چالش پلیس ایران و یوروپل در مقابله با جرایم سایبری سازمان‌یافته

مهرداد تیموری[۱]، مژگان پورفتحی[۲]، امیرمهدی عزاداری[۲]

[۱]استادیار گروه حقوق کیفری و جرم‌شناسی، دانشگاه آزاد اسلامی واحد تبریز، تبریز، ایران
mehrdadteymoori1@gmail.com
[۲]دانشجوی کارشناسی ارشد حقوق کیفری و جرم‌شناسی، دانشگاه آزاد اسلامی واحد تبریز، تبریز، ایران
{mojganpoorfathii,azadariamir1351}@gmail.com

چکیده

جرایم سایبری از جهت انگیزه مجرمانه و نیز اهمیت رفتار مجرمانه و آثاری که به بار می‌آید باهم برابر و هم نوع نخواهد بود؛ ولی یک ویژگی مشترک در انجام رفتار مجرمانه در فضای مجازی و فضای حقیقی می‌باشد که مخدوش‌شدن امنیت می‌باشد. عدم پویایی دستگاه‌های اجرایی، عدم تبادل اطلاعات و یافته‌های سایبری بین‌المللی و نبود تجهیزات مؤثر شرکت‌های فعال در این امر سایبری و از سوی دیگر رقابت شدید اقتصادی بین کشورها و عدم وجود قانون‌گذاری هماهنگ و همسو بافرهنگ مردمان سرزمین‌ها در سطح جهانی سایت جنایی اجرایی ایران را نیز سرگردان کرده است. روش تحقیق به‌صورت نظری بوده و روش جمع‌آوری اطلاعات به‌صورت کتابخانه‌ای است روش تجزیه‌وتحلیل داده‌ها به‌صورت توصیفی و تحلیلی است. در نتیجه با پویا نمودن و عدم طفره‌رفتن از همکاری با کشورهای دیگر و نهادهای رسمی اجرایی بین‌المللی مانند پلیس اتحادیه اروپا (یورو پل) موجب می‌شود که با استفاده از تجربیات و آموزش‌های آنان پیشرفت‌های چشمگیری در برابر چالش‌های پیشرو مناسب‌تر اقدام نمایند. مشارکت بسیار فعال بخش خصوصی که کامل‌کننده سیاست جنایی اجرایی کشور می‌باشد با آموزش و آگاهی دادن کاربران به‌صورت رایگان در فضای مجازی مبارزه با جرایم سایبری و جرایم سازمان‌یافته بسیار کارآمد خواهد بود.

کلمات کلیدی: جرایم سازمان‌یافته، جرایم رایانه‌ای، یوروپل، پیشگیری از جرم، پلیس ایران.

۱ مقدمه

امروزه بشر به منظور تأمین آسایش و رفاه خود به تکنولوژی دست یافته است که در برخی موارد منجر به بروز برخی از جرایم شده است رشد و توسعه در تکنولوژی منجر به تنوع جدید در ساختارهای اجتماعی، اقتصادی و فرهنگی شده است ولی همگام با رشد و پیشرفت تکنولوژی همواره یکی از جرایمی که نظم و امنیت بین‌المللی را در حوزه‌های مختلف با تهدید روبرو می‌کند جرایم رایانه‌ای و جرایم سازمان‌یافته است.

یکی از چالش‌های جدید حقوق کیفری مقابله با جرایم سایبری است. با توجه به گستردگی و شبکه‌ای بودن فضای سایبر چالش‌های جدی به‌وجود می‌آید. وقتی صحبت از چالش است از ابتدا، امنیت آرامش و آسایش در فکر جریان می‌یابد افراد و کاربران در فضای سایبر تجربه اجتماعی از تعامل تبادل و اشتراک‌گذاری، اطلاعات کسب‌وکار، بازی و تفریح و بحث‌های گروهی به‌صورت غیرفیزیکی انجام می‌دهند. در سیاست امنیت سایبری سعی بر قابل دسترس بودن به یکپارچگی‌ای که شامل اعتبار و صحت است و نیز محرمانه بودن است.

مبارزه با جرایم امنیت سایبری نیازمند یک روش جامع است ارائه معیارهای تکنیکی به تنهایی نمی‌تواند از هیچ جرمی جلوگیری کند. در این فضا همانند فضای حقیقی تامین امنیت و صیانت از کاربران آن مورد توجه قرار گرفته و برخی از آموزه‌های عمومی تأمین امنیت محیط مادی نیز در این محیط به کار می‌رود. سطوح امنیت در فضای سایبری ، سایبری در دو حوزه امنیت دو حوزه امنیت فرد و اجتماع و امنیت ملی و حاکمیتی مطرح می‌باشد. با توجه به منافع مالی سرشار و ساختار خاص فضای سایبر و همچنین سامانه‌های حفاظتی در برابر مجرمان سایبری و نیز حضور مؤثر دولت‌ها در قالب پلیس‌های سایبری در این محیط زمینه‌های توسعه جرایم. سازمان‌یافته سایبری را فراهم آورده است. محور اصلی سیاست جنایی هر کشور در پیشگیری و مقابله با جرایم است. متأسفانه امروز شاهد هستیم – جرایم سایبری در فضای مجازی هر روز روبه افزایش است و با توجه به قوانین کیفری موجود به نظر می‌رسد که دولت نتوانسته است در زمینه سیاست جنایی پیش گیرنده موفق عمل نماید، لذا هر ساله شاهد ورود خسارت‌های هنگفت مالی و حیثیتی به اشخاص اعم از حقیقی و حقوقی هستیم، بنابراین اتخاذ یک سیاست جنایی تقنینی قضایی و اجرایی مناسب در جهت کاهش آمار جرایم ارتکابی رایانه‌ای به‌ویژه مطالعه قوانین و سیاست‌های اتحادیه اروپا در این این زمینه مفید به نظر می‌رسد.

لذا هدف اصلی نگارنده در این نوشتار شناسایی بستر و جلوه‌های حقوق در امر مبارزه با جرایم رایانه‌ای و جرایم سازمان‌یافته در ایران و اروپا و سپس چالش‌ها و موانع فراروی اجرای کارآمد و مؤثر و تدابیر لازم با بهره گیری از قوانین و مقررات حاکم در ایران و اتحاد اروپا توسط پلیس ایران و اروپا می‌باشد. پژوهش حاضر درصدد پاسخ گویی به این سؤال‌های اساسی زیر است.

۱. چه چالش‌هایی در رابطه با پلیس ایران و یوروپل در مقابله با جرایم اینترنتی و سازمان‌یافته موجود است؟

۲. راهکارهای مقابله با جرایم اینترنتی و سازمان‌یافته چیست و از چه طریقی امکان‌پذیر است؟

۳. پلیس ایران و یوروپل در راستای کاهش این جرایم چه همکاری‌هایی را می‌توانند انجام می‌دهند؟

فرضیه‌های پژوهش

جنبه‌ی بین‌المللی جرایم، تغییر ماهیت دلایل اثبات جرم، ناهماهنگی قوانین کشورهای مختلف، فقدان همکاری متقابل کشورها و فقدان ساختار و رویه واحد ازجمله چالش‌های موجود در این زمینه هستند که با الگوبرداری از اتحادیه اروپا و با همکاری در عرصه بین‌المللی و وضع قوانین جدید می‌توان گامی مؤثر برداشت.

