فصل‌نامه دیدگاه‌های حقوقی، دانشکده علوم قضایی و خدمات اداری
شماره چهل‌ودوم و چهل‌وسوم ۱۳۸۶، صص ۱۲۶-۱۰۹

راهکارهای مقابله با جرم کلاهبرداری رایانه‌ای در حقوق کیفری ایران

۱- دکتر حسین میرمحمدصادقی[۱]
۲- محمدرسول شایگان[۲]

چکیده

با توجه به رشد سریع تکنولوژی رایانه‌ای و تحول عصر اطلاعات و گسترش ارتباطات شبکه‌ای و در عین حال سهولت ارتکاب جرایم مرتبط با فناوری‌های نوین، بحث روز آمد شدن و لزوم تدوین قوانین بسیار ضروری است. کلاهبرداری رایانه‌ای از قدیمی‌ترین اشکال جرایم رایانه‌ای با ابعاد مالی است. هرچند تدابیر کلی در مقابله با انواع روش‌های کلاهبرداری تقریبا مشابه است اما با تفاوت‌های موجود در شیوه‌های گوناگون کلاهبرداری بهره‌گیری از روش‌های مقابله متناسب ضرورت می‌یابد. بخشی از شیوه‌های مقابله نیازمند ایجاد فرهنگ بهره‌گیری از رایانه و آگاه ساختن افراد و سازمان‌ها در مورد مخاطرات سیستم‌های رایانه‌ای است. همچنین نظارت دائمی سازمان‌ها بر روی سیستم‌های رایانه‌ای و تدابیر امنیتی از قبیل حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و حفاظت اطلاعات در مقابله با کلاهبرداری رایانه‌ای از اهمیت ویژه‌ای برخوردار است. دیگر اینکه صرف جرم‌انگاری یک رفتار برای مقابله با آن کافی نیست بلکه اعمال ضمانت اجرای مقرر در مورد مرتکب جرم نیز ضرورت دارد و آن مستلزم کشف جرم و تعقیب و دستگیری مرتکب می‌باشد اما با توجه به اینکه ارتکاب جرایم رایانه‌ای مستلزم حضور مرتکب در محل وقوع نتیجه جرم نیست و همچنین با توجه به جنبه فرامرزی جرایم رایانه‌ای و محدود بودن اختیارات مراجع قانونی در حوزه مرزهای جغرافیایی در این راستا بر لزوم همکاری‌های بین‌المللی در زمینه کشف، تعقیب و استرداد مجرمان تاکید می‌گردد.

واژگان کلیدی:

فضای سایبر، کلاهبرداری رایانه‌ای، تدابیر حفاظتی، مقابله کیفری، همکاری‌های بین‌المللی

۱- دانشیار دانشکده حقوق دانشگاه شهید بهشتی.
۲- دانشجوی کارشناسی ارشد حقوق کیفری و جرم‌شناسی دانشکده علوم قضایی و خدمات اداری، شماره تماس: ۰۹۱۸-۸۳۷۶۲۶۸.
Mr_shaiegan@yahoo.com

مقدمه

به موازات گسترش فناوری‌های نوین اطلاعات و ارتباطات، بشر شاهد ظهور نسل جدیدی از جرایم می‌باشد که شناخت آن، مستلزم مطالعات جرم‌شناختی جدیدی است. با توسعه روابط افراد در فضای سایبر[1] (مجازی) اغلب کشورها به منظور قاعده‌مند کردن روابط و اقدامات افراد در محیط مجازی به تدوین قوانینی در این زمینه مبادرت نموده‌اند. قانونگذار ایران نیز از قافله عقب نمانده و در این رابطه قوانینی را وضع نموده است که در ادامه به آنها اشاره خواهیم کرد.

اگرچه نمی‌توان هیچ جامعه‌ای را بدون جرم تصور نمود. در مقابل، انسان نیز هیچ‌گاه نسبت به وقوع جرم بی‌تفاوت نبوده و در راستای مبارزه با آن در تلاش است. با این حال جهت مقابله با ارتکاب جرم در محیط مجازی نیازمند تدابیر و راهکارهای نوینی هستیم. لذا هدف این نوشتار این است که در جهت مقابله با جرم کلاهبرداری رایانه‌ای که یکی از مصادیق جرایم مالی[2] رایانه‌ای محسوب می‌شود تدابیر و راهکارهای لازم را ارائه نماید. بنابراین پس از تبیین سابقه تاریخی و مفهوم جرم کلاهبرداری رایانه‌ای راهکارهای مقابله با این جرم ذیل دو عنوان پیشگیری غیر کیفری (که خود شامل پیشگیری اجتماعی و وضعی می‌باشد) و پیشگیری کیفری مورد بررسی قرار خواهد گرفت. آنچه در پیشگیری اجتماعی مورد تاکید است خنثی‌سازی انگیزه ارتکاب جرم در مرتکب جرم می‌باشد و در بحث پیشگیری وضعی که محیط ارتکاب جرم را مورد توجه قرار می‌دهد. راهکارهای مقابله با جرم کلاهبرداری رایانه‌ای از قبیل تدابیر حفاظت فیزیکی، حفاظت کارکنان، حفاظت اطلاعات و حفاظت ارتباطات که در واقع سلب فرصت و ابزار ارتکاب جرم از دسترس مجرمان بالقوه را در پی‌خواهد داشت مورد اشاره قرار گرفته است. در نهایت ذیل عنوان پیشگیری کیفری الزامات قانونگذار به جرم انگاری رفتارهای قابل ارتکاب در محیط‌های رایانه‌ای و همچنین اعمال کیفر بر مرتکب جرم و چالش‌هایی که پلیس و دستگاه قضایی در کشف جرم، تعقیب و دستگیری مجرمان با آن روبرو هستند مورد بحث قرار خواهد گرفت. با این توضیح که با توجه به اینکه مجرمین فضای سایبر با دسترسی به ابزارهای مشابه و به شیوه‌های یکسانی به اهداف متنوع جنایی خود دست می‌یابند اتخاذ تدابیر مورد اشاره تقریبا در پیشگیری سایر مصادیق جرایم ارتکابی در فضای سایبر نیز صادق است.

1 -Cyber space
2 - Financial Crimes

۱- تبیین پیشینه و مفهوم جرم کلاهبرداری رایانه‌ای

در این قسمت پس از ذکر سابقه تاریخی جرم کلاهبرداری رایانه‌ای به اختصار مفهوم این جرم از لحاظ حقوقی و تطبیق آن با جرم کلاهبرداری سنتی مورد بررسی قرار خواهد گرفت.

