فصـــــلنامه بیـــن المللـــــی قـــانـــون یـــار
License Number: 78864 Article Cod:Y8SH29A546704 ISSN-P: 2538-3701

تشریح علل، پیامدها و آثار جرایم رایانه ای با هدف محدودسازی عوامل جرم زا

(تاریخ دریافت ۱۴۰۳/۰۴/۲۹، تاریخ تصویب ۱۴۰۳/۰۶/۰۲)

پرستو فتاحی زاده
دکترطاهره پارسا جم[۱]

چکیده

جرایم رایانه‌ای جرایمی سازمان یافته اند که از طریق اشخاص حرفه‌ای و با سواد انجام می‌شوند و همیشه قوانین رایانه‌ای امروزه برای مجازات مجرمین کافی اما کامل نمی‌باشد چون هر روز جرایم جدیدی به وجود می آید که برای مجازات آنها نیاز به قوانین جدید داریم همانگونه که جرایم اینترنتی همیشه درحال روز شدن هستند بایستی تلاش کرد تابتوان با نو شدن جرایم قوانینی را که در زمینه جرایم جدید قابل اعمال باشد ارائه کرد. برای پیشگیری از این جرایم باید همه دستگاه‌ها تلاش کنند و مردم نیز توصیه‌های مسئولین را در این مورد جدی بگیرند ودر هنگام استفاده از اینترنت و رایانه مورد استفاده قرار دهند تا مورد سوء استفاده دیگران قرارنگیرند. به هرصورت مطالعه علمی این جرایم، با تعمق برعلل گرایش کاربران به بزهکاری های مجازی و نیز بررسی عوامل تاثیرگذار در بزه دیدگی افراد در فضای سایبری، جهت حذف یا محدودسازی عوامل جرم زا ضروری به نظرمی رسد. در این مقاله ارکان جرایم سایبری بررسی شده و آثار سیاسی، فرهنگی، روانی و اجتماعی این پدیده تشریح می شوند تا گامی در جهت محدودسازی عوامل جرم زا برداشته شود.

واژگان کلیدی: جرم رایانه ای، فضای سایبری، عوامل جرم زا، رایانه، اینترنت

---

[۱] نویسنده مسئول

بخش اول: انواع جرم‌های رایانه‌ای

هک کردن: عبارتست از نفوذ به یک سیستم کامپیوتری بدون داشتن مجوز، مالکیت یا صلاحیت لازم. هک کردن یعنی غلبه کردن بر سیستم‌های امنیتی یک سیستم کامپیوتری برای دسترسی غیر قانونی به اطلاعات ذخیره شده. لو رفتن رمز عبور به قصد دسترسی به اطلاعات خصوصی افراد یک سازمان یکی از رایج‌ترین تخلفات رایانه‌ای است. یکی از خطرناک‌ترین خلاف کاری‌های رایانه‌ای عبارتست از هک کردن آدرس IP تا بدین وسیله خلافکار خود را به جای شخص دیگری جا بزند و افکار شوم یا جنایات مورد نظر خود را اجرا کند.

فیشینگ[۱] : عبارتست از تلاش برای بدست آوردن اطلاعاتی مانند رمز عبور، شناسه عبور و جزئیات کارت اعتباری با جا زدن خود به عنوان یک منبع قابل اعتماد. فیشینگ نوع بسیار خاصی از جرائم رایانه‌ای است که برای فریب دادن شما در زمینه افشای جزئیات مالی و شخصی شما، طراحی شده است. مجرمان رایانه‌ای، یک وب سایت جعلی ایجاد می‌کنند که بسیار شبیه به وب سایت بانک (یا هر وب سایت دیگری که تراکنش‌های مالی در آن انجام می‌شود سپس تلاش می‌کنند تا شما را به منظور بازدید از این سایت و تایپ کردن اطلاعات محرمانه خود نظیر اطلاعات شخصی و ورود به سایت، و گرفتن کلمه عبور فریب دهند. نوعاً مجرمان رایانه‌ای تعداد زیادی نامه‌های الکترونیکی ارسال می‌کنند که حاوی یک فراپیوند به سایت جعلی است.

حمله فیشینگ نوعی دیگر از جرایم سایبری است که در آن، مجرم یک کپی تقریباً ۱۰۰ درصد شبیه یک وب سایت بنگاه تجاری، ایجاد می‌کند. و تلاش می‌کند تا کاربران را برای افشای جزئیات شخصی خود نام کاربری، کلمه عبور[۲]، و غیره از طریق یک فرم در سایتی جعلی فریب دهد که این اجازه را به مجرم می‌دهد با استفاده از این اطلاعات پول به دست آورد.

[۱] Phishing
[۲] PIN

فیشرها یا مجرمان فیشینگ از تکنیک‌های متعددی برای فریب دادن کاربران به منظور دسترسی به سایت جعلی استفاده می‌کنند. مثلاً، ارسال ایمیل‌هایی که به نظر می‌آید از یک بانک باشد. این ایمیل‌ها اغلب از لوگوهای قانونی و یک سبک تجاری خوب استفاده می‌کنند و سربرگ نامه را به گونه‌ای طراحی می‌کنند که شبیه این به نظر برسد که به بانکی قانونی تعلق دارند. به طورکلی، این نامه‌ها به دریافت‌کنندگان اطلاع می‌دهند که بانک، زیرساخت IT خود را تغییر داده و از تمامی مشتریان می‌خواهد که اطلاعات کاربری خود را مجدداً تصدیق کنند هنگامی‌که دریافت کننده، روی لینک موجود در ایمیل کلیک می‌کند، به سایتی جعلی هدایت می‌شود که از او می‌خواهد اطلاعات شخصی خود را وارد کند.

بررسی و شناخت گروه ویروس‌های کامپیوتری: دسته ویروس‌های کامپیوتری (شامل ویروس‌ها، کرم‌ها، نرم‌افزارهای جاسوسی و غیره) در حقیقت نرم افزارهایی هستند که خود را تکثیر و منتشر می‌کنند و کامپیوترهای موجود در یک شبکه را بدون اطلاع کاربران آلوده کرده و به آنها صدمه می‌زنند. ویروس‌ها از طریق فایل‌های سیستم یک شبکه کامپیوتری، اینترنت یا هر وسیله نقل انتقال اطلاعات مانند حافظه فلش، و غیره وارد کامپیوترهای دیگر می‌شوند. ویروس‌های کامپیوتری کدهایی هستند که با هدف ضربه زدن به یک سیستم رایانه‌ای یا از بین بردن اطلاعات نوشته شده‌اند. نوشتن ویروس کامپیوتری در همه جای دنیا یک جرم است به گونه‌ای که نویسنده ویروس در برابر تمام خسارت‌های وارده به همه کامپیوترهای آلوده شده مسئول است.

