تاریخ دریافت: ۱۴۰۱/۱۲/۴ تاریخ پذیرش: ۱۴۰۲/۳/۲۵ صفحه ۱۳۸ تا ۱۵۸

سازو کارهای پیشگیرانه در مواجهه با بزه جاسوسی رایانه‌ای؛ راهکارها و پیشنهادها

احمد پورابراهیم[۱]

چکیده

از گذشـــته تا به امروز یکی از دغدغه‌های اصلی حفظ امنیت و بقای دولت‌ها و ملت‌ها، ســـعی در ارتقای سطح توانایی برای کنترل، پیشگیری و مبارزه با پدیده‌های ضد امنیتی خصوصاً جاسوسی بوده است. جاسوسی رایانه‌ای که خود چهره جدید و وسیعی از جاسوسی بشمار می‌رود - با توجه به وضعیت رایانه‌ای بودن اکثریت منابع اصلی اطلاعات و زیرســـاخت‌های حیاتی کشورها- یکی از مهمترین دغدغه‌های کشـــورها در این برهه از زمان می‌باشـــد که باید هر روز بیش از دیروز مدنظر و مـــورد توجه قرار گیرد. گرچه در راســـتای مقابله بـــا این نوع جرائم قانون‌گذار در مراحل مختلف عکس‌العمل نشـــان داده و نســـبت به مصادیق پدیده‌های مجرمانه ســـایبر جرم‌انگاری کرده، اما همچنان با روند فزاینده ظهور، گســـترش و دسترســـی ارزان به فناوری‌های اطلاعاتی، شاهد رشد آمار جرائم رایانه‌ای و پیچیده‌تر شدن روش‌های ارتکاب جرم خواهیم بود. بی توجهی به این مهم در آینده‌ای نزدیک، فعالیت‌های جامعه را دچار صدمات جبران‌ناپذیر نموده و امنیت اجتماعی کشور را دســـتخوش تهدید جدی خواهدکرد. از آنجا که پلیس به عنوان ضابط دادگستری وظیفه کشف جرائم را برعهده دارد، در کنار آموزش قضات و سایر مقدمات قضایی، آموزش پلیس نیز باید در سر فصل برنامه‌ریزی‌ها قرار گیرد. با توجه به اهمیت این موضوع، در این راستا پژوهش حاضر به بررسی پدیده جاسوسی رایانه‌ای و راهکارهای پیشگیری از آن با روش توصیفی – تحلیلی پرداخته‌است

واژگان کلیدی: جاسوسی رایانه‌ای، جرایم رایانه‌ای، پیشگیری، راهکارها

۱. دکترای حقوق کیفری و جرم شناسی .ahmad.pourebrahim@chmail.ir

Preventive Mechanisms in Encountering with the Crime of Computer Spionage; Solutions and Suggestions

Ahmad Pour Ebrahim[1]

Abstract

Since past time till now, one of the main concerns of maintaining security and survival of governments and nations has been to try to improve capabilioty level of controlling, preventing and combating the phenomenon of counter-security, especially espionage. Computer espionage which is per se considered as a new and massive figure of espionage, regarding computer nature of most major resources of information and critical infrastructure of countries, is one of the most important concerns of countries at this time which should be considered and noticed a lot more than yesterday. Although in line with combating this kind of crime, legislators have shown reactions at various stages and have incriminated the examples of cyber criminal phenomena, we will witness increase in the emeregence, spread and cheap access to information technologies and statistics of computer crimes and complexities of the methods of committing such crimes. Lack of attention to this important issue in the near future, it will inflict irreparable damage on the society's activities and it will threaten the State social security, as well. Since police, as judicial force is in charge of detecting crimes, in addition to judges and other judicial officials' training, police training should also be included in their lesson plans. Regarding the importance of this issue, the present research attempts to investigate computer espionage and its preventive solutions using descriptive-analytical method.

Key Words: Computer Espionage, Computer Crimes, Prevention, Solutions

1. Ph.D in Criminal Law and Criminology.. ahmad.pourebrahim@chmail.ir

مقدمه

پیدایـــش رایانه و پـــس از آن دنیای مجازی اینترنت، همراه خود دســـتاوردهای مثبت و منفی بی‌شماری داشته و دارد. از جمله پیامدهای منفی آن، پیدایش جرائم نوظهور رایانه‌ای و اینترنتی اســـت. ویژگی‌های خاصی چون تخصصی و علمی بودن، دارای حیثیت عمومی و خصوصی بودن، پیچیدگی خاص، دشـــوار بودن تعین صلاحیت کیفری، جهانی بودن، دشـــوار بودن کشف بزهکار که در این دســـت از جرائم بروز کرده اســـت آن را از دیگر جرائم متمایز می‌نماید. این جرائم را در حالت کلی به ســـه دســـته می‌توان طبقه بندی کرد: الف- جرایم رایانه‌ای فرهنگی شامل: جرائم بر ضد مالکیت فکری و جرائم اخلاقی چون جرائم توهین و اهانت به دین مبین اســـلام و مقدســـات آن و جرائم افشـــای محتوا اســـرار خصوصی افراد. ب- جرائم امنیتی شامل: ۱- جرائم علیه امنیت داده‌ها مانند: جرائم علیه کاربرد مجاز داده‌ها همچون جاسوسی، دسترسی غیرمجاز و جرائم علیه صحت داده‌ها: همچون جعل. ۲- جرائم علیه امنیت سیستم. ج- جرائم مالی از قبیل کلاهبرداری و سرقت. لذا با ایجاد شبکه‌های رایانه‌ای و ارتباط جهانی، این شبکه‌ها زندگی اجتماعی بشر را وارد مرحله تازه‌ای کرده و فضای مجازی را به ارمغان آورده اســـت. در نتیجه ایجاد فضای مجازی برای زندگی بشر، شکل جدیدی از روابط اجتماعی، تجارت، دوستی و... به وجود آورده است که ضرورت توجه به وقایع در حال وقوع از ضروریات اجتناب ناپذیر به شـــمار می‌رود. از آنجا که بخش مهمی از زندگی اجتماعی، تأمین امنیت آن است و این مهم از مسئولیت‌های نیروی انتظامی است توجه به آنچه به وقوع پیوسته و در حال وقوع است نیز ضروری به نظر می‌رسد (عابدینی، ۱۳۸۸: ۱۴۶).