پلیس ایران و لیورپول نیز می‌توانند در راستای تعقیب متهمان این جرایم و بازجویی از آنها در امور مربوط به ارائه دلایل جرم و اعلام دقیق محل وقوع آن به یکدیگر یاری رسانند.

۲ مفهوم‌شناسی

۱.۲ مفهوم جرایم رایانه‌ای

مهم‌ترین چالش در خصوص جرایم رایانه‌ای تعریف آن است طیف گسترده‌ی افعال مجرمانه‌ای که ذیل این مفهوم جا دارند و ماهیت متغیر آن که ناشی از پیشرفت لحظه به لحظه فناوری اطلاعات و شیوه‌های سوءاستفاده از آن است ارائه تعریف جامع مانع و خالی از مناقشه را مشکل و چه بسا غیرممکن می‌سازد. تا آنجا که در کنوانسیون جرایم سایبری ۲۰۰۱ در بوداپست نیز تعریفی از این جرایم به عمل نیامده است.طبق تعریف ارائه شده از سوی گروهی از کارشناسان سازمان همکاری و توسعه اقتصادی (OECD) در سال ۱۹۸۳، جرایم رایانه‌ای را هر عمل غیرقانونی غیراخلاقی یا غیرمجاز نسبت به پردازش خودکار یا انتقال داده‌ها عنوان کرده‌اند (ذبیح الله، ۱۴:۱۳۹۶) [۱]. سازمان ملل متحد در سال ۱۹۹۴ در شماره ۴۴ نشریه بین‌المللی سیاست جنایی با اذعان بر اینکه در زمینه جرایم رایانه‌ای تعریف مورد توافق و مشترکی وجود ندارد جرایم رایانه‌ای را از یک سو شامل فعالیت‌های مجرمانه با ماهیت سنتی مثل سرقت و جعل دانسته که همگی معمولاً در همه جا مشمول ضمانت اجراهای کیفری می‌شوند و از سوی دیگر شامل فعالیت‌های مجرمانه نوینی که در آن‌ها رایانه امکان اینگونه سواستفاده‌ها را مهیا ساخته و پیش از این امکان‌پذیر نبوده است، می‌داند (تقی زاده، زمردی و حاجیان،۱۱۲:۱۳۹۶) [۲]. در حقیقت سازمان ملل متحد به نوعی از طبقه‌بندی جرایم رایانه‌ای اشاره دارد نه تعریف جرم رایانه‌ای. برخی از سازمان‌های بین‌المللی قانون‌گذاران کشورهای مختلف و متخصصین حقوق کیفری با توجه به عوامل مختلفی همچون تفاوت سطح کاربری و بهره برداری از فناوری اطلاعات در کشورهای مختلف تعاریف متعدد مطرح کرده‌اند ولی در یک جمع‌بندی و به اختصار از نظر قانون‌گذاری و جرم‌انگاری چنین تشریح و تعریف می‌گردد که هر جرمی که به موجب حکم صریح قانون، سیستم و یا داده رایانه‌ای به عنوان موضوع یا وسیله آن اعلام شده و در نتیجه جزء عنصر مادی آن باشند، جرم رایانه‌ای نامیده می‌شود.

عده‌ای دیگر از دیدگاه جرم‌شناسی چنین تعریف می‌کنند هر جرمی که سیستم یا داده رایانه‌ای عملاً موضوع و یا وسیله ارتکاب آن باشد اعم از اینکه قانون‌گذار رایانه را به عنوان وسیله ارتکاب آن اعلام کرده یا نکرده باشد جرم رایانه‌ای نامیده می‌شود.

گروه سوم از دیدگاه آیین دادرسی کیفری به جرم رایانه‌ای نگریسته و چنین بیان می‌کنند که هر جرمی که رایانه به نحوی به عنوان موضوع یا ابزار جرم در آن نقش داشته باشد و یا دلایل یا اطلاعات مربوط به آن در رایانه ذخیره یا پردازش یا منتقل شده باشد، جرم رایانه‌ای نامیده می‌شود (خرم آبادی، ۴۱:۱۳۸۳) [۳].

با توجه به شناخت مصادیق مجرمانه این جرم می‌توان به تعریفی مصداقی به شرح ذیل دست یافت: «هر رفتار ضد رایانه و موضوعات مرتبط با آن که قانون برای برای آن کیفر تعیین کرده باشد، جرم رایانه‌ای است» (عالی‌پور، حسن: ۴۱). در واقع جرم رایانه‌ای جرمی است که رایانه در آن موضوعیت دارد.

جرایم مرتبط با جرایم رایانه‌ای، جرایم اینترنتی و جرایم سایبری می‌باشد، که در رابطه با جرایم رایانه‌ای یک اتاق، یک کاربر و سخت‌افزار یعنی کامپیوتر به عنوان ابزاری ضروری و لازم در برقراری ارتباط در شبکه اینترنت می‌باشد. رایانه به‌دلیل حجم کم، سرعت پردازش بالا و عملکرد سریع به‌عنوان ابزاری مشروع برای اهداف نامشروع می‌تواند دخیل باشد. «سایبراسپیس» یا فضای سایبری در زبان فارسی فضای مجازی ترجمه شده‌است که این ترجمه معادل دقیق برای این واژه نیست زیرا محیط سایبر محیط حقیقی و واقعی است نه مجازی. هر چند جهان سایبر به شکل مادی و ملموس احساس‌شدنی نیست و به شکلی پنهانی و مخفی و پوشیده می‌باشد ولی می‌تواند نمودی فیزیکی در نتیجه و آثار داشته باشد.

استگانوگرافی[1] یا پنهان نگاری در این فضا جهت انجام جرایم سایبری به‌طور عمده مدنظر مجرمین می‌باشد، زیرا بسیاری از جرایم در فضای سایبر عملاً کشف نمی‌شوند و لذا رقم سیاهه جرایم کشف نشده در این حوزه از جرایم کشف‌شده بسیار بیشتر است. هر چند باید توجه کرد که با افزایش دانش و توسعه تکنولوژی و با قابلیت ضبط و ثبت در کشورهای متفاوت، جلوی این پوشیده بودن را می‌توان به مقدار زیادی گرفت.

فضای سایبر با گستره جهانی است و جرم سایبر در این فضای گسترده اتفاق می‌افتد و برخلاف دیدگاه برخی افراد، این جرایم زیرمجموعه‌ای از جرایم اینترنتی نمی‌باشد.

