌های اجتماعی و نه به مثابه عنصر لاینفک وقوع آن می‌نگرد

نظریه اجتماعی باید به تقاطع‌های زمانی - مکانی که اساساً در تمام هستی اجتماعی: همچنین عقیده دارد که وجود دارد و تاکنون به آن عنایت نشده، توجه داشته باشد. فعالیت‌های اجتماعی همیشه از سه عنصر متفاوت و «مقاطع زمانی، فضایی و پارادایمی تشکیل شده است و تمام اعمال اجتماعی در یکی از این ابعاد قرار می‌گیرد (همان: ۶۱) ویژگی فضای سایبر که بی‌چهرگی و گمنامی است فضای اجتماعات مجازی را متفاوت از اجتماعات در عالم واقع می‌سازد و زمینه‌های برقراری ارتباطات بدون ترس از شناخته شدن را فراهم می‌سازد. تحقیقات نشان می‌دهد که یکی از دلایل عمده گرایش مردم به جرایم اینترنتی گمنامی آنها در محیط‌های با واسطه (Lipson, 2002, Williams, 2002) کامپیوتر می‌باشد.

ویژگی اجتماعات مجازی را از اجتماعات واقعی جدا می‌سازد ولی به هرحال قرار گرفتن در شرایط گروه خاص زمینه‌های بدست آوردن اطلاعات و دانش جدید و یا مهارت‌های جدید چه در جهت مثبت و یا منفی را برای افراد فراهم می‌آورد. در نظریه ساترلند قرار گرفتن در حلقه روابط گروه‌های صمیمی زمینه یادگیری را فراهم می‌آورد. اگر یک اجتماع مجازی را همانند حلقه روابط درون گروه‌های صمیمی در نظر بگیریم زمینه‌های یادگیری و ردو بدل شدن تجارب را فراهم می‌آورد.

در فضای سایبر شرایط قاعده مند سازی افراد متفاوت می‌باشد. زیرا عوامل کنترلی همچون نیروی پلیس و قدرت متمرکزی در این فضا وجود ندارد و تعامل بین افراد با بی‌چهرگی و گمنامی اتفاق می‌افتد که ناشناسی را «عده‌ای از کاربران در این با خود به همراه دارد. همه این عوامل شرایطی را موجب می‌شوند که ممکن است فضا بر اساس هنجارهای لحظه‌ای عمل کنند که در واقع تفسیر گری از شرایط آنومیک می‌باشد.» (صادقی، ۱۳۸۷: ۹۴).

پیشینه تحقیق:

- کشتی ارای و اکبریان (۱۳۹۰) با معرفی عصر جدید به عنوان عصر پرشتاب ارتباطات، ورود بسیار ساده و سریع، حداقل محدودیت برای دسترسی، برقراری ارتباط با سراسر دنیا به اشکال مختلف و عدم وجود محدودیت زمانی و مکانی، دسترسی به پایگاه های اطلاعاتی مختلف و شرکت در فعالیت های اقتصادی، علمی، فرهنگی، هنری، مذهبی و را از ویژگی های بی بدیل آن بر شمرده اند.

- یاسمی نژاد، آزادی و اموی (۱۳۹۰) در پژوهش خود به این نتیجه دست یافتند که فضای مجازی می تواند امنیت اجتماعی را مورد تهدید قرار دهد، زیرا اینترنت با وجود این که می تواند به عنوان ابزاری قدرتمند در عرصه اطلاع رسانی به کار گرفته شود تا آن جا که گاهی از آن به عنوان انفجار اطلاعات هم نام برده می شود، ولی این فناوری مدرن با تمام فوایدی که دارد، تهدیدها و خطرهایی نیز برای جامعه و بشر داشته است. به طوری که امروزه، بخش عمده ای از جرایم مربوط به حوزه ی کامپیوتر، اینترنت و فضای مجازی است که امنیت اجتماعی را هدف قرار داده اند.