جرم جاسوســـی از جمله جرایمی اســـت که در طبقه اول جرایم علیه امنیت و آســـایش عمومی قرار دارد، چرا که اســـتقلال و امنیت و تمامیت ارضی کشـــور و اساس حکومت را به خطر می‌اندازد و موجب فاش شـــدن اســـرار و اطلاعات میشود (شجوده، ۱۳۹۸: ۱۲). گرچه برخی معتقدند (سان تزو) جاسوســـی خوب مقدمه پیروزی اســـت. هیچ زمانی در طول تاریخ نام کشوری به افتخار برده نشده است که بدون سرویسهای جاسوسی و اطلاعاتی قوی توانسته باشد کاری انجام دهد(اندلمن، دماراتش، ۱۳۹۰ : ۱۶۲ و ۱۶۳).

برخی از علمای علم حقوق در تفکیک جرم جاسوسی و خیانت به کشور دچار اشکال شده اند و اظهار میدارند که در حال حاضر تفکیک جرایم فوق عملی نیســـت و عده‌ای نیز، ممیز اساســـی این دو جرم را تابعیت و ملیت مرتکب قرار داده اند (شامبیاتی، ۱۳۹۶: ۱۰۲).

برخی از متون قانونی کشـــورهای اروپایی فرق اصلی جرم جاسوســـی و خیانت به کشور را عنصر

تابعیت مرتکب میدانند. یعنی اگر مرتکب جرم از اتباع کشوری باشد و جرم بر ضد آن کشور وقوع یافته باشـــد، عمل ارتکابی خیانت به کشـــور محسوب میشود و در صورتیکه مرتکب خارجی باشد، عمل او جاسوســـی خواهد بود. از طرف دیگر قانونگذاران و محاکم نیز معیار مناســـبی برای تمایز جرایم جاسوسی و خیانت به کشور مشخص نکرده اند به طوری که گاهی عمل واحد، هم جاسوسی و هم خیانت محسوب میشود. به هر حال بنابر اصل تفکیک بین معنا و مفهوم خیانت و جاسوسی در فقه، بدون ملاحظه جنبه‌های کاربردی آن در صحنه سیاست و حکومت، جاسوس لزوما باید کافر حربی باشـــد و الا مســـلمانان و کافر ذمی اگر مرتکب عمل مشابهی شوند، خائن محسوب میشوند. در نظام اســـلامی در شـــرایط کنونی، کافر یا مسلمان بودن چندان دخالتی در این موضوع ندارد و عملا تابعیت سیاسی است که تعیین کننده است(زینلی، ۱۳۹۸: ۲٤٤).

اهداف تحقیق

۱) بررسی ماهیت پدیده جاسوسی رایانه‌ای و جایگاه آن در قوانین ایران

۲) ارائه پیشنهاد و راهکار برای پیشگیری و مقابله با این جرائم

مبانی نظری و پیشینه تحقیق

مبحث اول: مفاهیم و مبانی جاسوسی رایانه ای

هنگامی که از امنیت رایانه‌ها و شـــبکه‌های رایانه صحبت می‌شـــود، مباحث زیادی قابل طرح و بررســـی می باشـــند، موضوعاتی که هر کدام به تنهایی می‌توانند در عین حال جالب، پر محتوا و قابل درک باشند. اما وقتی صحبت از کار عملی برمی آید قضیه تاحدودی پیچیده می‌شود. ترکیب علم و عمل احتیاج به تجربه دارد و نهایت هدف علم، بعد کاربردی آن است. اما در مورد جاسوسی اینترنتی باید گفت که جاسوسی از طریق اینترنت مسئله‌ای که در گذشته نه چندان دور، تنها ذهن اندیشمندان علوم ارتباطات و اطلاعات را به خود مشغول کرده است. " کیث لیتل " تکنسین رایانه در آمریکا می‌گویند: هر روز تعداد بیشتری از مشتریان از او می‌خواهند برای حفظ حریم شخصی آنها اقداماتی انجام دهد. او نیز رایانه‌های آنان را برای یافتن هر گونه برنامه شیطانی جستجو کرده، نرم افزارهای امنیتی در آن نصب می‌نماید (در این جنگ جهانی نه از ارتش‌های کلاسیک خبری است نه از تسلیحات مرگبار. اینجا فقط رایانه است و کابل و ایده.

جاسوسی اینترنتی عموما به صورت دستیابی به اطلاعات از طریق برنامه‌هایی معرفی می‌شود از

راه نصب نرم افزارها و یا حین گردش افراد در محیط وب وارد رایانه شـــخصی آنان شـــده و تا زمانی که کاربر به شـــبکه جهانی وصل اســـت، اطلاعاتی را که روی‌هارد رایانه او ذخیره شده است، برای پایگاه‌های مطلوب خود می‌فرستند اما این تنها یکی از انواع جاسوسی الکترونیکی است نوع دیگر کـــه امروزه تقریبا همه ما آنان را می‌شناســـیم و بـــرای جلوگیری از بروز چنین خبر چینی‌های در رایانه‌های خویش انواع دیوارهای آتش و نرم‌افزار ضد جاسوسی را نصب می‌کنیم.