قانون‌گذار، قانون جرایم رایانه‌ای مشتمل بر ۵۶ ماده و ۲۵ تبصره به عنوان مواد ۷۳۰ تا ۷۸۳ قانون مجازات اسلامی (بخش تعزیرات) و با عنوان فصل جرایم رایانه‌ای منظور نمود. بعد از تصویب قانون آئین‌دادرسی جرایم نیروی مسلح و دادرسی الکترونیکی و الحاق آن به قانون آیین دادرسی کیفری بخش مربوط به آئین دادرسی یعنی مواد ۷۵۶ تا ۷۷۹ ملغی گردید. جرایمی که در قانون جرایم رایانه جرم‌انگاری شده است را می‌توان در چند بخش تقسیم‌بندی کرد:

۱. جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی؛ که این جرایم شامل دسترسی غیرمجاز در بسیاری از موارد به‌عنوان مقدمه و تسهیل‌کننده سایر جرایم رایانه‌ای می‌باشد که برخی این جرم را به جرم مادر یا زاینده تعبیر می‌نمایند؛ دسترسی غیر مجاز با دیگر جرایم رایانه‌ای اگر همراه گردد، موضوع مشمول تعدد مادی خواهد بود: شنود غیر مجاز، جاسوسی رایانه‌ای.

۲. جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی که این جرایم شامل جعل رایانه‌ای، تخریب و اخلال در داده ها یا سامانه‌های رایانه‌ای و مخابراتی، سرقت و کلاهبرداری رایانه‌ای است.

۳. جرایم علیه عفت و اخلاق عمومی و شخصیت معنوی مانند هرزه‌نگاری (که علاوه بر ماده ۶۴۰ قانون مجازات بخش تعزیرات قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز می‌نمایند نیز به این موضوع پرداخته است)، هتک حیثیت از طریق انتشار محتوای صوتی و تصویری تغییر یافته یا تحریف شده و ... .

[1] Steganography

به‌عنوان مصادیق یا روش روند نفوذ به سیستم‌ها از طریق کاربرد حیله‌های گوناگون در خصوص افراد جهت افشای کلمات عبور و اطلاعات مربوط که مهندسی اجتماعی نامیده می‌شود از طریق تماس‌های تلفنی مانند میس کال یا تبلیغات ماهواره‌ای با وعده جایزه‌های خوب و غیره صورت می‌گیرد.

۲.۲ جرایم سازمان‌یافته

به‌رغم توجه محافل حقوقی و جرم‌شناسان به بحث جرایم سازمان‌یافته در سال‌های اخیر و نیز امضاء سند پذیرش کنوانسیون مبارزه با جرایم سازمان‌یافته موسوم به پالرمو در سال ۲۰۰۰ توسط ایران، نظام تقنینی رویکرد دقیق و منسجم در قبال تعریف و جرم‌انگاری این دسته از جرایم نداشته است و به نظر می‌رسد به رغم اقدامات انجام شده در حوزه تقنین و تشکیل شورای عالی فضای مجازی هنوز نقشه راه یکپارچه برای مدیریت کل فضای مجازی وجود ندارد این موضوع می‌تواند ناشی از تأخیر در نهادسازی و قانون‌گذاری و سرعت تحولات این فضا باشد.

تعریف‌های زیادی از جرم سازمان‌یافته ارائه شده است که با وجود تفاوت‌هایی که دارند از حیث مفهوم مشترک هستند با این حال تعریف مناسب که در مرحله عمل به کار رفته است تعریف سازمان پلیس جنایی بین‌المللی (اینترپل) ارائه کرده است که جرایم سازمان‌یافته به فعالیت‌های غیرقانونی گروهی مجرمانه با ساختار یکپارچه و متحد اطلاق می‌شود که هدف اساسی آن از این فعالیت‌ها به دست آوردن پول از این راه بوده و غالباً با ایجاد ترس و فساد ادامه حیات می‌دهد.

ولی تعریف جامع‌تر جرم سازمان‌یافته عبارت از فعالیت‌های غیرقانونی و هماهنگ گروهی منسجم اشخاص است که با تبانی با هم و برای تحصیل منافع مادی و قدرت به ارتکاب مستمر مجرمانه شدید می‌پردازند و برای رسیدن به هدف از هر نوع ابزار مجرمانه نیز استفاده می‌کنند (شمس ناتری، ۲۵:۱۳۸۰) [۴]. تعریف اینترپل از کنوانسیون سازمان ملل متحد علیه جرایم سازمان‌یافته و فراملی مصوب سال ۲۰۰۰ مشهور به کنوانسیون پالرمو استنباط می‌شود در این کنوانسیون جرایم سازمان‌یافته به جرایم شدید یا خاص پیش بینی شده در کنوانسیون اطلاق می‌گردد که توسط گروهی متشکل از سه نفر یا بیشتر و با هدف تحصیل مستقیم یا غیر مستقیم منفعت مالی یا مادی برای مدتی ارتکاب می‌یابد [۱۲]. در قانون ایران تعریف از جرایم سازمان‌یافته دیده نمی‌شود بلکه در چند ماده مثلاً ماده ۷۵۴ قانون مجازات اسلامی در بندهای«د» و «ه» ماده ۴ قانون تشدید مجازات اختلاس و رشا و ارتشا و کلاهبرداری، تبصره ۴ ماده ۳ قانون پول‌شویی دیده می‌شد که در این مواد مقنن در خصوص، تشدید مجازات استفاده کرده است. البته در مورد سردستگی گروه مجرمانه سازمان‌یافته ماده ۱۳۰ قانون مجازات اسلامی، صرفاً تعریفی از گروه و سردستگی ارائه نموده است.

۱.۲.۲ ویژگی سازمان مجرمانه

از آنجا که جرایم سازمان‌یافته به‌طور عمده توسط سازمان‌ها و گروه‌های مجرمانه ارتکاب می‌یابد، ابتدا به ویژگی‌های سازمان مجرمانه می‌پردازیم و سپس به ویژگی‌های جرم سازمان‌یافته خواهیم پرداخت. لذا سازمان نقش مهمی را در ارتکاب و جهت‌دهی جرایم ارتکابی دارد که دارای ویژگی‌های زیر می‌باشد.

۱. غیرایدئولوژیک بودن سازمان یا گروه مجرمانه: جرایم را تنها با اهداف اقتصادی و کسب منافع مادی

انجام می‌دهند و با دلبستگی‌های مذهبی و سیاسی اقدام به ارتکاب جرم نمی‌کند. هدف این گروه فقط کسب پول و قدرت و منفعت مادی است. شاید این گروه‌ها گاهی به مبارزات سیاسی هم روی آورند ولی هدف اساسی کسب قدرت سیاسی نیست.

۲. وجود سلسله مراتب: باید سازمانی فعال که قابلیت طراحی ،تبانی، هدایت و ارتکاب جرم را داشته باشد. این سازمان نیاز به مدیر و مجریان دارد که هر کدام با موقعیتی ویژه و بر اساس نظر افراد مافوق خود انجام وظیفه می‌کنند [۱۳].

۳. استمرار جرم در طول زمان: در برخی موارد، برخی از افراد جهت ارتکاب جرم خاصی دور هم جمع شده و با هماهنگی و هم فکری اقدامی مجرمانه را به صورت جمعی برای یک بار انجام می‌دهند این سازمان‌یافته به معنای مورد نظر نیست شاید جرایم گانگستری برای مدتی محدود باشد آنچه لازم است این است که گروه مجرمانه برای یک دوره طولانی یا غیر مقید به زمانی خاص ولی مستمر تشکیل شده باشد [۱۴].