- ابری (۱۳۸۷) نقش مثبت فضای مجازی را در عرصه ی ظهور خلاقیت مورد تأکید قرار داده است، زیرا فناوری دیجیتالی و جامعه ی شبکه ای، افراد را به سوی زندگی ای سوق داده است که در آن می توانند با اتخاذ نقشی فعال و خلاق، به صورت فردی یا جمعی در ساختن چیزی جدید سهیم باشند، در فرایند هم آفرینی شرکت کنند و به خودیابی خویشتن کمک کنند. کیفیت آزادی بخشی اینترنت، کاربران اینترنتی را دعوت می کند تا به تفکر، تجربه، بازی، فعالیت های گروهی و ارتباط بپردازند. اینترنت همواره محیطی را خلق کرده است که همگان می توانند با تکیه بر توانایی ها و استعداد های خود دست به ابداع و خلاقیت بزنند. از میان رفتن محدودیت مکان، زمان، نبود کنترل و انتقاد، ناشناس ماندن، امکان خیال پردازی و تنوع گوناگون محیط های اینترنتی فرصت مناسبی را برای بروز خلاقیت فراهم می کند.

دو فضایی شدن آسیب ها و ناهنجاری های فضای مجازی: مطالعه تطبیقی سیاستگذاری های بین المللی عنوان پژوهشی است که عاملی و حسنی (۱۳۹۱) انجام داده اند. در این مقاله تحت پارادایم دو فضایی شدن به به مفهوم سازی عمده ترین آسیب های فضای مجازی پرداخته شده و با مطالعه تطبیق سیاستگذاری ها در برخی کشورهای پیشرو، راهبردهای اتخاذ شده دسته بندی شده اند. نتایج این تحلیل تطبیقی نشان می دهد که سیاست ها و برنامه های فرهنگی و اجتماعی کشورها را می توان به سیاست های سلبی

و ایجابی تقسیم کرد. سیاست های سلبی شامل سیاست ها و برنامه های حذف، کنترل و نظارت و سیاست های ایجابی فرهنگی و اجتماعی جوامع، برنامه ها و سیاست هایی معطوف به تولید محتوا، مدیریت محتوا، برنامه های دیجیتال سازی اطلاعات آنالوگ و دسترس پذیر ساختن اطلاعات و محتوا در شبکه اینترنت است.

ماهیت پلیس در ایران

تعریف لغوی و مفهوم پلیس: در بررسی فرهنگ لغات به ویژه فرهنگ های معتبر فارسی واژه پلیس مترادف با کلماتی نظیر نظم، پاسبان، شهربانی، آجان، کلانتری، ژاندارم و... آمده است که اکثر این واژه ها در گذر زمان و در طول تاریخ اهمیت خود را از دست داده اند.

واژه پلیس در فرهنگ فارسی این گونه تعریف شده است: سازمانی در داخل کشور که متصدی حفظ نظم و مالافراد است (رجبی، ۱۳۸۸: ۲۲)

اینترنت به عنوان شاهراه اطلاعاتی و با قدمت بیست ساله در جهان و سابقه ای حدود ۱۲-۱۰ ساله در کشورمان از آمار ۲۵۰۰۰ کاربر در سال ۲۰۰۰ به ۳۲ میلیون کاربر در سال ۲۰۰۹ رسیده است.

با پیشرفت کشورهای توسعه یافته، در فضای سایبر و وابستگی بی چون و چرای این کشورها به فناوری و اطلاعات روز دنیا و منسوخ و نابود شدن روش های سنتی در این کشورها ضرورت ایجاد پلیس سایبری از سالیان پیش احساس شده است و کشورهای توسعه یافته همزمان با پیدایش تکنولوژی های جدید نسبت به ایجاد این پلیس و وضع قوانین و مقررات توأمأ اقدام و با این تدبیر فعالیت مجرمین را سخت تر کرده اند. وجود انواع جرایم در فضای مجازی نشان دهنده این نکته است که جرایم سنتی، امروزه شکل جدیدی به خود گرفته و در دنیای مجازی ظاهر می شوند. با این تفاوت که شناخت و دستگیری مجرمین در دنیای مجازی بسیار دشوارتر از دنیای واقعی است. زیرا گمنامی و پنهان کردن هویت یکی از قابلیت های فضای مجازی است.