تعریف شورای اروپا از جاسوسی رایانه‌ای

شورای اروپا جاسوسی رایانه‌ای را اینگونه تعریف می‌کند که «تفتیش و بررسی ابزارهای لازم یا افشـــا یا انتقال یا اســـتفاده از اسرار تجاری یا بازرگانی بدون حق یا بدون هیچ توجیه قانونی دیگر با قصد خواه ایجاد ضرر اقتصادی به شـــخص حق اســـرار و خواه به قصد کسب یک منفعت اقتصادی غیر قانونی برای خود یا دیگران.

در این تعریف عملا این تعریف را از موارد دیگر اسرار من جمله اسرار امنیتی و اطلاعاتی و حتی فرهنگی خارج گردد و شامل موارد دیگر نمی‌شود که این ابزار است و با عنوان جاسوسی رایانه‌ای هماهنگـــی ندارد ثانیا در مورد قصد مرتکب از ارتکاب این جرم که در تعریف فقط منافع اقتصادی مدنظر قرار گرفته که این نیز درست به نظر نمی‌رسد چرا که ممکن است خود جاسوس به خاطر و قصد مســـائل غیراقتصادی و صرفا مســـائل ملی و یا حتی اذیت کردن اقدام کند که مشمول این موارد هم نمی‌شـــود ثانی در این تعریف در اصل تعریف جاسوســـی رایانه‌ای بیان نشده است بلکه صرفا مصادیق جاسوسی رایانه‌ای آن هم نه کامل بیان شده که به نظردرست نمی‌رسد.

از ســـال ۱۹۸۵ تا ۱۹۸۹ کمیته ی برگزیده ی کارشناسان جرایم رایانه‌ای شورای اروپا به بحث درباره ی مسائل حقوقی جرایم رایانه‌ای پرداختند. این کمیته در فهرستی تحت عناوین "فهرست حداقل" و "فهرســـت اختیاری" را به شـــورای را به شورای اروپا پیشنهاد کرد که مورد تصویب واقع شد که در بند (ب) فهرست اختیاری، جاسوسی رایانه‌ای را داین گونه تعریف می‌کند: (جاسوسی رایانه‌ای عبارت است از کسب اسرار حرفه‌ای یا تجاری از راه‌های نادرست یا افشاء انتقال و یا استفاده از این اسرار بدون داشتن حق یا هرگونه توجیه قانونی، با قصد وارد کردن زیان اقتصادی به فردی که محق در نگه داشتن اسرار است یا تحصیل یک امتیاز اقتصادی برای خود و یا یک شخص ثالث).

با توجه به اینکه جرم جاسوســـی ســـنتی و جاسوسی رایانه‌ای سنتی دارای عنصر مادی یکسان هستند قانون گذار هم در هنگام وضع ماده ۷۸۰ قانون مجازات اسلامی به این موضوع توجه داشته

است. در ماده ی مزبور مقرر شده (در مواردی که سیستم رایانه‌ای یا مخابراتی به عنوان وسیله ارتکاب جرم بکار رفته و در این قانون برای عمل مزبور مجازاتی پیش بینی نشده است، مطابق قوانین جزایی مربوط عمل خواهد شد).

از عبارت قانون گذار می‌توان چنین استنباط کرد که اصولا در جرایمی که از رایانه به عنوان وسیله‌ای در جهت ارتکاب به آن جرایم بکار می‌رود با جرایمی که از رایانه استفاده نشده تفاوت ماهوی خاصی وجود ندارد. از جمله قوانینی که بنظر می‌رسد جاسوسی سنتی رایانه‌ای را به عنوان وسیله‌ای در جهت ارتکاب جرم و برداشت اطلاعات استفاده می‌شود مورد توجه قرار داده است. ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح مصوب ۹ دی ۱۳۸۲ است. در این ماده قانون گذار مجازات تسلیم اطلاعات طبقه بندی شده رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند را به مجازات جاسوسی سنتی احاله داده است. با توجه به نص صریح فصل جرایم رایانه‌ای قانون مجازات اسلامی، در مواردی که شخص نظامی از رایانه مانند سایر ابزار به عنوان وسیله ی ارتکاب جرم جاسوسی استفاده کند بر اساس ماده‌ی ۷۸۰ قانون فوق الذکر، ماده ی ۱۳۱ قانون مجازات جرایم نیروهای مسلح حاکم خواهد بود و مرتکب مشمول مجازات‌های مقرره در هر مورد خاص است. اما در صورتی که شخصی نظامی از رایانه نه به عنوان وسیله بلکه فراتر از آن و به عنوان موضوع جرم استفاده کند و به اطلاعات موجود در آن بدون این که مجوز دسترسی به آنها را داشته باشد دست یابد، طبق ماده ی ۷۵٤ قانون مجازات اسلامی از موجبات تشدید مجازات مرتکب خواهد بود. در معنی وسیع، کلمه کی جاسوسی دو دسته اقدام را شامل می‌شود: دسته ی اول، اقدامات مقدماتی که عبارت از تفحص و تحصیل اطلاعات مخفی است، دسته ی دوم عملیات اجرایی است که ایجاد ارتباط و رساندن اطلاعات مزبور به کسانی است که باید از آن بهره برداری کنند. دسته اول اقدامات مقدماتی جاسوسی ممکن است متضمن قصد جاسوسی نباشد. به عنوان مثال متهم صرفا از لحاظ کنجکاوی میل به دانستن یا اینکه حسب غفلت یا بی احتیاطی اقدام کرده است. اما دسته ی دوم (عملیات اجرایی جاسوسی) همیشه کاشف از وجود اراده ی خاصی به آگاه کردن یک کشور خارجی و اسرار کشور دیگر و انتفاع از آن‌ها به ضرر کشور است. در حقوق ایران معنای جاسوسی تا کنون با معنای دوم انطباق داشته است. چنانچه موارد ۵۰۱ و ۵۰۲ قانون مجازات اسلامی و ماده‌ی ۳٤ مجازات جرایم نیروهای مسلح بر این امر دلالت دارند (رهامی، ۱۳۹۱: ۱۸۰).

