

مقاله

بخش پایانی

سری جدید | شماره ۱ | ۱۳



افزایش

جرایم رایانه‌ای

مرتبط با مواد مخدر

همگام با گسترش پدیده

جهانی شدن

گزارش ویژه
دفتر مقابله با مواد مخدر و جرم
سازمان ملل متحد

ترجمه: محمدرضا نبوتی

چالش‌هایی را که در برابر پلیس وجود دارد، می‌توان به چهار نوع تقسیم کرد:

۱. چالش‌های ساختاری و ذهنیت‌ها:

در خاتمه جنگ سرد، پلیس و سازمان‌های اطلاعاتی ملزم به اجرای اصلاحات ساختاری و بررسی اولویت‌هایی شدند که هنوز به طور کامل اجراء نشده‌اند. امروزه مبارزه با جرایم موادمخدر در سطح فراملی نیازمند جهشی دیگر است. این امر نه تنها رویکرد ساختاری بلکه یک ذهنیت یا رویکرد جامع را می‌طلبد.

پلیس‌ها به شکل سنتی از سلسله مراتب ساختاری مبتنی بر مرزبندی جغرافیایی پیروی کرده‌اند. جرایم فراملی موادمخدر این رویکرد را به دلیل عملیات‌های لازم در چند حوزه قضایی یا ساختار شبکه‌های کوچک تری که در حال حاضر وجود دارد، با چالش روبه‌رو ساخته است.

آزادسازی ارتباط‌های تلفنی نیز ضربه‌های ناخواسته‌ای بر موضوع تحقیق‌های مربوط به جرایم بود که دولت‌ها را با چالش برای جلوگیری از استفاده غیرمجاز (بدون دخالت در استفاده قانونی آن که امروزه از جایگاه اقتصادی بالایی برخوردار است)، روبه‌رو ساخت.

اقدام‌های پلیسی و راهبردهای تحقیقاتی به دلیل فقدان چارچوب مناسب برای همکاری‌های عملی در برخورد با مجرمینی که از تکنولوژی‌های پیشرفته استفاده می‌کنند، با مشکل روبه‌رو بوده است. هنوز این بخش موضوعی مبهم است و جرایم به شکل صحیح تعریف نشده و شناسایی مجرمین و محل اختفای آنان مشکل است.

پلیس‌های مبارزه با موادمخدر برای مقابله با این چالش‌ها باید اشکال جدید همکاری، راهبردهای نوین و مهارت‌های حرفه‌ای جدیدی را توسعه و به کار گیرند که همگی نیازمند منابع عظیم مالی است. اگر قرار است پلیس‌های مبارزه با موادمخدر در مقابله با سازمان‌های قاچاقچی به صورت مؤثر عمل کنند، باید شبکه‌های عملیاتی و کارآمدی را در سطح جهانی سازماندهی کنند. آن‌ها همچنین باید ارتباط‌های اطلاعاتی و عملیاتی را با سایر ارگان‌های پلیس، به منظور

جلوگیری از دوباره کاری و اتلاف منابع توسعه دهند. اگر چه این امر آغاز شده، اما شکاف بین مجرمین و توانمندی‌های تحقیقاتی پلیس‌ها هنوز آشکار است.

۲. چالش‌های حقوقی:

آشکارترین نارسایی قانونی که پلیس‌های مبارزه با موادمخدر با آن روبه‌رو هستند، قوانین جامع مربوط به جرایم مرتکب شده در محیط‌های الکترونیکی است. برخی کشورها هیچ‌گونه قوانینی در این رابطه ندارند و برخی تدابیری را به صورت ناشیانه در قوانین موجود خود گنجانده‌اند، اما تعداد کمی از کشورها به صورت نسبتاً مناسبی قوانین کیفری خود را به روز کرده‌اند.

حتی پس از اینکه قوانین وضع و در سطح ملی اجرا می‌شود، بسیاری از مشکلات همچنان ادامه خواهد یافت، مگر اینکه دولت‌ها هم‌زمان ماهیت فراملی جرایمی که در آن از تکنولوژی پیشرفته استفاده می‌شود و ممکن است در کشوری شروع و عواقب آن در کشور دیگر مشاهده شود، را نیز مد نظر قرار دهند.

در حال حاضر، هیچ‌گونه دستورالعملی راجع به اینکه قوانین کدام کشور در تعقیب یک جرم حاکم خواهد بود، یا اینکه اگر مجرم در کشور دیگری مقیم است، چگونه تصمیم‌های دادگاه اجرا شود و براساس کدام مقررات تحقیقات فرا ملی انجام خواهد گرفت، وجود ندارد. نتایج دو بررسی انجام شده نشان می‌دهد که بسیاری از کشورها آمادگی مقابله با چالش جرایمی که در آن از تکنولوژی پیشرفته استفاده می‌شود را ندارند. یک شرکت مدیریت مشاوره‌ای، ۵۲ کشور را در سراسر جهان برای قوانین علیه جرایمی که از تکنولوژی پیشرفته استفاده می‌شود مورد بررسی قرار داد و دریافت که ۳۳ کشور هیچ‌گونه قوانینی در این زمینه نداشته، ۹ کشور قوانینی جزئی را در این رابطه به کار گرفته و ۱۰ کشور قوانینی را در این رابطه وضع و اجراء می‌کنند که اختیارات لازم را جهت تعقیب کیفری جدی‌ترین اشکال جرایم رایانه‌ای مهیا می‌سازد.

در اغلب کشورها ارائه دهندگان خدمات اینترنتی در فارم از پارچوب قانونی مشخص فعالیت می‌کنند و تحت هیچ گونه نظارت قانونی قرار ندارند



در میان آن گروه از کشورها که قوانین خود را به‌روز کرده‌اند، برخی مانند فیلیپین، تنها این امر را در رابطه با موارد بسیار شدید مانند انتقال ویروس‌های رایانه‌های مختل‌کننده نظیر «لاو یو» (دوستت دارم) که هشتاد درصد رایانه‌های دولت ایالات متحده را آلوده و حدود ده میلیارد دلار خسارت وارد کرده، اعمال کرده‌اند.

در اروپای غربی تکمیل پرسشنامه مربوط به جرایم مواد مخدر از طریق اینترنت نشان داد که دولت‌ها به‌طور عموم قادر به وضع قوانین لازم‌الاجرا علیه این‌گونه جرایم نیستند و همکاری میان پلیس و ارائه‌دهندگان خدمات اینترنتی به‌صورت داوطلبانه و به‌طور غیررسمی صورت گرفته است.