۱-۱- تبیین سابقه تاریخی جرم کلاهبرداری رایانه‌ای

از لحاظ سابقه تاریخی، می‌توان قضیه الدون رویس در دهه ۱۹۶۰ را تاریخ قطعی اولین سوء استفاده‌های مالی دانست. رویس حسابدار یک شرکت در آمریکا بود وی به علت اختلافش با شرکت، با گنجاندن دستورالعمل‌های اضافی در برنامه‌های سیستم‌های رایانه‌ای شرکت، در قیمت کالاها تغییراتی را ایجاد نموده و مبالغ به‌دست آمده را به حساب‌های مخصوصی واریز می‌کرد. او توانست در مدت شش سال بیش از یک میلیون دلار برداشت کند اما چون نتوانست عملکرد سیستم را متوقف کند در نهایت خود را به مراجع قضایی معرفی و به ده سال حبس محکوم شد (دزیانی، ۱۳۸۳ : ص۳۹). این قضیه در ابتدا از حیث ساختار توصیفی متنازع فیه بود چون با پدیده جرم کلاهبرداری رایانه‌ای به مفهوم دهه نود آشنایی دقیقی وجود نداشت لذا هر یک از افراد نامی بدان نهادند. در نهایت با تعریف کلاهبرداری رایانه‌ای امروزه این قضیه را جرم کلاهبرداری رایانه‌ای توصیف می‌کنند (دزیانی، ۱۳۷۵: ص۵۳) در مورد ارتکاب اولین جرم کلاهبرداری رایانه‌ای در ایران اظهار نظر دقیقی نشده است با این حال از لحاظ سابقه قانون‌گذاری به‌طور کلی می‌توان گفت با الحاق تبصره۳ به ماده ۱ قانون مطبوعات در تاریخ ۷۹/۱/۳۰ با این مضمون که «کلیه نشریات الکترونیکی مشمول مواد این قانون است»، اولین واکنش قانونی نسبت به جرایم رایانه‌ای بروز پیدا کرد. تصویب قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای در تاریخ ۷۹/۱۰/۴ اقدام دیگر قانون‌گذار در قبال جرایم تجارت الکترونیکی بود. واکنش بعدی قانون‌گذار تصویب «قانون جرایم نیروهای مسلح» در تاریخ ۸۲/۱۰/۹ بود که در ماده ۱۳۱ سوء استفاده‌های مالی نظامیان با استفاده از رایانه (کلاهبرداری و اختلاس) را جرم‌انگاری نمود. تصویب قانون تجارت الکترونیکی در تاریخ ۸۲/۱۰/۱۷ واکنش قانونی دیگر نسبت به جرایم تجارت الکترونیکی بود که به تنظیم روابط تجاری در فضای مجازی پرداخته است.

در نهایت قانون‌گذار با تصویب قانون جرایم رایانه‌ای در پنجم خرداد ماه ۱۳۸۸ که به جرم‌انگاری رفتارهای قابل ارتکاب در فضای سایبر اختصاص یافته، در فصل سوم تحت‌عنوان سرقت و کلاهبرداری مرتبط با رایانه، به جرم‌انگاری کلاهبرداری رایانه‌ای مبادرت نموده است.

۱-۲- تبیین مفهوم جرم کلاهبرداری رایانه‌ای

در حقوق کیفری ایران پیش از تصویب قوانین مربوط به جرم انگاری رفتارهای قابل ارتکاب در محیط‌های رایانه‌ای که وصف آن گذشت کلاهبرداری یک جرم شناخته شده در ماده یک قانون تشدید مجازات مرتکبین ارتشاء، اختلاس و کلاهبرداری مصوب ۱۳۶۷ بود. در قانون مذکور از کلاهبرداری تعریفی ارائه نشده و تنها به ذکر مصادیقی از جرم اکتفا شده است که عبارتند از: ۱- مغرور کردن اشخاص به وجود شرکت، تجارت خانه، موسسات موهوم یا داشتن اختیارات موهوم ۲- امیدوار کردن افراد به امور غیر واقع یا ترساندن از امور غیر واقع ۳- اختیار کردن اسم، عنوان یا سمت مجعول. با این حال کلاهبرداری تعریف شده است به «بردن مال دیگری از طریق توسل توأم با سوءنیت به وسایل یا عملیات متقلبانه» (میرمحمدصادقی، ۱۳۸۵: ص ۵۱) بنابراین از لحاظ رکن مادی با توجه به مصادیق مذکور که تمثیلی نیز می‌باشند کلاهبرداری تنها به صورت فعل مثبت مادی واقع می‌شود و این جرم با ترک فعل محقق نمی‌شود. دیگر اینکه مرتکب باید با توسل به وسایل متقلبانه و اغفال بزه دیده موفق به بردن مال شود لذا کلاهبرداری از جرایم مقید است که وقوع نتیجه در ارتکاب جرم شرط است. از لحاظ رکن روانی، کلاهبرداری یک جرم عمدی است که بایستی علاوه بر احراز سوء نیت عام یعنی علم به تعلق مال به غیر و تقلبی بودن وسیله ارتکاب جرم، سوء نیت خاص یعنی قصد حصول نتیجه مجرمانه (بردن مال غیر) نیز احراز گردد.

در مورد کلاهبرداری رایانه‌ای همانطور که قبلا متذکر شدیم با تصویب قانون تجارت الکترونیکی در ماده ۶۷ [۱]، کلاهبرداری رایانه‌ای در بستر مبادلات الکترونیکی جرم‌انگاری شد. همچنین در قانون جرایم رایانه‌ای ذیل فصل سوم تحت عنوان سرقت و کلاهبرداری مرتبط با رایانه در ماده ۱۳ مقرر شده است: «هرکس به‌طور غیر مجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یاد دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰۰۰۰۰۰۰) ریال تا یکصد میلیون (۱۰۰۰۰۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.» لازم به ذکر است با توجه به سکوت قانونگذار، در مقام جمع بین دو ماده مذکور می‌توان گفت

۱-ماده ۶۷ قانون تجارت الکترونیکی: «هرکس در بستر مبادلات الکترونیکی، با سوءاستفاده و یا استفاده غیر مجاز از «داده پیام»ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف «داده پیام»، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تا ۳ سال و پرداخت جزای نقدی معادل مال مأخوذه محکوم می‌شود».

هیچ یک ناسخ دیگری نیست زیرا ماده ۶۷ مذکور خاص ارتکاب جرم در بستر مبادلات الکترونیکی است و از طریق مداخله در عملکرد برنامه یا سیستم رایانه‌ای با فریفتن دیگران یا گمراهی سیستم‌های پردازش خودکار و نظایر آن محقق می‌شود و ماده ۱۳ قانون جرایم رایانه‌ای عام است که به‌طور مطلق هر نوع تحصیل مال یا منفعت و... را که به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی و ... صورت گرفته باشد را در برمی‌گیرد.

در نتیجه اگر عمل ارتکابی در بستر مبادلات الکترونیکی شرایط مذکور در ماده ۶۷ را دارا باشد مشمول آن ماده، در غیر این صورت مشمول قواعد عام ماده ۱۳ قانون جرایم رایانه‌ای می‌باشد. بنابراین رکن قانونی جرم کلاهبرداری رایانه‌ای ماده ۶۷ قانون تجارت الکترونیکی و ماده ۱۳ قانون جرایم رایانه‌ای است که هیچ یک تعریفی از جرم کلاهبرداری رایانه‌ای ارائه نداده‌اند اما با توجه به فحوای مواد مذکور می‌توان این جرم را این گونه تعریف کرد: «تحصیل خدمات و امتیازات مالی و یا بردن مال دیگری از طریق سوء استفاده یا استفاده غیرمجاز از داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور.»