۴. ارتکاب فساد اداری: بهره‌گیری از فساد اداری در جهت حفظ اعضای خود از تعقیب و محاکمه و یا به انجام رساندن امور جاری خود در ادارات دولتی یک ویژگی خاص برای این سازمان‌ها است مثلاً فاسد نمودن مدیران عالی و کارمندان اجرائی یا دخالت در انتخابات پارلمانی جهت فرستادن نمایندگان مورد نظر خود به مجلس و کسب موفقیت‌های لازم در این جهت برای موجه نشان دادن فعالیت‌های نامشروع خود می‌توان نام برد.

۵. استفاده از ارعاب و خشونت: در مواجهه با گروه‌های رقیب یا ماموران که قبلاً با این سازمان همکاری می‌کردند و دیگر علاقه‌ای به همکاری ندارند از ارعاب استفاده می‌شود مثلاً ارعاب و تهدید ماموران برای افشاء اسرار و همکاری سابق را می‌توان نام برد.

۶. تأمین و ارائه کالاها و خدمات غیرقانونی

۷. تقلب در پرداخت مالیات و دیگر عوارض دولتی

۸. ارتکاب تهیه پول

۲.۲.۲ ویژگی‌های جرم ارتکابی

به عنوان جرم سازمان‌یافته، بعضی از نویسندگان ویژگی «شدت» را در نظر گرفته‌اند و این در پیش‌نویس کنوانسیون پالرمو در سال ۲۰۰۰ در ماده ۲ «شدت جرم» از «ویژگی‌های جرایم سازمان‌یافته» قلمداد شده و بر مبنای آن مفاد کنوانسیون باید تنها نسبت به جرم‌های شدید قابل اعمال می‌باشد یعنی جرایمی که توسط سازمان مجرمانه ارتکاب یافته و دارای مجازاتی با حداقل ۴ سال حبس باشد. گرچه از جمله شرایط دیگر آن اقتصادی بودن جرم است که به هدف مرتکبان برمی‌گردد ولی ویژگی شدید بودن به ماهیت جرم برمی‌گردد

[۱۲]. از آنجایی که امروزه به دلایل مختلف بسیاری از جرایم سازمان‌یافته از حیث مرتکبان جرایم، مکان ارتکاب جرم و قلمرو تاثیر گذاری آن‌ها، محدود به مرزهای جغرافیایی یک کشور نمی‌باشد، آنها به دو گروه جرایم سازمان‌یافته فراملی و جرایم سازمان‌یافته داخلی تقسیم شده است.

جرم فراملی به جرم‌هایی اطلاق می‌شود که اقدامات مقدماتی یا ارتکاب جرایم یا اهداف مورد نظر از اجرای آن‌ها به صورت مستقیم یا غیرمستقیم بیش از یک کشور را در برمی‌گیرد. از جمله عواملی که در گسترش جرم سازمان‌یافته در خارج از مرزها مؤثر بوده و به آن جنبه‌ای فراملی بخشیده است، توسعه صنایع مربوط به ارتباطات سریع از راه دور و رایانه‌ای شدن آن‌ها، ضرورت وجود اقتصاد جهانی و آزادی آن و پایان جنگ سرد میان دو ابرقدرت شرق و غرب بوده است (شمس ناتری، ۳۴:۱۳۹۷) [۴].

در بند ۲ از ماده ۳ کنوانسیون پالرمو معیارهایی حصری برای تشخیص ماهیت فراملی یک جرم مقرر شده است:

الف) جرم در بیشتر از یک کشور ارتکاب یافته باشد.

ب) چنانچه جرم در یک کشور ارتکاب پیدا کند ولی بخش اساسی از تدارک طراحی هدایت یا کنترل جرم در کشور دیگری رخ دهد.

ج) محل ارتکاب جرم یک کشور باشد ولی یک گروه مجرمانه سازمان‌یافته که در بیش از یک کشور به فعالیت مجرمانه اشتغال دارد جرم را مرتکب شده است.

د) جرم در یک کشور ارتکاب یافته ولی آثار قابل توجهی در کشور دیگر داشته است (امامی، ۴۴:۱۴۰۱).

۳ نقش و جایگاه پلیس در جرایم سایبری سازمان‌یافته

پلیس در راستای تامین امنیت جامعه که وظیفه پیشگیری از جرایم و کنترل مجرمان را به عهده دارد. سعی در شناسایی نقاط ضعف و قوت با تجزیه و تحلیل اطلاعاتی و آماری است این به خاطر این است که پلیس مسئولیت انگیزش و تسهیل تلاش‌های پیشگیری اجتماعی از جرم را بر عهده دارد. همچنین مسئولیت جمع آوری و تحلیل اطلاعات مورد نیاز به منظور تهیه یک طرح بهینه برای پیشگیری از جرم بر عهده پلیس است و مصائب و مشکلات نمی‌توانند به نحو مؤثری مورد برخورد قرار گیرند مگر آنکه یک جامعه به طور دقیق چگونگی آنها را درک کند به بیان دیگر ما نمی‌توانیم امیدوار باشیم که تلاش‌های پیشگیری از تکرار جرم مجرمان موفقیت آمیز باشند مگر آنکه مشکلات و آماج فرصت جرم را به دقت شناسایی و سپس راهبردهای پیشگیری از جرم را برای برخورد با آن‌ها طراحی کنیم (شری‌زاده: ۶۵). در حقیقت سیاست جنایی اجرایی سیاستی است که قوه مجریه و اعضای آن از جمله پلیس، برای سیاست جنایی تقنینی و به منظور پیشگیری از وقوع جرم یا گسترش آن در جامعه اتخاذ می‌کنند. در این عرصه نقش و عملکرد پلیس در مرحله رویارویی با پدیده جنایی یعنی کشف جرایم و تعقیب متهمین و نیز در مرحله پاسخگویی به جرایم یعنی سطوح اجرای احکام و تصمیمات در راستای پیشگیری از پدیده جنایی مطرح می‌شود. کلیه سیاست‌های اجرایی نهاد پلیس

باید بر پایه اصل پیشگیری باشد، زیرا هزینه‌هایی که امر پیشگیری به دنبال دارد خیلی کمتر از هزینه‌های مواجهه با جرم می‌باشد (حیدری، شهبازی و شیبانی، ۴۳:۱۳۹۷) [۵].

