تدقیق نقش و جایگاه مدیریت پلیس در مقابله و پیشگیری از جرایم سایبری

محمد پورخیری
کارشناس حرفه ای آسیب شناسی اجتماعی _ پیشگیری از اعتیاد
روح اله یاری زاده
کارشناس ارشد حقوق جزا و جرم شناسی

چکیده

با ظهور فناوری اطلاعات و ارتباطات و تأثیر فراوان آن در زندگی روزمره انسانها، زمینه سوء استفاده از رایانه و تکنولوژی وابسته به آن توسط افراد سودجو و فرصت طلب جهت انجام اعمال مجرمانه متداول گردیده است. با افزایش کاربران در فضای مجازی و کاربرد های متنوع مبادلات و معاملات در این فضا و کثرت تبادل اطلاعات، ارتکاب جرایم و یا بزه دیدگی در این فضا وجود دارد با توجه به رشد سریع فضای مجازی و وابستگی انسان ها به تکنولوژی سایبری از یک سو و سهولت ارتکاب جرایم مربوط به فناوری نوین از سوی دیگر، چالش هایی را پیشروی نظام کیفری قرار داده است. پس از گذشت زمانی کوتاه از پیشرفت فناوری اطلاعات و ارتباطات این ضرورت حیاتی محرز گردید که دغدغه حقوق کیفری بر سر پدیده های مجرمانه رایانه ای، بیشتر در حقوق جزای شکلی یا همان آیین دادرسی کیفری نهفته است. به طور کلی، آنچه امروز تحت عنوان جرم سایبر (Cyber Crime) قرار میگیرد، دو طیف از جرایم است: گروه اول جرایمی هستند که نظایر آنها در دنیای فیزیکی نیزوجود دارد و فضای سایبر بدون تغییر ارکان مجرمانه شان، با امکاناتی که در اختیار مجرمان قرار میدهد، ارتکابشان را تسهیل میکند. جرایم تحت شمول این حوزه بسیارگسترده اند و از جرایم علیه امنیت ملی و حتی بین المللی نظیر اقدامات تروریستی گرفته تا جرایم علیه اموال و اشخاص را در برمی گیرند. نمونه ای از این طیف، تشویش اذهان عمومی از طریق سایبر است. اما طیف دیگر جرایم سایبر، به سوء استفاده های منحصر از این فضا مربوط میشود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست. جرایمی نظیر دسترس غیرمجاز به داده ها یا سیستم ها یا پخش برنامه های مخرب نظیر ویروس ها، جز در فضای سایبر قابلیت ارتکاب ندارند و به همین دلیل به آنها جرایم سایبری محض (Pure Cyber Crime) نیز گفته میشود.

واژگان کلیدی: فضای سایبر، جرایم سایبری، رسیدگی به جرایم سایبری، پلیس

مقدمه

پا به پای پیشرفت های بشر در زمینه تکنولوژی، سهمیه خلاقیت های کامپیوتری و سایبری از همه افزون تر است. شاهد این ادعا ورود کامپیوتر در تمام فعالیت های اجتماعی، اقتصادی و حقوقی است که هر روزه می توان به راحتی آن را مشاهده نمود. این پیشرفت آنقدر در عرصه های مختلف زندگی رسوخ یافته که می توان ادعا نمود کامپیوتر از اجزای جدا نشدنی زندگی افراد در عصر حاضر شده است به گونه ای که کم کم زندگی بدون آن دشوار یا شاید ناممکن است. سرعت و گسترش ارتباطات اجتماعی در حوزه های علمی، هنری و غیره و امکان دسترسی آسان به انبوه اطلاعات فقط گوشه ای از این تکنولوژی است. از میان چهار وظیفه و قابلیت اصلی اینترنت یعنی ایجاد ارتباط، اطلاع رسانی، سرگرمی، خرید و فروش، جنبه اطلاعاتی آن مفیدترین آنها می باشد. در گذشته ای نه چندان دور نیروهای انتظامی بطور فیزیکی از افراد و اماکن محافظت و مراقبت می کردند اما ورود این تکنولوژی به زندگی انسان مخصوصاً در حوزه های اقتصادی و مالی نحوه محافظت از اموال و حتی حیثیت افراد در این فضا و تامین امنیت آنها هم به نوبه خود تغییر شکل داده است. امروز به علت ظهور جرایم سایبری و رشد روزافزون آنها همزمان با رشد و گسترش فناوری های نوین، دغدغه نظامهای مختلف جوامع بشری نیز گسترش پیدا کرده است. تکنولوژی های سایبر با دارا بودن عملکردهای بسیار مشخص نظامی میتوانند به طور مستقیم بر میدان نبرد تأثیرگذار باشند. بخش نظامی هر کشوری برای آموزش و تجهیز نیروها، سیستم های جنگ افزاری، ماهواره ها و شبکه های ارتباطی یا داده پردازی اطلاعات به تکنولوژی های سایبری وابسته است. درواقع میتوان گفت فضای اطلاعاتی و سایبری به همان نسبت که میتواند فرصتهای بسیار زیادی را برای نیروهای نظامی هر کشور به وجود آورد، به همان میزان نیز میتواند تهدیدهای بزرگی را برای این بخش ایجاد کند. بنابراین امروزه سرنوشت جنگ را دیگر تخریب ها، انفجارها و عملیات فرسایشی تعیین نمیکنند بلکه ازهم گسیختگی ظرفیت های فرماندهی و کنترل در فضای مجازی میتواند بسیار برای نتیجه برخوردها تعیین کننده باشد. علاوه بر این، امروزه بعد اطلاعاتی به عنوان یکی از ابعاد محوری جنگ در همه عملیات ها، رزم ها و نبردهای آینده دخیل خواهد بود. همچنین در جنگهای آینده، کسب برتری سریع در حوزه اطلاعاتی یکی از عوامل مهم موفقیت خواهد بود.