مصادیق مورد اشاره در مواد مذکور از قبیل ورود، محو، توقف داده پیام و مداخله در عملکرد برنامه یا سیستم رایانه‌ای تمثیلی است و گویای آن است که کلاهبرداری رایانه‌ای نیز با فعل مثبت واقع می‌شود و ترک فعل نمی‌تواند تشکیل دهنده رکن مادی جرم باشد. دیگر اینکه کلاهبرداری رایانه‌ای از لحاظ مقید بودن به نتیجه و لزوم احراز سوءنیت خاص با نوع سنتی خود تفاوتی ندارد با این حال موضوع کلاهبرداری رایانه‌ای «داده‌ها به عنوان نماینده اموال مادی» در سیستم‌های پردازش داده‌هاست (نوری، ۱۳۸۳: ص۲۳) تفاوت اصلی بین کلاهبرداری سنتی و کلاهبرداری رایانه‌ای در روش ارتکاب آنها خلاصه می‌شود. در نوع سنتی این جرم، مرتکب با توسل به وسایل تقلبی، مالباخته را اغفال می‌کند تا با رضایت (هرچند معیوب) مال خود را به او تسلیم کند. از این رو ناآگاهی قربانی از متقلبانه بودن، شرط تحقق جرم است (حبیب‌زاده، ۱۳۸۰ : ص۷۲) لزوم فریب خوردن قربانی جرم کلاهبرداری نشان می‌دهد که ارتکاب این جرم تنها علیه یک «انسان» قابل تصور است (میرمحمدصادقی، ۱۳۸۵: ص۷۶) و با فریب یک ماشین این جرم محقق نمی‌شود. این در حالی است که با توجه به مفاد ماده ۶۷ قانون تجارت الکترونیکی امکان فریب ماشین‌ها و سیستم‌های پردازش خودکار و وقوع کلاهبرداری رایانه‌ای وجود دارد. دیگر اینکه وجود رابطه مستقیم و قاطع بین توسل به وسایل متقلبانه با اغفال قربانی و بردن مال او شرط ضروری تحقق جرم کلاهبرداری سنتی است (میرمحمدصادقی، همان: ص۶۴)با این حال مانورهای متقلبانه که در کلاهبرداری سنتی به صورت انجام افعال، طرح اقوال و... به منظور بردن مال، غیرمتجلی می‌گردد در کلاهبرداری با استفاده از فناوری‌های اطلاعات و ارتباطات

شکل سوءاستفاده از انواع داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور را به خود می‌گیرد. (قناد، ۱۳۸۷: ص۱۳۴)

۲- مفهوم پیشگیری از جرم

پیشگیری از جرم یک امر غریزی است. انسان بالفطره پیش‌گیرنده از جرم بوده، همین که انسان از زمانی که تاریخ به یاد دارد بالفطره به‌طور غریزی از خود دفاع به‌عمل می‌آورده، خود این یک نوع پیشگیری به حساب می‌آید. (حسینی، ۱۳۸۳ : ص۴۰) همواره پیشگیری در ارتکاب جرم موثرتر و سودمندتر از مبارزه و مجازات می‌باشد. در جرایم رایانه‌ای نیز، پیشگیری باید به‌عنوان هدف عمده هرگونه سیاست‌گذاری در این خصوص باشد. در اصطلاحات سیاست جنایی وقتی از پیشگیری از بزهکاری سخن به میان می‌آید، منظور استفاده از راهکارهای متعدد برای ممانعت از وقوع جرم است (اردبیلی، ۱۳۸۳: ص۱۱۹) پیشگیری از جرم ،مجموعه اقدامات پیشگیرانه با هدف تحدید خطر وقوع پدیده‌های جنایی از راه ناممکن ساختن یا دشوار کردن یا کاستن از احتمال وقوع آنها بدون تاکید بر تهدید به مجازات است (اظهار نظر کارشناسی درباره لایحه پیشگیری از جرم، ۱۳۸۵: ص۱).

در مجموع می‌توان گفت پیشگیری از جرم در مفهوم کلی آن عبارتست از تاثیرگذاری بر عوامل جرم‌زا به نحوی که این عوامل جرم‌زا تقلیل یافته یا در شکلی آرمانی از بین برود. (معظمی، ۱۳۸۴: ص۱۵۲). در یک دسته‌بندی، پیشگیری از جرم به پیشگیری غیرکیفری که جلوگیری از وقوع جرم با تکیه بر مجازات‌ها در چارچوب نظام کیفری می‌باشد، در قالب دو نوع پیشگیری عام و خاص مطرح است. مقابله با جرایم رایانه‌ای و به‌طور اخص کلاهبرداری رایانه‌ای نیازمند اتخاذ یک سیاستگذاری عالمانه و برنامه‌ریزی همه‌جانبه است و هر جرم یا هر طبقه از مجرمین برنامه‌های خاصی را برای مقابله می‌طلبند به نحوی که امروزه بایستی مقابله با جرایم رایانه‌ای به صورت تخصصی و مستقل مورد مطالعه قرار گیرد. بنابراین در این قسمت به تبیین تدابیر و راهکارهای مقابله با وقوع جرم کلاهبرداری رایانه‌ای، در چارچوب دسته‌بندی‌ای که در بالا از پیشگیری به عمل آمده پرداخته خواهد شد.

۲-۱-پیشگیری غیرکیفری از جرم کلاهبرداری رایانه‌ای

پیشگیری از ارتکاب جرم شامل مداخلات غیرکیفری در مورد علت‌های نزدیک جرایم است که با هدف خاص کاهش دادن احتمال ارتکاب جرم و یا تقلیل میزان سنگینی جرایم مذکور صورت می‌گیرد. (صدیق، ۱۳۸۵: ص۲۱۳) همانطور که اشاره شد پیشگیری غیر کیفری بر دو نوع است، پیشگیری اجتماعی و پیشگیری وضعی. پیشگیری اجتماعی به‌طور مستقیم در مقام

جلوگیری از مجرم شدن افراد است، یعنی جلوگیری از تبدیل شدن بزهکاران بالقوه به بزهکاران بالفعل. در صورتی که پیشگیری وضعی، بیشتر به حمایت از آماج‌های جرم و نیز بزه‌دیدگان بالقوه و اعمال تدابیر فنی، به دنبال پیشگیری از بزه‌دیدگی افراد است (نجفی ابرند آبادی، ۱۳۷۸: ص۱۴۰)

۲-۱-۱- پیشگیری اجتماعی از جرم کلاهبرداری رایانه‌ای

پیشگیری اجتماعی مجموعه اقدامات و تدابیری است که بر خود فرد تاثیر می‌گذارد و پیش از ارتکاب جرم صورت می‌گیرد. در پیشگیری اجتماعی سعی بر این است که با افزایش آگاهی افراد و تربیت صحیح آنها، به‌ویژه قشر جوان و نوجوان جامعه و همچنین از بین بردن زمینه‌های اجتماعی وقوع جرم، نظیر فقر و بیکاری، انگیزه‌های مجرمانه از مجرمان سلب گردد. (نجفی ابرندآبادی، ۱۳۸۲: ص۱۲۰۸) پیشگیری اجتماعی شامل اقدام‌هایی است که به‌طور مستقیم یا غیرمستقیم، هدف‌شان تاثیرگذاری بر شخصیت افراد است تا از سازمان دادن فعالیت خود حول انگیزه‌های بزهکارانه بپرهیزند (کی‌نیا، ۱۳۷۰: ص۷۸) بنابراین کارکرد اصلی پیشگیری اجتماعی، خنثی‌سازی انگیزه‌های سوء است که در صورت محقق شدن آن با وجود ابزار و فرصت ارتکاب جرم، شخص از آن دوری می‌جوید. پیشگیری اجتماعی بر دو نوع است:

۱- پیشگیری اجتماعی رشد مدار که سعی دارد چنانچه کودکی به هر دلیلی از خود مظاهر بزهکاری را بروز داد با مداخله زودرس در وی و محیط پیرامونش از مزمن شدن بزهکاری در آینده جلوگیری کند.