ارکان جاسوسی رایانه‌ای

هرچند جاسوسی عمدتاً توسط سازمان‌های جاسوسی دولتی صورت می‌گیرد و در این میان جاسوسی‌های بی شمار کشورهایی نظیر ایالات متحده و اتحاد جماهیر شوروی در دهه هشتاد قرن بیستم میلادی، این دوران را به دهه جاسوسی معروف کرده اما این جرم در کشورهای مختلف و توسط افراد و سازمان‌های گوناگون نیز ارتکاب می‌یابد. به ویژه با رایانه‌ای شدن امور و تجهیز مراکز دولتی حساس به رایانه و اینترنت، احتمال وقوع جاسوسی به نسبت گذشته افزایش یافته است. با این تفاوت که درفضای سایبر که هر لحظه مقیاس عظیمی از اطلاعات مبادله می‌شوند، ارتکاب جاسوسی از هر کاربر اینترنتی که خلاقیت نفوذ در سیستم داشته باشد، بر می‌آید. جاسوس رایانه‌ای نه منحصراً از طرف دولت یا شرکتی خاص مامور به جاسوسی است و نه اینکه لزوماً قصد ابتدایی اش نفوذ به سیستم رایانه‌ای متضمن اطلاعات حساس یا طبقه بندی شده است، بلکه در برخی موارد کسب اطلاع در فضای سایبر بدون نیت سوء ضد امنیت ملی داشته باشد. جاسوسی رایانه‌ای در گام نخست متضمن نفوذ یا دستیابی غیرمجاز به سیستم رایانه‌ای یا حامل داده است که اطلاعات طبقه بندی یا داده‌های حساس در آن ذخیره یا پردازش شده باشند. بنابراین هک یا نفوذ به سیستم رایانه‌ای معمولاً مقدمه جاسوسی است. اما دستیابی به سیستم و جمع آوری اطلاعات می‌تواند به طرق مختلفی صورت بگیرد که مهمترین آنها عبارتند از:

الف- مهندسی اجتماعی: حملات مهندسی اجتماعی عبارت است از روند نفوذ به سیستم‌های رایانه‌ای از طریق کاربرد حیله‌های گوناگون در خصوص افراد جهت افشای کلمات عبور و اطلاعات مربوط به موارد آسیب پذیر شبکه. مهندسی اجتماعی نوعی نفوذ غیرمجاز یا هک شفاهی به شمار می‌رود که در آن مرتکب با تماس تلفنی یا ارتباط از طریق پست اینترنتی یا گپ زنی و با معرفی خود به عنوان یکی از کارکنان شرکت یا یک شخص معتبر سعی در تخلیه اطلاعاتی مخاطب خود پیرامون سیستم رایانه‌ای مربوطه می‌کند. در مهندسی اجتماعی، مرتکب قبل از اینکه به دانش فنی مربوط به نفوذ به سیستم رایانه‌ای متکی باشد، متکی به میزان نفوذ کلامی یا رفتاری خویش است. گفتنی است که صید اطلاعات مالی نوعی مهندسی اجتماعی به شمار می‌رود که با توجه به جنبه مالی آن شیوه مناسبی برای جاسوسی‌های صنعتی و تجاری است.

ب- به کارگیری افزارهای جاسوسی: عبارت است از دستیابی غیرمجاز به سیستم با استفاده از افزارهای جاسوسی یا تروجان.

ج- افشـــای اطلاعات سیســـتم: عبارت است از افشـــای غیرمجاز اطلاعات سیستم اعم از اینکه دستیابی مجاز بوده است یا خیر.

د- ســـرقت اطلاعات: عبارت اســـت از تحصیل غیرمجاز اطلاعات از طریق دستیابی به سیستم دیگری.

ه- رهگیری داده: عبارتست از رد گیری و دریافت اطلاعات در حال انتقال به ویژه در شبکه‌های بی سیم.

همین طور ممکن اســـت جاسوسی از طریق ارسال پیام‌های ناخواسته الکترونیکی یا اسپم واقع شـــود. پیام‌های ناخواســـته هم می‌توانند حامل نرم افزارهای جاسوســـی باشند و هم ممکن است شـــرایط تخلیه اطلاعاتی دریافت کننده پیام ناخواسته را فراهم سازند و ساده تر از همه جاسوسی رایانه‌ای ممکن است با فریب یا تحریکی متصدی حفظ اطلاعات رایانه‌ای اعم از سیاسی، اقتصادی، و صنعتی روند رو به رشدی دارد.

تا پیش از تصویب قانون جرائم رایانه‌ای در سال ۱۳۸۸، علی رغم سکوت مقررات کیفری ایران اما به طور تلویحی می‌توان در قانون مجازات بزه‌های نیروهای مسلح مصوب ۱۳۸۲/۱۰/۹ از جاسوسی رایانه‌ای ســـراغ گرفت. ماده ۱۳۱ این قانون مقرر مـــی‌دارد: هرگونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تاخیر تاریخ نسبت به تاریخ حقیقی و نظایر آنکه به طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم افزارهای مربوط صورت گیرد و همچنین اقداماتی از قبیل تســـلیم اطلاعات طبقه بندی شـــده رایانه‌ای به دشـــمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند، افشاء غیرمجاز اطلاعات، سرقت اشیاء دارای ارزش اطلاعاتی مانند سی دی یا دیسکتهای حاوی اطلاعات یا معدوم کردن آن‌ها یا ســـوء اســـتفاده‌های مالی که نظامیان به وســـیله رایانه مرتکب شوند جرم محسوب و حسب مورد مشمول مجازات‌های مندرج در مواد مربوط به این قانون می‌باشند. ماده فوق در جایی که اشاره می‌کند: ... همچنین اقداماتی از قبیل تسلیم اطلاعات طبقه بندی شده رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند یا افشاء غیرمجاز اطلاعات ... به جاسوسی رایانه‌ای اشـــاره دارد. ماده مزبور در صدد جرم انگاری جدیدی برآمده تا بزه‌های نظامیان در فضای ســـایبر نیز مشـــمول تدابیر کیفری گردد؛ زیرا هرچند ماده مزبور کیفر را به مواد مربوطه ارجاع داده اما با جرم محســـوب کردن تســـلیم اطلاعات طبقه بندی شده رایانه‌ای یا افشای غیرمجاز اطلاعات، جرم انگاری جدیدی نموده که این خود الگویی برای جرم انگاری جاسوسی رایانه‌ای و تسری آن به افراد غیرنظامی اســـت. جاسوســـی رایانه‌ای نظامیان هم از نوع جاسوسی نظامی و سیاسی است و با