در اغلب کشورها، ارائه‌دهندگان خدمات اینترنتی در خارج از چارچوب قانونی مشخص فعالیت می‌کنند و تحت هیچ‌گونه نظارت قانونی قرار ندارند، یا نظارت بسیار کمی روی آن‌ها اعمال شده است. در اصل، اینترنت به‌عنوان ابزار ارتباطی و تبادل اطلاعات در خصوص تولید و فروش غیرقانونی مواد مخدر مورد استفاده قرار گرفته است. کلیه کشورها، به استثنای دو کشور، استفاده از کذبندی اطلاعات توسط جنایتکاران در سایر زمینه‌ها را گزارش کرده‌اند. به‌طور تقریبی، کلیه کشورها یک مرجع هماهنگی برای تبادل اطلاعات پیرامون جرایم مرتکب شده از طریق اینترنت داشته‌اند. این مرجع در برخی کشورها نهادهای مختلف از جمله پلیس، گمرک، مسئولین مخابرات و واحدهای تحقیقات جرایم رایانه‌ای بوده است.

ردیابی و کشف شواهد و نیز شواهد قابل قبول دادگاه از جمله موارد مهم هستند. پروسه درخواست و تهیه مجوز بازرسی در چند محدوده قضایی و زمان مورد نیاز برای اجراء آن ممکن است در دنیای واقعی غیرقابل انجام باشد و به مجرم اجازه دهد که شواهد اتهام برانگیز علیه خود را در زمینه معامله‌های غیرقانونی مواد مخدر نابود کند.

مشکلات دیگری نیز به‌دلیل ماهیت اطلاعات الکترونیکی وجود خواهد داشت. روش معمول در تهیه مجوز

تجسس برای اطلاعات ذخیره شده (که براساس سوءظن انجام می‌گیرد) و مجوز کنترل اطلاعات (عملیات مخفیانه) متغیر است و عملیات‌های مخفیانه با کنترل‌های بیشتری انجام می‌گیرند.

با این وجود، داده‌های الکترونیکی مثل پیام‌هایی که از طریق پست الکترونیکی مخابره می‌شوند، به‌عنوان داده‌های ذخیره شده و نیز داده‌های ارسال شده محسوب می‌شوند. بررسی اصول حقوقی در این زمینه ضروری به‌نظر می‌رسد.

از آنجا که امکان تغییر داده‌های الکترونیکی بدون باقی‌گذارن هرگونه رد و اثری وجود دارد، مقبولیت شواهد جرم الکترونیکی در دادگاه بسیار مشکل است. پلیس باید روش‌های شفاف و امنی را که به آن‌ها توانایی اثبات صحت داده‌های الکترونیکی را روی کاغذ بدهد اتخاذ کنند. در صورتی که پروسه کشف رمز نیاز باشد، مهارت و مراقبت بیشتری جهت تضمین اینکه مسئولین پیگیری پرونده به‌جعل شواهد متهم نشوند، لازم خواهد بود.

علاوه بر این، اثبات صحت متن و منبع شواهد بدون اینکه در دادگاه عمومی تکنولوژی و روش‌های خواندن متون فاش شود، مشکل است.

۳. چالش‌های فنی و منابع:

چالش‌های فنی و منابع پیش‌روی پلیس در برخورد با جرایم مواد مخدری که با استفاده از تکنولوژی جدید صورت می‌گیرند، بسیار چشمگیر هستند. به‌روز ماندن با تکنولوژی یعنی به‌روز کردن مداوم تجهیزات و افراد و نیز ارتباط مستمر با شبکه «۲۴/۷» (که بیست و چهار ساعته و هفت روز هفته فعال است) جهت تضمین انجام به‌موقع تحقیق‌ها، برای بسیاری از کشورهای در حال توسعه ممکن است کار بسیار سختی باشد و شکاف میان توانمندی‌های کیفی و تحقیقاتی را بیشتر کند.

در برخی از این کشورها که به‌بهشت اطلاعات معروف هستند، مجرمین ارائه‌دهندگان خدمات اینترنتی خود را پیدا می‌کنند، حساس‌ترین اطلاعات را ذخیره می‌کنند و اطلاعات رمزدار نیز دور از

دسترس پلیس قرار دارد.

کشورهایی که پلیس خود را به‌طور مناسب مجهز نمی‌کنند، یا از استانداردهای پائینی در زمینه امنیت الکترونیکی برخوردارند، ممکن است شرکت‌های الکترونیکی تجاری از حلاء موجود سوءاستفاده کنند، لذا این کشورها از لحاظ اقتصادی نامطلوب تشخیص داده شده و ممکن است با خطر بلوکه شدن پیام‌های الکترونیکی‌شان توسط سایر شبکه‌ها روبه‌رو شوند.

حتی کشورهای توسعه یافته نیز به‌دلیل پائین بودن حقوق بخش دولتی در مقایسه با بخش خصوصی از کمبود مأمورین تحقیق و بازپرسان ماهر رنج می‌برند.

مقوله کدگذاری که تجارت الکترونیکی را تحت شرایط نسبتاً امنی تسهیل می‌کند، برای پلیس هم یک موهبت، هم بلائی جان است. استفاده از رمز، محرمانه ماندن اطلاعات را تضمین می‌کند و با استفاده از سیستم تأیید دیجیتالی از دسترسی غیرمجاز به سیستم‌های اطلاعاتی جلوگیری به‌عمل می‌آید. این امر همچنان ابزار ارزشمندی جهت ارتباط‌ها و حفاظت از منابع و اطلاعات برای پلیس ارائه می‌کند. با این وجود، به‌نظر می‌رسد سیستمی که استفاده از رمز را برای مجرمین مهیا می‌سازد، از فواید استفاده از آن برای پلیس بیشتر است.

پلیس‌های مبارزه با مواد مخدر بدون داشتن توانایی در کنترل و درک ارتباط‌ها در زمینه‌های پیشگیری، شناسایی و پیگرد قانونی با مشکل روبه‌رو خواهند بود. گزارش شده است که از سال ۱۹۹۴ هر یک از تحقیق‌های عمده‌ای که توسط پلیس فدرال امریکا درخصوص جرایم سازمان یافته در ایالات متحده به‌عمل آمده با استفاده از تجهیزات الکترونیکی مراقبتی بوده است. در انگلستان در سال‌های ۲۰۰۷ و ۲۰۰۸ کنترل ارتباط‌ها نقش به‌سزایی در انجام عملیات‌ها ایفاء کرد و در این زمینه ۱۲۰۰ نفر دستگیر، ۱۱۵ تن انواع مواد مخدر و ۴۵۰ اسلحه و مهمات کشف و ضبط شد.

۴. موضوع‌های مربوط به حقوق شخصی و آزادی بیان: در کلیه کشورهای دموکراتیک، تحقیق درخصوص زندگی

شخصی متهمین به منظور پیشگیری یا شناسایی جرم باید با توجه به رعایت حقوق مربوط به اموال شخصی و ارتباط‌های خصوصی انجام گیرد. همچنان که قوانین در زمینه جرایم رایانه‌ای توسعه می‌یابند و از آنجا که نظرهای این صنعت قدرتمند، گروه‌های مردمی و نیز پلیس باید در هرگونه سیاست‌گذاری لحاظ شود، دست‌یابی به یک توافق همه‌جانبه امری بسیار مشکل است.