وسایل سایبری[1]: عبارت است از استفاده از فناوری ارتباطات به خصوص اینترنت برای آزار و اذیت افراد. تهمت، ارسال نرم افزارهای مخرب و تخریب اطلاعات‌و تجهیزات کامپیوتری دراین گروه قرار می‌گیرند. این خلافکاران اغلب کاربران را از طریق چت‌روم ها، تالارهای تبادل نظر و اجتماعات اینترنتی شکار می کنند سپس اطلاعات آنها را بدست می‌آورند (مثلاً شماره تلفن و آدرس، محل کار و غیره) و با استفاده از این اطلاعات قربانیان خود را مورد

[1] Cyber stalking

اذیت و آزار قرار می‌دهند. ایمیل‌های تهدید آمیز، مزاحمت تلفنی و مانند این‌ها انجام می‌دهند و این مورد یکی از جرم‌های رایانه‌ای خطرناک است که در سراسر دنیا مجازات سنگینی برایش قرار می گیرد.

هویت جعلی: هویت جعلی یا خود را به جای کس دیگر جا زدن یکی از جدیدترین کلاه برداری‌هایی است که به کمک آن پول‌های زیادی ربوده شده و سودهای کلانی نصیب کلاه برداران می‌شود. در این شیوه کلاه بردار خود را به جای مالک جا می‌زند. یا از هویت شخص دیگری برای بدست آوردن کالا یا خدمات مورد نیاز خود استفاده می کنند. مهاجرت غیر قانونی، تروریسم و ایمیل‌های سیاه در زمره این جرائم قرار می گیرد.

در انواع جرائم رایانه‌ای همه جرایم در یک چیز مشترک است و آن هم بهره برداری غیر قانونی از فناوری جدید رایانه‌ای و ارتباطات برای فعالیت‌های خلاف کارانه است. همان طور که فناوری جدید راهی برای مقابله ارائه می دهد از آن سو هم جنایتکاران از آخرین فناوری-ها سود می‌برند. و همیشه یک قدم از سیستم‌های امنیتی جلوتر هستند. و هیچ راهی امن تر از احتیاط نیست پس مراقب ایمیل های ناشناس، چت روم‌ها، حافظه‌های فلش، وب سایت‌های مشکوک و غیره باشید و سعی کنید اطلاعات بیشتری درباره امنیت در اینترنت پیدا کنید.

بخش دوم: ویژگی های جرایم رایانه‌ای

این گونه جرایم را می‌توان به سه دسته تقسیم کرد:

۱- جرایم علیه اشخاص : جرایم علیه اشخاص را می‌توان اذیت و آزارهای اینترنتی دانست که می‌تواند به اشکال جنسی، نژادی، مذهبی و غیره رخ دهد. این جنبه معمولاً با حوزه دیگری به نام حریم خصوصی شهروندان تداخل پیدا می کند که خود حوزه بسیار گسترده و قابل توجه دیگری است. از دیگر جرایم این دسته می توان به جرایمی مانند پورنوگرافی کودکان و

آزار و اذیت‌ها با استفاده از رایانه اشاره کرد که یکی از گسترده‌ترین و شایع ترین جرایم موجود است.

۲- دسته دوم شامل خرابکاری های کامپیوتری و تبادل برنامه های خطرناک است. جرایم علیه اموال

۳-جرایم علیه دولت‌ها : شایع ترین نمونه این جرایم، سرقت اطلاعات یا آسیب رساندن به رایانه‌ها و سیستم است. این در حالی است که در برخی سیستم های حقوقی، اموال غیرعینی و غیرملموس قابل سرقت نبوده و آسیب وارده باید حتماً دیده شود. مشکل دیگر موجود در این عرصه، ارایه نشدن تعریف‌های لازم درباره جوانب مختلف این تکنولوژی و جرایم محتمل در درون آن است.

نقض قوانین کپی رایت (حق مؤلف) را نیز می توان یکی دیگر از جرایم شایعی دانست که امروزه از طریق رایانه و شبکه جهانی اینترنت به شدت در حال انجام است. یک مورد از موارد ثبت شده حمله به برنامه «یاهو مسنجر» در ساعت ۱۰:۳۰ دقیقه هفتم فوریه ۲۰۰۰ بود که سه ساعت طول کشید و در این زمان، «پینگ» یاهو به یک گیگابایت درثانیه کاهش یافت.

کلاهبرداری و ایجاد اختلال در سیستم‌های مالی و بانکی برای انتقال وجوه و پول به حساب مجرم یکی از جرایم مهمی است که تا کنون خسارات زیادی را در کشورهای مختلف جهان به همراه داشته است. انتشار ویروس «ملیسا» در سال ۱۹۹۹ یک نمونه مشهود دیگر است. این ویروس در مارس ۹۹ برای نخستین بار در اینترنت ظاهر شده و با سرعت زیادی در سیستم‌های کامپیوتری آمریکا و اروپا منتشر شد. برآورد شده که انتشار این ویروس در سراسر جهان، خسارتی هشتاد میلیونی از خود بر جای گذاشت. این ویروس تنها در آمریکا ۱/۲ میلیون کامپیوتر متعلق به یک پنجم بزرگ ترین تجارت‌های این کشور را آلوده کرد.

«دیوید اسمیت»، طراح این ویروس، در نهم دسامبر ۱۹۹۹ به علت طراحی و انتشار این ویروس به ارتکاب جرایم ایالتی و فدرال متهم شد. تروریسم رایانه‌ای، آخرین موج جرایم به وجود آمده در این عرصه است که نگرانی‌های گوناگونی را در میان کشورها پدید آورده است. استفاده تروریست ها از شبکه به صورت های گوناگون برای تبادل اطلاعات به صورت رمزی و کد شده و حتی در قالب پورنوگرافی کودکان و استخدام نیرو از این راه، معضلی است که در آینده ای نه چندان دور، می تواند به مهم ترین چالش بین المللی برای کشورها تبدیل شود. در عین حال، معاملات مواد مخدر از طریق اینترنت و سرویس‌های پست الکترونیکی نیز زمینه دیگری است که باندهای قاچاق مواد مخدر به راحتی از آن برای انجام معاملات و ردیابی محموله های غیرقانونی قرص ها و تبلیغ محصولات خود از آن استفاده می‌کنند. پلیس فدرال آمریکا هم اکنون دارای یک شاخه جرایم اینترنتی و رایانه‌ای بوده که چهار زمینه عمده را به عنوان هدف خود بیان کرده است که در درجه نخست، مبارزه با جرایم جدی رایانه‌ای و گسترش آن است.