پلیس فتا، به‌عنوان زیر مجموعه‌ای از سازمان پلیس در ایران می‌باشد. در اساسنامه تشکیل پلیس فتا این‌گونه آمده است که هدف از تشکیل پلیس فضای تولید و تبادل اطلاعات می‌توان تأمین امنیت فضای مجازی، صیانت از هویت دینی، ملی و ارزش‌های انسانی در جامعه، حفظ حریم خصوصی و آزادی مشروع، صیانت از منافع، اسرار و اقتدار ملی در فضای تولید و تبادل اطلاعات، ممانعت از تعرض به ارزش‌ها و هنجارهای جامعه، حفظ زیرساخت‌های حیاتی کشور در مقابل حملات الکترونیک، اعتماد و آسودگی خاطر آحاد شهروندان جامعه برای انجام تمامی امور قانونی ازجمله فعالیت‌های اقتصادی، اجتماعی و فرهنگی به‌منظور صیانت از حاکمیت و اقتدار ملی دانست. پلیس فتا با استفاده از نیروهای متخصص و آگاه به فناوری نوین الکترونیک اقداماتی جدی در جهت رفع آسیب‌های سایبری و جرایم فضای مجازی انجام داده است که موجب تأمین سلامت و امنیت در فضای مجازی شده است [۶]. پلیس فتا تنها پلیس فعال در حوزه امنیت سایبری می‌باشد که اقدامات پیشگیرانه جهت حفاظت از اطلاعات مالی به عمل آورده است که در تاریخ ۳ بهمن ۱۳۸۹ به دستور فرمانده نیروی انتظامی ایران شروع به کار کرد. پلیس به دو قسم تقسیم می‌شود پلیس عملیاتی که ماهیت عملکردشان اساساً پیگیری می‌باشد نه پیشگیری و پلیس ستادی که بنا به دستور مقام قضایی به رصد سایت‌ها یا درگاه‌های الکترونیکی می‌پردازد.

هشداردهی و آگاه‌سازی عمومی از فواید و مضرات فضای سایبر از وظایف پلیس ستادی می‌باشد که این هشدارها بیشتر در جهت حفظ حریم خصوصی است و پلیس ستادی بنا به دستور مقام قضایی در صورت تحقق یافتن جرم سعی در اعمال تدابیر واکنشی از جمله فیلتر نمودن سایت‌ها بوده و بیشتر اقداماتشان در جهت پالایش محتوا می‌باشد (وطنی و اسدی، ۱۱۸:۱۳۹۵) [۷].

پلیس فتا می‌تواند در راستای پیشگیری از جرایم سایبری به طور مداوم به داده‌های حاصل از تبادل اطلاعات دسترسی داشته و کلیه ارائه کنندگان خدمات مکلفند که در این خصوص با پلیس همکاری کنند.

شیوه‌های پیشگیری از جرم با آموزش همگانی و ارائه آموزش‌های مورد نیاز به اشخاص و سازمان‌هایی که احتمال دارد در معرض جرایم سایبری قرار گیرد و نیز استفاده از متخصصین دارای مدرک جرم شناسی سایبری بوده و علاوه بر این متخصصین تحصیل کرده خدمت گرفتن از مجرمین با سابقه و حرفه‌ای در این زمینه می‌تواند مثمر ثمر باشد چرا که همیشه مجرمین یک قدم از نهادهای امنیتی جلوتر می‌باشد و با توجه به اینکه دامنه سنی از ۱۰ تا ۶۰ سال و دامنه مهارت آن‌ها از تازه کار تا حرفه‌ای گسترده می‌شود، استفاده از تجربیات این قشر نیاز به علوم دیگر جنایی می‌باشد چون بین این افراد مرتکبین اتفاقی و مجرمین واقعی پراکنده می‌باشد.

با توجه به تنوع علل ایجاد جرم جهت پیشگیری مشارکت تمامی افراد و نهادهای دخیل، در این مورد لازم می‌باشد و علاوه بر این باید مقررات جامعی در زمینه فعالیت و ساماندهی سازمان‌های دخیل، در خصوص جرایم رایانه‌ای تدوین گردد.

پلیس اروپا (یوروپل) یک مجمع همکاری امنیتی در میان وزیران کشور و دادگستری جامعه اروپا که ۱۹۷۶ ایجاد شد. هلموت کهل صدراعظم آلمان پیشنهاد یک آژانس پلیس اروپا مشابه اداره تحقیقات فدرال

(FBI) را ارائه کرد و اداره پلیس اروپا فعالیت‌های خود را از ژوئیه ۱۹۹۹ آغاز کرد (امامی ۷۵). کمیسیون اروپا بر پایه مطالعات امکان سنجی انجام شده تصمیم به ایجاد مرکز مبارزه با جرایم سایبری و یوروپل گرفت و نهایتاً در سال ۲۰۱۳ مرکز مبارزه با جرایم سایبری اروپایی را برای تقویت اجرای قانون جهت مقابله با جرایم اینترنتی در اتحادیه اروپا و همچنین کمک به محافظت از شهروندان اروپایی کسب و کار دولت در قبال جرایم اینترنتی ایجاد کرد که ۳ وظیفه بر عهده این مرکز در نظر گرفته شد، اول جرایم سایبری که توسط گروه‌های سازمان‌یافته انجام می‌شود به ویژه افرادی که سودهای بزرگی از اقداماتی نظیر کلاهبرداری آنلاین به دست می‌آورند دوم جرایم سایبری که صدمات جدی به قربانیان خود وارد می‌کند مانند سوء استفاده جنسی آنلاین،کودکان سوم جرایم سایبری که بر زیرساخت‌های مهم و سیستم‌های اطلاعاتی تاثیر می‌گذارد این مرکز مشارکت مهمی نیز با تیم‌های واکنش اضطراری رایانه شرکت‌های مهم اینترنتی و خدمات مالی صنعت ضد بدافزار تولید کنندگان نرم افزار و دانشگاه‌ها آغاز نموده است.(مرکز جرایم سایبری اروپا۴:۲۰۱۴). یوروپل دارای ساختار منسجم و پیشرفته است و در رویکرد استراتژی، یوروپل در دو حوزه«استراتژی و توسعه» و«توسعه و مدیریت اشخاص ذی نفع»فعالیت می‌نماید. یکی از اهداف اصلی یوروپل اختیار اجرای قانون اتحادیه اروپا با پشتیبانی و حمایت عملیاتی در حوزه متعدد کیفری می‌باشد که در زمینه جرایم رایانه‌ای عبارت است از حملات سایبری تقلب در پرداخت کارت تجارت غیرقانونی آنلاین از جمله مواد مخدر، اسلحه گرم، قاچاق انسان، ارزهای مجازی، اسناد جعلی، پول‌شویی و تقلبی.

۴ چالش‌های پلیس در قبال جرایم رایانه و سازمان‌یافته

مولفه‌هایی مانند داشتن جنبه بین‌المللی، شکل تعریف واحد از جرایم مجازی، تغییر ماهیت دلایل اثبات جرم، مسائل خاص مرحله کشف، ناهماهنگی قوانین کشورهای مختلف، فقدان کاری متقابل به ویژه در حوزه پیشگیری از جرم و آئین دادرسی، فقدان ساختار و رویه واحد چالش‌های موجود در این فضا می‌باشند که به بیان آن‌ها می‌پردازیم.

۱.۴ عدم هماهنگی پلیس با نهادهای دیگر کشورها

جرایم رایانه‌ای طبع جهانی دارند و مقابله با آن‌ها اقدامات یکسان بین‌المللی را می‌طلبد و چون این جرایم در سیستم‌های قضایی کشورهای مختلف به‌صورت یکسان تعریف نشوند تلاش‌های پلیس برای برخورد هماهنگ با این جرایم غامض و پیچیده خواهد شد (حیدری، شهبازی، شیبانی، ۴۸:۱۳۹۸) [۵]. با توجه به جنبه فراملی بودن جرایم رایانه‌ای در حوزه پیشگیری از جرم و آئین دادرسی، کشف جرایم سایبری تعقیب متهمان دستگیری، انتقال محکومان، نیابت قضایی و بازجویی رویه یکسانی در کشورها بخصوص ایران در بعد بین‌المللی به چشم نمی خورد.