یافتن این راه‌حل، چالشی دیگر در برابر موضوع مبارزه با موادمخدر است. قوانین اخیر پیرامون ذخیره اطلاعات برای حفاظت بیشتر حقوق فردی و اطلاعات شخصی بوده است، به گونه‌ای که ارائه دهندگان خدمات اینترنتی عموماً اطلاعات مشتریان خود را بیش از آنکه برای ارسال صورت‌حساب ایشان لازم است، نگهداری نخواهند کرد.

ملزم ساختن ارائه دهندگان خدمات اینترنتی برای نگهداشتن سوابق مشتریان به منظور تحقیق‌های جنایی هم از لحاظ حقوق شخصی و هم هزینه‌های آن که مورد توجه مسئولین این صنعت و گروه‌های طرفدار حقوق مدنی است، امری بسیار حساس به نظر می‌رسد.

استفاده از اینترنت برای تبادل اطلاعات درخصوص طرز تهیه موادمخدر و ارسال پیام‌های تبلیغی جهت مصرف موادمخدر مشکلات پلیسی دیگری را به وجود آورده است. از یک سو تحریک مردم برای تولید یا مصرف موادمخدر ناقض ماده ۳ کنوانسیون ۱۹۸۸ است و از سوی دیگر، بسیاری از کشورها آزادی بیان را حق لاینفک افراد می‌دانند و هرگونه سانسور ارتباط‌ها را رد می‌کنند.

ارائه غیرقانونی موادمخدر، روان‌گردان یا مواد اولیه شیمیایی برای فروش باید به‌عنوان یک جرم قابل پیگرد در هر یک از کشورهای عضو عهدنامه‌های بین‌المللی کنترل موادمخدر محسوب و مشاوره در خصوص چگونگی تهیه موادمخدر یا مواد اولیه شیمیایی برای اهداف غیرقانونی باید به‌عنوان ترغیب و تحریک و ناقض ماده ۳ کنوانسیون ۱۹۸۸ تلقی شود.

با این وجود، یک سایت اینترنتی که

آزادسازی مصرف غیرپزشکی موادمخدر در آن ترغیب می‌شود، لزوماً در این طبقه‌بندی قرار نمی‌گیرد و برای ممنوع کردن این گونه سایت‌ها ممکن است با اصول آزادی بیان در بسیاری از کشورها در تناقض باشد.

یکی از زمینه‌های جرایم اینترنتی که در آن پیشرفت‌های قانونی حاصل شده، مبارزه علیه سایت‌های مربوط به تصاویر مستهجن از کودکان است، اما دلیل آن فعالیت‌هایی است که در سطح جهانی علیه این موضوع مطرح و آن‌را محکوم کردند. دلیل دیگر این موضوع این است که حتی در اختیار داشتن این تصاویر در بسیاری از کشورها جرم محسوب می‌شود. در این گونه موارد، ارائه دهندگان خدمات اینترنتی در صورت اثبات ارائه خدمات مربوط به دسترسی به سایت‌های دارای تصاویر مستهجن کودکان تحت پیگرد قانونی قرار خواهند گرفت. جرایم مربوط به ارائه تصاویر مستهجن کودکان در اینترنت تنها جرمی است که در کنوانسیون جرایم رایانه‌ای شورای اروپا مطرح شده است.

چالش‌های آتی:

براساس تجزیه و تحلیل‌های مذکور و با توجه به وضعیت کنونی در جهان، سازمان ملل متحد بر این باور است، در صورتی که اقدام‌های لازم در سطح ملی و بین‌المللی صورت نگیرد، تحول‌های ذیل غیرقابل اجتناب خواهد بود:

۱. فرصت انجام کلیه اشکال جرایم ممکن است با گسترش سرمایه‌گذاری، تجارت و ارتباط‌های اینترنتی افزایش یابد. رشد و وابستگی متقابل اقتصادهای ملی کار را برای سازمان‌های جنایتکار جهت آمیختن فعالیت‌های غیرقانونی خود با فعالیت‌های اقتصادی مجاز، آسان خواهد کرد
۲. با توجه به روند ارتکاب جرایم فراملی در شبکه اینترنت، بی‌شک میزان این جرایم به‌صورت تصاعدی افزایش خواهد یافت.
۳. جرایم سازمان یافته ممکن است استفاده از تکنولوژی جدید را برای اهداف تهاجمی و دفاعی خود ادامه دهند. سایت اینترنتی «IT warrior» به یک

آشکارترین نارسایی قانونی که پلیس‌های مبارزه با موادمخدر با آن روبه‌رو هستند قوانین جامع مربوط به جرایم مرتکب شده در محیط‌های الکترونیک است

مولفه اجتناب‌ناپذیر گروه‌های سازمان‌یافته جنایتکار در خواهد آمد.

۴. تطهیر پول از طریق اینترنت ممکن است با رشد شرکت‌های خدمات مالی اینترنتی افزایش یابد. این امر به‌ویژه در صورتی که اقدام‌ها علیه تطهیر پول همچنان در سطح پائین اولویت باقی بماند و شرکت‌های خارجی همچنان از تحقیقات مبرا باشند، عملی خواهد شد. سیستم‌های بانکی زیرزمینی نیز با استفاده از تکنولوژی اطلاعات امنیت بیشتری خواهند داشت.

۵. جرایم موادمخدر ممکن است گسترش یابد. این‌گونه جرایم می‌تواند توسط افراد بیشتری صورت گیرد که اغلب آن‌ها از اعضاء گروه‌های سازمان‌یافته جنایتکار نیستند و در هیچ یک از طبقه‌بندی‌های جرایم گنجانده نمی‌شوند.

۶. به دلیل اینکه نسل جدید در سنین پائین با رایانه آشنا می‌شوند، افراد جوان ممکن است به‌صورت فزاینده‌ای مرتکب جرایم رایانه‌ای شوند.

۷. سازمان‌های جنایتکار ممکن است از تحول‌های علمی برای سرمایه‌گذاری هر چه بیشتر در تولید داروهای ساختگی برای بازارهای غیرقانونی سوءاستفاده کنند.

۸. پلیس ممکن است با افزایش استفاده از سیستم‌های رمزبندی و سایر ابزارهای اختفا توسط سازمان‌های قاچاق موادمخدر از توانایی کمتری برای کنترل و نظارت بر فعالیت‌های آن‌ها برخوردار باشند.

۹. حوزه‌های قضایی بدون قوانین مناسب علیه جرایم مربوط به تکنولوژی اطلاعات ممکن است به مکان‌های امن تبدیل شوند.

۱۰. چارچوب‌های سنتی برای استرداد و معاضدت قضایی ممکن است تا حد اکثر ممکن تحریف شوند.