۲-پیشگیری اجتماعی جامعه‌مدار که در پی خنثی‌سازی عوامل جرم‌زا در محیط اجتماعی است (آقاجانی، ۱۳۸۴: ص۴۶)

الف)پیشگیری اجتماعی رشد مدار سایبری

نکته بسیار مهم در برخورد و مبارزه با جرایم رایانه‌ای، استانداردهای فنی و اخلاق حرفه‌ای افراد می‌باشد. مسلما زمانی می‌توان از افراد انتظار عملکرد صحیح داشت که به راستی به وی تفهیم شود که چه تدابیر امنیتی باید به‌کار گیرد و چه اخلاق شغلی را رعایت کند. بنابراین مشخص است چه در زمینه اخلاق حرفه‌ای و چه در زمینه اتخاذ تدابیر امنیتی، دولت‌ها، شرکت‌ها و حتی اشخاص می‌باید در زمینه آموزش، شناسایی، فرا گرفتن و استفاده از رایانه و تکنولوژی نوین ارتباطی موجود در شبکه‌های بین‌المللی اهتمام ورزند (باستانی، ۱۳۸۳: ص۱۲۰) طیف وسیعی از مجرمان و بزه‌دیدگان جرایم رایانه‌ای را افراد کم سن و سال تشکیل می‌دهند. لذا از جمله تدابیر بسیار موثر در پیشگیری از جرایم رایانه‌ای ارائه آموزش کافی و اطلاع رسانی به هنگام است. آگاه ساختن افراد و ارائه آموزش‌های لازم از سنین کودکی می‌تواند نقش شایان

توجهی در مقابله با جرم رایانه‌ای داشته باشد. اولین محیطی که توجه متصدیان پیشگیری رشد مدار را به خود جلب می‌کند، خانواده و به تبع آن والدین است. چنانچه بتوان در ابتدا توصیه‌ها و آموزش‌های لازم را به والدین منتقل و آن‌ها را با خطرها و در عین حال مزایا و مطلوبیت‌های فضای سایبر آشنا کرد، می‌توان امیدوار بود تا حدود زیادی اهداف این تدابیر به ثمر بنشیند. در کنار خانواده نقش دوستان، مربیان و دیگر مسئولین آموزشی و تربیتی نیز در شکل‌گیری شخصیت کودکان در استفاده از فضای سایبر حائز اهمیت است.

ب)پیشگیری اجتماعی جامعه مدار سایبری

هدف از تدابیر پیشگیری اجتماعی جامعه‌مدار، جلوگیری از شکل‌گیری یا بروز انگیزه مجرمانه در عموم جامعه به وسیله دو اقدام اصلی است: ۱)ترغیب و تسهیل بروز انگیزش‌های مشروع و سودمند ۲)برحذر داشتن از ناهنجاری‌های سایبری.

چنانچه کاربران ملاحظه کنند که با ورود به شبکه اینترنت می‌توانند امور خود را به‌طور بهینه به پیش‌ببرند و این تحول مثبت را در زندگی‌شان احساس کنند، اولویت کاربری‌شان را در فضای سایبر به امور بیهوده اختصاص نخواهند داد (گزارش تاملی بر فیلترینگ۵، ۱۳۸۷: ص۳۶).

هنوز بسیاری از افراد با کارکرد اصلی این فناوری آشنا نیستند و ابزارهای الکترونیکی و ارتباطی را یک وسیله سرگرمی تلقی و در همین حد از آن بهره‌برداری می‌کنند، برای تغییر این نگرش باید از رسانه‌های ارتباط جمعی مثل تلویزیون و... استفاده کرد. راهکار دیگر تدوین «کدهای رفتاری» برای مشاغل گوناگون و الزام به آگاهی از مفاد آن است. یک کد رفتاری می‌تواند به وسیله هر سازمانی، اصولا برای الزام اعضای سازمان و تعیین مبنایی برای روند انضباطی برقرار شود. کلاهبرداری رایانه‌ای در فضای مجازی می‌تواند از طریق افزایش تدابیر آموزشی برای گروه‌های حمایتی مصرف‌کنندگان و بسط تدابیر امنیتی خصوصی کاهش یابد. غالباً دولت‌ها قادر به حمایت مستقیم از شهروندان خود در زمینه جرایم ارتکابی در فضای سایبر نمی‌باشند اما می‌توانند صرفا ابزارهای کافی اتخاذ کنند تا به واسطه آن شهروندان بتوانند خودشان از خودشان حمایت کنند. (دزیانی، ۱۳۸۱: ص۴۶)

۲-۱-۲- پیشگیری وضعی از جرم کلاهبرداری رایانه‌ای

به دنبال عدم توفیق کامل پیشگیری اجتماعی در کاهش و مهار جرم، توسل به پیشگیری وضعی جهت کنترل بزهکاری مورد توجه قرار می‌گیرد. پیشگیری وضعی شامل مجموعه اقدام‌ها و تدابیری است که به سمت تسلط بر محیط و شرایط پیرامونی جرم و مهار آن متمایل است. (نجفی ابرند آبادی، ۱۳۷۸: ص۱۴۰) هدف تدابیر پیشگیرانه وضعی، سلب فرصت و ابزار ارتکاب جرم از دسترس مجرمان بالقوه است. این نوع پیشگیری برخلاف پیشگیری اجتماعی به جای

تکیه بر فرد، بر محیط توجه دارد. در خصوص تدابیر پیشگیرانه سایبری گزینه‌های متنوعی وجود دارد اما قبل از پرداختن به این تدابیر، آنچه از اهمیت برخوردار است مشخص نمودن نحوه مورد حمله قرار گرفتن یا آسیب‌پذیر بودن سیستم رایانه‌ای است که در ابتدا اشاره‌ای به آن خواهیم داشت.

۲-۱-۲-۱- حملات و تهدیدها

تعیین خطرات متوجه سیستم، مهمترین اقدام در ایجاد یک برنامه حفاظت رایانه‌ای مناسب برای آن سیستم و مقابله با جرم کلاهبرداری رایانه‌ای است. در جلوگیری از وقوع جرم نخستین گام، ارزیابی آن دسته از دارایی‌هایی است که باید مورد حمایت قرار گیرند. گام بعدی این است که دارایی‌های ارزیابی شده در برابر کدام خطرات باید حمایت شوند و این خطرات از چه منابعی ناشی می‌شود.

سخت‌افزارها، نرم‌افزارها، داده‌ها و ارتباطات به روش‌های مختلفی در معرض خطر هستند. یک خطر احتمالی به سیستم رایانه‌ای ممکن است یک شخص (نفوذ کننده غیرمجاز)، یک شیء (نرم‌افزار یا سخت‌افزار ناقص) یا یک اتفاق (آتش، رعد و برق و...) باشد که ممکن است به سیستم حمله‌کند. اشخاص، بزرگترین تهدید حفاظت رایانه محسوب می‌شوند. حملات مالی[1] رایانه‌ای اغلب به‌وسیله کارمندان داخلی که فنون الکترونیکی آگاهی دارند انجام می‌شود.