علل جرایم در فضای مجازی

جرایم وابسته به فضای مجازی تنها می توانند با استفاده از کامپیوتر، شبکه کامپیوتری و یا دیگر اشکال فن آوری ارتباطات و اطلاعات مرتکب شوند. فعالیت های جرایم اینترنتی به سرعت در حال رشد و در حال تحول هستند. بنابراین مقابله با جرایم اینترنی باید به عنوان یک اولویت استراتژیک تلقی می شود .وسوءاستفاده از فناوری رایانه ای و اینترنتی می تواند امنیت و آسایش عمومی و موجودیت یک جامعه را به خطر اندازد و تأثیر های منفی فراوانی را بر روی زندگی افراد داشته باشد. با کمی دقت این موضوع مشخص می شود که اکثر مرتکبین این جرایم را جمعیت جوان تشکیل می دهد. این مجرمان از ظرفیت جنایی بالایی برخوردار بوده و هم دارای استعداد فراوان برای انطباق اجتماعی اند.جرم عبارت است از فعل و یا ترک فعلی که در قانون برای آن مجازات تعیین شده است و جامعه با ابزار مجازات آن را نکوهش قرار می دهد. اگر قرار باشد جرم شناسی سایبری به عنوان یک شاخه مجزا معرفی شود، چالش های متعددی پیش روی جرم شناسان سایبری امروزی قرار خواهد گرفت. این چالش ها عبارت اند از: -1 مشکلات آموزشی -2 تحقیق در زمینه جرم شناسی سایبری -3 ،حرفه ای سازی این رشته.

بررسی چالشهای جرایم سایبری

1 – چالش های حقوق بین الملل عمومی: حقوق بین الملل عمومی، مجموعه قواعد و مقررات حاکم بر روابط دولت ها را مورد مطالعه قرار میدهد. بدین صورت که دولت ها در جهت منافع ملی خود، درصدد آن هستند که با رعایت چارچوب های قانونی و حقوقی اتخاذ شده دو یا چند جانبه، اقدامات خود را سازماندهی کنند. حال این منافع ملی میتواند منافع اقتصادی، نظامی، امنیتی، اجتماعی،

سیاسی و ... را شامل شود .پایه و اساس حقوق بین الملل عمومی، بر وجود چالش های فراگیر در زمینه های بالا، دولتها با سایر دولتها در منطقه، فرامنطقه یا جهان استوار است. برای مثال، زمانی که کشورها در خصوص برداشت منافع و منابع ملی با سایر کشورها به چالشی برخورد میکنند، تنها میتواند این چالش را با رجوع به مفاد معاهدات منعقده یا مورد قبول آنان مرتفع کرد. بنابراین، نقطهٔ تکامل و پیشرفت حقوق بین الملل عمومی، وجود چالش های مشترک فی مابین کشورها و تلاش درجهت رفع حداقلی آنهاست؛ اما یکی از چالش هایی که امروزه دولت ها با آن روبه رو هستند، ظهور پدیدهٔ فراملی فضای سایبری و به تبع آن جرایم سایبری است.

2 – چالش های حقوق بین الملل خصوصی: از ویژگی های مهم جرایم رایانه ای و جرایم اینترنتی، ماهیت فراملی بودن اینگونه جرایم است که به دلیل قابلیت های فنی رایانه ها و اجزای مرتبط با آن، امکان ذخیره سازی، حرکت، استفاده از داده ها از طریق شبکه ها و ایجاد ارتباط و انتقال سریع درسطح وسیع بین سیستم های رایانه ای افزایش یافته است، به طوری که دامنهٔ گسترش سیستم های رایانه ای از محیط رایانه و شبکهٔ داخلی به سطح بین المللی، گسترش پیدا کرده و موجب خلق نسل جدید جرایم رایانه ای یعنی جرایم در محیط سایبری شده است که ماهیت و خاصیت کاملاً فراملی و بین المللی دارند. به هر حال، امروزه جرایم رایانه ای تبدیل به یک پدیدهٔ مجرمانهٔ کاملاً بین المللی شده است. در مسائل بین المللی، اولین اثر جرایم رایانه ای، بحث صلاحیت است. علی الخصوص در قواعد حاکم بر صلاحیت سرزمینی و مکان ارتکاب، مقام صالح دچار مشکل میشود. زیرا جرایم رایانه ای، فراملی بوده که موجب تعدد محل ارتکاب و تعدد صلاحیت ها میشوند. در بحث صلاحیت ها، علاوه بر موضوعاتی از قبیل تابعیت مجرم، تابعیت بزه دیده، نوع جرم ارتکابی (جاسوسی و ...) بحث صلاحیت شخصی و واقعی نیز مطرح میشود.