رویکردهای جدید به جرایم رایانه‌ای درون / بین ساختارهای انتظامی:

نیروهای پلیس چند کشور از جمله کانادا، انگلستان و ایالات متحده واحدهای ویژه مبارزه با جرایم رایانه‌ای را تشکیل داده‌اند. هنگ‌کنگ توانمندی‌های خود را در زمینه اطلاعاتی و انتظامی در سطح بین‌المللی

افزایش داده و بخش مبارزه با جرایم رایانه‌ای را شامل ۷۶ افسر آموزش دیده برای مبارزه با جرایم داخلی تأسیس کرده است.

پلیس فدرال استرالیا یک سیستم مدیریت تحقیقات اینترنتی که تحت عنوان (PROMIS) شناخته می‌شود تشکیل داده است. دفاتر رابط پلیس فدرال استرالیا در سراسر جهان از این سیستم جهت تبادل اطلاعات، تصاویر و سایر اطلاعات مربوط به تحقیقات را با همکاران خود استفاده می‌کنند.

در اسپانیا واحد تحقیقات مرکزی در خصوص جرایم رایانه‌ای و اداره جرایم تکنولوژی جدید وزارت کشور مجدانه در امر پیشگیری از استفاده از اینترنت برای تبلیغات غیرقانونی مواد تحت کنترل از جمله مواد روان‌گردان فعالیت می‌کنند. طرح ملی مبارزه با موادمخدر برای سال‌های ۲۰۱۲ - ۲۰۰۸ شامل ایجاد یک نهاد نظارتی برای استفاده از تکنولوژی جدید به‌وسیله سازمان‌های قاچاقچی موادمخدر از جمله استفاده از اینترنت می‌شود.

استفاده از تکنولوژی جدید برای مبارزه با جرایم موادمخدر:

از سال ۱۹۹۷ که نخستین بار سازمان ملل متحد توجه دولت‌ها را به ارسال پیام‌هایی برای تبلیغ مصرف موادمخدر توسط رسانه‌های الکترونیکی جلب کرد، بسیاری از مسئولین بهداشتی از اینترنت به‌عنوان یک ابزار سریع، ارزان و مناسب برای پخش اطلاعات واقعی در خصوص موادمخدر و سوءمصرف آن استفاده کرده‌اند.

در ایالات متحده مرکز ارزیابی مبارزه با موادمخدر مبتنی بر تکنولوژی دفتر ملی سیاست کنترل موادمخدر پژوهش‌های علمی و تکنولوژیکی را به‌منظور استفاده ارگان‌های انتظامی مورد حمایت قرار داده است. روش‌های جدیدی برای تجزیه و تحلیل تأثیرهای موادمخدر بر انسان‌ها و برای کشف موادمخدر پنهان شده در درون یا بیرون بدن، کانتینرها، وسایل نقلیه یا سایر فضاها بسته توسعه یافته است.

نرم‌افزارهای مربوط به رایانه‌های با سرعت بالا هویت قاچاقچیان موادمخدر را از طریق اثر انگشتانشان شناسایی می‌کند

در حال حاضر، ابزارهایی بدون مزاحمت برای مسافری جهت بازرسی در گمرکات به کار گرفته می‌شود. این ابزارها از جمله دستگاه‌های اشعه ایکس و گاما، تجهیزات قابل حمل جهت کشف موادمخدر در کشتی‌ها، کوبه‌های قطار و کانتینرها از هر اندازه در بازرسی‌های دریایی و بنادر و کنترل سریع مسافری و بار آنها هستند.

برنامه‌های رایانه‌ای ویژه قضایی اجازه استفاده از تکنولوژی و تکنیک‌های رایانه‌ای را در ضبط و ربط کشفیات و شواهد جهت به دست آوردن اطلاعات از سیستم‌های رایانه‌ای برای تحقیقات ارائه می‌کند. برنامه‌های نرم‌افزاری وجود دارد که می‌تواند اطلاعات را برای به دست آوردن لغات، یا عبارات کلیدی کنترلی یا برخی از اطلاعات مخابراتی الکترونیکی مثل پیام‌هایی را که به حساب بانکی یا مصرف‌کننده به خصوص فرستاده یا از آن ارسال شده را با مجوز دادگاه دریافت کنند.

سایر پیشرفت‌ها در زمینه استفاده ابتکاری از فن‌آوری موجود شامل ابداع نمونه‌های پیشرفته رایانه برای شناسایی موارد غیرعادی در معامله‌های مالی است. نرم‌افزارهای مربوط به رایانه‌های با سرعت بالا هویت قاچاقچیان موادمخدر را از طریق اثر انگشتانشان شناسایی می‌کند. شبکه‌ای نیز تشکیل شده که به مسئولین ذیربط اجازه می‌دهد، اسناد مالکیت اموال را با سایر اطلاعات از قبیل برگه‌های مالیاتی این افراد مقایسه کنند. بدین ترتیب، مزیت مشهودی را که مجرمین با استفاده از ابزارهای تکنولوژی جدید دارند، می‌توان به امتیازی برای پلیس تبدیل کرد.

تحولات در بخش خصوصی: بخش خصوصی برای واکنش و تسهیل ایمنی علیه جرایم الکترونیکی با پلیس متحد شده‌اند. ارائه‌دهندگان خدمات اینترنتی شبکه‌های بین‌المللی را جهت همکاری با پلیس از طریق خط مستقیم ارتباطی در زمینه مبارزه با استفاده از اینترنت در خصوص ارائه تصاویر مستهجن کودکان همکاری می‌کنند. در صورتی که مطالبی در خصوص تصاویر مستهجن کودکان در یک سایت اینترنتی ملاحظه شود، این

خط مستقیم محل سایت را مشخص کرده و در صورتی که سایت مربوط داخل کشور باشد، پلیس یا ارائه‌دهنده خدمات اینترنتی مربوط را از موضوع آگاه ساخته تا مطالب را حذف کنند و اقدام‌های لازم را به عمل آورند. بسیاری از کشورها سیستم‌های ملی خود را به همین ترتیب اداره می‌کنند.

در ایالات متحده، همکاری بین بخش خصوصی و عمومی، پلیس را قادر می‌سازد به دنبال اطلاعات در خصوص جرایم الکترونیکی، ضعف‌های موجود و سایر خطرهایی که مالکین یا متصدیان زیربنای حیاتی مانند نیروگاه‌های مولد برق را تهدید می‌کند، پردازند.