اشکال متفاوتی از شیوه‌های کلاهبرداری رایانه‌ای وجود دارد. گاه مجرم از ابتدا داده‌های نادرست به رایانه وارد می‌کند (دست‌کاری اطلاعات ورودی)، گاه در پردازش صحیح رایانه دست می‌برد (دست‌کاری برنامه‌ها و...) یا اینکه متعاقبا نتایج صحیحی را که رایانه نشان می‌دهد تحریف می‌کند (دست‌کاری اطلاعات خروجی). اکثر دست کاری‌های رایانه‌ای از نوع دست کاری اطلاعات ورودی است. این نوع دست‌کاری را می‌توان از طریق اضافه کردن یا حذف، تغییر، تعویض اطلاعات ورودی یا ارسال آن به محل مناسب، مرتکب شد. در مقایسه با دست‌کاری اطلاعات ورودی که انجام آن بدون داشتن اطلاعاتی در خصوص پردازش داده‌ها ممکن است، روش‌های دست‌کاری در برنامه، بیشتر به رایانه‌ها مربوط می‌شود و از همه مهمتر کشف آنها بسیار مشکل‌تر است. (نوری، ۱۳۸۳: ص۲۶) ساده‌ترین و رایج‌ترین روش کلاهبرداری رایانه‌ای، دست‌کاری آگاهانه داده‌ها و اطلاعات در هنگام ورود آن به سیستم و یا تغییر آن در مراحل بعدی است. از دیگر روش‌های ارتکاب این جرم، حذف یا کسر بدهی‌های شرکت یا افراد، دست‌کاری اطلاعات از سوی حریم شکنان که به روش‌های گوناگون دسترسی غیرمجاز به سیستم راه

1 -Financial Attacks

یافته‌اند و... می‌باشد. در کلیه موارد یاد شده با دست کاری در داده‌ها و یا اعداد و ارقام، افراد منافع نامشروعی را به‌دست می‌آورند.

در مقابل، انواع خاصی از کلاهبرداری‌های رایانه‌ای وجود دارد که مجرمین از طریق فریفتن افراد به کسب مال مبادرت می‌نمایند و از رایانه بیشتر به عنوان کانالی برای تبلیغ کالا یا خدمات و یا ابزار خرید و فروش در معاملات تجاری الکترونیکی استفاده می‌شود. نمونه‌های این نوع کلاهبرداری شامل فروش کالا برای تحویل آن، دریافت پول برای عرضه کارت اعتباری بدون تحویل آن یا تحویل نمونه تقلبی آن می‌باشد. (گزارش طرح شناخت کلی جرایم رایانه‌ای و شیوه‌های مبارزه با آن، ۱۳۸۷: ص۷۹) برخی مواقع مجرمین از شیوه «استراق سمع تلفنی» جهت شنود خطوط ارتباطی بهره می‌گیرند تا با دست‌یابی به یک سری اطلاعات در جهت مقاصد مجرمانه خود از آن بهره بگیرند.

۲-۱-۲-۲- روش‌های حفاظت از سیستم‌های رایانه‌ای

تدابیر متنوعی برای حفظ سیستم‌های رایانه‌ای از حملات وجود دارد، از جمله آن: تدابیر نظارتی است که در فضای فیزیکی نیز نمونه‌هایی از آن در قالب دوربین‌های مداربسته جهت کنترل اماکن وجود دارد. اما آنچه در فضای سایبر به کار می‌رود، مجموعه‌ای از برنامه‌های رایانه‌ای است که بر حسب نوع برنامه‌ریزی‌ای که برای‌شان صورت گرفته، کلیه داده‌های راجع به مبادلات الکترونیکی کاربرانی که به هر دلیل در مظان ارتکاب جرم هستند را جمع آوری می‌کنند تا مسئولان ذیربط به صورت زنده آنها را بررسی کنند. این اقدام تا حدی مورد توجه مجریان قانون کشورها قرار گرفته که برخی از آن‌ها پلیس گشت سایبر[1] نامیده شده‌اند، زیرا به‌گونه‌ای اوضاع سایبری را تحت کنترل دارند که هر گونه وقوع جرم یا دیگر ناهنجاری را به اطلاع مراجع ذیربط می‌رسانند(گزارش حریم خصوصی در فضای سایبر، ۱۳۸۵: ص۲۱).

به‌طور کلی روش‌های حفاظت از سیستم‌های رایانه‌ای عبارتند از: حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و حفاظت عملیات، که هدف همه آنها سخت‌تر ساختن دسترسی مجرمان به سیستم‌های رایانه‌ای می‌باشد که مورد بررسی قرار خواهند گرفت. از جمله مهمترین تدابیر لازم برای مقابله با جرم کلاهبرداری رایانه‌ای بهره‌گیری از روش‌های حفاظتی و امنیتی است. سیستم امنیتی نامطلوب در اکثر موارد، علت وقوع جرم است. تدابیر امنیتی نامطلوب در بیشتر موارد حاصل بی‌اطلاعی از مشکلات موجود در زمینه امنیت داده‌ها است.

1 - Cyber Patrol

الف)حفاظت فیزیکی[1]

حفاظت فیزیکی به معنای حفظ رایانه، تجهیزات رایانه، رسانه‌های رایانه‌ای و تمامی سیستم، در مقابل سوانح طبیعی، انواع مختلف حوادث و حملات عمومی است (استرکی، ۱۳۸۳: ص۷۵).

جرایم رایانه‌ای قابل پیش‌بینی نیستند، به همین جهت اتخاذ تدابیری که ارتکاب آن‌ها را با دشواری مواجه سازد ضرورت دارد. اولین حلقه حفاظت فیزیکی اقداماتی است که مجرمین را از نفوذ به ساختمان محل استقرار رایانه‌ها مایوس نماید، به‌طوری که تدابیر مناسب برای درب‌های ورودی اطاق‌های محل نگهداری سیستم‌رایانه‌ای اتخاذ شود. همچنین جهت جلوگیری از استراق سمع تلفنی اتخاذ اقدامات لازم جهت حفاظت از رمز عبور، نام فایل‌ها و سایر اطلاعات محرمانه ضروری است. پیش از نفوذ افراد غیرمجاز و وقوع جرم، می‌توان برنامه‌های حفاظت فیزیکی را از طریق بازرسی منظم از تمهیدات حفاظت فیزیکی یا بازرسی غیر مترقبه از فیلترها و موانع حفاظت فیزیکی مورد ارزیابی قرار داد.(استرکی، همان: ص۱۷۲)

ب) حفاظت کارکنان[2]

تدبیر حفاظت کارکنان، افرادی را پوشش می‌دهد که به نحوی مجاز به کار با سیستم می‌باشند. اغلب جرایم مالی رایانه‌ای توسط افراد مذکور و نه حریم شکنان مجرم صورت می‌گیرد (گزارش طرح شناخت کلی جرایم رایانه‌ای و شیوه‌های مبارزه با آن، همان: ص۶۹). در برخی موارد، اعمال سیاست‌های سازمان، منظم و مدون نیست. به عنوان مثال در برخی از سازمان‌ها کارکنان اجازه ندارند اطلاعات محرمانه سازمان را با خود به منزل ببرند. از سوی دیگر به آنها اجازه داده می‌شود از منازل خود با استفاده از یک مودم به بانک اطلاعاتی سازمان متصل شوند. در این صورت اطلاعات سازمان قابل نسخه‌برداری خواهد بود. از نظر حفاظت کارکنان، اقدامات لازم جهت ارتقاء سطح امنیت پرسنلی عبارتند از: ۱)تحقیقات لازم پیش از استخدام ۲) نظارت و کنترل کافی مدیران بر عملکرد کارکنان ۳)دادن آموزش‌های لازم به کارکنان، زیرا گاهی وقوع جرم ناشی از ثبت اشتباه یا تغییر اطلاعات به وسیله کارمند است ۴)اجرای برنامه کاری چرخشی برای کارکنان، زیرا برخی حملات نفوذکنندگان غیرمجاز به زمان زیاد و یا کنترل مستمر نیازمند است که در صورت اجرای راهکار فوق امکان شناسایی برخی حملات درازمدت خواهد بود. (استرکی، همان: ص۸۳) قابل ذکر است که در این‌باره، بایستی شدیدترین احتیاط‌ها در مورد کارکنان اخراجی یا کارکنانی که داوطلبانه از کار کناره‌گیری کرده‌اند اتخاذ شود.