۱) شناسایی و دستگیری مجرمان جنسی که از اینترنت برای توزیع و تولید پورنوگرافی کودکان استفاده می کنند.

۲) مبارزه با فعالیت‌های مجرمانه‌ای که مالکیت معنوی کشور آمریکا را هدف قرار می‌دهد.

۳) امنیت ملی و بازار رقابت را به خطر می‌اندازد.

۴) سرکوب شبکه‌های مجرمانه بین المللی سازمان یافته که در فعالیت‌های جعل و سرقت هویت اینترنتی فعالیت دارند.

از جرایم شایع دیگر در محیط اینترنت می‌توان به پورنوگرافی اینترنتی کودکان اشاره کرد که در همه جهان جرم به شمار رفته و مرتکبین آن به شدت از سوی کشورها و پلیس بین الملل تحت تعقیب قرار می گیرند. اینترپل چند ماه پیش موفق شد با بازسازی چهره فیلتر شده یک

مجرم جنسی کودک آزار با استفاده از روش‌های پیچیده کامپیوتری و پیگیری‌های دقیق وی را شناسایی کرده و سرانجام با همکاری پلیس تایلند موفق به دستگیری این مجرم فراری شود که عکس اعمال مجرمانه خود را در شبکه اینترنت منتشر کرده بود. سازمان‌های بین المللی گوناگون دیگری نیز در این زمینه جرایم الکترونیکی فعالیت دارند که مهم‌ترین آن‌ها عبارتند از: شورای اروپایی، سازمان ملل متحد، اتحادیه اروپا، سازمان کشورهای آمریکایی، گروه ۸، سازمان همکاری‌های اقتصادی آسیای‌شرقی، اتحادیه‌کشورهای جنوب شرق آسیا، سازمان همکاری ها و توسعه اقتصادی، ناتو، اتحادیه آفریقا، اتحادیه عرب و سازمان همکاری‌های شانگ‌های، اما شاید بهترین مرجع بین المللی در این زمینه برای الگو گرفتن دیگر کشورها و ایجاد روندی مشابه، کنوانسیون جرایم رایانه‌ای و اینترنتی، شورای اروپایی باشد که شمار بسیاری از کشورهای اروپایی به آن پیوسته و عضویت برای کشورهای غیر عضو این شورا نیز آزاد است. هدف اصلی این معاهده که همه کشورها امکان پیوستن به آن را دارند همان گونه که در مقدمه آن نیز ذکر شده، ایجاد سیاست کیفری واحد با هدف حمایت از جامعه در برابر جرایم رایانه‌ای و اینترنتی با در پیش گرفتن قانون‌گذاری‌ها و تقویت‌همکاری بین‌المللی‌است. این کنوانسیون نتیجه چهارسال فعالیت کارشناسان شورای اروپایی و کشورهای دیگر بوده و دارای یک پروتکل الحاقی با موضوع تبلیغات نژادپرستانه و تبلیغ تنفر از طریق شبکه‌های کامپیوتری مصوب مارس ۲۰۰۶ بوده و هم اکنون نیز بحث تروریسم رایانه‌ای و اینترنتی در دستور کار این کنوانسیون قرار دارد.

بخش سوم: آثار مخرب جرایم رایانه‌ای

بند اول: آثار و آسیب‌های روانی

✓ اعتیاد مجازی

اعتیاد مجازی، استفاده بیش از حد از اینترنت است تا آنجا که بدون استفاده از آن فرد احساس کمبود می‌کند و روابط او با محیط متأثر از استفاده مکرر و دیوانه وار فرد شده از حالت عادی خارج می‌شود.این اختلال روانی در کشورهایی که استفاه از اینترنت آسان و ارزان است، بسیار چالش زا بوده و تا آنجا که نهادهای مختلف را درگیر کرده است. در کشوری، مثل آمریکا تعداد معتادان به اینترنت از سایر معتادان بیشتر است، تا جایی که برخی معتادان ۱۸ ساعت از وقت روزانه خود را در اینترنت صرف می‌کنند. در آمریکا به قدری فاجعه بار است که کلیساها، پیشوایان مذهبی با فریادهای کمک خواهی زن و شوهر، یا یکی از آنها، برای رهایی از این نوع اعتیاد مواجه هستند و مؤسسه های مشاوره ای مسیحی در حال تدوین مشاوره‌های اعتیاد به اینترنت می‌باشند. پیامدهای اعتیاد به اینترنت و حتی کار زیاد با اینترنت، که در حدّ اعتیاد نباشد، نتایج و پیامدهای زیان بخشی برای فرد و جامعه در پی داشته و آسیب-های شدید جسمانی، مالی، خانوادگی، اجتماعی و روانی را به همراه دارد. یکی از پیامدهای فردی و اجتماعی اعتیاد و کار زیاد با اینترنت، انزوا و کناره‌گیری اجتماعی است. پوت نام (۱۹۹۱م) معتقد است در طی ۳۵ سال گذشته کاهش چشم گیری در ارتباطات اجتماعی افراد در آمریکا رخ داده است. مردم کمتر به رأی گیری و کلیسا می روند، به ندرت موضوعات سیاسی را با همسایه‌ها در میان گذاشته یا عضویت گروه‌های داوطلبانه را قبول می‌کنند، مهمانی شام کمتری دارند و کمتر به منظور اجتماعی دور هم جمع می‌شوند. این موضوع پیامدهای عمده‌ای برای جامعه و فرد دارد، زیرا وقتی مردم از نظر اجتماعی درگیر باشند، سالم‌تر و خوشبخت تر زندگی می‌کنند.

از دیگر پیامدهای اعتیاد اینترنتی مشکلات خانوادگی و تأثیر آن بر روابط زناشویی، والدین و فرزندان است. امروزه اصطلاح «بیوه اینترنتی» برای همسر معتاد به اینترنت اطلاق می‌شود. آمار نشان می‌دهد که اعتیاد به اینترنت ممکن است به فروپاشی خانواده و طلاق منجر شود. شاید باور کردن اینکه شخصی همسر خود را فقط به علت ارتباط با فرد دیگر در اینترنت ترک می‌کند، برای کسانی که به اینترنت اعتیاد پیدا نکرده‌اند، وحشتناک به نظر برسد؛ ولی این مسئله هر روز در دنیای اینترنت اتفاق می‌افتد. دکتر یانگ معتقد است: اگرچه زمان تنها عامل تعیین کننده در تعریف اعتیاد به اینترنت نیست، ولی عموماً معتادان بین ۴۰ تا ۸۰ درصد از وقت خود را با جلساتی که ممکن است هر کدام حتی تا ۲۰ ساعت طول بکشد، صرف می‌کنند و این کار باعث می‌شود تا اختلالاتی در میزان و زمان خواب کاربر به وجود آید. در موارد شدید، حتی قرص‌های کافئین برای تسهیل زمان طولانی‌تری در اینترنت بودن مصرف می‌شود. این اختلال، خستگی بیش از اندازه ای در بدن ایجاد می‌کند، که کارکرد درسی و شغلی را تحت تأثیر قرار می‌دهد و ممکن است نظام ایمنی بدن را ضعف کند و فرد، آسیب پذیری بیشتری به بیماری‌ها پیدا کند. افزون بر این، به علّت عدم ورزش و حرکات مناسب، مشکلات عصب‌های مچ و درد پشت، چشم درد و مانند آن به وجود می‌آید.