3_ چالش های حقوق ماهوی و شکلی ایران: در طول قرون متمادی، سیستم های قضایی بر موضوعات ملموس و عینی متمرکز شده اند و مقررات جزایی به حمایت از این دسته موضوعات پرداخته است. این در حالی است که امروزه اموال غیر مادی اهمیت بسیار یافته اند. داده ها و اطلاعات تبدیل به نوعی دارایی شده اند که میتوان موضوع ارتکاب جرم واقع شود و رژیم حقوقی مربوط به موضوعات این چنینی، تنها نمیتوانند بر مبنای قیاس با قواعد موجود و مختص به موضوعات مادی بنا شود؛ زیرا نحوهٔ ارزیابی و حمایت داده ها و اطلاعات با آنچه در خصوص اشیای مادی مقرر است تفاوت قابل ملاحظه ای دارد. بدین سان که اشیای مادی را میتوان به افراد خاصی نسبت داد، ولی اطلاعات کالایی عمومی است که علی الاصول بنابر قاعدهٔ (دسترسی آزاد به اطلاعات)بایستی به صورت آزادانه در جامعه جریان داشه باشد. بنابراین، همچون اموال مادی مشمول حمایت انحصاری واقع نمی شود. علاوه بر این، در راستای حمایت از اطلاعات، نه تنها باید منافع مالک یا دارندهٔ آن مدنظر قرار گیرد، بلکه منافع کسانی که به نحوی با محتوای اطلاعات سرو کار دارند نیز باید محفوظ بماند. پس ملاحظه میشود که نمیتوانیم به قواعد موجود در زمینهٔ اموال مادی بسنده کنیم و به تغییر در طرح و چهارچوب قضایی جاری نیازمندیم .حقوق جزایی ماهوی در ارتباط با جرایم رایانه ای، از دو لحاظ با مشکل مواجه است: از یک سو، اوصاف و عناصر متشکله جرایم کلاسیک دستخوش تحولاتی گشته اند؛ تا جایی که نمیتوان تعاریف مجرمانهٔ موجود در متن قانونی را به جرایم رایانهای مشابه تسری دارد و از سوی دیگر، عناوین مجرمانهٔ نوینی نیاز است تا برخی دیگر از راههای سوء استفاده رایانه ای را که به طور جدی جوامع بشری را تهدید میکند، به عنوان جرم شناسایی کنیم.

بخش، یافته های پژوهش گزارش می شود. یافته ها باید همراه با جدول، نمودار، شکل و ارائه آمار و ارقام به فارسی و نیز شامل توصیف و تحلیل دادهها باشد.

تأسیس پلیس سایبری در نظام حقوقی ایران

همزمان با توسعه و کاربردپذیری رایانه و سیستمهای رایانهای، جرائم رایانهای همه بوجود آمدهاند. اگر چه دامنه و حوزهی وقوع جرم در هر حوزه با توجه به ویژگیها و وسعت کاربرد و استفاده متفاوت بوده است. از سال 1960 تاکنون سه نسل از جرائم رایانهای برشماری شدهاند. نسل اول که مقارن سالهای دهه هفتاد و هشتاد، اوایل دهه نود میلادی است. و چون استفاده از اینترنت در آن زمان شیوع نداشت، عمدهی جرائم مرتبط با رایانهها بوده و از اینرو این دسته از جرائم صرفاً به«جرائم رایانهای» یاد میشوند. نسل دوم جرائم

رایانه‌ای از اوایل دهه‌ی هشتاد تا اوایل دهه‌ی نود به وقوع پیوستند، که به«جرائم علیه داده‌ها» تعبیر می‌شوند. در این نسل«داده‌ها» صرف‌نظر از اینکه در رایانه قرار داشته باشد. در اواسط‌ها و ابزارهای انتقال مورد توجه قرار گرفت و دیگر تأکیدی بر رایانه نبود. نسل سوم جرائم رایانه‌ای نیز هم زمان با فراگیر شدن اینترنت از اوایل دهه‌ی 1990 میلادی به‌وجود آمدند.این جرائم که با گسترش کاربرد شبکه و اینترنت به وجود آمدند، نام جرائم سایبری را به خود گرفتند.

گسترش جرائم سایبری در دنیا، خصوصاً در کشورهایی که بیشترین استفاده‌کنندگان رایانه و اینترنت در دنیا محسوب می‌شوند. باعث شد که حکومت‌ها به فکر ایجاد سازوکار قانونی و حقوقی رسیدگی و مبارزه با این‌گونه جرائم بیافتند.

کنوانسیون‌های بین‌المللی نیز برای تشریک مساعی در روند شناسایی جرم و مجرمین، همکاری در پی‌جویی و تعقیب قضایی و پلیسی مجرمان و تبادل دانش و اطلاعات پلیس در شناخت و کشف علمی جرائم سایبری نیز تشکیل شدند. که از مهم‌ترین آنها می‌توان به کنوانسیون بوداپست در سال 2001 اشاره کرد. از کشورهای فعال پیش‌رو در پی‌جویی و مبارزه با جرائم رایانه‌ای می‌توان به ایالات متحده‌ی آمریکا، روسیه، چین، کره جنوبی، انگلستان، هند، فرانسه و آلمان اشاره کرد.

در همین راستا کشور ایران نیز از این قاعده مستثنی نبوده است و با کوشش‌های فراوان توانست پلیس مستقلی برای رسیدگی به جرائم سایبری تأسیس نماید.که به‌طور مفصل در این فصل مورد بررسی قرار خواهد گرفت.

شیوه تأسیس پلیس فتا در ایران

توسعه‌ی روزافزون زیر ساخت‌های فناوری اطلاعات و ارتباطات در کشور و افزایش کاربران و استفاده‌کنندگان از اینترنت و سایر فناوری‌های اطلاعاتی، ارتباطی و مخابراتی نظیر خطوط تلفن‌های ثابت و همراه، شبکه‌های دیتای کشوری و محلی به ارتباطات ماهوارهای از جمله دلایلی است، که لزوم ایجاد و توسعه‌ی سازوکاری برای برقرای امنیت در فضای تولید و تبادل اطلاعات جمهوری اسلامی ایران را توصیه می‌کند.