توجه به تعبیر «افشـــاء غیرمجاز اطلاعات» هم از نوع جاسوســـی صنعتی و اقتصادی. در ارتکاب این بزه‌های رایانه و سیستم در نقش وسیله جرم ظاهر می‌شود و در واقع وجه افتراق جاسوسی رایانه‌ای با جاسوســـی‌ای که در مواد قبل به کار برده شـــده، در عنصر وسیله جرم نهفته است. از آنجا که نفوذ یا ارســـال اطلاعات از طریق رایانه ســـریع و راحت است، قانونگذار به جای اینکه این حالت را کیفیت مشـــدده مجازات تلقی نماید مبادرت به جرم انگاری آن نموده اســـت. با توجه به اطلاق ماده ۱۳۱، دارنده اطلاعات طبقه بندی شـــده اعم اســـت از کســـی که به امانت آنها را در دست دارد یا اتفاقاً به آنها دســـت یافته اســـت اما به هر حال این ماده به طور کامل به مصادیق جاسوسی رایانه‌ای نظامیان نپرداخته (به شکلی که ماده ۲۴ قانون مورد بحث به جاسوس پرداخته)؛ چون صرفاً به مرحله نهایی جاسوســـی از طریق رایانه اشـــاره کرده و رفتارهای مقدماتی مانند نفوذ غیر مجاز به سیســـتم حامل اطلاعات طبقه بندی شده یا جمع آوری آنها را در نظر نگرفته است.

انواع جاسوسی رایانه‌ای

پیش از پرداختن به انواع جاسوســـی‌ها باید ذکر کنیم که این تفکیک انواع جاسوســـی بر مبنای روش‌های ارتکاب جرم انجام شده است. یعنی ملاک تفکیک نوعی از نوع دیگر، روش مورد استفاده بوده اســـت و می‌بینیم که زمانی که جاسوســـی از طریق نصب برنامه بر روی کامپیوتر در فضای مجازی رخ می‌دهد دقیقت نقطه تفکیک دو نوع عمده جاسوسی اینترنتی و رایانه‌ای است. در مورد راههای انجام جاسوسی رایانه‌ای می‌توان به موارد زیر اشاره کرد:

۱-رایـــج تین راه جاسوســـی رایانـــه ای، کپی کردن فایل‌های داده اســـت به خصوص در زمینه برنامه‌هایی که به تعداد انبوه تولید و به فروش می‌رسند. در خصوص برنامه‌هایی که به تعداد انبوه تولید نمی‌شوند و دیگر داده‌ها، کپی کردن عمدتا به وسیله برنامه‌های کمکی یا بوسیله برنامه‌های خودساخته، صورت می‌گیرد.

۲-نوع دیگر جاسوسی رایانه ای، جاسوسی شخصی سنتی است که آن هم به دو دسته جاسوسی شـــخصی سنتی و جاسوسی فنی سنتی تقسیم میشود: جاسوسی شخصی سنتی: روش‌های این نوع جاسوســـی عبارت اند از رشـــوه دادن به کارمندان یا اخاذی از آنها، فرستادن مأمور در قالـــب کارمند تازه وارد برای دوره‌های کوتاه کاری (این روش به ســـلام - خداحافظ معروف است) یا به وسیله مصاحبه با کارمندان شرکت موردنظر که در جستجوی کار جدید به سراغ آگهی‌های دروغین می‌آیند و در ضمن مصاحبه وضعیت فعلی کارشان هم توصیف می‌کنند.

موضوع جرم جاسوسی رایانه‌ای

موضوع بزه جاسوســـی رایانه ای، داده‌های سری هستند. طبق تبصره ۱ ماده ۳، داده‌های سری داده‌هایی اســـت که افشـــای آنها به امنیت کشـــور یا منافع ملی لطمه می‌زند. سری بودن، ویژگی اطلاعات دارای ارزش سیاسی است. دلیل پیش بینی جاسوسی رایانه‌ای در قانون جرائم رایانه‌ای و پیرو آن داده‌ها در قانون ماده پیش گفته، خاموشی قانون مجازات انتشار و افشای اسناد محرمانه و ســـری دولتی مصوب ۱۳۵۳ درباره داده‌های ســـری است. این قانون به اسناد پرداخته و تعریفی که از آن به دســـت داده اســـت، داده‌های دارای ارزش اطلاعاتی را در بر نمی‌گیرد. طبق ماده یک این قانون، اســـناد دولتی عبارتند از هر نوع نوشـــته یا اطلاعات ثبت یا ضبط شده مربوط به وظایف و فعالیت‌های وزارتخانه‌ها و موسســـات دولتی و وابســـته به دولت و شـــرکت‌های دولتی از قبیل مراســـلات، دفاتر، پرونده، عکس‌ها، نقشـــه‌ها، کلیشه‌ها، نمودارها، فیلم‌ها، میکروفیلم‌ها و نوارهای ضبط صوت که در مراجع مذکور تهیه و یا به آن رسیده باشد. دلیل پیش بینی داده‌های سری نیز بیرون کردن داده‌های محرمانه از تنگنای پشتیبانی کیفری است؛ زیرا گستره داده‌های محرمانه به اندازه‌ای است که می‌توان هر اطلاعاتی را در زیر آن قرار داد و چون در رویه نیز، برچسب محرمانه بودن بدون نیاز و توجیه بر روی اســـناد قرار می‌گیرد، در قانون جرائم رایانه‌ای به داده‌های ســـری بســـنده شده است. داده‌های سری نیز با پشـــتوانه قانون مجازات انتشار و افشای اسناد محرمانه و ســـری تعریف شـــده اســـت. بر پایه دنباله ماده یک این قانون اسناد دولتی سری اسنادی است که افشای آنها مغایر با مصالح دولت و یا مملکت باشد. اسناد دولتی محرمانه اسنادی است که افشای آنها مغایر با مصالح خاص اداری سازمانهای مذکور در این ماده باشد.