✓ بحران هویت

هویت، واجد و دارای سه عنصر است: شخصی، فرهنگی و اجتماعی، که هریک در تکوین شخصیت فرد نقش مهمی را ایفا می‌کند. در مقایسه‌ها، هویت شخصی، ویژگی بی همتای فرد را تشکیل می‌دهد و هویت اجتماعی در پیوند با گروه ها و اجتماعات مختلف قرار می‌گیرد. اینترنت صحنه فرهنگی و اجتماعی است، که فرد خود را در موقعیت های متنوع نقش ها و سبک های زندگی قرار می‌دهد و این خود زمینه‌ای برای آسیب پذیری شخصیت کاربر و موجب چند شخصیتی شدن کاربر می‌شود.

از این روست که ساختار و چینش پایگاه های شخصی (WebLoge) به گفته میلر (Miler) نشان از شخصیت آن کاربر است. جوانان در این محیط از آسیب پذیری بیشتری برخوردارند، به ویژه در دورانی که هویت ایشان شکل می گیرد، این خطر پررنگ تر می شود. دکتر محمد عطاران معتقد است: با امکانات و گزینه‌های فراوانی که رسانه های عمومی، از جمله اینترنت در اختیار جوانان می گذارند، آنان دائماً با محرک‌های جدید و انواع مختلف رفتار آشنا می-شوند. چنین فضایی هویت نامشخص و پیوسته متحولی را می‌آفریند، خصوصاً برای نسلی که در مقایسه با نسل قبل با محرک‌های فراوانی مواجه است. همچنین از طریق رسانه‌های جمعی، افراد، خطّ مفروضی میان فضای عمومی و خصوصی را تجدید سازمان می کنند و این امکانی است که جوانان فعالانه از آن استفاده می کنند. جوان، به خصوص در دوران بلوغ که مرحله شکل گیری هویت اوست و همواره به دنبال کشف ارزش‌ها و درونی کردن آنها می‌باشد، با اینترنت و حجم گسترده، حیرت انگیز و گوناگون اطلاعات مواجه می‌شود و ناچار که در این دنیای مجازی، هویت خویش را از طریق جستجو پیدا کند و بدین سان، ممکن است برخی و شاید تعداد زیادی از نوجوانان راه را در اینترنت گم کنند و دوران هویت یابی خویش را بیش از پیش با بحران سپری کنند. از سوی دیگر، گاهی برخی از ویژگی‌های شخصیتی، مانند سن، تحصیلات، محل سکونت و حتی جنسیت در اینترنت از بین می‌رود، به عنوان نمونه، بسیاری از افرادی که در اتاق‌های چت مشغول گفتگو با یکدیگر می‌باشند. با مشخصیاتی غیرواقعی ظاهر شده و از زبان شخصیتی دروغین که از خود ساخته‌اند و آن را به مخاطب یا مخاطبان خود معرفی کرده‌اند، صحبت می کنند و با این حال، چه تأثیراتی که همین شخصیتهای ناشناس بر یکدیگر دارند. از جمله نتایج بحران هویت نیز کم رنگ شدن علایق کاربران به وطن خویش است، که نتایج خطرناکی چون خیانت به کشور و خودکم بینی و وابستگی فرهنگی و شخصیتی به کشورهای بیگانه خواهد بود. یکی از ریشه‌های وقوع جرایم امنیتی، وجود بحران هویت است که در جرایم جاسوسی و خیانت به کشور بیشتر رخ می‌نماید.

✓ انحرافات جنسی

از جمله آثار مخرّب جرایم رایانه‌ای، به ویژه جرایم مرتبط با محتوا (به قول قانون مجازات جرایم رایانه‌ای) به وجود آمدن انحرافات جنسی و اختلالات جنسی است. اینترنت به دلیل رویکرد آزاد اندیشی در روابط جنسی از سوی گردانندگان اصلی آن (یعنی غرب و به ویژه آمریکا) و نگرش تجاری نسبت به مسائل جنسی موجب پدید آمدن پدیده کثیفی به نام هرزه نگاری و هنر پلید شهوانی و رواج سرسام آور آن گردید، که مرزهای اخلاقی را درهم می-شکند و تهدیدی برای فرهنگ‌ها، به ویژه فرهنگ‌های دینی، چون فرهنگ اسلامی است. اصولاً، پورنوگرافی به عنوان نمایش تصویری و یا کلامی، رفتارهای جنسی است که با هدف ارضای خواسته های جنسی دیگران تعریف می‌شود. این گونه مطالب و تصاویر که در پی تحریک جنسی دیگران عرضه می گردد، معمولاً به ارضای غیرطبیعی جنسی مراجعه کنندگان آن می انجامد.نکته دیگر اینکه رجوع به اینترنت برای دسترسی به مطالب مستهجن[1]، صرفاً به افراد نابهنجار خلاصه نمی‌شود و حجم قابل توجهی از مراجعان را افراد طبیعی تشکیل می‌دهند. اصولاً اینترنت به جوی دامن زده که در سایه ویژگی های خاص خود به تدریج به شکل گیری ناهنجاری‌های جنسی در کاربران خود می‌انجامد و منشأ به وجود آمدن بسیاری از جرایم رایانه‌ای (به ویژه محتوایی) و مقمه‌ای برای جرایم جنسی می گردد.