مقررات مربوط به مندرجات سایت‌های اینترنتی: ابزارهای مختلفی جهت کنترل دسترسی به اینترنت و مندرجات سایت‌های آن وجود دارد. سایت‌های اینترنتی را می‌توان به طور کلی سانسور کرد. این امر در کشورهایی که دسترسی به اینترنت تحت کنترل دولت است، به سادگی انجام می‌گیرد. در سایر کشورها، ارائه‌دهندگان خدمات اینترنتی یا مدیران سایت‌های اینترنتی را می‌توان در صورتی که آگاهانه مطالبی را که تحت هر یک از قوانین کشور میزبان از جمله قوانین مبارزه با موادمخدر غیرقانونی یا زیان بخش باشد، تحت تعقیب قرار داد. ارائه‌دهندگان خدمات اینترنتی می‌توانند مطالب مندرج در سایت‌ها را با مقرراتی که خود به صورت داوطلبانه و به عنوان شیوه عمل انتخاب می‌کنند، مانند ایتالیا یا ژاپن اجازه استفاده بدهند، یا با اداره کنندگان سایت‌ها توافق‌نامه‌هایی را داشته باشند تا حوزه‌های قضایی و محل پرداخت خسارات ناشی از جرایم را روشن کنند. یکی از ارائه‌دهندگان خدمات اینترنتی در کانادا شرایط استفاده از خدمات خود را مبتنی به قوانین این کشور به مصرف و اداره کنندگان سایت‌ها از پیش اعلام می‌دارد.

هر یک از مصرف‌کنندگان خدمات اینترنتی می‌توانند مندرجات ناخواسته سایت‌ها را با توجه به معیارهای تعیین شده از طریق برنامه‌های نرم‌افزاری بلوکه یا فیلتر کنند. این برنامه‌ها به صورت گسترده‌ای در بازار

به دلیل اینکه نسل جدید در سنین پائین با رایانه آشنا می‌شوند افراد جوان ممکن است به صورت فزاینده‌ای مرتکب جرایم رایانه‌ای شوند

وجود دارند که برخی از آن‌ها سیستم‌های درجه‌بندی و پروسه ثبت شکایت را نیز در بر می‌گیرند. یک شرکت نرم‌افزاری در ایالات متحده مندرجات سایت‌ها را با توجه به لیست اختصاص سایت‌ها که به‌طور مداوم به‌روز می‌شوند، فیلتر می‌کند. این شرکت در حال حاضر بیش از ۶۰۰۰ سایت را در لیست سیاه خود قرار داده که مندرجات آن‌را به دلایل مختلف از جمله ترغیب مصرف غیرقانونی مواد مخدر نامناسب تشخیص داده‌اند.

ابتکارات منطقه‌ای و بین‌المللی علیه جرایم مرتبط با تکنولوژی جدید:

جرایم مرتبط با تکنولوژی جدید هنوز یک پدیده به‌نسبت نو محسوب می‌شود و لذا تعداد کمی از کشورها ابزار لازم را جهت اندازه‌گیری وسعت یا تأثیر آن در اختیار دارند. از این‌رو ابتکار خاصی نیز برای مقابله با آن اتخاذ نکرده‌اند. با این وجود، سازمان‌های منطقه‌ای و بین‌المللی از قبیل سازمان ملل، گروه هشت، اینترپول و شورای اروپا تلاش‌های جدی خود را جهت مقابله کلی با جرایم مرتبط با تکنولوژی جدید آغاز کرده‌اند. این ابتکارات نمونه‌ای کارآمد را جهت طراحی اقدام‌ها علیه جرایم مرتبط با تکنولوژی جدید در زمینه مواد مخدر ارائه می‌کند.

از سال ۱۹۹۰ کمیسیون پیشگیری از جرم و جنایت، تلاش‌های بین‌المللی را جهت توسعه چارچوب جامع برای دستورالعمل‌ها و استانداردهای مبارزه با جرایم رایانه‌ای ترغیب کرده است. این تلاش‌ها شامل انتشار راهنمای پیشگیری و کنترل جرایم رایانه‌ای در سال ۱۹۹۴ است که شامل پیشنهادهایی جهت موزون کردن قوانین اساسی و آیین‌نامه‌ای بوده و درخواست همکاری بین‌المللی در این زمینه کرده‌اند. تعدادی اجلاس‌های کارشناسی تحت نظارت مؤسسه پیشگیری از جرم و درمان مجرمین آسیا و خاور دور جهت آماده کردن مطالب کارگاه آموزشی جرایم مرتبط با شبکه‌های رایانه‌ای برگزار شد که در پانزدهم آوریل سال ۲۰۰۰ در چارچوب دهمین کنگره پیشگیری از جرم

و درمان مجرمین سازمان ملل، تشکیل شد.

متعاقب قطعنامه ۱۹۹۹/۲۳ شورای اقتصادی اجتماعی، دبیر کل دستور بررسی پیرامون تدابیر مؤثر برای پیشگیری و کنترل جرایم مرتبط با رایانه و تکنولوژی جدید را صادر کرد. در آن گزارش، چند گزینه از جمله پیش‌نویس یک سند بین‌المللی علیه جرایم مرتبط با رایانه و گزینه‌هایی برای راهبردهای کوتاه‌مدت شامل ایجاد برنامه جهانی سازمان ملل علیه جرایم مرتبط با رایانه و تکنولوژی جدید ارائه شد. در سپتامبر ۲۰۰۱ کمیسیون جرم و جنایت طرح عمل اجرای پیشنهادهای دهمین کنگره را به تصویب رساند. طرح عمل علیه جرایم رایانه‌ای و تکنولوژی جدید اقدام‌های ملی از جمله موارد ذیل را خواستار شد:

الف) جرم شناختن سوءاستفاده از اطلاعات الکترونیکی.

ب) توسعه و اجرا قواعد عمل جهت تضمین شناسایی و تحقیقات درخصوص جرایم مرتبط با رایانه و ارتباطات دوربرد. ج) تضمین اینکه پرسنل پلیس آموزش لازم را جهت پاسخ به تقاضای کمک برای ردیابی ارتباطات دوربرد داشته و به تجهیزات مورد نیاز مجهز باشند.

در سال ۱۹۹۵ اینترپول یک کنفرانس بین‌المللی برگزار و کتاب‌های راهنمایی برای مأمورین تحقیق جرایم مربوط به اطلاعات تکنولوژیکی به‌منظور تعیین استانداردهای لازم برای تحقیقات فنی تهیه کرد. یک واحد مرکزی و چهار گروه کاری از افریقا، آمریکا، آسیا و اروپا در زمینه جرایم مرتبط با تکنولوژی جدید تشکیل شد که وظیفه اصلی ایشان، ارائه آموزش و همکاری‌های منطقه‌ای بود. بخش فرعی مواد مخدر اینترپول یک سایت امن اینترنتی دارد که در دسترس اداره‌های ملی کشورها است و کشفیات مواد مخدر جدید، فعالیت قاچاقچیان و سایر هشدارهای مفید را در اختیار نیروهای پلیس قرار می‌دهد. امنیت پروژه‌های جدید با هدف مبارزه با قاچاقچیان مواد مخدر و با استفاده از ارتباط‌ها به شیوه کدبندی شده بین اعضاء صورت می‌گیرد. اینترپول

ارائه دهندگان فدماات اینترنتی باید نطوط مستقیم تلفنی را به عموم مردم بهت گزارش دادن مطالب اهانت‌آمیز یا غیرقانونی سایت‌های اینترنتی اعلام کنند

به منظور امن کردن تجارت و صنعت علیه جرایم رایانه‌ای با بخش خصوصی نیز همکاری می‌کند.