این چالش در پلیس اروپا (یوروپل) به علت همکاری‌های حقوقی با اینترپل در مقابله با جرایم سایبری بسیار کمتر به چشم می‌خورد .بند دوم از ماده ۴۲ اساسنامه تشکیل پلیس کشورهای عضو اروپا بیان می‌دارد یوروپل در راستای وظایف بیان شده در ماده ۳ اساسنامه می‌تواند روابط خود را با دولت‌ها و سازمان‌های دیگر

از جمله اینترپل جهت مبارزه با جرایم و پیشگیری از آن‌ها برقرار کند. یوروپل در جهت مقابله با جرایم مواد مخدر و سایر جرایم از جمله جرایم سایبری طبق توافق‌نامه همکاری ۶ دسامبر سال ۲۰۰۱ با سازمان ملل همکاری می‌کند و این نیز این چالش را برای پلیس اروپا کمتر می‌کند (امیری، ۱۳۹۴: ۵۴) [۸].

۲.۴ عدم تطبیق با نیازهای روز پلیس

ماهیت خاص دلایل الکترونیکی به‌گونه‌ای می‌باشد که پذیرش آن‌ها را در مراجع قضایی با چالش‌های ویژه‌ای مواجه کرده است. به‌منظور مقابله با این چالش‌ها ماموران پلیس باید به روش‌های خاص و جدید جمع‌آوری دلایل مذکور مطابق با نیازهای روز که مرکب از چهار مرحله جمع‌آوری مدرک، بررسی، تجزیه و تحلیل و ارائه گزارش می‌باشد، دست یافته و به نحو صحیحی اجرا نماید (پرویزی، ۱۳۸۵). با توجه به ویژگی فرامرزی بودن برخی جرایم سایبری قانون ایران و کنوانسیون جرایم سایبری راهکاری در خصوص جمع‌آوری موجود در خارج از کشور ارائه نکرده‌اند و این امر به‌عنوان مهم‌ترین چالش در پلیس سایبری کشورها مطرح شده و راهکاری در این خصوص ارائه نشده است (جلالی، ۴۷:۱۳۹۴) [۹].

تهدیدها در فضای مجازی گستردگی فراوانی دارد که می‌تواند ناشی از تهدیدات خارجی یعنی از سوی کسانی که به یک کشور خارجی از قبیل بخش‌های نظامی و آژانس‌های امنیتی و شاید شرکت‌هایی که به دولت‌ها وابسته هستند باشد و شاید تهدیدات ناشی از گروهک‌های تروریستی و گروه‌های افراطی باشد که به دولت خاصی وابسته نباشند و یا تهدیدات از ناحیه افراد می‌باشد که شامل جنایتکاران و سازمان‌های جنایی است. این گروه نه تنها جرایم سازمان‌یافته بزرگ را در فضای مجازی مرتکب می‌شوند، بلکه به‌صورت انفرادی نیز اقدام می‌کنند در فضای مجازی تهدیدسازان می‌توانند کاربران داخل سازمان‌ها و نیروهای خودی نیز باشند (حسن بیگی، ۱۲:۱۳۸۴) [۱۰]. نداشتن تخصص کافی نهادهای اجرایی همگام با پیشرفت روز افزون فناوری‌ها در راستای تعقیب و کشف جرایم رایانه‌ای چالش محسوب می‌شود نتایج ضعیف ناشی از عدم هماهنگی سطح دانش نیروهای پلیس در سال‌های اخیر از نظر نهادهای بین‌المللی و منطقه‌ای مسئول مبارزه با جرایم پوشیده نمانده است و همه به این اجماع رسیده‌اند که برای ایجاد فضایی امن و جلوگیری مؤثر از جرایم سایبری نیازمند ارتقاء دانش تخصصی می‌باشد. میزان ادله جمع آوری توسط پلیس از دیگر چالش‌ها می‌باشد به نظر می‌رسد ادله الکترونیکی در چهارچوب نظرات کارشناس اعتبار می‌یابد ولی نوع نگاه مراجع رسیدگی کننده به جرایم سایبری و میزان تخصص و آشنایی آن‌ها با ادله الکترونیکی نقش تعیین کننده در سرنوشت تعقیب و اثبات این جرایم دارد. جهت تقویت پلس ایران در این حوزه باید به آخرین نوآوری‌ها دست یافته و از طریق همکاری با اینترپل و یوروپل از تجارب آن‌ها بهره مند شد.

۳.۴ چالش‌های فنی

جرایم رایانه‌ای و سازمان‌یافته بیشتر مواقع ماهیتی فنی و تخصصی دارند ارائه دهندگان خدمات سایبری بسیاری اوقات اشخاص حقیقی و حقوقی غیر دولتی هستند عدم تناسب آموزش‌های تخصصی با نیازهای جامعه امنیت پائین شبکه‌های مخابراتی ضعف زیرساخت‌های مخابراتی و نبود استانداردهای مناسب در ارتباط با تبادل اطلاعات موجب چالش‌های فنی می‌شود. این چالش‌ها به سه حوزه دسترسی غیر مجاز، استفاده غیر

مجاز و ریزش ناخودآگاه اطلاعات تقسیم می‌گردد. لذا چنانچه کشورها بصورت مستقل مبادرت به آموزش واحدهای فنی خود نمایند و هماهنگی و تعامل کارآمد و اثر بخش میان تمامی دست اندرکاران این حوزه به وجود نیاید و مرکز فرماندهی واحد برای آنها پیش بینی نشود لطمات جبران ناپذیری برای کاربران ایجاد خواهد شد.

در فضای سایبر برای حفاظت تدابیری لازم است که ناظر به کنترل ورودی و خروجی و کنترل ابزاری ارتکاب جرم را تسهیل می‌کند.

۴.۴ هماهنگ نبودن هنجارهای ملی و بین‌المللی

تنوع نظام‌های سیاسی، اجتماعی و فرهنگی کشورها مانعی اساسی در راه ایجاد یک وفاق برای هنجارگذاری در فضای مجازی محسوب می‌شود. سیاست جنایی عموم کشورها در قبال جرایم سایبری و سازمان‌یافته به این نتیجه رسیده است که رویکرد ملی به تنهایی برای مقابله با این جرایم کافی نیست این چالش برای پلیس ایران در مقایسه با یوروپل نمود بیشتری پیدا می‌کند. نیاز به ارتقاء فرهنگ سایبری و تدابیر در مولفه‌های فرهنگی در جامعه به شدت مورد نیاز به نظر می‌رسد.

۵.۴ استنادپذیری ادله

مشکل جمع آوری ادله و ارزیابی آن‌ها در جرایم فضای مجازی در اکثر کشورها وجود دارد. مشکلات ناشی از ادله الکترونیک به سه قسم تقسیم می‌شود.