دلایل رجوع و اقبال مردم به این گونه مطالب را در عرصه اینترنت می توان در این موارد خلاصه نمود:

الف. گمنامی: ناشناخته ماندن مراجعان در عرصه اینترنت، به نوعی اعتماد به نفس در افراد را دامن می زند و این حالت، نوعی رفتار غیرمسئولانه را در فرد شکل می‌دهد. مراجعان درچنین شرایطی است که به خود اجازه می‌دهند تا برخلاف رفتارهای طبیعی به راحتی از دسترس زوج اینترنتی خود دور شوند و یا بلافاصله به فرد دیگری روی آورند. اصولاً در چنین فضایی

[1] Obscenity

است که فرد می‌تواند در معرفی خود هرگونه که می‌خواهد عمل کند و همین ویژگی، خود محرکی است تا کاربران اینترنتی به استفاده از هویت جعلی روی آورند و این را می‌توان از جمله ویژگی‌های فرهنگ فضای مجازی برشمرد، که این خود زمینه‌ای برای ارتکاب جرایم فضای سایبر نیز هست.

ب. سهولت

مطالب شهوانی و تصاویر سکسی به آسانی در دسترس همگان قرار دارند. عرضه گسترده این مطالب و وجود تعداد بی‌شمار اتاق‌های گفت‌وگوی سکسی، هر کاربری را به داشتن اولین تجربه در این حوزه تحریک می‌کند. یک زن یا شوهر کنجکاو به راحتی و دور از دیدگان همسرش وارد این فضاها می‌شود و گفت وگوهای سکسی با دیگران را تجربه می‌کند چنین سهولتی است که بسیاری را به تجربه رفتارهای ناهنجاری جنسی نه در فضای فیزیکی، بلکه در فضای مجازی هدایت می‌کند. به ویژه اگر نظارت نهادهای مسئول در کشورها در این زمینه کم رنگ و ناتوان باشند.

بند دوم: آثار اجتماعی و فرهنگی

✓ تزلزل در ارکان خانواده

یکی از آثار جرایم مربوط به محتوا، همچون هرزه نگاری و ترویج مطالب مستهجن، تزلزل در روابط زناشویی است؛ چرا که از آثار هرزه نگاری اعتیاد جنسی است، که در جوامعی که اینترنت ارزان در اختیار افراد قرار دارد، شیوع بسیاری دارد. در این موارد زنان از همسران خود شکایت دارند که به ایشان بی توجهی کرده و بیش از آنکه از بودن در کانون خانواده و در کنار همسر لذت ببرند از صرف وقت در اینتنت و فضای مجازی و لذت‌های منحرف جنسی و غیر آن لذت می‌برند. بخشی از عوامل طلاق در این قبیل کشورها اعتیاد به اینترنت، به ویژه اعتیاد جنسی مجازی است. کسانی که به خاطر سودی کثیف رو به ترویج تجارت جنسی مجازی آورده‌اند و نهادهایی که بی تفاوت یا کم تفاوت از کنار این قبیل مسائل می‌گذرند،

خواسته یا ناخواسته یکی از مهم‌ترین گروه‌های اجتماعی؛ یعنی خانواده را رو به انحیاط و نابودی و یا حداقل ضعف می‌کشانند. دیگر، زن و شوهر از کنار یکدیگر بودن کمتر لذت می‌برند و بیشتر وقت خود را صرف لذت‌های رنگارنگ، اما پلید در فضای مجازی می‌کنند. در نتیجه محبت به عنوان رکن اصلی و اساسی خانواده روبه سستی می‌رود. فرزندانی که در این محیط بار می‌آیند، دچار انحراف اخلاقی شده و سلات روانی و روابط جنسی پاک از بین می‌رود. از این روست که نتیجه اباحه گری جنسی به افزایش پدیده‌هایی، مثل فرزندان تک والدینی، زنان و مردانی که تنها زندگی می‌کنند، بچه های نامشروع وغیره خواهد انجامید. بنابراین لزوم نظارت سخت گیرانه و دقیق در فضای مجازی از سوی نهادهای مسئول و والدین رخ می‌نماید. وظیفه نهادهای فرهنگی نیز در فرهنگ سازی در جهت بهره برداری صحیح از اینترنت بسیار مهم و تأثیرگذار است.

✓ کاهش امنیت و احساس آرامش، به ویژه در کاربران اینترنتی

یکی از آثار جرایمی؛ از قبیل دسترسی غیرمجاز، شنود و دریافت غیرمجاز، جعل داده ها، تخریب و ایجاد اختلال در داده‌ها، اختلال در سیستم، ممانعت از دستیابی، سرقت داده ها؛ کاهش امنیت شهروندان جامعه و به خطر افتادن حریم خصوصی ایشان است. شاید بعضی وقت‌ها در مجاورات خصوصی، چیزی را بگوییم که امید داشته باشیم که خوانندگان آن را به فراموشی بسپارند یا چیزی را بنویسیم که بعدها از آن پشیمان گشته و امیدوار باشیم که خوانندگان برگه‌های ما را در لابه لای دیگر برگه‌های متعدّد و متفرق بایگانی خویش گم کنند و دیگر به خواندن آنها مبادرت نورزند؛ ولی فناوری اطلاعات به همه این امکان را می‌دهد، که همه اطلاعات حال و گذشته را به گونه‌ای سامان مند بایگانی و ذخیره نموده و هر وقت که آن را لازم داشتند، فورا بیابند. از این جهت، اگر حریم‌خصوصی شما در زمان و مکانی خاص افشا گردد. امید نداشته باشید که کاربران رایانه‌ها آن را فراموش کنند، چرا که فناوری اطلاعات این امکان را سلب کرده است. اینکه شما چه چیزهایی خریده‌اید و از کجا آنها را تهیه کرده‌اید، پولش را از کجا آورده‌اید و چقدر به چه کسی اهدا کرده‌اید و از چه کسی چه انتظاراتی

دارید و با چه کسانی نامه پراکنی می‌کنید، همه و همه در دنیای رایانه‌ای، درون بلندگوهایی پخش می‌شود، که اوّلاً: امکان شنیدن آن برای همگان وجود دارد و ثانیاً: هرگز آوای مکرر و باقی آنها خاموش نمی‌شود و همواره با هرعملیات الکترونیکی شما، بر حجم آنها اضافه می‌شود. امروزه حریم خصوصی اشخاص در معرض خطراتی است، که قبل از فناوری اطلاعات هرگز وجود نداشت، همان طور که قبل از پیدایش فناوری الکتریسیته هیچ کس درمعرض خطر برق گرفتی نبود، حال باید مواظب بود که توسعه فناوری، حریم خصوصی افراد را به آتش نکشد. اینکه چه کسانی در قبال این خطرات پیش آمده مسئولیت دارند؟ و یا با چه تدابیری باید این احساس عدم امنیت را کاهش داد؟ سؤال‌هایی است که در این باره مطرح است. البته مقابله با جرایم رایانه‌ای و حفاظت دقیق از داده‌ها، هم از طریق دولت و هم از طریق سازمان های خدمت رسان و هم از طریق خود افراد، در کاهش این ناامنی بسیار مؤثر خواهد بود. در این مسر کارشناسان واگذاری IP و استفاده از پروکسی[1]، نصب دیوار آتشین، نصب ضد ویروس و ضد جاسوس اینترنت و کار فرهنگی را توصیه می‌کنند.