همچنین توسعه‌ی خدمات الکترونیک در کشور نظیر دولت الکترونیک، بانکداری الکترونیک، تجارت الکترونیک آموزش الکترونیک و سایر خدمات از این دست، نیز لزوم ایجاد پلیسی تخصصی در مجموعه نیروی انتظامی جمهوری اسلامی ایران را برای تأمین امنیت و مقابله با جرائمی که در این فضا به وقوع می‌پیوندند، را آشکار می‌کند. از سوی دیگر با توجه به تصویب قانون جرائم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضابط قضایی برای این قانون و نیز مصوبات کمیسیون افتای دولت جمهوری اسلامی ایران مبنی بر تشکیل پلیس فضای تولید و تبادل اطلاعات، این پلیس در بهمن ماه سال 1389 به دستور سردار فرماندهی محترم نیروی انتظامی جمهوری اسلامی ایران، تشکیل گردید.

وظایف و مأموریت‌های این نهاد ایجاد امنیت وکاهش مخاطرات برای فعالیت های علمی، اقتصادی، اجتماعی در جامعه‌ی اطلاعاتی حفاظت و صیانت از هویت ملی و دینی، مراقبت و یا پیش از فضای تولید و تبادل اطلاعات برای پیشگیری از تبدیل شدن این فضا به بستری برای انجام هاهنگی‌ها و عملیات برای انجام و تحقق فعالیت‌های غیرقانونی و ممانعت از تعرض به ارزش‌ها و هنجارهای جامعه در فتا از جمله وظایف و مأموریت‌های پلیس فضای تولید و تبادل اطلاعات نیروی انتظامیاست.

کنوانسیون جرائم سایبر و پروتکل الحاقی آن

پیش‌نویس کنوانسیون جرائم سایبر توسط کمیته ای به نام کمیته تخصصی جرائم سایبرتهیه شده است. کمیته تخصصی جرائم سایبر در 4 فوریه 1997 توسط کمیته وزرای شورای اروپا به منظور تهیه پیش‌نویس کنواسیون مزبور تشکیل شد. این کمیته کار خود را در آوریل 1997 شروع کرد و نسخه اولیه پیش‌نویس کنوانسیون جرائم سایبر درآوریل 2000 تهیه و نشر گردید.

نسخه نهایی پیش‌نویس کنواسیون و گزارش توجیهی آن در ژوئن 2001 تهیه و جهت تأیید، تسلیم کمیته اروپایی مشکلات ناشی از جرم شد. این پیش‌نویس پس از تأیید آن مرجع جهت تصویب و امضاء به کمیته وزرای اروپا تسلیم گردید و نهایتا" در 23 نوامبر 2001 در بوداپست به تصویب رسید. و به امضای کشورهای عضو شورای اروپا و چهار کشور امریکا، کانادا، آفریقای جنوبی، ژاپن رسید. این سند

از آن به بعد مبنای روابط بین اعضای شورا و سایر کشورهای جهان شد. طبق اعلام شورای مزبور این طرح کنوانسیون سازمان ملل برای سایر کشورها نیز قابل تسری خواهد بود و این بر اهمیت مضاعف آن دلالت دارد.

اهداف اصلی کنوانسیون عبارتند از:

1- هماهنگ کردن عناصر تشکیل‌دهنده جرم در حقوق جزای ماهوی داخلی و مقررات راجع به آن در حوزه جرائم سایبر

2- اعطای اختیارات لازم درآیین دادرسی کیفری داخلی برای تحقیق و تعقیب این‌گونه جرائم و همچنین سایر جرائمی که به وسیله سیستم‌های رایانه‌ای ارتکاب می‌یابند، یا ادله الکترونیکی مرتبط با جرائم.

3- پایه ریزی رژیم سریع و کارآمد همکاری بین‌المللی

هدف این کنوانسیون تکمیل معاهدات و ترتیبات دو جانبه یا چندجانبه لازم اجرا میان اعضای کنوانسیون است، از جمله این اسناد عبارتند از:

- کنوانسیون اروپایی استرداد، آماده برای امضاء مصوب 13 دسامبر 1957 پاریس
- کنوانسیون اروپایی معاضدت دوجانبه در موضوعات کیفری، آماده برای امضاء مصوب 20 آوریل1957 استراسبورگ
- پروتکل الحاقی به کنوانسیون اروپایی معاضدت دوجانبه در موضوعات کیفری آماده برای امضاء مصوب 17 مارس 1978 استراسبورگ

تصویب قانون جرائم رایانه‌ای در ایران

قانون گذار ایران به نوبه خود، قانون جرائم رایانه‌ای را که حاصل مطالعات کارشناسان فناوری اطلاعات و ارتباطات و حقوق دانان بود، در تاریخ 1388/3/5 تصویب نمود. این قانون که از مفاد کنوانسیون بزه‌کاری سایبر شورای اروپا(23نوامبر2001) نیز برای تهیه و تنظیم آن استفاده شده است.

دراوایل دهه 1380موضوع جرائم رایانه‌ای در ایران مطرح گردید. در آن سال‌ها جرائم رایانه‌ای عموماً در استفاده از رایانه در ساده‌سازی جرائم قدیمی مثل جعل خلاصه می‌شد. به نحوی که بیشتر پرونده‌های مجرمانه‌ی رایانه‌ای که در پلیس آگاهی به آن رسیدگی می شد، به استفاده از رایانه و نرم‌افزارهای رایانه‌ای در جعل اسناد نظیر کارت پایان خدمت، مدارک تحصیلی، چک‌های مسافرتی و سایر اسناد و اوراق بهادار خلاصه می گردید. با گسترش کاربری رایانه و توسعه‌ی شبکه‌ی اینترنت و به تبع آن افزایش جرائم رایانه‌ای و سایبری، دولت وقت جمهوری اسلامی ایران، نسبت به تهیه لایحه‌ی جرائم رایانه‌ای اقدام نمود. نهایتا با برگزاری جلسات کارشناسی کمیسیون‌های مختلف مجلس شورای اسلامی و طی چندین مرحله رفت و بازگشت میان مجلس و شورای محترم نگهبان این قانون مشتمل به 56 ماده و 25 تبصره تاریخ 1388/4/5 در مجلس شورای اسلامی تصویب و در تاریخ 1388/3/20 به تأیید شورای محترم نگهبان رسید .

