به نام خدا

عنوان :

جرم شناسی سایبر

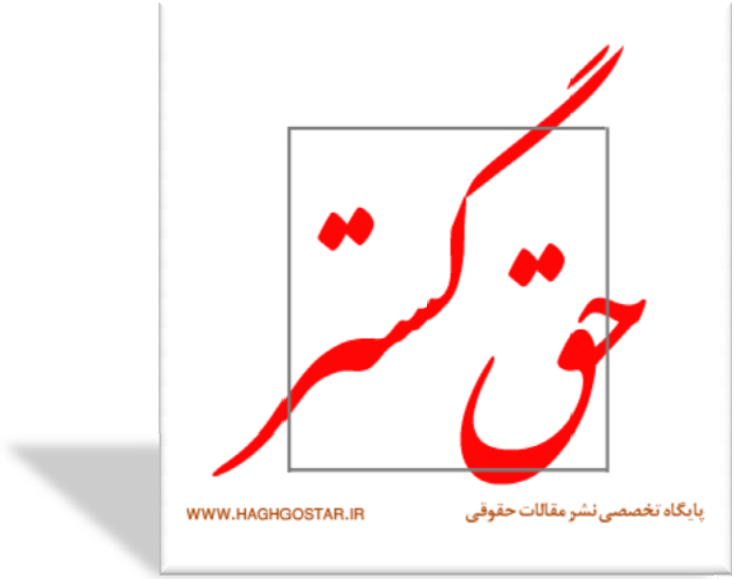
نویسنده :

عبدالرضا طرزی

کارشناس ارشد حقوق و قاضی ویژه جرایم سایبری

ناشر :

پایگاه نشر مقالات حقوقی،حق گستر



الف - تعریف جرم شناسی سایبری (cyber criminology):

با الهام از تعاریف ارائه شده از جرم شناسی سایبری و تطبیق آن با تعاریفی که تاکنون از جرم شناسی ارائه شده است می توان گفت: (جرم شناسی سایبری مطالعه عوامل ایجاد جرم در فضای مجازی و تأثیرات آن بر دنیای حقیقی و راهکارهای پیشگیری از حدوث اینگونه جرایم می باشد).

مطالعات عینی پرونده های جرایم سایبری نشان می دهد ایجاد شخصیت مجازی با ذهنیت عدم شناسائی و البته سهولت و گستردگی ارتکاب برخی بزه ها در فضای مجازی بستر مناسبی را برای بروز خلأهای

شخصیتی و روانی فراهم می سازد لذا ما بر این باور هستیم که شخصیت واقعی یک بزهکار سایبری را باید در همان شخصیت مجازی وی جستجو کرد به دیگر سخن شخصیت مجازی که بزهکار سایبری از خود ساخته است در واقع همان (خود واقعی) اوست که به دلایل مختلف امکان بروز آن در دنیای حقیقی را نداشته است پس بنا به قول پروفسور گاستون استفانی فرانسوی (شناخت شخصیت بزهکار) امر مهمی در مطالعات جرم شناسی سایبری است.

ب - شخصیت شناسی بزهکاران سایبری:

واکاوی شخصیت این دست از بزهکاران نشان می دهد که آنان به نوعی فاقد قدرت انتزاعی بوده و قادر به تصور و تجسم عاقبت رفتار خود نمی باشند تا با مدد آن خودکنترلی در جلوگیری از ارتکاب جرم در فضای مجازی داشته باشند اینگونه افراد به نوعی تحت تأثیر حال میباشند و رفتارهای خود را بدون هرگونه محاسبه و اندیشه عمیق انجام می دهند بعنوان مثال در پرونده ای بزهکار سایبری صرفا بخاطر عصبانیت ضمن غیرفعال نمودن دیتابیس سایت دانشگاه اقدام به ایجاد اختلال در سامانه رایانه ای نموده و ساعتها هزاران دانشجو را جهت ثبت نام و انتخاب واحدهای درسی با مشکل موجه ساخت و در توضیح عمل خود (عصبانیت آنی و عدم توجه به آنچه که پیش خواهد آمد) را علت رفتار مجرمانه خود بیان داشت و یا در پرونده دیگری بزهکار سایبری به هنگام برنامه نویسی با قطعی موقتی سرویس اینترنتی مواجه شده و بر اثر عصبایت آنی مبادرت به هک بالغ بر ۱۰ هزار اکانت کاربران آی اس پی مربوطه نمود. بزهکاران سایبری علی رغم توان فنی و هوش بالائی که دارند افرادی ناتوان بوده و با پناه بردن به (غار فضای مجازی) سعی در جبران کاستی ها دارند لکن در این التجاء نیز ناتوانند و در اندک زمانی از پناهگاه ساختگی خود خارج شده و به اصطلاح دست خود را رو می کنند. شاید به مدد همین امر است که نهادهای تعقیب کننده جرایم سایبری علی رغم پیچیدگی دنیای مجازی در بازه زمانی کوتاهی قادر به شناسائی بزهکاران سایبری میباشند.