در ژوئن ۱۹۹۶ سران کشورهای گروه هشت، چهل پیشنهاد گروه ارشد کارشناسی جرایم سازمان یافته فراملی را به تصویب رساندند. در پیشنهاد شانزده، از کشورها تقاضا شده است، قوانین خود را به منظور تضمین جرم شناختن سوءاستفاده از تکنولوژی مدرن مورد تجدیدنظر قرار دهند و منابع مالی و فنی مناسبی را جهت مبارزه با آن پیش‌بینی کنند. در ژانویه ۱۹۹۷ گروه لیون جهت اجراء این پیشنهادها ایجاد شد. در اجلاس وزراء کشور و دادگستری کشورهای گروه هشت که در دسامبر ۱۹۹۷ در واشنگتن برگزار شد، شرکت کنندگان اصول طرح عمل برای مبارزه با جرایم مرتبط با تکنولوژی جدید را (در آن از کشورها تقاضا شده است، قوانینی را جهت تحقیق و پیگرد جرم مرتبط با تکنولوژی جدید و نیز تقویت نظام‌های بین‌المللی برای استرداد مجرمین و معاضدت قضایی به تصویب رسانند) مورد تأیید قرار دادند. شرکت کنندگان بر لزوم یک رویکرد مشترک برای مقابله با مشکل جرایم مرتبط با تکنولوژی جدید تأکید کردند. در این طرح، اقدام از ایجاد یک ارگان بین‌المللی مورد قبول برای تعیین استانداردها برای بخش‌های خصوصی و دولتی در زمینه‌های ارتباط‌های امن و قابل اعتماد و تکنولوژی‌های داده‌پردازی نیز حمایت شده است.

در اوایل سال ۲۰۰۱ ارگان‌های انتظامی کشورهای عضو گروه هشت و نه کشور دیگر، به صورت روزانه در ارتباط بودند و از طریق شبکه «۲۴/۷» (۲۴ ساعته و ۷ روز هفته) به تبادل اطلاعات در خصوص تحقیقات در زمینه جرایم جدی مرتبط با تکنولوژی جدید پرداخته‌اند. مدتی قبل، گروه لیون یک کنفرانس بین‌المللی در زمینه آموزش جرایم رایانه‌ای برای مأمورین تحقیق کشورهای عضو گروه هشت برگزار کرد. در این سمینار، روش‌های عملی و استاندارد در خصوص دسترسی به داده‌های رایانه‌ای در آن سوی مرزها، معاضدت قضایی سریع و فعالیت

برای توسعه روش‌ها برای شناسایی منبع و مقصد ارتباط‌ها نیز مورد بررسی قرار گرفت.

در کلیه نقاط جهان، مکانیزم‌هایی برای بررسی جرایم مرتبط با تکنولوژی جدید و واکنش مناسب علیه آن در حال توسعه است. لیکن، موضوع مبارزه با جرایم مواد مخدر با استفاده از تکنولوژی جدید هنوز کمتر توسعه یافته است. در برخی مناطق جهان، اغلب اقدام‌ها در رابطه با موضوع کلاهبرداری، تصاویر مستهجن کودکان و فعالیت‌های مزاحمین رایانه‌ای متمرکز و در برخی دیگر بیشتر به فعالیت‌های تظهير پول و جرایم اقتصادی پرداخته شده است. در پرتو وقایع اخیر جهانی، در حال حاضر توجه بیشتری به استفاده از تکنولوژی جدید توسط شبکه‌های تروریستی جلب شده است.

دولت ژاپن از طریق ارگان ملی پلیس در ایجاد یک شبکه ارتباطی اینترنتی که ۲۱ کشور را در آسیا برای تبادل اطلاعات در خصوص جرایم مرتبط با تکنولوژی جدید به هم متصل می‌کند، سرمایه‌گذاری کرده است. هم‌اکنون هشت کشور در مرحله اول این اقدام به تبادل اطلاعات در این زمینه می‌پردازند.

در پیشنهاد پنجم، از ۳۰ پیشنهادی که برای مقابله با جرایم سازمان یافته در ژوئیه ۱۹۹۷ توسط شورای اروپا تصویب شد، بر بررسی جرایم مرتبط با تکنولوژی جدید تأکید و در ژانویه ۱۹۹۸ تکمیل شد. در اجلاس ویژه شورای اروپا که در اکتبر ۱۹۹۹ در فنلاند برگزار شد، سران کشورهای عضو اتحادیه اروپا تصویب کردند که باید تعاریف و مجازات‌های مشترکی برای جرایم مرتبط با تکنولوژی جدید تعیین شود. در اوایل سال ۲۰۰۱ به‌عنوان بخشی از طرح اقدام اتحادیه اروپا برای مبارزه با مواد مخدر (۲۰۰۴-۲۰۰۰) گروه کاری شورای وزیران در زمینه قاچاق مواد مخدر یک ارزیابی در خصوص خطرهای استفاده از اینترنت در ارتباط با مواد مخدر و نیز بررسی مفاد قانونی موجود در کشورهای عضو را مورد بررسی قرار داد. اولین مرحله آن تجزیه و تحلیل ارسال یک پرسشنامه از

جرایم مرتبط با تکنولوژی جدید هنوز یک پدیده به نسبت نو محسوب می‌شود و لذا تعداد کمی از کشورها ابزار لازم را جهت اندازه‌گیری وسعت یا تأثیر آن در اختیار دارند

طریق دفتر پلیس اروپا (یورپول) برای کشورهای عضو بود (بند ۳۲ ملاحظه شود). کمیسیون اروپا بهبود تأثیر اقدام‌ها علیه تجارت غیرقانونی موادمخدر در اینترنت را که اهمیت آن در راهبرد مبارزه با موادمخدر اتحادیه اروپا برای سال‌های ۲۰۰۴-۲۰۰۰ مورد تأکید واقع شده را مورد توجه قرار خواهد داد.

در ژانویه ۱۹۹۹ پارلمان و شورای اروپا یک طرح اقدام چند سالانه را برای ترغیب استفاده امن‌تر از اینترنت از طریق مبارزه با مندرجات غیرقانونی و مضر سایت‌ها در شبکه‌های جهانی به تصویب رسانده‌اند.

کنوانسیون شورای اروپا در جرایم رایانه‌ای، پیشرفته‌ترین همکاری بین‌المللی در زمینه جرایم مرتبط با تکنولوژی جدید تا این تاریخ است.