کارکردها و محدوده‌های نقش پیشگیرانه پلیس در فضای سایبر

نقش پلیس در پیشـــگیری اجتماعی از جرائم ســـایبری

پلیس به عنوان ضابط عام دادگستری، از کنشـــگران اصلی در برابر پدیدۀ مجرمانه و نهاد اصلی شناســـایی و بررسی جرم، در مقایسه با سایرنهادها، ارتباط نزدیکتری با بزه دیدگان دارد. از نظر رده بندی درون سازمانی، پلیس یکی از نهادهای پیشرو مبارزه با جرائم رایانه ای در کشور به شمار میآید. در ســـال 1378 ،با برگزاری نخســـتین همایش جرائم رایانه ای در کشور، این موضوع را به اثبات رساند و یکی از ادارات کل خود را البته همراه با جرائم خاص نظیر کلاهبرداری و جعل(به رسیدگی جرائم رایانه ای اختصاص داد) پیش بینی، شناســـایی و ارزیابی خطر وقوع جرم از یکســـو و اتخاذ تدابیر و اقدام های لازم برای از بین بردن یا کاهش جرم در قالب برنامه ملی از ســـوی دیگر، از مؤثرترین روش های کاربردی پیشـــگیری از جرم به شـــمار می آیند. پیشـــگیری اجتماعی شامل مجموعه اقدامات پیشگیرانه از جرائم است که به دنبال حذف یا خنثی کردن آن دسته از عواملی است که در تکوین جرم مؤثر است. این نوع پیشگیری، بر مبنای علت شناسی جرائم استوار است و با دخالت در محیط های اجتماعی، مانع از شکل گیری رفتار بزهکارانه و خنثی ســـازی عوامل جرم زا میشود. به عبارت دیگر، پیشگیری اجتماعی از جرم، راهبردی است که برخورد با علل ریشه ای اقدامات مجرمانه و بزه دیدگی را مدنظر قرار می دهد. به همین دلیل، در بررسی شیوه های پیشگیری از جرائم سایبری،از این نوع تقســـیم بندی استفاده میشـــود. پیش

از پرداختن به جزییات این نوع پیشگیری، مناسب است به قطعنامۀ هشتمین کنگرۀ سازمان ملل متحد در خصوص پیشگیری از جرم و اصلاح مجرمان که در سیزدهمین اجالس سازمان ملل متحد توسط مجمع عمومی سازمان در قالب قطعنامه شمارۀ 45/121 تأیید شد، اشاره شود. در این قطعنامه، از کشورهای عضو خواسته شده است که در صورت لزوم با مدنظر قرار دادن این موارد، تلاش های خود را در مبارزه با جرائم رایانه ای شدت بخشند: مدرنیزه کردن قوانین و دادرسی کیفری؛ ارتقای ضوابط پیشگیرانه و امنیتی رایانه؛ گزینش راه هایی برای حساس کردن عامه مردم، قوۀ قضاییه و پلیس به عنوان مجری قوانین نسبت به این مسئله و اهمیت پیشگیری از ارتکاب جرم های رایانه ای و دادن آموزشهای کافی به مأموران و عوامل مسئول در زمینه پیشگیری، تحقیقات، تعقیب و احقاق حق در جرائم رایانه ای. در میان اقدامات پیشگیری اجتماعی که میتواند به کاهش جرائم سایبری کمک کند، میتوان به برنامه های خانواده مدار، تدابیر آموزشی -سایبری، بالابردن سواد رسانه ای، تنظیم کدهای رفتاری، اطلاع رسانی و اطلاع گیری، توجه به حکمرانی خوب و شاخص های آن، مشارکت و اجماع گری، ارتقای پاسخ گویی و شفافیت، فرهنگ سازی و تولید رسانه ای اشاره کرد پیشگیری اجتماعی در دو شاخه پیشگیری اجتماعی جامع همدار و پیشگیری اجتماعی رشدمدار قرار میگیرد. تدابیر پیشگیری اجتماعی جامعه مدار توسط پلیس، سعی در بر طرف کردن زمینه های اجتماعی بروز انگیزه های مجرمانه و منحرفانه را داردتدابیر پیشگیرانه اجتماعی رشد مدار توسط پلیس، دومین اقدام مهم برای خنثی سازی عوامل اجتماعی جرم زا و انحراف زا است. منظور از پیشگیری رشد مدار، مجموعه اقداماتی است که در دوران رشد و تکامل شخصیتی و جسمی اشخاصی به اجرا در می آید که در معرض ارتکاب این جرائم قرار دارند. با توجه به اینکه پیشگیری رشد مدار برخالف پیشگیری جامعه مدار، با قشر جوان و نوجوان سروکار دارد، خط مشیها و اقدامات پلیس، رویکردی تربیتی و آموزشی داشته و در این نوع پیشگیری، قدرت شناخت و تمیز آنها تقویت میشود و مهارت های زندگی اجتماعی در فضای مجازی را می آموزند تا بتوانند در هنگام مواجهه با معضالت و انحرافاتی که در فضای سایبر با آن مواجه میشوند، واکنش های منطقی و صحیح از خود بروز دهند.