نیروی انتظامی با گسترش دامنه اطلاعات و توانایی های سخت افزاری و نرم افزاری خود و همچنین افزایش آگاهی و آموزش نیروی متخصص و کارآمد به عنوان پلیس الکترونیک، می تواند به پیشگیری از وقوع جرم، کشف جرایم اینترنتی و مجازی، و... اقدام نماید.

با آموزش صحیح و کارشناسانه در سطح جامعه می توان استفاده صحیح، کاربردی، علمی و مناسب از این دنیای مجازی ۱ را ترویج داد و تا حد امکان از ناهنجاریها و مخاطرات آن پرهیز نمود.

غفلت و نا آگاهی در نحوه استفاده از فناوری باعث بروز خسارات جبران نا پذیری خواهد شد. همانگونه که در دنیای حقیقی ۲ رعایت مقررات، موازین اخلاقی و حقوقی الزامی و ضروری است. این واقعیت نیز در دنیای مجازی و فناوری اطلاعات مصداق است و باید شناخته و رعایت شود تا سبب بروز خطا و ناهنجاری نشود. (پورنقدی: ۱۳۸۸، ۵۷)

پلیس سایبر ۳ در ایران

تاکنون قوه قضاییه برای آموزش قاضی هایی که بتوانند در حوزه جرایم رایانه ای به شکایت ها رسیدگی کنند، دوره های خاصی برگزار و دادگاه های جداگانه به نام دادگاه الکترونیک برپا کرده است. در همین زمینه پلیس نیز برای ایجاد امنیت بیشتر در این فضا و حضور پررنگ تر در این بخش، دست به اقداماتی از جمله راه اندازی گشت های اینترنتی زده است، اما گویا این اقدام نیز با توجه به این که هنوز عمر زیادی از آن نمی گذرد، نتوانسته به برقراری امنیت کامل در این فضا کمک کند بسیاری از کارشناسان معتقدند راه اندازی پلیس سایبر در ایران دیر اتفاق افتاده است، اما لایحه جرایم رایانه ای در سال ۱۳۸۲ به مجلس تقدیم شد و متأسفانه برای سال های زیادی مسکوت ماند، تا در نهایت در سال ۱۳۸۸ تصویب شد.

در واقع درباره آمار جرایم رایانه ای، مستندات، پرونده هایی است که بر اساس شکایت های اشخاص حقیقی و حقوقی تشکیل شده است و بدون شک تعداد واقعی جرایم اتفاق افتاده بیش از پرونده های موجود است. بر اساس پرونده های موجود بیش از ۵۰ درصد از شکایت ها به موضوع برداشت غیر مجاز از بانک ها باز می گردد و ۲۳ درصد از شکایت ها به بحث هتک حیثیت و ایجاد مزاحمت برای افراد و هم چنین نشر اکاذیب در اینترنت اختصاص دارد. ۱۰ درصد پرونده ها نیز مربوط به کلاهبرداری های مالی در اینترنت یا از طریق اینترنت است و ۷ درصد نیز شامل نفوذ غیر مجاز و هک سیستم های رایانه ای است.