جرم‌یابی رایانه‌ای

واژه لاتینی Forênsis ریشه لغت فارنزیک (Forensic یا Forensics2) بوده که به معنای «در حضور دادگاه یا دیوان» است[1]. در کاربرد جدید، اصطلاح فارنزیک (یا فورنزیکس) مترادف است با «عدله قانونی» یا «مربوط به دادگاه». از آنجا که در عصر حاضر این اصطلاح پیوند نزدیکی با علوم برقرار کرده به عنوان علم فارنزیک هم از آن یاد می‌شود.

---

۱. در روم باســـتان اتهامـــات جنایـــی در انجمنی عام (Forum A) در حضور مردم مطرح می‌شـــد و در آنجا متهم و متهمّ‌علیـــه بایـــد به طرح اســـتدلال‌های خود در دفاع از خود یا علیه دیگری می‌پرداختند. هر طرف که از اســـتدلال قوی‌تری برخوردار می‌بود، می‌توانست برنده دعوا باشد.

علم فارنزیک در مفهوم عام شامل جمع‌آوری، حفظ و ارزیابی مدارک و شواهد، بررسی و تجزیه و تحلیل داده‌های پیدا و پنهان به صورت علمی و طبق موازین حقوقی به منظور ارائه به مراجع ذی‌صلاح است. این علم شامل چندین شاخه اصلی می‌شود. موارد زیر از جمله مهم‌ترین آنها به حساب می‌آیند:

فارنزیک علوم فیزیولوژیکی که به زیرشاخه‌هایی نظیر فارنزیک شیمی، بیولوژی، دندانپزشکی و نظایر آن تقسیم می‌شود.

فارنزیک علوم رفتاری که فارنزیک روانشناسی از زیرمجموعه‌های اصلی آن است.

فارنزیک دیجیتالی که دربرگیرنده فارنزیک رایانه‌ای، صوتی و تصویری، تلفن‌های همراه، پایگاه داده‌ها و نظایر آن است.

فارنزیک دیجیتالی طبق تعریف مرکز ملی علوم فارنزیک مستقر در دانشگاه فلوریدای مرکزی[1] آمریکا عبارت است از: [فرآیند] شناسایی، جمع‌آوری، حفظ و نگهداری، بررسی و تجزیه و تحلیل مدارک دیجیتالی. بنا بر تعریف همین مرکز، هر گونه اطلاعات قابل استناد ارزشمندی که ذخیره یا به صورت باینری جابه‌جا شده‌اند، جزو مدارک دیجیتالی به شمار می‌روند. این مدارک نه‌تنها رایانه‌ها را در مفهوم رایج آنها (رایانه‌های شخصی و سرورها) دربر می‌گیرند بلکه شامل صدا و تصویر گرافیکی و فیلم‌های دیجیتال نیز می‌شوند.

فارنزیک رایانه‌ای به طور مشخص دربرگیرنده فرآیندی روش‌مند از جمع‌آوری و تجزیه و تحلیل داده‌های سیستم‌ها، شبکه‌ها، تبادلات بی‌سیم و وسایل ذخیره‌سازی رایانه‌ای است که طی آن عناصر حقوقی و علوم رایانه‌ای با یکدیگر ترکیب می‌شوند تا مدارک محکمه‌پسندی به مراجع قضایی ارائه شود. در واقع هدف اصلی از کاربرد دانش فارنزیک رایانه‌ای تضمین صحت و قابل اطمینان بودن مدارک ارائه‌شده به مراجع رسیدگی‌کننده به جرائم مربوطه است.

جنبه حقوقی فارنزیک رایانه ای

از موارد مهم حقوقی مطرح در جرم یابی یا فارنزیک دیجیتال اصل رعایت حریم خصوصی اشخاص است. طبق موازین اکثر نظام‌های حقوقی، تمامی سازمان‌ها، تشکیلات و سامانه‌های رایانه‌ای موظف به رعایت این اصل با حفظ و تامین امنیت داده‌ها و اطلاعات اشخاص، که به صور

1. National Center For Forensic Science (NCFS) At The University Of Central Florida (Www.Ncfs.Org)

مختلف نزد آنها قرار گرفته اســـت، هســـتند. رعایت ملاحظات حقوقی چنین اصلی ضمن کمک به بالا بردن سطح اعتماد به این سازمان‌ها و تشکیلات، در صورت بروز اتفاقی برای داده‌ها و اطلاعات، کمک خواهد کرد از بار مسوولیت‌های حقوقی آنها در قبال خسارت‌های احتمالی کاسته شود.

اگرچه اصل رعایت حریم خصوصی اشخاص (چه حقیقی و چه حقوقی) از اصول مهم گنجانده‌شده در نظام‌های حقوقی دنیای امروز اســـت اما به نظر می‌رســـد برخورداری کامل از این حق اساســـی با مجهز شـــدن دنیای مدرن به ابزارهای پیشـــرفته رایانه‌ای و گسترش فضاهای مجازی، با مشکل جدی مواجه شده است. حداقل در فضاها و شبکه‌های مجازی رایانه‌ای موجود به نظر تحقق کامل آن چون رویایی دست‌نیافتنی است.