چهل و سه عضو شورای اروپا همراه با ژاپن، کانادا و ایالات متحده (ناظر) و افریقای جنوبی در پروسه تهیه پیش‌نویس فعالیت کرده‌اند و می‌توانند کنوانسیون را امضاء کنند. این کنوانسیون موضوع‌هایی چون، حدود قضایی، استرداد، کنترل ارتباط‌ها و تهیه و نگهداری اطلاعات را در بر می‌گیرد. لیست فعالیت‌هایی را که باید تحت قوانین داخلی هر کشور جرم شناخته شوند و از جمله دسترسی غیر مجاز، مداخله در سیستم و اطلاعات، اقدام‌هایی چون جعل و کلاهبرداری از طریق رایانه، کمک یا مشارکت در ارتکاب این‌گونه جرایم در این کنوانسیون وجود دارد.

این کنوانسیون مکانیزم مشروحي را برای همکاری و هماهنگی بین‌المللی در خصوص تحقیقات و پیگرد مجرمین ارائه می‌کند. اعضا این کنوانسیون باید اختیارات لازم را برای جست‌وجوهای کامپیوتری، کشف و ضبط اطلاعات رایانه‌ای، تهیه آمار مورد نیاز جهت ارائه اطلاعات تحت کنترل و تهیه یا نگهداری سریع اطلاعات آسیب‌پذیر به مسئولین ذیربط ملی خود تفویض کنند. مفاد این کنوانسیون را می‌توان به‌عنوان ابزاری برای همکاری‌های قضایی در زمینه مبارزه با موادمخدر استفاده کرد. برای مثال، زمانی که مسئولین یک کشور

نیاز به شواهد الکترونیکی در خصوص فعالیت‌های قاچاقچیان موادمخدر، مشتریان یا اموال ایشان در کشور دیگری دارند، می‌توانند از آن کشور، جست‌وجوی بانک‌های اطلاعاتی مورد استفاده قاچاقچیان یا کنترل ارتباط‌های الکترونیکی آن‌ها مانند پست الکترونیکی و غیره را تقاضا کنند.

با این وجود، صنایع خصوصی و گروه‌های مردمی به برخی از مفاد کنوانسیون جرایم رایانه‌ای اعتراض کرده‌اند. یکی از کنسرسیوم‌های صنایع تکنولوژی اطلاعات اعتراض کرده است که این کنوانسیون باعث پدید آوردن مشکلاتی برای ارائه‌دهندگان خدمات اینترنتی در زمینه حفظ و نگهداری اطلاعات خواهد شد و راه را برای اقدام‌های حقوقی علیه ایشان توسط شخص ثالث گشوده و فعالیت‌های مجاز اینترنتی را محدود خواهد ساخت. گروه‌های طرفدار آزادی‌های مدنی نیز نگرانی خود را در خصوص تدابیری که متجاوز حقوق فردی در این کنوانسیون می‌خوانند، اعلام کرده‌اند. با این وجود، سازمان ملل متحد بر این عقیده است که این‌گونه ابزارهای قانونی به تلاش‌ها علیه قاچاق و سوء مصرف موادمخدر کمک خواهد کرد.

نتایج و توصیه‌ها

نتایج: تکنولوژی‌های جدید ارتباطی به‌مثابه نیروی محرکه اقتصاد جهانی امروز است و به همین دلیل نه شایسته است که از گسترش و تکمیل آن جلوگیری کرد و نه می‌توان این کار را انجام داد. با این حال، باید قبول کرد که جهانی شدن و تکنولوژی‌های جدید باعث تسهیل برخی از فعالیت‌های جنایتکارانه در زمینه قاچاق موادمخدر شده و مشکلات اضافی را برای ارگان‌های انتظامی ایجاد کرده است. اگر چه همکاری بین پلیس و این صنعت در اغلب مواقع در سطح خوبی بوده است، لیکن بخش‌های خصوصی و دولتی همیشه با هم در توافق کامل نیستند و دلیل آن این است که وظیفه شرکت‌ها حفظ حقوق مشتریان

و به‌دست آوردن سود برای سهامداران خود است. اگرچه تمرکز اصلی اقدام‌های کنونی در خصوص جرایم رایانه‌ای اغلب موضوع اشاعه تصاویر مستهجن از کودکان و جرایم اقتصادی کلاهبرداری، مزاحمت و دزدی‌های علمی و هنری از طریق اینترنت است، لیکن نشانه‌هایی نیز دال بر استفاده روز افزون از تکنولوژی جدید در زمینه قاچاق و ساخت موادمخدر غیرقانونی به چشم می‌خورد. به همین دلیل، فقدان مفاد مربوط به موادمخدر در قوانین موجود علیه جرایم رایانه‌ای باعث نگرانی است. اگر قرار است پلیس‌ها بتوانند با چالش‌های موجود مقابله کنند، باید یک برنامه عمل در سطوح بین‌المللی و ملی با هدف جلوگیری از جرایم موادمخدر مرتبط با تکنولوژی جدید در متن اقدام‌های کنونی علیه جرایم رایانه‌ای وجود داشته باشد. شایان ذکر است، بسیاری از کشورهای در حال توسعه به‌طور غریزی برای راهنمایی حقوقی و فنی در این زمینه به سازمان ملل متحد مراجعه خواهند کرد.

در خصوص محتویات مربوط به موادمخدر در سایت‌های اینترنتی، ابزارهای تکنولوژیکی، پلیس و آموزش، به‌ویژه فعال شدن والدین در این امر ضروری است. با توجه به مشکلات تحقیقات و شناسایی و تعداد بی‌شمار سایت‌های اینترنتی در خصوص موادمخدر، استفاده از نرم افزارهای بلوکه و فیلتر کردن اطلاعات از اهمیت ویژه‌ای در امر مقابله با استفاده از اینترنت برای پخش پیام‌های تبلیغاتی برای سوء مصرف موادمخدر برخوردار است و ممکن است واقعی و عملی‌تر از روی آوردن به قوانین جزایی باشد.

ارائه ابزارهای فنی و قانونی به ارگان‌های انتظامی و سایر مؤسسه‌های ملی مسئول مبارزه با جرایم موادمخدر جهت توسعه توانائی‌های مناسب برای مقابله از اهمیت بسزایی برخوردار است، اما این امر به تنهایی کافی نیست.

سازمان ملل متحد معتقد است، چالش‌های پلیس تنها از طریق همکاری و مشارکت دولت‌ها، صنایع تکنولوژیکی اطلاعات

و مردمی که خواست‌های متفاوتی نیز دارند، قابل حل است. نگرانی‌هایی که توسط گروه‌های طرفدار حقوق بشر در خصوص تعرض به حقوق شخصی و امکان بالقوه جهت محدود کردن آزادی بیان اعلام شده، واقعی است و باید به آن توجه شود.