---

1 -Physical Security
2 -Personnel Security

ج)حفاظت ارتباطات[1]

گونه‌ای دیگر از تدابیر امنیتی و حفاظتی، حفاظت ارتباطات است که شامل حفاظت از پست، نمابر، تلفن، ارتباطات پست صوتی و همچنین حفاظت از اطلاعات انتقال داده شده از یک رایانه به رایانه دیگر از طریق اتصال شبکه می‌شود. مجرمین حرفه‌ای ممکن است سیستم رایانه را برای ارتکاب کلاهبرداری یا مستقیما برای منفعت خودشان، مورد هدف قرار دهند. در این صورت تدابیر حفاظت ارتباطات (به عنوان مثال کلمات رمز عبور) مهمترین عامل برای دور نگهداشتن مجرمین حرفه‌ای است. حفاظت ارتباطات، روش‌ها و وسایل مختلفی را در بر می‌گیرد که شامل استفاده از کلمات رمز مناسب، حفظ اطلاعات انتقال داده شده، ایجاد یک حفاظ که سیستم‌ها و شبکه‌های داخلی را از دیگر شبکه‌ها حفاظت کند، کنترل دسترسی، روش‌های رمزنگاری، فناوری دیواره آتشین[2] و... می‌باشد.

شیوه‌های دسترسی در ایجاد امنیت رایانه‌های متصل به شبکه اهمیت زیادی دارند. یکی از ابزارهای کنترل دسترسی استفاده از رمز عبور است. فردی قادر به دسترسی خواهد بود که رمز صحیح عبور را در رایانه وارد نماید و سرقت یا نسخه برداری غیرمجاز از اطلاعات محرمانه نوعی تهدید آشکار است و نفوذکنندگان غیرمجاز درصدد دستیابی به رمز عبور یا سایر اطلاعات جهت نفوذ در سیستم هستند. یکی از شیوه‌های محدود نمودن دسترسی افراد به اطلاعات محرمانه، رمز نگاری اطلاعات و داده‌ها می‌باشد. در این فرآیند اطلاعات یا محتویات یک متن به اطلاعات و متون رمز تبدیل می‌شود. برخلاف گذشته که از یک کلید جهت رمز نمودن اطلاعات استفاده می‌شد، در شیوه‌های رمزنگاری جدید از دو کلید، جهت رمزنگاری یک پیام استفاده می‌شود. در این روش‌ها حتی امکان امضاء پیام نیز فراهم شده تا گیرنده پیام از هویت فرستنده آن مطلع شود. دیگر اینکه کابل‌ها و خطوط ارتباطی به راحتی قابل شنود و استراق سمع هستند. تمامی دستگاه‌های الکترونیکی از خود پرتوهای الکترومغناطیسی منتشر می‌کنند. دریافت و آشکارسازی آن پرتوها یکی از روش‌های استراق سمع است. افرادی که قصد استراق سمع دارند با استفاده از یک سری تجهیزات قادر به دریافت سیگنال‌هایی هستند که در اثر فشردن کلیدهای صفحه کلید رایانه در محیط منتشر می‌شوند. با تحلیل این سیگنال‌ها می‌توان به اطلاعات روی صفحه نمایشگر سیستم دست یافت. یکی از شیوه‌های جلوگیری از انتشار پرتوهای الکترومغناطیسی استفاده از عایق است.

---

1 -Communications Security
2 -Fire Wall

عایق، سیگنال‌های الکترومغناطیسی را تضعیف نموده و آن‌ها را به زمین هدایت می‌کند. (استرکی، همان: ص۲۱۱)

یکی از شیوه‌های موثر حفاظت در مقابل نفوذ افراد غیرمجاز نصب دیواره آتشین می‌باشد. دیواره آتشین یک روش نرم‌افزاری یا سخت افزاری است که بر کلیه ارتباطات شبکه اعم از ارتباطات بین شبکه داخلی و اینترنت یا بالعکس نظارت می‌کند. نرم‌افزاری که دیواره آتشین را تشکیل می‌دهد اطلاعات و داده‌های در حال تبادل شبکه را بررسی و مبادله اطلاعات و سایر عملیات مشابه را مجاز یا متوقف می‌نماید.(استرکی، همان: ۲۱۴)

د)حفاظت عملیات[1]

آخرین نوع از تدابیر حفاظتی، حفاظت عملیات است. حفاظت عملیات به معنی وضع تدابیری جهت شناسایی و مقابله با تهدیدهایی است که سیستم‌ها را به مخاطره می‌اندازد.

حفاظت عملیات دو مقوله از حفاظت رایانه را در بر می‌گیرد: ۱)روش‌هایی که می‌تواند آگاهی و اطلاع از وقوع جرایم احتمالی را در بین قربانیان بالقوه افزایش دهد. ۲) روش‌هایی که می‌تواند مجرمین رایانه‌ای را از ارتکاب جرم باز دارد. این فرآیند سه مرحله دارد: مرحله اول: مشخص کردن اطلاعاتی که یک مجرم رایانه نیاز دارد. مرحله دوم: مشخص کردن روش‌های احتمالی مجرمین برای کسب اطلاعات و مرحله آخر، توسعه اقدامات لازم جهت مقابله با عملی شدن روش‌های احتمالی. (استرکی، همان: ص۲۲۵). حفاظت عملیات فعالیتی پویاست. بنابراین با تغییر غیر منظم روش‌ها و دسترسی‌ها می‌توان تعادل حریف را بر هم زد. برای رسیدن به این منظور، فهرست اجزای ضروری اطلاعات، روش‌های نفوذ و شگردهای مقابله باید دائما تغییر پیدا کنند. مهمترین رکن حفاظت عملیات استمرار در توسعه روش‌های مقابله و حفاظت، آموزش کارکنان و کاربران سیستم است.

۲-۲- پیشگیری کیفری از جرم کلاهبرداری رایانه‌ای

وجود بزهکار نه فقط نظم اجتماعی را در خطر قرار می‌دهد، بلکه «قدرت دولت» را نیز در قبال جامعه تهدید می‌کند زیرا افزایش بزهکاران آشکار کننده ضعف دولت است و لذا دولت به شدت درصدد سرکوبی بزهکاری و به‌خصوص بزهکاران برمی‌آید (نوربها، ۱۳۷۷: ص۲۳) در سیاست جنایی، مسئله مقابله با جرم نیز نهفته است و چگونگی و کیفیت و انتخاب نوع کیفر و برخورد با بزهکاران نیز بیان می‌شود. (گزارش‌پیرامون پیشگیری از وقوع جرم، ۱۳۷۵: ص۲).

1 Operations Security

«پیشگیری واکنشی» پس از ارتکاب جرم و با استفاده از ابزارهای کیفری اعمال می‌شود. این نوع پیشگیری خود بر دو گونه است:

۱)پیشگیری واکنشی عام، که از طریق رعب‌انگیزی و عبرت‌آموزی به دنبال پیشگیری از ارتکاب جرم از سوی افراد جامعه می‌باشد.