ج - نگاهی گذرا به برخی جرایم سایبری :

عناوین جرایم سایبری بر اساس قانون جرایم رایانه ای جمهوری اسلامی ایران مصوب سال ۱۳۸۸ به شرح زیر است:

۱- دسترسی غیرمجاز به داده های رایانه ای یا مخابراتی

۲- شنود غیرمجاز محتوای در حال انتقال در سیستمهای رایانه ای یا مخابراتی

۳- دسترسی غیرمجازبه داده های سری در حال انتقال در سیستمهای رایانه ای یا مخابراتی یا حامل های داده یا تحصیل و شنود آن

۴- در دسترس قرار دادن داده‌های سری در حال انتقال در سیستمهای رایانه ای یا مخابراتی یا حامل های داده برای اشخاص فاقد صلاحیت

۵- افشا یا در دسترس قرار دادن داده های سری در حال انتقال در سیستمهای رایانه ای یا مخابراتی یا حامل های داده برای دولت، سازمان، شرکت یا گروه بیگانه

۶- نقض تدابیر امنیتی سیستمهای رایانه ای یا مخابراتی به قصد دسترسی به داده های سری در حال انتقال در سیستمهای رایانه ای یا مخابراتی یا حامل های داده

۷- تغییر غیرمجاز داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانهٔ آنها

۸- تغییر داده‌ها یا علایم موجود در کارت‌های حافظه یا قابل پردازش در سیستم‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانهٔ داده‌ها یا علایم به آنها

۹- حذف یا تخریب یا مختل یا غیرقابل پردازش نمودن داده های دیگری از سیستم های رایانه ای یا مخابراتی یا حاملهای داده بطور غیرمجاز

۱۰- از کار انداختن یا مختل نمودن سیستمهای رایانه ای یا مخابراتی بطور غیرمجاز

۱۱- ممانعت از دسترسی اشخاص مجاز به داده های یا سیستمهای رایانه ای یا مخابراتی بطور غیرمجاز

۱۲- ربودن داده های متعلق به دیگری بطور غیرمجاز

۱۳- تحصیل مال از طریق سامانه رایانه ای یا مخابراتی بطور غیرمجاز

۱۴- انتشار آثار مبتذل و مستهجن از طریق سامانه رایانه ای یا مخابراتی یا حامل های داده

۱۵- تسهیل دسترسی افراد به محتوای مبتذل و مستهجن از طریق سامانه رایانه ای یا مخابراتی یا حاملهای داده

۱۶- هتک حیثیت از طریق انتشار صوت و فیلم تحریف شده دیگری بوسیله سیستمهای رایانه ای یا مخابراتی

۱۷- نشر اکاذیب از طریق سیستم های رایانه ای یا مخابراتی به قصد اضرار به غیر یا تشویش اذهان عمومی

۱۸- ممانعت از پالایش محتوای مجرمانه از سوی ارائه دهندگان خدمات دسترسی

۱۹- استفاده غیرمجاز از پهنای باند بین الملل مبتنی بر پروتکل اینترنتی به منظور برقراری ارتباطات مخابراتی

۲۰- تولید یا انتشار یا توزیع یا معامله داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرائم رایانه‌ای به کار می‌روند.

۲۱- فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده‌ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند.

۲۲- آموزش نحوهٔ ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی.

د- علت شناسی جرایم سایبری (cyber criminal etiology):

علل و عوامل بسیاری در شکل گیری جرایم سایبری موثرند همچون عوامل اقتصادی. فرهنگی. سیاسی. مشکلات روحی و روانی نظیر: افسردگی.عصبانیت.حسادت.انتقامجوئی.حس تنفر.تفریح و سرگرمی.خودکم بینی و حقارت.حس رقابت و... در ادامه به برخی از این عوامل اشاره می شود.

۱- اقتصادی:

جرایمی نظیر (تحصیل مال بطور غیرمجاز از طریق سامانه رایانه ای) یا همان کلاهبرداری نمونه ای از این دست جرایم میباشد که عمدتا با اهداف اقتصادی بوقوع می پیوندد بعنوان مثال برخی بزهکاران سایبری از طریق فیشینگ به اطلاعات حسابهای بانکی کاربران دسترسی یافته و با وارد نمودن گذرواژه ها و دیگر اطلاعات در سامانه های مربوطه مبادرت به برداشت وجوه از حساب بانکی افراد می کنند.

گفتنی است در موارد بسیاری ارتکاب جرایم رایانه ای که به حسب ظاهر اقتصادی نیست با انگیزه های اقتصادی شکل می گیرد و بالعکس برخی جرایم سایبری به ظاهر اقتصادی با انگیزه های غیراقتصادی ارتکاب می یابد بعنوان مثال در پرونده ای فرد پس از نفوذ به سیستم رایانه ای قربانی خود و تحصیل اسناد و مدارک شخصی وی اقدام به اخاذی از وی نمود و بالعکس در پرونده ای دیگر متهم صرفا با هدف ابراز توانائی خود در هک مبادرت به نفوذ به حساب بانکی یکی از مشتریان بانک نموده و مبلغی را برداشت و آنرا عینا به بانک مسترد نموده تا فقدان امنیت شبکه بانکی و توانائی بالای خود در این زمینه را به رخ بکشد جالب آنکه در بیان علت رفتار مجرمانه خود اعلام نمود از آنجا که جویای شغل بودم خواستم توانایی خودم را به دیگران نشان بدهم بلکه زمینه اشتغال برایم فراهم شود!!