۱. ناشی از کشف و شناسایی ادله که به علت ماهیت غیر ملموس و غیر مادی ادله الکترونیکی مشکلات زیادی در فرآیند کشف و شناسایی ادله وجود دارد، از جمله اخفای جرم نامرئی بودن کدگذاری مدارک امحاء مدارک و فراوانی داده‌ها.

۲. قضایی، در مشکلات قضایی می‌تواند مرتبط با قدرت دستیابی و قابلیت جمع آوری ادله باشد و نیز میزان اعتبار ادله جمع آوری شده توسط ضابطان از دیگر چالش‌ها می‌باشد.

۳. تخصصی، در مشکلات تخصصی کمبود نیروی انسانی آموزش دیده در پلیس به چشم می‌خورد.

۶.۴ وجود نهادهای موازی

در ایران پراکندگی و تعدد نهادهای متولی پیشگیری از جرم، ناهماهنگی بین نهادهای ذیربط و نیز نبود یک سیاست علمی، هماهنگ و سنجیده باعث هدر رفتن امکانات و ظرفیت‌های سازمان‌ها و نیز خنثی شدن فعالیت‌های بخش‌های مختلف سیاست جنایی در پیشگیری از جرم خواهد شد. با وجود اینکه شورای عالی فضای مجازی به‌عنوان بالاترین نهاد حاکمیتی برای فضای سایبری ایران به فرمان مقام معظم رهبری و با نظارت رئیس جمهوری تشکیل شده است ولی با این حال در تقسیم وظایف میان دستگاه‌ها و ایجاد هماهنگی بین آن‌ها چندان موفق نبوده است.

از نهادهای دخیل در این فضا در ایران می‌توان مرکز بررسی جرایم سازمان‌یافته، فرماندهی پدافند سایبری سپاه پاسداران انقلاب اسلامی که با هدف مبارزه با رشد قارچ گونه جرایم سازمان‌یافته بین‌المللی و سوء استفاده از بستر اینترنت و سایر سامانه‌های ارتباطی در جهت انجام اقدامات تروریستی، جاسوسی اینترنتی و پول‌شویی و تخریب نظام فرهنگی و اجتماعی و هتک حرمت و توهین به مقدسات دینی و ارزشی انقلابی در سال ۱۳۸۶ راه‌اندازی شده است.

مصوبات شورای عالی فضای مجازی برای سایر نهادهای ذی‌ربط لازم الاجرا بوده و حق رد یا تأیید مصوبات این شورا را ندارند. اختیار تصویب قانون یا مصوبات لازم الاجرا این نهاد را در زمره نهادهای متعدد قانون‌گذاری در آورده است.

۵ راهکارهای رفع چالش پیش روی پلیس

بعضی از چالش‌ها صرفاً برای پلیس ایران در جهت پیشگیری و جلوگیری از گسترش جرایم رایانه‌ای و سازمان‌یافته می‌باشد و در برخی از موارد به صورت مشترک این چالش‌ها را در فراروی خود در تقابل این جرایم می‌بینند در ذیل راهکارهایی که به نظر رسیده است ارائه می‌گردد.

۱.۵ تقویت همکاری بین ذی‌نفعان

در فصل سوم کنوانسیون اصول کلی مربوط به همکاری بین‌المللی از قبیل پی جویی‌ها یا جمع آوری دلایل الکترونیکی یا رسیدگی قضایی راجع به جرایم رایانه‌ای در ماده ۲۳ بیان شده است. ماده ۲۴ نیز اصول مرتبط با استرداد مجرمان را روشن ساخته یکی از بزرگترین چالش‌ها در همکاری می‌باشد، حتی در ماده ۲۵ به اصول کلی راجع به همکاری دو جانبه اشاره شده است.

در راستای تقویت بنیادین سیاست اجرایی یک جامعه همکاری بین ذی‌نفعان و بازیگران اصلی، در این موارد پیشنهاد شده است که شامل همکاری و مشارکت‌های عمومی و خصوصی می‌باشد. به‌عنوان نمونه، کشورهای حوزه اتحادیه اروپا در زمینه استرداد مجرمان جرایم رایانه‌ای و جرایم سازمان‌یافته همکاری‌های مؤثری با یکدیگر و سایر کشورهای جهان دارند. کشور ایران نیز باید در جهت این همکاری با دولت‌های دیگر و بخش خصوصی توافق نامه‌هایی را در نظر بگیرد و بیشتر تلاش نماید تا مجرمان به کشورهای امن و ایمن پناهنده شده و موجب پیشگیری از تعدد جرایم شود.

۲.۵ تدابیر فنی

برای برون رفت از چالش‌های فنی می‌توان از دیوار آتش (Firewall) استفاده نمود که یک سری محدودیت را بین دو یا چند شبکه اعمال می‌کند و تا حد زیادی از دسترسی غیرمجاز دنیای بیرون به منابع داخلی جلوگیری می‌نماید. دیگر روش فناوری رمزنگاری است که جهت ممانعت از دسترسی دیگران به اطلاعات خصوصی افراد مورد استفاده قرار می‌گیرد. همچنین استفاده از نرم افزار ضد پایش می‌تواند راهگشا باشد (سایبانی و کریمی، ۱۳۹۷:۱۳۲۳) [۱۱].

باید برای ارزشیابی پیشرفت‌های فنی و حقوقی و رصد رمزگذاری ارائه شده مداوماً اظهار نظرها را گرفت و بررسی کرده و با توجه به علم آمار در این موارد نقاط ضعف را حذف کرد و نقاط قوت را ارتقاء بخشید که چنین ارزشیابی‌هایی در یوروپل مرسوم می‌باشد. برای افزایش ظرفیت قانونی و عملیاتی و فنی لازم برای مقابله با جرایم رایانه‌ای و جرایم سازمان‌یافته ایران می‌تواند با مشارکت در پروژه‌های مشترک با کشورهای دیگر که در این زمینه فعالیت می‌کنند بهره‌مند از پشتیبانی بین‌المللی گردد.

۳.۵ ارتقاء تخصصی و مهارتی

نهادها باید با انتشار متون و نشریات مختلف سطح آگاهی و تخصصی در جامعه را بالا برند چون هر چقدر آموزش همگانی به وسیله پلیس با همکاری ،رسانه‌ها نقش به سزایی در پایش و کاهش جرایم خواهد شد. خود پلیس می‌تواند سیاست‌های جنایی را به روزرسانی کرده و از طریق شرکت در کنفرانس‌های بین‌المللی، سطح آگاهی خود را افزایش داده و به آخرین دستاوردهای روز در این زمینه دست یابد. در این صورت حتی می‌تواند نیازمندی‌های خود را در جهت تجهیز مراکز تخصصی تامین کند و با این تجهیزات از یک سو و جذب افراد نخبه در نهاد تخصصی پلیس با همکاری آموزش و پرورش و دانشگاه‌های تراز اول کشور از سوی دیگر توان مقابله کشور را در مقابله جرایم رایانه‌ای و جرایم سازمان‌یافته افزایش دهد.