۲)پیشگیری واکنشی خاص، که با اعمال کیفر بر فرد بزهکار درصدد پیشگیری از تکرار جرم است. صرف نظر از اقدامات پیشگیرانه، به هرحال باید انتظار داشت که همچون سایر جرایم، جرم کلاهبرداری رایانه‌ای از سوی مجرمین در جامعه روی دهد. بنابراین مقابله با این جرم جدای از اقدامات عملی نیازمند اتخاذ تدابیر مناسب قانونی و قضایی است. اصولا جرم انگاری افعال به عنوان آخرین حربه علیه هنجار شکنان مورد توجه قرار می‌گیرد. وضع قانون مناسب یکی از مهمترین راهکارهای مقابله با وقوع جرم از سوی افرادی است که نقض هنجار نموده و تدابیر پیشگیرانه وضعی را هم خنثی کرده‌اند. در مورد مقابله کیفری آنچه حائز اهمیت است، این است که صرف جرم‌انگاری رفتار و تعیین ضمانت اجرای کیفری در رسیدن به مقصود یاری می‌رساند. این موضوع از آن جهت اهمیت دارد که با توجه به ناملموس بودن فضای سایبر در اکثر موارد، کشف و تعقیب جرایم ارتکابی در این محیط و اعمال مجازات مجرمان، چه در سطح ملی و چه در سطح بین‌المللی (به‌علت واجد جنبه فرامرزی بودن جرایم ارتکابی در فضای سایبر) با مشکلات و چالش‌هایی روبروست که به برخی از آنها اشاره خواهیم کرد.

از لحاظ کشف، به‌طور کلی، در جرایم رایانه‌ای «رقم سیاه» در مقایسه با جرایم کلاسیک بسیار بالاست. چرا که اکثر جرایم یا اصلا کشف نمی‌شوند یا به مقامات ذی‌صلاح گزارش نمی‌شود.

مشکلات کشف جرایم رایانه‌ای عبارتند از:

- به‌دلیل اخفای این نوع جرایم در اکثر موارد تعقیب جرم با مانع مواجه می‌شود.
- مجرمین قادرند فعالیت تعقیب جرایم ارتکابی را با استفاده از گذر واژه و کد گذاری با مشکلات حادی مواجه نماید.
- مجرمین می‌توانند با حذف و یا پاک کردن داده‌ها دلایل علیه خود را از بین ببرند.
- مانع دیگر، حجم زیاد داده‌های پردازش شده در سیستم‌های داده‌پردازی است که کنترل آنها ممکن نیست.
- عدم آشنایی مامورین تحقیق و قضات با رسانه‌های اطلاعاتی و ضعف آنها در برخورد با مسائل فنی جرایم رایانه‌ای.

از لحاظ ابعاد بین‌المللی نیز با توجه به اینکه مرتکب جرم رایانه‌ای لزوما حضور فیزیکی در محل وقوع جرم ندارد و با استفاده از ارتباطات شبکه بین‌المللی، اعمال مجرمانه خود را انجام می‌دهد و دیگر اینکه دست‌یابی به یک سیستم یا شبکه در جهت کشف، تعقیب و تحصیل دلیل، ممکن است پردازش داده‌ها در کشور دیگر محسوب شود که خود تعرض به حاکمیت دولت‌ها خواهد بود، بنابراین پی‌جویی جرایم رایانه‌ای و مقابله با آن مستلزم همکاری‌های بین‌المللی در قالب انعقاد موافقت‌نامه‌های چند جانبه کشورها در زمینه کشف و تعقیب جرایم ارتکابی در فضای سایبر، نیابت قضایی، استرداد مجرمان و... می‌باشد. در این راستا می‌توان طراحی سیستم‌های امنیتی را در سطح بین‌المللی توسعه داد. و بدین ترتیب امکان بهره‌مندی از تجربه کشورهای دیگر را فراهم نمود مانند همکاری در زمینه ضابطه‌مند کردن تدابیر امنیتی مربوط به کارت‌های عابربانک، امضاهای الکترونیکی و... از نمونه‌های بارز همکاری‌های بین‌المللی در مقابله با جرایم رایانه‌ای می‌توان به اقدامات پلیس بین‌المللی (اینترپل) در زمینه دوره‌های آموزشی مختلف در مورد کشف و پیگرد جرایم رایانه‌ای اشاره‌کرد.

نتیجه‌گیری

یکی از مصادیق جرایم رایانه‌ای که با انگیزه کسب منافع مادی نامشروع در محیط شبکه‌های رایانه‌ای ارتکاب می‌یابد جرم کلاهبرداری رایانه‌ای است. اساسا حوزه تاثیرگذاری جرایمی که در فضای سایبر واقع می‌شوند نسبت به جرایم سنتی بسیار گسترده است و به مراتب خسارات بیشتری نیز بر جای خواهند گذاشت، بنابراین همان‌طور که جوامع با وقوع جرم در دنیای فیزیکی مقابله می‌کنند ارائه راهکارهای مناسب در جهت مقابله و جلوگیری از وقوع جرم در محیط مجازی که از اوصاف و ویژگی متفاوتی نسبت به محیط واقعی برخوردار است امری ضروری است. دراین نوشتار سعی بر آن شد که راهکارهای غیرکیفری و کیفری در مقابله و جلوگیری از ارتکاب جرم کلاهبرداری رایانه‌ای ارائه شود بنابراین آنچه در به‌کارگیری راهکارهای غیر کیفری مورد توجه می‌باشد مقابله اجتماعی و وضعی در برابر وقوع جرم است. در تدابیر اجتماعی جهت مبارزه با جرم کلاهبرداری رایانه‌ای باید ارتقاء سطح فرهنگ افراد در استفاده از فناوری‌های نوین و تغییر نگرش افراد و آشنایی آنها از کارکرد اصلی این فناوری و تقویت نقش تربیتی و آموزشی والدین و موسسات آموزشی در کاهش ارتکاب جرم مورد تاکید قرار گیرد. با عدم توفیق مقابله اجتماعی در کاهش یا مهار جرم، مقابله وضعی با آن مطرح خواهد شد. هدف از مقابله وضعی، سلب فرصت ارتکاب جرم از سوی نفوذکنندگان به سیستم‌های رایانه‌ای است. در این رابطه شناسایی خطرات متوجه سیستم رایانه‌ای، مهمترین اقدام در جهت ایجاد یک برنامه

حفاظتی مناسب برای مقابله با جرم کلاهبرداری رایانه‌ای است. سیستم‌های سخت‌افزار و نرم‌افزار رایانه‌ای به شیوه‌های مختلفی در معرض خطر قرار می‌گیرند لذا باید تدابیر متنوعی برای حفاظت از سیستم‌های رایانه‌ای در مقابل حملات احتمالی اتخاذ گردد، که از آن جمله می‌توان بـه تـدابیر حفاظت فیزیکی از رایانه و تجهیزات مربوط به آن در مقابل حوادث و حملات احتمالی اشاره نمود و همچنین با توجه به اینکه غالب حملات مالی رایانه‌ای به وسـیله کارکنـان ادارات و موسـسات دولتی و غیردولتی صورت می‌گیرد اتخاذ تـدابیر حفاظـت کارکنـان کـه افـراد مجـاز بـه کـار بـا سیستم‌های رایانه‌ای را تحت پوشش قرار می‌دهد ضرورت دارد. دیگر اینکه تقویت تدابیر حفاظت ارتباطات که اطلاعات انتقال داده شده از یک سیستم به سیستم دیگر از طریق اتصال به شـبکه را در برمی‌گیرد و همچنین تدابیر حفاظت عملیات که با شناسایی اطلاعاتی که مجرمان در صدد دستیابی به آن هستند و شناخت روش‌های احتمالی کسب اطلاعات، اقدامات لازم را جهت مقابله با عملی شدن روش‌های احتمالی ارائه می‌دهد، امری اجتناب ناپذیر است.