امید است که با راه اندازی پلیس تخصصی، تمرکز بر روی این گونه جرایم بیشتر شود. به این دلیل که نیروهای به کار گرفته شده در این بخش باید علاوه بر تجربه های خدمتی از تجربه های فنی هم برخوردار باشند. در واقع هدف از راه اندازی پلیس

سایبری ایجاد امنیت بیشتر در فضای مجازی است. شایان ذکر است که بخش زیادی از تامین امنیت فضای سایبر به مردم باز می‌گردد و اگر افرادی که وارد این فضا می‌شوند به اندازه کافی احتیاط کنند، آسیب پذیری آنان کاهش می‌یابد. (شعاع کاظمی، ۱۳۹۰: ۹۶)

عصر بزرگراههای ارتباطی و گسترش فضای مجازی با همه امیدها برای تسریع و بهبود ارتباط انسان‌ها در سطوح محلی، ملی و بین‌المللی مدت‌هاست که از راه رسیده است. تکنولوژی‌های جدید ارتباطی و اطلاعاتی جنبش جهانی در حوزه ارتباطات و انتقال محتواها و پیام‌های ارتباطی در سزیه‌ترین زمان ممکن، به وجود آورده‌اند. در عین حال، همین تکنولوژی‌های جدید موجب تسهیل انجام اعمال خلاف قانون و رشد جرایم با استفاده از شیوه‌های جدیدتر شده‌اند. همان‌طور که در مورد تکنولوژی‌های دیگر هم صادق است، تکنولوژی ارتباطی جدید از یک طرف امکان بهبود روابط انسانی را افزایش داده، و از طرف دیگر تهدیدهای تازه‌ای برای آن فراهم کرده است. (راو‌داد، ۱۳۸۷: ۷۳)

هیچ‌جاى تعجب نیست که مجرمان اینترنتی در فضای مجازی مرتکب جرم شوند. عدم فشارهای قانونی و حضور پلیس موجب می‌شود که عده‌ای از استفاده‌کنندگان اینترنت براساس هنجارهای لحظه‌ای عمل کنند.

هنجارهای لحظه‌ای در واقع تفسیر دیگری از شرایط آنومیک است که دورکیم از آن یاد می‌کند، شرایطی که می‌تواند زمینه‌ساز وقوع رفتارهای انحرافی و مجرمانه گردد. گمنامی، بی‌چهرگی و بی‌نامی افراد در اینترنت نه تنها پیگرد قانونی جرم و مجرمان را در فضای رایانه‌ای مشکل می‌سازد، بلکه زمینه‌ساز آنها را نیز فراهم می‌آورد. (صادقی، ۱۳۸۷: ۹۴)

اشخاصی که در شرایط عادی زندگی، هیچ‌گونه تصویری از سرقت یا تجاوز به اموال دیگران ندارند، در مواجهه با فرصت‌ها و موقعیت‌های ارزشمندی که رایانه و اینترنت برای آن‌ها مهیا کرده، حتی لحظه‌ای دچار تردید، احساس گناه یا تزلزل در تصمیم‌گیری نخواهند شد.

شرط موفقیت هر سیاستی اهتمام به آموزش خانواده و آموزش کودکان و نوجوانان، تربیت نیروی انسانی متخصص در مقابله با این جرائم و در نهایت سازمان‌دهی جدید نیروی انتظامی و قوه قضاییه برای تاسیس پلیس سایبر و دادسرای جرائم سایبر است. رایانه و اینترنت ابزاری بسیار پیچیده می‌باشد و لازم است بدانیم، آنهایی که در

راستای خلاف مصالح بشر از آن استفاده می نمایند نیز افراد متخصص، فنی و نسبتاً باهوشی هستند که با رمز و رازهای تخصصی و فنی و امور پیچیده رایانه و اینترنت آشنا می باشند.

نیروی انتظامی و پلیس به عنوان حافظ نظم و امنیت در جامعه با حضور خود ضامن برقراری امنیت و آرامش خواهد شد. بنابراین نیاز جامعه به پلیس الکترونیک و آگاه به مسائل فناوری، محسوس و غیر قابل انکار است.