نقش پلیس در پیشگیری وضعی از جرائم سایبری

اقدامات پیشگیرانه وضعی پلیس، از جرائم سایبری را میتوان در چهار گروه بررسی کرد. محدود کنندۀ پلیس یا سلب کنندۀ در دسترس، تدابیر نظارتی پلیس، تدابیر صدور مجوز و ابزارهای ناشناس کننده و رمزگذاری. بنابراین، پیشگیری وضعی توسط نهاد پلیس شامل به سوی اشکال خاصی از جرائم تدابیری به منظور کاهش فرصت های مجرمانه است که اولاً شامل مدیریت، طراحی و دستکاری در محیط به صورت نظام مند و معطوف شده اند، ثانیا دائمی میباشند و در نهایت برای دشوارتر کردن و پرخطر کردن ارتکاب این جرائم نوظهور توسط پلیس پیشگیری، از آن استفاده میشود. بر این اساس، پلیس پنج راهبرد اصلی را برای پیشگیری وضعی از جرائم سایبری به کار میبندد: افزایش میزان تلاش به منظور جلوگیری از ارتکاب جرم رایانه ای، افزایش اطلاع رسانی خطرهای ناشی از ارتکاب جرم سایبری، کاهش دستاوردها، کاهش عوامل محرک و سلب توجیه های لذا این تدابیر، باید با حفظ حریم خصوصی اشخاص توسط پلیس و صرفا سایبری، صورت گیرد .

دوین برنامه ملی پیشگیری از جرم، مستلزم فرآیندی است که با در نظر گرفتن آن، سازوکارهای مهار جرم در هر جامعه مشخص شده و سپس به اجرا در می آیند. در همین خصوص، شرکت های امنیت خصوصی نیز از طریق مراقبت و نگهبانی و سازوکارهای کنترل ورودی ها و هشداردهنده ها، در پیشگیری از جرم مشارکت میکنند. در واقع، پیشگیری از جرم، گاهی آگاهانه و گاهی به طور ناخودآگاه، توسط واحدهای تأمین امنیت ادارات و پلیس اعمال و اجرا میشود. جرم سایبردر واقع،دربسترداد و ستدها یالکترونیکی وعلیه داده ارتکاب یافته است. واطلاعات وبه ندرت علیه سامانه های فیزیکی و سخت افزاری رخ میدهند. بنابراین،پیشگیری این جرائم، میتوان آثار منفی آن را در جامعه به حداقل رساند.

به تعبیر ساده، پیشگیری، هر اقدام سیاست جنایی بدون تأکید بر تهدید کیفری یا اجرای آن است که با هدف تهدید امکان پیش آمد جنایی از راه های گوناگون انجام میشود. با این وصف، قلمرو جرم شناسی امروزه بسیار گسترده شده با توجه به ویژگی های عمدۀ پیش گیری که عبارتن د از: غیرقهرآمیز بودن تدابیرپیشگیرانه، اختصاصی بودن این تدابیر، کاستن آثار جرم و در نظر گرفتن عوامل خطر و محیط اجتماعی دو نوع پیشگیری اجتماعی و پیشگیری وضعی توسط پلیس در میان انواع اقدامات پیشگیرانه این نهاد از

مقبولیت بیشتری برخوردارند

چالش های تقنینی تحقیقات نیروی انتظامی در جرایم سایبری

نیروی انتظامی به عنوان یکی از نهادهای امنیتی وانتظامی در جامعه از زمان تأسیس آن تا کنون با اتخاذ سیاست‌های پیشگیرانه به این امر اهتمام ورزیده است. فلسفه وجودی نهاد پلیس، با درنظر گرفتن قانون و حقوق مردم، برقراری نظم و امنیت و پیشگیری از وقوع جرم می‌باشد. پلیس به عنوان ضابط عام دادگستری، از کنشـــگران اصلی در برابر پدیدهٔ مجرمانه و نهاد اصلی شناســـایی و بررسی جرم، در مقایسه با سایرنهادها، ارتباط نزدیکتری با بزه دیدگان دارد. فناوری اطلاعات و ارتباطات ضمن تأثیرگذاری بر تمامی جنبه‌ها و شئون زندگی بشر بر جرائم، تهدیدها و آسیب‌ها نیز تأثیر گذاشته است و همین امر وظایف پلیس را تحت‌الشعاع قرار داده است، خواستار ضرورت شناخت بیشتر فضای مجازی توسط پلیس می‌باشد. با توجه به اینکه فضای مجازی در مقایسه با فضای واقعی از موقعیت جغرافیایی و فیزیکی مشخصی برخوردار نیست، سازمان پلیس باید با به دست آوردن آگاهی لازم از این فضا بتواند به‌طور صحیح و منطقی با آن مقابله نماید. در این خصوص باید بیان نمود که پلیس تازه تأسیس فتا برای تأمین امنیت فضای تولید و تبادل اطلاعات و حفظ هویت ملی و دینی و ارزش‌های انسانی و حفظ حریم خصوصی و آزادی مشروع تمام راهکارهای لازم را به کار بندد.