قابل ذکر است که در بحث امنیت سیستم‌های رایانه‌ای، امنیت مطلق وجود ندارد و همواره با دستیابی افراد به شیوه‌های نوین ارتکاب جرم کلاهبرداری در محیط سیستم‌های رایانه‌ای، اتخـاذ تدابیر امنیتی متناسب با این شیوه‌ها ضرورت دارد. تنوع بسیار گسترده شیوه‌های ارتکاب این جرم مانع از وضع تدابیری است که بتوان تمامی آنها را تحت پوشش قرارداد بنـابراین مبـارزه مـوثر و منسجم با این جرم تنها بر پایه شناخت درست از ماهیت و شیوه‌های ارتکـاب جـرم امکـان‌پـذیر است.

اصولا جرم‌انگاری رفتارهای مجرمانه به عنوان آخرین حربه علیه هنجارشـکنان مـورد توجـه جرم شناسان قرار می‌گیرد. لذا تدابیر کیفری به‌عنوان ابزاری سرکوبگر آخرین راهکـار مقابلـه بـا وقوع جرم است. با این حال باید توجه داشت که صرف جـرم انگـاری و تعیـین ضـمانت اجـرای کیفری کافی نیست و تدابیر کیفری در صورتی در مقابله با جرم موثر است کـه امکـان کـشف و تعقیب جرم و مجازات مجرم وجود داشته باشد. لذا با توجه به اینکـه در فـضای سـایبر اصـل بـر ناشناختگی است در اکثر موارد کشف و تعقیب جرایم ارتکابی و اعمال مجازات مجرمـان چـه در سطح ملی و چه در سطح فراملّـی (بـه علـت واجـد جنبـه فرامـرزی بـودن جـرایم سـایبری) بـا چالش‌های فراوانی روبروست که در این راستا بایستی آموزش و بالا بردن سطح دانـش مـاموران کشف جرم در زمینه پی‌جویی جرایم ارتکابی در فضای سایبر و همچنین تقویـت همکـاری‌هـای بین‌المللی در سطوح مختلف طراحی سیستم‌های امنیتی فراملّی و انعقاد معاهدات همکـاری چنـد جانبه در زمینه معاضدت قضایی، استرداد مجرمان و ... از سوی کشورها مورد تاکید بیشتری قـرار گیرد.

در پایان لازم به ذکر است صرف تاکید بر یکی از تدابیر مذکور کافی به مقصود نخواهد بود بلکه به‌کارگیری کلیه تدابیر یاد شده در کنار هم می‌تواند در جهت مقابله با ارتکاب جرم کلاهبرداری رایانه‌ای راهگشا باشد.

منابع و مآخذ

۱- آزمایش، علی، «تقریرات درس حقوق جزای اختصاصی دوره کارشناسی ارشد» دانشکده حقوق دانشگاه تهران نیمسال تحصیلی ۷۲-۱۳۷۱.

۲- آقاجانی، علی، «راهکارهای قانونی در پیشگیری از جرایم رایانه‌ای از دیدگاه حقوقدانان و کارشناسان»، پایان‌نامه کارشناسی ارشد، دانشگاه علوم انتظامی (دانشکده فرماندهی ستاد) دی ماه ۱۳۸۴.

۳- اردبیلی، محمدعلی و حسینی، سید محمد، «نشست علمی در مورد پیشگیری از جرم در حقوق کنونی ایران»، مجله حقوقی دادگستری، ش۴۸و۴۹ پاییز و زمستان ۱۳۸۳.

۴- باستانی، برومند؛ «جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری»، چاپ اول، تهران، بهنامی، ۱۳۸۳.

۵- حبیب‌زاده، جعفر، «حقوق جزای اختصاصی»، جرایم علیه اموال، چاپ اول، تهران، سمت، ۱۳۸۰.

۶- دزیانی، محمدحسن، «شروع جرم کامپیوتری/سایبری»، خبرنامه انفورماتیک، شماره ۹۳، سال۱۳۸۳.

۷- «جرایم کامپیوتری از حیث حقوق جزای اختصاصی» خبرنامه انفورماتیک، شماره۸۲ سال ۱۳۷۵.

۸- دیویدچی، آیکاو و دیگران، «راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای»، ترجمه: اکبر استرکی و دیگران، چاپ اول، تهران، ۱۳۸۳.

۹- زیبر، اولریش، «حرکت به سوی هزاره جدید مسئولیت در اینترنت» ترجمه: محمدحسن دزیانی، خبرنامه انفورماتیک ش۸۳، مرداد ۱۳۸۱.

۱۰- «جرایم رایانه‌ای»، ترجمه: محمدعلی نوری و دیگران، چاپ اول، تهران، گنج دانش، ۱۳۸۳.

۱۱- قناد، فاطمه، «کلاهبرداری الکترونیکی در بستر فناوری‌های اطلاعات و ارتباطات»، مجله پژوهش و سیاست، شماره ۲۵، ۱۳۸۷.

۱۲- گزارش نهایی طرح «شناخت کلی جرایم رایانه‌ای و شیوه‌های مبارزه با آن»، کارفرما: نیروی انتظامی جمهوری اسلامی ایران، مجری: جهاد دانشگاهی علم و صنعت، آذرماه ۱۳۷۸.

۱۳- گسن، ریموند، «جرم‌شناسی کاربردی»، ترجمه مهدی کی‌نیا، چاپ اول، تهران، مجد، ۱۳۷۰.

۱۴- گسن، موریس، «اصول جرم شناسی» ترجمه: میر روح‌الله صدیق، چاپ اول، تهران، نشر دادگستر، ۱۳۸۵.

۱۵- مرکز پژوهش‌های مجلس شورای اسلامی، «گزارش تاملی بر فیلترینگ۵. برنامه اقدام برای تحقق برنامه سالم‌سازی فضای سایبر، شماره ۸۹۴۷، اردیبهشت ۱۳۸۷.

۱۶- مرکز پژوهش‌های مجلس شورای اسلامی، «گزارش حریم خصوصی در فضای سایبر»شماره ۸۰۶۹، آبان ماه ۱۳۸۵.

۱۷- مرکز پژوهش‌های مجلس شورای اسلامی، «گزارش پیرامون پیشگیری از جرم»، شماره ۳۷۲۵، آبان ماه ۱۳۷۵.

۱۸- مرکز پژوهش‌های مجلس شورای اسلامی، «اظهار نظر کارشناسی درباره لایحه قانون جرایم رایانه‌ای»، شماره ۷۵۵۲، آبان ماه۱۳۸۴.

۱۹- مرکز پژوهش‌های مجلس شورای اسلامی، «اظهار نظر کارشناسی درباره لایحه پیشگیری از جرم» شماره ۷۸۹۱، آذرماه ۱۳۸۵.

۲۰- معظمی، شهلا، «جرم سازمان یافته و راهکارهای جهانی مقابله با آن» چاپ اول، تهران، نشر دادگستر، ۱۳۸۴.

۲۱- میرمحمد صادقی، حسین، «جرایم علیه اموال و مالکیت» چاپ ۱۴، تهران، نشر میزان، ۱۳۸۵.

۲۲- نجفی ابرند آبادی، علی حسین، «تقریرات درس جرم‌شناسی دوره کارشناسی ارشد» تنظیم: رضا فانی، نیمسال اول سال تحصیلی ۸۳-۱۳۸۲.

۲۳- «پیشگیری از بزهکاری و پلیس محلی»، مجله تحقیقات حقوقی، شماره ۲۵ و۲۶، بهار و تابستان ۱۳۷۸.

۲۴- نوربهار، رضا، «زمینه جرم‌شناسی»، چاپ اول، تهران، گنج‌دانش، ۱۳۷۷.