✓ کاهش علایق و ارزش های ملی نزد کاربر

یکی از ویژگی‌های اینترنت، جهانی بودن آن است، که با وجود فوایدی که دارد، اثرات مخربی نیز بر فرهنگ‌های ملی جوامع می‌گذارد؛ چرا که کاربران با استفاده از اینترنت ضمن این که با زبان انگلیسی حاکم بر آن درگیر هستند، از زبان ملی خود دور می‌شوند، به عنوان مثال در چت های اینترنتی، فارسی زبانان بیشتر از الفبای انگلیسی به جای الفبای فارسی استفاده می‌کنند (که یکی از دلایل آن کمبود نرم افزارهای قدرتمند فارسی است). گسترش این کاربرد خود موجب تضعیف الفبای فارسی خواهد شد.

[1] Proxy

✓ تغییر هنجارهای فرهنگی

با توجه به تفاوت هنجارها از جامعه‌ای نسبت به جامعه دیگر، امکانات الکترونیکی از جمله فضای مجازی تبادل و تأثر فرهنگی را رونق می‌دهد. در این بین فرهنگ‌های ضعیف یا صاحبان فرهنگ‌های قدرتمند، اما کم تلاش متأثر از فرهنگ مهاجم قرار خواهند گرفت. فرهنگ اسلامی نیز در این تبادل گرچه فرهنگی با پشتوانه است، اما در صورتی که مسلمین در شناخت و شناساندن آن نکوشند در برابر فرهنگ مهاجم غرب دچار التقاط و تغییر خواهند شد.

✓ ناامنی مالی و سرمایه گذاری

یکی از اساسی‌ترین باورهای مورد قبول اغلب جوامع، مالکیت بر اموال است. در فضای مجازی، با مطرح شدن مال الکترونیکی، که به شکل پول الکترونیکی، داده‌ها و اسناد با ارزش و غیره است، لزوم حفظ امنیت مالی و مراقبت از آن برعهده حکومت خواهد بود. از این رو یکی از آثار کلاهبرداری و سرقت الکترونیکی، ناامنی سرمایه گذاری درحوزه اموال الکترونیکی است.

✓ کم رنگ شدن ارزش های مترقی

هرجامعه، صاحب ارزش‌هایی است که ناشی از فرهنگ آن است، اما برخی ارزش‌های مترقی در جوامع اسلامی است، که در اثر تأثیر از فرهنگ بی بندبار غرب در حال کم رنگ شدن است. ارزش‌هایی مثل حیا و عفت زن، اهمیت داشتن شخصیت انسان نه جنسیت آن، قبح عریان نمایی بدن به ویژه شرمگاه وغیره که در نتیجه رواج استفاده از مطالب مستهجن و ملاک شدن بولالهوسی در روابط انسانی در حال کم رنگ شدن است. دین چابنر در مقاله‌ای، چنین پیامدهایی را ناشی از رواج اباحه گری جنسی و هرزه نگاری دانسته و می گوید: «مطالعات دقیق و گسترده‌ای در طول این سال ها در این باره صورت نگرفته است، در نتیجه رواج بوالهوسی است که بلوتوث و ارسال تصاویر مستهجن در میان جوامع اسلامی رشد می‌یابد، روابط آزاد

دختر و پسر ترویج می‌شود، کم پوشی و عریان پوشی در میهمانی‌ها و عروسی ها، به ویژه در میان جوانان گسترش می‌یابد.

بند سوم: آثار سیاسی (تزلزل در حاکمیت و اقتدار سیاسی)

بارزترین ویژگی اینترنت، انباشت اطلاعات متنوع در آن است و این ویژگی آن را به بزرگ‌ترین انبار اطلاعاتی جهان تبدیل کرده است، به نحوی که خوب و بد، حقّ و باطل به شیوه‌های رنگارنگ به ارائه خواسته‌ها و دانسته‌های خود می‌پردازند. از این رو این کاربران هستند که در برابر حجم وسیعی از اطلاعات سردرگم می‌مانند و باید انتخاب کنند. برخی بر این عقیده‌اند که این آزادی اطلاعات گامی است در طریق دموکراسی؛ چرا که کاربران دسترسی به همه نوع اطلاعات دارند و لذا می‌توانند از میان آنها، آنچه به نظرشان درست تر می‌نماید، برگزینند و دنباله بهترین اندیشه در زمینه‌های مختلف سیاسی، فرهنگی و غیره است. اما آیا کاربران در انتخاب اطلاعات آزادی کامل دارند؟ آیا اطلاعات همانگونه که هست در اختیار کاربران قرار می‌گیرد، اینها سؤالاتی است که تأمّل در آن، نظر طرفداران آزادی اطلاعات را متزلزل می‌کند. به عنوان نمونه وقتی یک کاربر بخواهد از طریق جستجوگرهای قدرتمندی، چون گوگل و یاهو به دنبال موضوعی، مثلاً درباره ایران (کلمه Iran را تایپ کند) بگردد، آیا این موتورهای جستجو صادقانه مهم ترین و دقیق ترین اطلاعات را در این باره ارائه می‌دهند؟ اما حقیقت جز این است، چرا که مطالعات نشان می‌دهد، فضای حاکم بر اینترنت و ساختار تشکیل دهنده آن، همه براساس اهداف و سیاست‌های گرداننده اصلی اینترنت؛ یعنی آمریکا و از طریق شرکت‌های محوری، طرح ریزی شده است.