پیشینه تحقیق

مرتضوی و همکاران (۱۴۰۰)، پژوهشی با عنوان "سناریوهای پیشگیری از جرایم سایبری" انجام داد. براساس یافته‌های این پژوهش، ۳۱ عامل موثر بر پیشگیری از جرایم سایبری که عبارت است از: فرهنگ ســـازی و تولید رســـانه ای، اســـتفاده از ابزارهای امنیتی توسط کاربران، افزایش میزان تلاش برای ارتکاب جرم، کاهش عوامل محرک جرم، در اختیار داشتن نرم افزارها و سخت افزارهای پیشـــرفته و به روز، رصد و پایش ســـایت‌های اینترنتی و شبکه‌های اجتماعی مجازی، بهره برداری از اقدامات فنی و مخابراتی و... شناســـایی شـــد و در ادامه با توجه به دو عامل راهبردی در اختیار داشـــتن نیروها ی متخصص و آموزش دیده و ســـواد رســـانه‌ای چهار سناریوی سازگار با دو متغیر راهبردی شناســـایی گردید و مطابق با آن سناریوی مطلوب پیشگیری از جرایم سایبری سناریوی اول می‌باشـــد که در اختیار داشـــتن نیروهای متخصص و آموزش دیده و سواد رسانه‌ای هر دو در وضعیت مطلوب قرار دارند.

عرب‌زاده و همکاران (۱۳۹۹)، پژوهشـــی با عنوان "پیشـــگیری کیفری در حوزه جرایم فناوری اطلاعات باتاکید بر پیشگیری از تروریسم سایبری" انجام داد.این پژوهش در پی آن است با روش توصیفی از یک سو به بررسی انواع پیشگیری در حوزه جرایم فناوری اطلاعات بپردازد و همچنین راهکارهایی جهت رفع نواقص آن بیان دارد که از آن جمله میتوان به تدوین قوانین کارامد وتقویت علم پلیسی در این زمینه اشاره کرد و از سوی دیگر پیشگیری از تروریسم سایبری را به عنوان یکی از جرایم مهم این حوزه با نگاهی به اساســـنامه دیوان کیفری بینالمللی و پیش نویس کنوانســـیون جامع مقابله با تروریسم بین‌المللی ، مورد بررسی قرار دهد.

صبوری (۱۳۹۸) پژوهشـــی با عنوان بررســـی جرائم ســـایبری حوزه اجتماعـــی و راهبردهای پیشـــگیری و مقابله با آن در جمهوری اســـلامی ایران انجام داد. این پژوهش با هدف دســـتیابی به راهبردهای پیشـــگیری و مقابله با جرائم سایبری حوزه اجتماعی در جمهوری اسلامی ایران انجام گردید. روش این پژوهش «توصیفی-تحلیلی» از نوع «پیمایشـــی و اسنادی» است. یافته‌ها حاکی از این اســـت که حوزه اجتماعی فضای ســـایبر جمهوری اســـلامی ایران دارای موقعیت راهبردی رقابتی بوده و برای پیشگیری و مقابله با جرائم سایبری این حوزه لازم است تعداد ۱۲ راهبرد برتر احصاشده مورد استفاده قرار گیرد.

روش تحقیق

تحقیق حاضر از نوع مطالعات توصیفی- تحلیلی با تکنیک پیمایشـــی اســـت. براســـاس این نوع تحقیق از روش تحقیق کتابخانه‌ای و اســـنادی اســـتفاده شده است. که طبق آن با مراجعه به منابع و ماخذ علمی شامل کتاب، مجله‌ها و نشریات ادواری موجود در کتابخانه‌ها و همچنین سایت‌های اینترنتی حاوی تحقیقات و مقالات علمی معتبر اطلاعات مورد نیاز تحقیق گردآوری شـــده است. در این روش، برای جمع آوری اطلاعات بعد از ماخذشناسی و گردآوری منابع، از ابزارهای فیش و فرم‌های مربوط به نکته برداری استفاده شده است.

یافته‌های تحقیق

پیشگیری از جرائم سایبر

فضای ســـایبر همانند دیگر عناصر زندگی اجتماعی، از گزند یک پدیده بســـیار انعطاف پذیر و لاینفک از اجتماع به نام جرم در امان نمانده است. به طور کلی، آنچه امروز تحت عنوان جرم سایبر قرار می‌گیرد، دو طیف از جرائم اســـت: گروه اول جرائمی هســـتند که نظایر آنها در دنیای فیزیکی نیز وجود دارد و فضای ســـایبر بدون تغییر ارکان مجرمانه شـــان، با امکاناتی که در اختیار مجرمان قرار می‌دهد، ارتکابشـــان را تســـهیل می‌کند. جرائم تحت شمول این حوزه بسیار گسترده اند و از جرائم علیه امنیت ملی و حتی بین‌المللی نظیر اقدامات تروریســـتی گرفته تا جرائم علیه اموال و اشـــخاص را در بر میگیرند. نمونه‌ای از این طیف، تشـــویش اذهان عمومی از طریق سایبر است. اما طیف دیگر جرائم سایبر، به سوءاستفاده‌های منحصر از این فضا مربوط می‌شود که امکان ارتکاب آنها در فضای فیزیکی میســـر نیست. جرائمی نظیر دسترســـی غیرمجاز به داده‌ها یا سیستم‌ها یا