مراکز دخیل یا ذی نفوذ در امنیت فضای مجازی

به مقوله امنیت در فضای مجازی می توان از دیدگاه های مختلفی پرداخت می توان امنیت اخلاقی، فرهنگی، اقتصادی و یا حتی سیاسی را در آن بررسی نمود و یا از جنبه فنی به امنیت در فضای سایبر نگاه کرد. در این بخش سعی می کنیم که سازمان ها و نهادهایی که در امنیت فضای مجازی از جنبه های گوناگون دخیل هستند را به اختصار بررسی نماییم.

مجمع تشخیص مصلحت نظام

مجلس شورای اسلامی

وزارت ارتباطات و فناوری اطلاعات

وزارت کشور

وزارت علوم و تحقیقات و فناوری

وزارت آموزش و پرورش

حوزه های علمیه

صدا و سیما

وزارت فرهنگ و ارشاد اسلامی

سازمان تبلیغات اسلامی

قوه قضاییه

نیروی انتظامی

با توجه به گستره عملکرد و مسولیت نیروی انتظامی به عنوان سازمانی که مسولیت مستقیم برخورد با جرائم را بر عهده دارد با ظهور جامعه مجازی این مسولیت نیز بر عهده کارکنان مسولیت پذیر و ساعی این نهاد قرار داده شده که با آموزش و بکارگیری نیروهای متخصص و پلیس آگاه به فناوری های روز، همگام و هماهنگ با سایر سازمان

ها به خصوص قوه قضاییه نقش انکار ناپذیر خود را در پیشگیری و مقابله با تهدیدات و جرائم و همچنین در سالم سازی فضای مجازی ایفا کند. (هاتف، ۱۶۲:۱۳۸۷)

راهکارها:

به منظور پیشگیری و کاهش آسیب های اجتماعی در فضای مجازی راهکارهایی مطرح شده اند که در صورت اجرای به موقع و مناسب می توانند ثمر بخش واقع شوند: - با توجه به اینکه بیشتر استفاده کنندگان از فضای مجازی نوجوانان و جوانان هستند، فرهنگ سازی برای کاهش پیامدهای آن ضروری است. لذا اطلاع رسانی، آموزش نحوه استفاده صحیح از این فناوری می تواند مؤثر واقع گردد. - استفاده از ظرفیت هایی همچون رسانه های دیداری و شنیداری، روزنامه ها، مجلات، نشریات برای نهادینه شدن فرهنگ سایبری.

برگزاری جلسات آموزشی از سوی مصادر امور فرهنگی در شهرستان ها به منظور آشنا نمودن و اطلاع رسانی به والدین در مورد فناوری های جدید به ویژه اینترنت و شبکه های اجتماعی مجازی.

برگزاری کلاس های آموزشی در مدارس جهت آگاهی دادن به نوجوانان و جوانان در مورد مزایا و معایب فناوری های جدید و نحوه ی استفاده ی صحیح از آنها. تشویق به شرکت در فعالیت های اجتماعی و تقویت این گونه رفتارها توسط والدین. وضع قوانین سختگیرانه تر جهت برخورد با مجرمان جرایم اینترنتی و اجرایی نمودن این قوانین.

آگاهی و هوشیاری بیشتر پلیس سایبری در مورد انواع جدید جرایم رایانه ای و اقدام در جهت نا کارآمد کردن دسیسه های دشمنان در این زمینه.

پخش آگهی های آموزنده از سوی وزارت فرهنگ و ارشاد اسلامی در رادیو و تلویزیون در جهت افزایش آگاهی خانواده ها در خصوص خطرات ناشی از اینترنت.

گذراندن اوقات بیشتری با فرزندان در فضای بیرون از خانه به طوری که فرزندان از نظر عاطفی، احساس خلأ نکنند و جهت جبران این کمبود به فضای مجازی پناه نبرند. پخش برنامه های کوتاه آموزشی درباره مزایا و معایب اینترنت از زبان ورزشکاران و هنرمندان محبوبی که عموماً جوانان آنها را الگوی خود قرار می دهند.