به عنوان نمونه می‌توان به دو مورد اشاره کرد:

۱. وب سایت مشهور و موتوری جستجوی قدرتمند گوگل و بسیاری از موتورهای جستجوی مشهور اینترنت براساس برخی از سیاست های سانسوری که در فوق به آن اشاره شد، اقدام به ارائه اطلاعاتی از پیش تعیین شده براساس کلید واژه‌های کاربر می‌کنند که

معمولاً شمار زیادی از کاربران، این نتایج را که در ردیف‌های اول تا ۵۰ نتایج جستجو قرار دارد، مورد استفاده نهایی خود قرار داده و استنباط های نهایی و برداشت های کلّی خود را براساس این موارد، کسب و معرفی می‌کنند. به عنوان مثال کلید واژه هایی، مانند ایران، عراق، کره، هنگامی که در باکس جستجو تایپ شده و جستجو می‌شود، در بالاترین فهرست نتایج جستجو، صفحات وبی نشان داده می‌شود که به نوعی تعلّق مستقیم و یا غیرمستقیم آشکار به بخش های اطلاعاتی و امنیتی آمریکا دارد. مثلاً در مورد عراق، عراقی که از نگاه اسناد سازمان جاسوسی آمریکا و بخش‌های اطلاع رسانی دیگر داخل و خارج از آمریکا مورد بررسی و مطالعه قرار گرفته است، به کاربران جستجوگر کلید واژه عراق، معرفی می‌شود. سرچشمه اصلی این امر تلاش گسترده آمریکائیان مبنی بر تسلّط بلامنازع بر شاهراه جهانی اطلاع‌رسانی و ارائه تصویری از جهان براساس نگاه آمریکا و سیاست جهانی آن به هر شهرند دهکده جهانی است، که از طریق مکانی به نام اینترنت، جهان را زیرکاوش خود قرار می‌دهند.

۲. از دیگر مواردی که می‌توان از آن به عنوان نوعی از دیپلماسی انحصارطلبی آمریکا در اینترنت به شمار آورد و آن را زمینه ساز بستر شعار: «جهان یا اینترنت را از نگاه آمریکا بنگرید»، دانست، ایجاد پایگاه‌های خبری متعدد در اینترنت توسط سازمان‌هایی است که توسط ایالات متحده مورد حمایت معنوی و مادی قرار می‌گیرند تا حجم قابل توجهی از اطلاعات خبری و رسانه‌ای که در اینترنت منتشر و در اختیار اکثر کاربران شبکه در اقصی نقاط جهان قرار می‌گیرد، به گونه‌ای مرتبط با آنچه آن را می توان دیپلماسی انحصارطلبی رسانه‌ای آمریکا خواند قرارگیرد. به عنوان مثال، شبکه اینترنتی ورلدنیوز، که دارای بیش از پانصد سایت اینترنتی خبری و اطلاعاتی به بیش از ۱۰ زبان زنده دنیا می‌باشد و همواره اخبار منتشر شده توسط سایت‌های خبری مختلف این شبکه عظیم خبری در فهرست های بالایی نتایج جستجو قرار می‌گیرد، با روزآوری مرتب و مکرر خود و انتشار حجم قابل ملاحظه‌ای از اخبار و اطلاعات متنوع در اینترنت، تفسیر خبری و اطلاعاتی خاصی را به کاربران وب ارائه می‌کند که در ورای آن نوعی خط دهی مبتنی بر سایبر آمریکایی قرار دارد. نوعی نسخه پیچی

خودخواهانه و انحصارطلبی برای فضای اطلاعاتی شناور در اینترنت که روزانه مورد استفاده حجم عظیمی از شهروندان دهکده جهانی قرار می‌گیرد. به هر حال دیپلماسی نوین واشنگتن که بر محور اطلاعات، ارتباطات و تلاش برای مونوپول کردن این روند در رسانه‌ای اثرگذار و فراگیر بنام اینترنت، بنیانگذاری شده است، بیش از پیش یافتن راه‌های امنیتی مطمئن با ضریب اثرگذاری بیشتر و اثرپذیری مخرب کمتر را جستجو می‌کند که در نهایت، راه اندازی پلیس اینترنتی به مرکزیت آمریکا و به اختیار درآوردن رسانه وب را در سال‌های آینده هدف قرار داده است. امری که شدیداً مغایر با اصول فراگیری است، که اینترنت را شاهراهی برای تسریع ارتباطات و انتشار بهینه و غیرسانسوری اطلاعات توسط هر شخص و در هر مکان با رعایت حقوق مادی و معنوی مربوط تصور می‌کند. قطعاً هرکاربری که بداند برای وی برنامه‌های از پیش تعیین شده‌ای در رسانه سایبر تهیه شده و حقّ انتخاب و عمل بیشتر و بهتری را ندارد و همواره پلیسی مخفی و غیرتأیید شده توسط کشورهای حاضر در اینترنت، پست الکترونیک، وبلاگ، سایت اینترنتی و عملکردهای مختلف او را زیرنظر خواهد داشت، همواره دیسکانکت بودن را بر آنلاین بودن، ترجیح خواهد داد. همچنان‌که می‌دانیم، اطلاعات در تصمیم گیری-های سیاسی مردم بزگ ترین نقش را دارند، لذا اطلاعات انبوه در انباری به نام اینترنت می تواند نقش پررنگی در هدایت افکار عمومی و گزینش‌های سیاسی کاربران داشته باشد. در این شرایط نحوه ارائه اطلاعات در انتخابات یک کشور بسیار تاثیرگذار خواهد بود و خواهد توانست در نحوه چینش مهره‌های هیئت حاکمه کشورها مؤثر باشد. از این رو اینترنت می‌تواند تهدیدی علیه حاکمیّت کشورها باشد و با ارائه اطلاعات هدفمند و همسو با رسانه‌های آمریکایی هرصدای مخالف دیدگاه‌های آمریکا را منزوی و کم اثر کند. در نتیجه با کار هماهنگ رسانه‌ای، انتخابات کشورها را به جهتی که آمریکا و همدستانش می‌خواهند، سوق دهد. بدین سبب است که عمده کرده و برای مقابله با این روند تدابیری، چون فیلتر و مسدود کردن سایت‌هایی که در جهت تزلزل حاکمیت ایشان اطلاعات ارائه می‌کنند، اتخاذ می‌نمایند.

به همین ترتیب تقریباً در تمام کشورهای عربی حاشیه خلیج فارس، کنترل قوی دولتی بر محتوا و توزیع اطلاعات وجود دارد. این کنترل‌ها به علل مذهبی، سیاسی و فشارهای داخلی صورت می‌گیرد. روش اصلی کنترل اطلاعات الکترونیک در این کشورها انحصار مخابرات در شرکت‌های دولت است. اسرائیل نیز در میان کشورهای خاورمیانه تلاش بسیاری در جهت دستیابی به امنیت کرد، تا آنجا که با صرف هزینه کلانی به تولید Checkpoint با پیشنیه و ریشه در کاربردهای نظامی - بعنوان یکی از قابل اطمینان ترین و پرفروش‌ترین فایروال‌های جهان که کشورهای عربی نیز به آن متکی هستند، در جهت سیاست‌های اینترنتی خود اقدام کرد

بخش چهارم: تشدید مجازات ماموران دولتی در این جرایم

در برخی جرایم مثل کلاهبرداری یا جعل مجازات ماموران دولتی تشدید می‌شود در جرایم رایانه‌ای نیز همینطور است و چنانچه مأموران دولتی که مسئول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سامانه‌های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آنها قرار گرفته است بر اثر بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سامانه‌های مذکور شوند مجازات شدیدتری خواهند داشت. بر اساس ماده ۵ قانون جرایم رایانه‌ای این اشخاص به مجازات زیر محکوم می‌شوند: حبس از ۹۱ روز تا ۲ سال یا جزای نقدی از پنج میلیون (۵.۰۰۰.۰۰۰) ریال تا چهل میلیون (۴۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات. بعلاوه این اشخاص به انفصال از خدمت از شش ماه تا دو سال نیز محکوم خواهندشد.