استفاده از هوش مصنوعی در جهت ارتقاء توانایی پلیس در پیشگیری از جرایم سازمان‌یافته با مسلح کردن با تکنولوژی روز نیز بجا خواهد بود.

۶ نتیجه‌گیری

با توجه به مباحث یاد شده در مقاله حاضر به نظر می‌رسد نه‌تنها سیاست جنایی اجرایی در ایران بلکه در کشورهای پیشرفته‌تر از نظر تکنولوژی همانند کشورهای اروپایی نیز در مقابله و پیشگیری جرایم سایبری و جرایم سازمان‌یافته کارایی مؤثری ندارند. علیرغم افزایش این جرایم پلیس‌ها نتوانسته‌اند به‌طور مؤثر به تهدیدات مطرح شده واکنش نشان دهند و این به دلیل آماده نبودن بستر و زمینه برای سیاست اجرایی کارآمد در پلیس ایران و اروپا می‌باشد. فقدان آشکار قانون مؤثر جهت ساماندهی این نوع سیاست مانع همکاری‌ها در بعد بین‌المللی می‌شود. مشکل دیگر سیاست اجرایی استانداردهای فرهنگی مختلف بین کشورها می‌باشد که گاهی ممکن است اختلاف اخلاقی و سیاسی بین کشورها در این زمینه به‌وجود آید. چالش دیگر سیاست اجرایی این است که تحقیق پیگرد استرداد مجرمان به‌علت همکاری ضعیف بسیار مشکل می‌باشد لذا می توان با الگوبرداری از اتحادیه اروپا ابتدا با همکاری در عرصه بین‌المللی و سپس با وضع قوانین جدید با تبیین سیاست اجرایی کشور و با همکاری نهادهای اجرایی کشورهای مختلف به‌منظور تحقیقات در مورد مجرمان گامی مؤثر برداشت؛ زیرا در این زمینه هیچ پلیس جهانی برای اجرای مقررات وجود ندارد. قشر جوان که اصلی‌ترین کاربران در فضای سایبر می‌باشند، اگر همواره با ارتقا سطح دانش، آگاهی آن‌ها نیز افزایش یابد، می‌تواند در راستای کاهش چالش سیاست اجرایی کشور باشد. علاوه بر آموزش و ارتقای آگاهی، نیاز به مشارکت همه‌جانبه در جامعه می‌باشد تا انگیزه‌هایی که منجر به رفتارهای مجرمانه می‌شود را بتوان به‌صورت

اجتماعی مهار نمود و گرنه توان نهادهای رسمی دولتی که درون خود به علت موازی هم عمل کردن گاه گاه نتیجه عکس و نامطلوب می‌گیرند و باهم همکاری مؤثر ندارند برای پیشگیری کافی به نظر نمی‌رسد. و نیاز به تشکیل یک سری سازمان‌های مردم نهاد که متخصص امر درخصوص مبارزه با جرایم سایبری و سازمان‌یافته می‌باشد احساس می‌شود. درضمن، همکاری‌های منطقه‌ای با کشورهای اطراف و همچنین به‌صورت بین‌المللی موجب تبادل اطلاعات شده و در ایجاد نظم عمومی جامعه و کاهش جرایم مؤثر خواهد بود. با توجه به فرهنگ مناطق و کشورهای متفاوت با تعدیل قوانین و هماهنگ‌سازی حقوق جزایی داخلی با حقوق جزایی بین‌المللی، یافتن و مسترد کردن مجرمان با همکاری‌های چند جانبه و پس از بازجویی‌ها به کیفر رساندن آن‌ها، باعث کاهش انجام این جرایم شده و نیز از تکرار این جرایم توسط مجرمین جلوگیری خواهد بود.

سپاس‌گزاری

نویسندگان مقاله از تمامی افراد و یا نهادهای پشتیبان و یاری‌گر سومین کنفرانس فضای سایبر سپاس‌گزاری و قدردانی می‌نمایند.

مراجع

[۱] ذبیح الله نژاد، وحید، «ماهیت جرایم رایانه ای و مجازی (سایبری) و نقش پلیس فتا در پیشگیری و کشف این جرایم»، دانش انتظامی پلیس پایتخت، شماره ۳، صفحات ۸-۲۴،۲۷، ۱۳۹۶.

[۲] تقی زاده مهرداد؛ زمردی، کیوان، حاجیان، مهدی، «نقش اتحادیه اروپا در قاعده‌مندسازی جرایم سایبری»، مطالعات بین‌المللی، پلیس ۸(۲۹)، صفحات ۱۰۴-۱۴۳، ۱۳۹۶.

[۳] خرم آبادی، عبدالصمد، «تاریخچه تعریف و طبقه‌بندی جرم‌های رایانه‌ای مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات»، مطالعات حقوقی فضای مجازی، ۱۳۸۳.

[۴] شمس ناتری، محمد ابراهیم، «جرایم سازمان‌یافته در آینه سیاست کیفری اسلامی»، ایران و اسناد بین‌المللی، پژوهشگاه حوزه و دانشگاه، ۱۳۹۷.

[۵] حیدری مسعود؛ شهبازی ،امید؛ شیرانی پویا، «چالش و فرصت‌های پیش روی پلیس در برخورد با جرایم سایبری»، کارآگاه ۱۲(۴۵)، صفحات ۴۱-۴۵، ۱۳۹۷.

[۶] احدی، فاطمه، تیموری، مهرداد، «واکاوی ساختار پلیس فتا در رویکرد نظریه جرم‌شناسی رئالیسم چپ‌گرا»، مطالعات حقوقی فضای مجازی، شماره ۱، صفحات ۴۴-۶۸، ۱۴۰۱.

[۷] وطنی، امیر؛ اسدی، حمید، «سیاست جنایی جمهوری اسلامی ایران در جرایم سایبری با تاکید بر ویژگی‌های خاص این جرایم»، پژوهشنامه حقوق اسلامی، شماره ۴۳، صفحات ۹۹-۱۲۶، ۱۳۹۵.

[۸] امیری، سروش، «همکاری‌های بین‌المللی اینترپل و امنیت بین‌المللی»، فصلنامه سیاست، سال دوم، شماره ۶، ۱۳۹۴.

[۹] جلالی فراهانی امیرحسین، «درآمدی بر آیین دادرسی کیفری جرایم سایبری»، ۱۳۹۴.

[۱۰] حسن بیگی، ابراهیم، «توسعه شبکه ملی دیتا»، (چالش فراروی و تهدیدهای متوجه امنیت ملی)، مطالعات مدیریت، ۱۲(۴۸)، صفحات ۱-۲۸، ۱۳۸۴.

[۱۱] سایبانی، علیرضا کریمی، اصغر، «سیاست جنایی ایران در خصوص جرایم مالی رایانه‌ای مطالعات علوم سیاسی حقوق و فقه»، شماره ۴، صفحات ۱۲۴-۱۴۲، ۱۳۹۷.

[12] "United nations convention against transnational organized crimes, art.2.par.b,"

[13] R. J.Kelly. *Encyclopedia of Organized Crime in the United States, wespart*. Green press, 2002.

[14] B. M.Cherif and edvardo Vetere. *Organized Crime*. NewYork, Transnational publishers Inc, 1998.