طراحی بازی های رایانه ای به گونه ای که در آنها انواع خطرات موجود در فضای مجازی و راهکارهایی جهت آشنایی و مقابله با آنها تعبیه شده است.

طراحی و تدوین بخشی در کتاب های درسی در ارتباط با آشنایی دانش آموزان با فناوری های جدید، اینترنت و خطرات بالقوه آنها.

ساخت و پخش فیلم ها و سریال هایی با موضوع اینترنت و مزایا و معایب آن .
استفاده از آموزه های دینی از جمله امر به معروف و نهی از منکر به عنوان نوعی کنترل اجتماعی توسط هر شخص .

هنجارسازی های مثبت و ترویج فرهنگ استفاده از اینترنت و فضای مجازی .

نتیجه گیری:

ارتباط از طریق فضای مجازی در سال های اخیر جایگاه قابل توجهی در بین نسل جوان جامعه ما پیدا کرده است. شبکه های اجتماعی در ابعاد مختلف زندگی افراد (فردی و اجتماعی) تأثیرگذارند. در شکل دهی به هویت نقش دارند و حتی روی ابعاد اقتصادی و اجتماعی و سیاسی جوامع هم تأثیرگذارند. امروزه با توجه به نقشی که تاکنون در ابعاد مختلف زندگی داشته اند، نمی توان آن ها را نادیده گرفت. در حال حاضر اینترنت ابزاری مناسب برای توسعه ی افکار و اندیشه های بشری محسوب می شود به شرط آن که در راه صحیح استفاده شود. افراد باید برای ورود به دنیای مجازی اطلاعات کافی در اختیار داشته باشند تا دچار مشکلات مالی و اجتماعی نشوند. ارتباطات سالم در فضای مجازی و لزوم هوشیاری جوانان و خانواده ها نسبت به تهدیدات فضای سایبری در درجه ی نخست اولویت قرار دارد .پیشگیری از آسیب های اجتماعی و توجه والدین به رفتار فرزندان بسیار مهم می باشد و برای جلوگیری از هم پاشیدگی خانواده ها، والدین باید تا حدودی به فناوری های روز دنیا مسلط باشند و آگاه باشند که تغییر در رفتار فرزندان به معنای ایجاد تغییر در طرز فکر آنهاست و هنگامی که بنیان فکری و شخصیت آنها به صورت ناصحیح شکل گیرد، راه نفوذ شیادان به حریم خصوصی افراد و محیط امن خانواده باز می شود. لذا، چنانچه خانواده ها نسبت به شیوه های جدید ارتباط فرزندان خود آگاهی و شناخت کافی و لازم را داشته باشند، از انجام بسیاری از جرایم و ارتباطات پنهانی آنان جلوگیری به عمل می آید.

اینترنت اجتماع بشری به وجود می آورد که شهروندان را در لحظه با هم مرتبط می کند و آنها را وارد فضایی متفاوت از دنیای واقعی می کند فضایی که به آن و فضای مجازی گفته می شود. فضای مجازی دارای ویژگیهایی متفاوت از دنیای واقعی است از جمله ویژگیهای اساسی این فضا ، گمنامی ، عدم وجود نیروهای کنترل و قدرت

متمركز، و آزادی بی حد و حصر می باشد. فضای مجازی با ویژگیهای منحصر به فردش زمینه فعالیت‌های آزادانه را برای کاربران فراهم می سازد. همانطور که در جوامع بشری به یک سازمان نظامی جهت حفظ و برقراری نظم و امنیت نیاز است در دنیای مجازی نیز به این اصل مهم و ضروری نیازمندیم. نیروی انتظامی می تواند با تربیت نیروی متخصص در زمینه علوم کامپیوتری و فناوری اطلاعات و تشکیل همیارپلیس و پلیس مجازی در فضای سایبر به رعایت نظم و امنیت در دنیای مجازی و اینترنت کمک نماید و این امر موجب می شود که وقوع جرم کاهش می یابد و در صورت لزوم هم به پیگیری و کشف آن بپردازد. وجود نیروهای متخصص و آگاه به فناوری در نیروی انتظامی نه تنها موجب تامین سلامت و امنیت فضای مجازی می شود، بلکه یکی دیگر از وظایف پلیس، آگاهی و اطلاع رسانی عمومی در مورد مخاطرات و معضلات اجتماعی و امنیتی موجود در دنیای مجازی میباشد.