نتیجه گیری و پیشنهادها

در عصر نوین اطلاعات، نیاز جوامع به رایانه و اینترنت افزایش یافته است .این موضوع به افراد فرصت طلب و تبه کار اجازه میدهد تا مقاصد شوم خود را در فضای سایبری، به دلیل نامحدود بودن و احتمال کم ردگیری آنها، دنبال کنند .هرچه بیشتر تکنولوژی کامپیوتری توسعه یابد جرایم سایبری نیز توسعه پیدا خواهد نمود و در ایران نیز جرایم سایبری در حال افزایش است .مطالعه جرایم سایبری و شناخت قوانین و طبقه بندی انواع جرم سایبری برای افزایش آگاهی در رابطه با مسائل حقوقی و انواع شیوههای ارتکاب جرم، برای مقابله با جرایم سایبری ضروری میباشد .در این مقاله برای بررسی جرایم سایبری به انواع طبقه بندی که کشورهای اروپایی و همچنین کشور ایران در این زمینه انجام دادهاند، پرداخته شد که شامل :طبقه بندی جرایم سایبری در اسناد منطقه ای و بین المللی (طبقه بندی سازمان توسعه و همکاری اقتصادی، طبقه بندی کمیته وزرای شورای اروپا، طبقه بندی کنوانسیون جرایم سایبر)و طبقه بندی جرایم سایبر در ایران میباشد .هم چنین برای شناخت بیشتر انواع راههای مختلف ارتکاب جرم، به شرح بیشتر مصادیق جرایم سایبری پرداخته شده است زیرا که با شناخت دقیق تر و با ارائه راهکارها، بهتر میتوان به پیشگیری و مقابله با جرایم سایبری پرداخت.

نو ظهور بودن فناوری اطلاعات و ارتباطات رایانه ای سبب شده تا اقدامات مقطعی و ضربتی برای کنترل کوتاه مدت جرایم سایبری مطلوب سیاست گذاران و نظام عدالت کیفری قرار گیرد؛ چراکه این اقدامات کم هزینه سبب میشود تا چنین به نظر آید که دستگاه عدالت کیفری برای برخورد با منحرفان، فاقد برنامه لازم نمیباشد .نمونه این اقدامات تدابیر وضعی است که با اثر گذاری بر موقعیت های جرم زا به دنبال آن است که در سایه ی تدابیر محدود کننده و نظارتی، بزه را برای بزهکار دشوار جلوه دهد و با تغییر در معادله هزینه -فایده، او را از ارتکاب جرم باز دارد.

بهترین روش برخورد درست با مجرمان فضای سایبر در ایران وقتی قابلیت اجرا پیدا میکند که نقش مردم در آن به خوبی دیده شود و بتوان بخشی از آموزش درست استفاده کردن از فضای سایبر را به مردم واگذار کرد. مردم زمانی میتوانند به صورت هماهنگ و درست در چهارچوب قانون و همکاری داوطلبانه عمل نمایند که بستر ارتباطات بین آنها و پلیس و میتوان به تحقق این کار مهم که پیشگیری قبل از وقوع جرم و برخورد با مجرمان بعد از عمل مجرمانه است در عمل کمک کرد . مهمترین رکن آن آموزش به مردم با کمک گرفتن از فناوری، در جهت همکاری به موقع آنان با جرایم سایبری است.شبکه های اجتماعی جدید نیز بستری مناسب برای همکاری افراد برای مبارزه با جرایم سایبری ایجاد نموده اس . شرط موفقیت هر سیاستی، اهتمام در آموزش خانواده و آموزش کودکان و نوجوانان، تربیت نیروی انسانی متخصص در مقابله با جرایم سایبری میباشد .هم چنین تدوین و اجرای تدابیر امنیتی برای مقابله با جرایم سایبری امری

ضروری است. با آموزش اخلاق مجازی به درک خطر رفتارهای مضر و غیر قانونی آنلاین و یادگیری این که چگونه از خودمان محافظت کنیم دست می یابیم .همچنین به کاربران اینترنتی پیشنهاد میشود که بدون شناخت نسبت به ارتباط ایمیل، چت و وبکم در فضای مجازی اقدام نکنند تا مورد سوء استفاده های موجود در این حوزه قرار نگیرند .یکی از مسایلی که هر کاربر اینترنتی دارای وبلاگ یا سایت باید به آن توجه نماید، قوانین و مقررات حاکم بر فضای مجازی می باشد تا با آموزش پیشگیری از جرم، به کاهش آن کمک نمایند. قوانین سخت گیرانه ی پلیس سایبری پس از دستگیری مجرمان سایبری نیز اقدامی جهت پیشگیری از ارتکاب جرم توسط مجرمان می باشد.

فعال نمودن انجمن های اولیا و مربیان در زمینه آگاهی بخشی درباره آسیب های اجتماعی اینترنت محور.

پخش برنامه های آموزشی سواد رایانهای در شبکههای های مختلف صدا و سیما.

تدوین و انتشار جزوات و کتاب های ویژه استفاده مناسب و آگاهی دهنده در سطح عمومی، مدارس، دانشگاهها.

بررسی جرایم سایبری و اجرای برنامهها و سمینارها و سخنرانیهای آموزش محور و آگاهی دهنده از فضای سایبر، امکانات و تهدیدات آنها در سطح نهادهای متفاوت و موسسات پژوهشی در سطح شهرها و در سطح عمومی، مدارس، دانشگاهها.

ایجاد انجمنهای دانشجویی و دانش آموزی مبارزه با جرایم سایبری و آموزش آنان برای همکاری آنان با پلیس سایبر؛ زیرا که حضور این قشر در شبکه های اجتماعی سایبری فرصتی برای تعامل با پلیس سایبری و پیشگیری از جرایم سایبری ایجاد کرده است.

ایجاد برنامههای محافظتی (ضد هک و ضد ویروس)توسط متخصصین رایانهای و نصب این گونه برنامهها بر روی سیستمهای دولتی و سیستمهای خانگی در جهت مقابله با خرابکاران سایبری.