نتیجه گیری

جرایم رایانه‌ای یکی از پدیده‌های نوظهوری است که گرچه برخی از جرایم آن شباهت‌هایی با جرایم سنتی دارد، اما تفاوت‌هایی در روش و ماهیت و نوع جرم دارد که از لحاظ جرم‌شناسی و کیفرشناسی و حقوق کیفری پژوهش‌های نوی را می‌طلبد. جرایم‌رایانه‌ای به دلیل تأثیرات

ناگواری که بر جامعه اطلاعاتی و کاربران دارد، برخورد جدی‌تری را از سوی دولت مردان سیاسی و قضایی می‌طلبد. نظارت و فیلترکردن دقیق تر و جدی‌تری، چه برای جلوگیری از آسیب امنیتی و چه آسیب‌های فرهنگی را می‌طلبد. امروزه با افزایش استفاده از اینترنت، از آن برای انواع مختلفی از جرائم از جمله، سرقت اطلاعات شخصی، سرقت پول از حساب های بانکی کاربران، گسترش پرونوگرافی و غیره، استفاده می شود. تقریبا هر شخصی که از اینترنت برای منافع شخصی خود استفادهمی کند، می تواند قربانی جرائم اینترنتی باشد. کلاهبرداری های اینترنتی بسیار فریبنده بوده و سبب می شوند تا ما نتوانیم جلوی خود را گرفته و با کلیک کردن روی لینک های مشکوک، به یکی از قربانیان جرائم اینترنتی تبدیل می شویم. امروزه، ما از اینترنت برای مقاصدی چون ارتباطات ایمیلی (از طریق جیمیل، یاهو و...) بانکداری آنلاین، خرید آنلاین، شبکه های اجتماعی، چت، تماشای فیلم و... استفاده می کنیم. دستیابی به هر کدام از این اهداف ممکن است ما را قربانی جرائم اینترنتی کند؛ بنابراین باید با دقتی فوق العاده از اینترنت استفاده کنیم. حقوق ایران در زمینه جرایم رایانه‌ای گرچه تلاش های مفیدی داشته، ولی همچنان نیاز به کار و پژوهش در زمینه ابعاد مختلف آن دارد. ضمن اینکه در عرصه قانونگذاری کاستی‌هایی نیز وجود دارد که امید است با تصویب قانون مجازات جرایم رایانه‌ای که سال‌هاست در فراموشخانه مجلس مورد بی مهری است، گامی در این راه برداشته شود متخصصان معتقدند جرم جاسوسی رایانه‌ای، با شدت و پیچیدگی بیشتری در سطح وسیع جهانی ادامه پیدا خواهد کرد. رفته رفته جاسوسی اینترنتی به عنوان ابزاری برای حصول برتری در رقابت بی‌پایان کشورها در زمینه‌های صنعتی، اقتصادی، نظامی وغیره تبدیل خواهد شد وکشورهای بیشتری وارد صحنه بازارکار رایانه‌ای می‌شوند. این جنگی است که در آن نیازی به استفاده از پیاده نظام، هواپیما جنگنده و موشک نیست. کلید موفقیت در این جنگ اطلاعات است، عوامل جاسوسی رایانه‌ای و اینترنتی نقش پیاده نظام این جنگ پسامدرن را بازی می کنند.

در حال حاضر با عنایت بـه پیشـرفت‌های لحظـه‌ای در عرصـه رایانـه و فضـای سـایبر ضـرورت آموزش بیش از پیش مشخص شده و برای اجرای یک سیاست کیفری مـؤثر جهـت پیشـگیری از جرایم رایانه‌ای به‌خصـوص جاسوسـی رایانـه‌ای و اینترنتـی، ایـن آموزش‌هـا بایـد در مقـاطع مختلف زمانی تکرار و روزآمد شوند.

منابع و مآخذ

الف) منابع فارسی

۱) باستانی، برومند. جرائم کامپیوتری و اینترنتی جلو های نوین از بزهکاری، ۱۳۹۰. تهران: انتشارات بهنامی

۲) باقری اصل، رضا، «کنوانسیون جرایم سایبر و گزارش توجیهی آن» ، گروه ارتباطات و فناوری های نوین، گروه کارشناسان، کمیسیون حقوقی و قضایی مجلس، شماره ۷۶۴۶، ۱۳۸۴، ص .

۳) پروتکل الحاقی به کنوانسیون جرایم سایبری در خصوص جرمانگاری اعمال نژادپرستی و موضوعات بیگانه ستیزی ارتکاب یافته از طریق رایانه. . ETS شماره ۱۸۹.

۴) توصیه نامه ی شماره ۸۹، صادر شده توسط کمیته ی وزیران در ۱۳ سپتامبر ۱۹۸۹ در چهارصد و بیست و هشتمین نشست وزرا؛ با موضوع جرایم مرتبط با رایانه.

۵) حسینی خواه، نورالله، ۱۳۹۰، پلیس و جرایم رایانه ای، تهران :انتشارات معاونت تربیت و آموزش ناجا.

۶) خداقلی، زهرا، جرایم کامپیوتری، ۱۳۸۳، چاپ اول، انتشارات آریان، ص ۳۸.

۷) زندی، محمدرضا، تحقیقات مقدماتی در جرایم سایبری، انتشارات جنگل، ۱۳۸۹.

۸) سالاری شهر بابکی، میرزا مهدی، کلاهبرداری و ارکان متشکله ان، ۱۳۹۳، تهران: میزان.

۹) صابری، سیاوش و انصاری دوست، شیما، جرائم رایانه ای در حقوق ایران. مطالعات علوم سیاسی، حقوق و فقه. ۳ (۱): ۱۳۹۶. ص ۱۴۱-۱۴۹.

ب) منابع لاتین

۱) Marshall, H., Jarret & Bailie, W. (۲۰۰۷). michael, Prosecuting of cyber crime, published by legal education executive office for united states Attorneys, second edition, Department of justice,Washington D.C.

۲) Twels, Joseph (۲۰۰۹). computer fraud,published by john willey and son, new jersey.