دانش پلیس سایبر در مبارزه با جرم و جنایت باید پیوسته به روز در آید تا بتواند سهم بهتری در ایجاد و حفظ و ارتقای امنیت داشته باشد. بدین منظور نیروی انتظامی باید تمام امکانات و روش های نوین را برای آموزش کارکنان خود بکار گیرد. پلیس سایبر باید با محدود کردن دامنه ی فعالیت مجرمان در فضای سایبر، موجب اطمینان خاطر کاربران را فراهم نماید.

آگاهی نوجوانان، جوانان و خانواده های آنها در مورد آسیبهای احتمالی فضای مجازی و کنترل هر چه بیشتر کاربران در فضای مجازی با طرحهایی که امید است هر چه زودتر به مرحله اجرا در بیاید از جمله همیار سایبری و گشت سایبری می تواند موجب اطمینان خاطر و سالم سازی فضای سایبری گردد.

همانگونه که از نتایج تحقیق مشخص گردید هر چه کاربران در فضای سایبری کمتر احساس کنند که گمنام می مانند احتمال وقوع جرم و فعالیت های مجرمانه کمتر می شود. و توجه هر چه بیشتر به مراکز خدمات اینترنتی همچون کافی نت ها با کنترل پلیس فتا فعالیت مجرمانه کاربران در این مراکز نیز کاهش می یابد. در پایان آنچه بیش از همه مورد تاکید می باشد توجه و آگاهی هر چه بیشتر خانواده و نظارت بر فعالیت اینترنتی فرزندان در منزل موجب می شود تا آسیب های وارده بر نوجوانان و جوانان کاهش یابد.

پیشنهادهات

آگاهی بخشی به نوجوانان در مورد فعالیت های مجرمانه در فضای مجازی برای معلمان و مسولان مدارس و کارشناسان آموزش و پرورش دوره های ضمن خدمت در مورد این آسیب ها برگزار شود تا بتوانند از آخرین یافته ها در مورد مشکلات محیط سایبر آگاه و به اطلاع دانش آموزان برسانند پیشنهاد می شود در سایت های مدارس، افرادی را به عنوان همیار سایبری آموزش دهند تا آنها بتوانند با راهنمایی دانش آموزان، به کاربران اینترنت کمک کنند تا آنان را به سمت پایگاه های آموزشی و سودمند هدایت کنند.

تربیت نیروی متخصص در پلیس فتا جهت استفاده در فضای سایبری.