در چارچوب همکاری بین دولت و بخش صنعت، فعالیت صنایع در شناسایی آسیب‌پذیری و کمک به مسئولین انتظامی در امر ارزیابی خطر و نیز کمک به حل مواردی که پیش می‌آیند، مورد نیاز است. هم‌زمان، بخش صنعت باید توجه داشته باشد که پیروی از مقررات سازمانی و همکاری از کانال‌های غیررسمی با پلیس ممکن است همیشه برای مقابله با خطر کافی نباشد. وقایع اخیر جهان هم‌اکنون ضرباتی را بر قوانین کیفری مربوط به تحقیقات و پیگرد وارد کرده است، لیکن تنها گذر زمان تأثیرهای سوء کامل آن‌را نشان خواهد داد. در حال حاضر، تنها می‌توان گفت که نیاز به مدرنیزه و سازگار کردن ساختارهای انتظامی با شرایط متغیر و چالش‌های جدید عمیق‌تر شده است. به تکنولوژی‌های جدید نباید به‌صورت یک دشمن در امر مبارزه با جرایم موادمخدر نگریست، بلکه باید به‌عنوان ابزارهای بالقوه در امر پیشگیری از مصرف، تولید، ساخت و قاچاق موادمخدر مورد استفاده قرار گیرند. سازمان ملل متحد پاسدار سه عهدنامه بین‌المللی کنترل موادمخدر است که هدفشان بهداشت و رفاه اجتماع است. **توصیه‌ها:** ضروری‌ترین وظیفه دولت‌ها وضع قوانین اساسی و رویکردهای مناسب در سطح ملی برای مقابله با جرایم مرتبط در محیط‌های الکترونیکی است. زمانی که جرایمی در زمینه قاچاق موادمخدر توسط یک گروه سازمان یافته جنایتکار (همان‌گونه که در کنوانسیون سازمان ملل علیه جرایم سازمان یافته فراملی آمده است) انجام می‌گیرد، عوامل تشدیدکننده به‌وجود می‌آیند. باید برای تضمین اینکه جرایم، مجازات‌ها، ضوابط و معیارهای دلیل در کشورهای سراسر جهان یکسان باشد و به‌منظور جلوگیری از رشد بهشت‌های اطلاعاتی، اقدام‌هایی

صورت بگیرد. کشورهای در حال توسعه که خطر این‌گونه سوءاستفاده‌ها در آن‌ها زیاد است، باید مورد حمایت و کمک قرار گیرند.

ارگان‌های انتظامی و مسئولین قضایی باید منابع و تجهیزات مناسبی برای تحقیق، شناسایی، دستگیری و پیگرد قانونی مجرمینی که از تکنولوژی‌های جدید در زمینه فعالیت‌های قاچاق موادمخدر بهره می‌جویند، در اختیار داشته باشند.

واحدهای بین‌ارگانی متخصص تکنولوژی جدید در زمینه موادمخدر باید در سطح ملی ایجاد شوند. سیستم شبکه‌های «۲۴/۷» باید به‌گونه‌ای گسترش یابند تا کشورهای بیشتری را در بر گیرد. این واحدها باید ترتیب‌های لازم را برای همکاری با سایر ارگان‌های موجود علیه جرایم رایانه‌ای داشته باشند.

جهت حفاظت از اطلاعات موجود در بانک‌های اطلاعاتی، ارگان‌های انتظامی موادمخدر در برابر حملات رایانه‌ای باید از این اطلاعات حفاظت زیربنایی مناسب به‌عمل آید.

سرمایه‌گذاری‌هایی در خصوص ارائه تجهیزات و آموزش مناسب فنون قضایی و مهارت‌های تکنولوژیکی باید برای سیاست‌گذاران و نیروهای انتظامی و مأمورین تحقیق به‌عمل آید. دولت‌ها باید راه‌های جذب متخصصین توانمند تکنولوژی جدید را برای همکاری با ارگان‌های انتظامی موادمخدر بیابند.

باید سعی شود کنوانسیون جرایم رایانه‌ای در اسرع وقت به‌تصویب برسد و سایر فعالیت‌های این‌گونه در جهان مورد حمایت قرار گیرند.

دولت‌ها باید داروخانه‌های اینترنتی را در هر جا که فعالیت می‌کنند یا موادمخدر تجویزی را تحویل می‌دهند، ملزم به دریافت مجوز کنند و یک سیستم نظارتی ایجاد کنند. از آنجا که در حال حاضر فروش موادمخدر از طریق اینترنت در سیستم‌های کنترلی ملی و بین‌المللی پیش‌بینی نشده‌اند، فروش آن باید به‌طور کلی ممنوع شود.

دولت‌ها باید به ارتقاء سطح آگاهی‌های عمومی به‌ویژه در بین والدین و معلمان

کمک کنند. این حقیقت که جوانان استفاده‌کننده از اینترنت در معرض پیام‌های تبلیغی برای مصرف موادمخدر هستند و قابلیت دسترسی به ابزارهای تکنولوژیکی لازم جهت بلوکه یا فیلتر کردن این‌گونه پیام‌ها را دارند، باید مورد تأکید قرار گیرد.

دولت‌ها باید از ایجاد سایت‌های اینترنتی که به‌صورت جذاب اطلاعات غیرمغرضانه را درخصوص مصرف موادمخدر غیرقانونی ارائه می‌دهند، حمایت کنند. برای مثال، در این سایت‌ها توضیح قوانین مربوط به در اختیار داشتن موادمخدر غیرمجاز، مصرف و قاچاق آن در کشور و نیز تشریح موادمخدر و تأثیرها آن قابل ارائه هستند.

موضوع تدوین کنوانسیون سازمان ملل علیه جرایم رایانه‌ای را می‌توان مورد توجه قرار داد. چنین کنوانسیونی می‌تواند یک طبقه‌بندی و تعریف جهانی را برای جرایم مرتبط با تکنولوژی جدید و رایانه‌ای ارائه کند و چارچوب لازم برای هماهنگ کردن قوانین و همکاری‌های بین‌المللی در زمینه تحقیق‌ها و پیگرد قانونی جرایم فرامرزی را که توسط ابزارهای الکترونیکی مرتکب یا تسهیل شده‌اند، به‌دنبال داشته باشد. همچنین، می‌توان یک بند در زمینه جرایم موادمخدر در نظر گرفت که در آن به دولت‌ها یادآوری شود، هر نوع تبلیغات برای موادمخدر و روان‌گردان باید ممنوع اعلام شود. مفاد کنوانسیون باید در زمینه‌های امنیت و حفاظت از جرم با توجه به آزادی‌های مدنی، شخصیتی و خصوصی به‌صورت متعادل تدوین شود.

ارائه دهندگان خدمات اینترنتی باید خطوط مستقیم تلفنی را به عموم مردم جهت گزارش دادن مطالب اهانت‌آمیز یا غیرقانونی سایت‌های اینترنتی اعلام کند و آگاه باشند که برخی از مطالب سایت‌های مربوط به موادمخدر ممکن است ناقض مفاد کنوانسیون‌های بین‌المللی کنترل موادمخدر باشد و مؤسس‌های مالی باید اقدام‌های خود علیه تظهير پول را با توجه به تحولات تکنولوژیکی مورد بررسی قرار دهند.♦