- منابع انتهای مقاله:

-بهزاد لک، شناسایی و پیشگیری از کمین سایبری در فضای مجازی، کارآگاه، دوره دوم .سال پنجم
-زبیر، ارلیش، ۳۱۳۱ ، جرایم رایانه ای، ترجمه محمدعلی نوری و ضا نخجوانی و مصطفی بختیاروند و احمد مقدم، چاپ نخست، تهران نشر گنج دانش.
-فقیهی، ابوالحسن و موسوی کاشی، زهره، مدل سنجش بهره وری (اثربخشی و کارایی) در بخش خدمات دولتی ایران، مجله مدیریت دولتی، دوره دوم، شماره چهارم ، بهار و تابستان 1389، 126-107
-محسنی، منوچهر، ۳۱۳۰ ، جامعه شناسی جامعه اطلاعاتی، تهران: نشر دیدار.
- بهرهمند، حمید و داودی، ذوالفقار (بهار و تابستان 1397 .)پیشگیری اجتماعی از جرائم امنیتی – سایبری. مطالعات حقوق کیفری و جرمشناسی. دورهٔ 48 ،شمارهٔ 1.
- پاکزاد، بتول)1388 .)تروریسم سایبری. رساله دکتری حقوق جزا و جرم شناسی. دانشگاه شهید بهشتی.
- دشتی، بیتا و افشاری، مریم (بهار و تابستان 1398) مطالعه تطبیقی جرائم سایبری در ایران و حقوق بین الملل. پژوهشنامه حقوق تطبیقی. سال سوم، شمارهٔ 4.
- رضوی، محمد 1387 جرائم سایبری و نقش پلیس در پیشگیری از این جرائم و کشف آنها. فصلنامه دانش انتظامی. سال نهم، شمارهٔ اول.
- صبح خیز، رضا پاییز 1394 . چالش های حقوقی جرائم سایبری در نظام حقوق بین الملل و نظام حقوقی ایران. فصلنامه پژوهشهای اطلاعاتی و جنایی. سال دهم، شمارهٔ سوم.

- صالحی، سهراب و کشفی، سید مهدی)1395 .)جنگ سایبری از منظر حقوق بین الملل با نگاه به دستورالعمل تالین. فصلنامه مطالعات قدرت نرم. شمارهٔ 14.

- کرد علیوند، روح الدین و میرزایی، محمد)تابستان 1397 .)گونه شناسی جرائم سایبری با نگاهی به قانون جرائم رایانه ای و آمار پلیس فتا. مجلهٔ حقوقی دادگستری. سال هشتاد و دوم، شمارهٔ یکصد و دوم.

-ورویی، اکبر و مؤمنی پور، حسین)1390 .)از علت شناسی تا پیشگیری جرائم سایبری.

- بهره مند، حمید؛ کورهپز، حسین و سلیمی، احسان)1393 .)راهبردهای وضعی پیشگیری از جرائم سایبری. مجلهٔ آموزههای حقوق کیفری.

Grant, H. (2015). Social crime prevention in the developing world: exploring the role of police in crime prevention, Switzerland: springer.

- Solange Ghernaouti-Hélie (2010). We Need a Cyberspace Treaty: Regional and Bilateral Agreements Are Not Enough, Inter Media, vol. 38, Issue 3.

-Ploug, Thomas (May 2017). Ethics in Cyberspace: How Cyberspace May Influence Interpersonal Interaction, Ballerup28. Denmark, Springer pub: 2009, P 70(NATO Cooperative Cyber Defence Centre of Excellence, Accessed 17.

Evolutions de Loffer de securiteprivee en france RIcpT,200TournYoL Du cLoS,Lorraine (-

جدول خلاصه نوع و اندازه قلم‌های مورد نیاز برای تدوین مقالات فارسی

عنوان	قلم (فونت)	اندازه	نوع قلم
عنوان مقاله	B Nazanin	16	پررنگ
نام و نام خانوادگی	B Nazanin	12	پررنگ
مشخصات نویسندگان	B Nazanin	11	نازک
نشانی پست الکترونیکی نویسندگان	Times New Roman	10	نازک
عنوان بخش‌ها	B Nazanin	12	پررنگ
عنوان زیر بخش‌ها	B Nazanin	11	پررنگ
متن چکیده و واژگان کلیدی	B Nazanin	12	نازک
متن اصلی	B Nazanin	12	نازک
زیر نویس فارسی	B Nazanin	10	نازک
زیر نویس لاتین	Times New Roman	9	نازک
عنوان جدول ها، شکل ها و نمودارها	B Nazanin	10	پررنگ
متن فارسی درون جدول ها	B Nazanin	10	نازک
متن لاتین درون جدول ها	Times New Roman	9	نازک
منابع و مراجع فارسی	B Nazanin	11	نازک
منابع و مراجع لاتین	Times New Roman	10	نازک

Template for English Abstract
(Times New Roman size 14)

First Author Times New Roman 10 pt bold (centered)**Affiliation**

Email@daneshpajoohan.ac.ir Times New Roman 10 pt

Second Author[1]Times New Roman 10 pt bold (centered)**Affiliation**

Email@daneshpajoohan.ac.ir

Third Author،Affiliation

Email@daneshpajoohan.ac.ir

1-1-

Abstract -2-1

The abstract appears before the keywords. Abstract must be about 200 words. However, it must be limited between 150 to 200 words. The abstract should clearly state, the objective, results and the conclusion of the work.

Keywords: maximum of eight keywords seperated by “,”. **-1-3**

1-Corresponding Author