فهرست منابع

- ✓ ۱-افروغ، عماد (۱۳۷۷). فضا و نابرابری اجتماعی. تهران
- ✓ ۲-پاکزاد، بتول (۱۳۹۰). تروریسم سایبری تهدیدی نوین علیه امنیت ملی. تهران، دفتر گسترش تولید علم.
- ✓ ۳-پور خاتون، اعظم و نیک طبع، سمانه (۱۳۹۰). آسیب شناسی روانی- اجتماعی پورنوگرافی در اینترنت. مجموعه مقالات برگزیده همایش منطقه ای، چاپ اول، بابل، صص ۳۳۲-۳۵۹.
- ✓ ۴-پور نقدی، بهزاد (۱۳۸۸) امنیت کامپیوتری و رویکرد انتظامی. دفتر تحقیقات کاربردی نیروی انتظامی استان سمنان.
- ✓ ۵-جاوید نیا، جواد (۱۳۸۷). جرایم تجارت الکترونیکی. تهران، نشر خرسندی.
- ✓ ۶-حسینی، بیژن (۱۳۸۳). جرایم اینترنتی علیه اطفال و زمینه های جرم شناسی آن. چاپ اول، انتشارات افراز.
- ✓ ۷-دهقان، علیرضا و نیک بخش، مرسده (۱۳۸۵). مطالعه شیوه ی رفتار افراد در محیط مجازی. فصلنامه مطالعات فرهنگی و ارتباطات، سال دوم، شماره ۶.
- ✓ ۸- ۷۳-راودراد، اعظم (۱۳۸۷). "مسائل اجتماعی زنان در اینترنت"، فصلنامه مطالعات فرهنگی و ارتباطات، صفحه ۹۰.
- ✓ ۹-روز بهانی، توران (۱۳۷۸) نقش خانواده به عنوان عامل و مانع بزهکاری. کارشناسی ارشد رشته پژوهش علوم اجتماعی، دانشگاه الزهرا.
- ✓ ۱۰-رضوی، محمد" (۱۳۸۶). جرایم سایبری و نقش پلیس در پیشگیری از آن ". فصلنامه دانش انتظامی، سال نهم، شماره اول.
- ✓ ۱۱-رجبی، ابراهیم (۱۳۸۸) پلیس و حقوق شهروندی. تهران. انتشارات مرکز تهیه و توزیع منابع آموزشی دانشگاهها ی ناشر علوم پلیسی.
- ✓ ۱۲-سجادی، بنت الهدی (۱۳۸۷). جوانان و جرایم اینترنتی. کارشناسی ارشد جامعه شناسی، دانشگاه الزهرا.

- ✓ ۱۳- شعاع کاظمی، مهر انگیز و مومنی جاوید، مهر آور (۱۳۹۰) آسیب های اجتماعی نوپدید، تهران، انتشارات آوای نور.
- ✓ ۱۴ - صادقی، سهیلا و محمدی، شهریار (۱۳۸۷) "نگاهی جرم شناسانه بر جرایم، امنیت و کنترل در اینترنت" فصلنامه مطالعات فرهنگی و ارتباطات، صفحه ۹۳-۱۱۶.
- ۱۵طهماسبی، هستی (۱۳۸۳) "هکرها در دام قانون". فصلنامه گزارش، شماره ۱۵۵، صفحه ۷۶-۷۲.
- ✓ ۱۶- طالع پسند، سیاوش (۱۳۸۷). جرم های رایانه ای و روشهای پیشگیری. مجموعه مقالات ویژه همایش فضاهای مجازی سمنان، صفحه ۱۲۰.
- ✓ ۱۷محسنی، منوچهر (۱۳۸۵). بررسی اثر استفاده از اینترنت بر انزوای اجتماعی کاربران. مجله جامعه شناسی ایران، دوره هفتم، ۹۵-۷۲.
- ✓ ۱۸-هاتف، مهدی (۱۳۸۷) چالش ها و چشم اندازهای امنیت در فضای مجازی. مجموعه مقالات ویژه همایش فضاهای مجازی سمنان. صفحه ۱۶۲
- [۱]Harre. N and bullen, P. (۲۰۰۰). "The internet its effectson safety and behavior". Psychology department . University oklland.
- [۲]Huey, L. J. (۲۰۰۲). Internet use still soaring. Canadian Journal of Criminology, ۲۴۳-۲۵
- [۳]Katyal, K.N. ۲۰۰۳. Digital architecture as crime control. The Yale Law Journal.
- [۴] Lipson, H. (۲۰۰۲). Tracking and tracing cyber-attacks: technical challenges and globalpolicy issues
- [۵]Williams, P. (۲۰۰۲). Organized crime and cyber-crime: implications on business.