۲- فرهنگی:

فقر فرهنگی و عدم پایبندی به ارزشهای جامعه و باورهای دینی یکی از عوامل مهم ارتکاب برخی بزه ها در محیط سایبر میباشد.پیش از این نیز اشاره شد که با خلق دنیای مجازی موانع بسیاری از بین رفته و ارتکاب جرایم تسهیل گردیده است. فضای سایبر شرایطی را به وجود آورده که بزهکاران می توانند در مکان هایی غیر از جاهایی که آثار و نتایج اعمال آن ها ظاهر می شود مرتکب جرم شده و به راحتی و با کمترین هزینه و اضطراب، بیشترین خسارات و صدمات را به بار آورده و در عین حال ناشناخته باقی بمانند. ارتکاب جرائمی نظیر انتشار آثار مبتذل و مستهجن از طریق سامانه رایانه ای یا مخابراتی یا حامل های داده و یا تسهیل دسترسی افراد به محتوای مبتذل و مستهجن نمونه ای از جرایم سایبری است که عدم توجه به اصول اخلاقی و ارزشهای جامعه موجد آن است. ایجاد سایتهای غیراخلاقی و ترویج بی بند و باریهای جنسی و روابط ناسالم دختران و پسران در قالب سایتهای دوستیابی. سایتهای پخش فیلمهای غیراخلاقی بصورت آنلاین و ... از مصادیق این جرایم میباشند.

۳- مشکلات روحی و روانی:

بخش عمده ای از جرایم رایانه ای ارتکاب یافته در کشور عزیزمان برخواسته از مشکلات روحی و روانی بزهکاران فضای مجازی میباشد. مردی صرفا به جهت اختلاف با همسرش و با قصد انتقام گیری از وی اقدام به انتشار عکسها و فیلمهای خصوصی همسر خود در سایتهای اینترنتی نمود. خانمی صرفا با هدف انتقامگیری از همسرش که مبادرت به ازدواج مجدد نموده است اقدام به انتشار عکسهای بدون حجاب خود در سایتهای اینترنتی نمود در پرونده دیگری مردی از روی حسادت اقدام به نصب نرم افزار شنود بر سیستم رایانه ای خانمی نموده و سپس متن چتهای خصوصی وی را دریافت و برای سایرین ارسال می نمود. در پرونده های متعدد دیگر افراد با ایجاد صفحات جعلی در سایتهای اجتماعی اقدام به آبروریزی و هتاکی به قربانیان خود می نمایند...

مصادیق این بخش از علل ارتکاب جرایم سایبری بسیار گسترده تر از سایر علل و عوامل میباشد که مطالعات جرمشناسی در این حیطه را می طلبد.

ه - بزه دیدگان جرایم سایبری:

قربانیان جرایم سایبری در واقع قربانیان پیشرفت تکنولژی (victimation as aby prodact of science and technology) هستند اما نکته قابل توجه در این بین آن است که بسیاری از بزه دیدگان جرایم سایبری استعدادی قابل توجه برای قربانی شدن (victimation) بروز می دهند و براحتی طعمه بزهکاران سایبری میشوند برخی کلاهبرداریهای اینترنتی ناشی از کسب اطلاعات به روشهای بسیار ساده و سوء استفاده از عکسها و اسرار شخصی نمونه هایی از این موضوع می باشد ما بر این باوریم که قربانی جرم سایبری همیشه بی گناه نیست و چه بسا خودش ناخواسته آغازگر بزه سایبری میباشد.

ضعف شخصیتی.فقدان اطلاعات کافی در رابطه با محیط مجازی و عدم دقت در محافظت از داده ها و ... مواردی است که قربانی بزه سایبری را در قربانی شدنش مساعدت می کند.

و – جرم شناسی پیشگیرانه در فضای سایبر:

در خاتمه این بحث باید گفت خسارات وارده در اثر جرایم سایبری به مراتب گسترده تر و جبران ناپذیرتر در مقایسه با جرایم سنتی میباشد مطالعه عینی جرایم سایبری گواه این واقعیت است که در بسیاری موارد انواع خسارات مادی و معنوی و روانی (psychological - material – moral) برای قربانی به ارمغان آورده می شود از سوی دیگر ماهیت خاص فضای مجازی این اقتضاء را دارد که به طور جدی به دنبال پیشگیری قبل از ارتکاب بزه (preventiol cyber) در فضای مجازی باشیم. ارتقاء سطح اطلاعات جامعه نسبت به فضای مجازی و اطلاع رسانی در زمینه جرایم سایبری و راههای مقابله با آن.ارتقاء سطح باورهای دینی و اخلاقی خصوصا در بین نوجوانان و جوانان نمونه هایی از پیشگیری از شکل گیری جرایم در فضای مجازی است.