پخش برنامه‌های مخرب نظیر ویروس‌ها، جز در فضای سایبر قابلیت ارتکاب ندارند و به همین دلیل به آنها جرائم سایبری محض نیز گفته می‌شود (جلالی فراهانی، ۱۳۸۹: ۱۳۶). همانگونه که ملاحظه می‌شود، به لحاظ امکان سوءاستفاده دو جانبه‌ای که از فضای سایبر وجود دارد، ضروری است برای آن چاره‌ای اندیشیده شود. با توجه به رویکرد کلی مقابله با جرائم که در دهه‌های اخیر شاهد تحولات شگرفی نیز بوده است، می‌توان دو گزینه را پیش رو قرار داد که عبارتند از: اقدامات کیفری و غیرکیفری. در زمینه اقدامات کیفری سعی می‌شود از طریق جرم انگاری هنجارشکنی‌ها و سوء استفاده‌های جدید و یا تجدیدنظر در قوانین کیفری گذشته، ارعاب انگیزی موثری درباره مجرمان بالقوه یا مکرر صورت گیرد تا به این ترتیب، از ارتکاب جرم بازداشته شود (نیازپور، ۱۳۸۲: ۱۲۴). اما رویکرد دوم که در بستر جرم شناسی تبلور یافته و با الهام از علوم دیگر نظیر پزشکی، روان شناسی، جامعه شناسی و ... پدید آمده، در این زمینه، تاکنون الگوهای مختلفی در عرصه جرم شناسی پیشگیرانه ارائه شده و مورد آزمون قرار گرفته است. از مهم ترین و موثرترین این الگوها می‌توان به پیشگیری اجتماعی و پیشگیری وضعی از جرائم اشاره کرد. به طور خلاصه، در پیشگیری اجتماعی سعی براین است که با افزایش آگاهی افراد و تربیت صحیح آنها، به ویژه قشر جوان و نوجوان جامعه و همچنین از بین بردن زمینه‌های اجتماعی وقوع جرم، نظیر فقر و بیکاری، انگیزه‌های مجرمانه از مجرمان سلب گردد. اما در پیشگیری وضعی، هدف سلب فرصت و ابزار ارتکاب جرم از مجرم یا انگیزه است (نجفی ابرند آبادی، ۱۳۹۶: ۱۰۸۲). با اینکه اتخاذ تدابیر پیشگیرانه نسبت به اقدامات کیفری از محاسن بسیاری برخوردار است، نباید از یاد برد که در اینجا نیز باید اصول و هنجارها را رعایت کرد. سیاستهای پیشگیری، به ویژه پیشگیری وضعی، برخلاف سیاستهای کیفری، تمامی افراد جامعه را در بر می‌گیرند، زیرا پرواضح است که شناسایی مجرمان بالقوه امکان پذیر نیست. لذا این اقدامات باید به نحوی اجرا شوند که افراد جامعه از حقوق اساسی شان محروم نگردند (نجفی ابرند آبادی، ۱۳۹۶: ۵۵۹).

از لحاظ منطقه‌ای و بین‌المللی یکی از اولین اقداماتی که در زمینه پیشگیری انجام گرفته، گزارش جرائم رایانه‌ای بودکه این گزارش تحلیل سیاست‌های قانونی، سازمان همکاری و توسعه اقتصادی اروپا بود که در سال ۱۹۸۶ میلادی منتشر شد. این یکی از اقداماتی است که برای روشن شدن جرائم رایانه‌ای صورت گرفت. در این نوع سند پنج نوع رفتار ذکر شد که قابلیت جرم انگاری تحت عنوان جرائم رایانه‌ای را داشتند. اولین مورد ورود، پاک کردن و یا متوقف سازی داده‌ها و برنامه‌های رایانه‌ای است که به طور عمدی و با قصد غیرقانونی انتقال وجوه یا هر چیز با ارزش دیگر

انجام می‌شود. دومین مورد ورود، پاک کردن و یا متوقف کردن داده‌ها و برنامه‌های رایانه‌ای است که به قصد جعل باشد. سوم، ورود، پاک کردن و یا متوقف کردن داده‌ها و برنامه‌های رایانه‌ای است که به صورت عمدی و با قصد جلوگیری از عملکرد سیستم رایانه‌ای و مخابراتی صورت می‌گیرد. چهارمین مورد تجاوز به حقوق انحصاری مالک یک برنامه رایانه‌ای است که مورد حمایت واقع شده است و قصد سوددهی تجاری دارد. آخرین مورد هم مربوط به دست یابی یا شنود در یک سیستم رایانه‌ای یا ارتباطی است که معمولاً به صورت آگاهانه و بدون کسب مجوز از دستگاه‌های مربوط اتفاق می‌افتد. دست یابی یا شنود در یک سیستم رایانه‌ای یعنی این که شخص دست به کاری بزند که وارد سیستم رایانه‌ای شود و یا شنود کند. چه با تلخی از تدابیر امنیتی باشد و چه با اهداف غیر شرافتمندانه اتفاق افتاده باشد. توصیه‌ای که از طرف کمیته شورای وزیران اروپا صورت گرفت بدین صورت است که در مورد جرائم رایانه‌ای یک فهرست حداقل و اختیاری، شامل دو دسته از جرائم رایانه‌ای را ارائه داده بود. فهرست حداقل این توصیه نامه عبارتند از کلاهبرداری رایانه ای، جعل رایانه ای، واردکردن خسارت به داده‌ها یا برنامه‌های رایانه ای، خراب کاری رایانه ای، دست یابی غیرمجاز رایانه ای، شنود غیرمجاز رایانه ای، تکثیر غیرمجاز برنامه حمایتی رایانه‌ای یا تکثیر غیرمجاز توپوگرافی. توصیه دیگر در رابطه با مشکلات آیین دادرسی کیفری در رابطه با فناوری اطلاعات بود (اینترنت و فضای مجازی) که باز هم از سوی همین شورا ارائه شد.

اقدامات و تدابیر پیشگیرانه در راستای مبارزه با جاسوسی رایانه ای

متخصصان معتقدند جرم جاسوسی رایانه ای، با شدت و پیچیدگی بیشتری در سطح وسیع جهانی ادامه پیدا خواهد کرد. رفته رفته جاسوسی سایبری به عنوان ابزاری برای حصول برتری در رقابت بی پایان کشورها در زمینه‌های صنعتی، اقتصادی، نظامی و ... تبدیل خواهد شد و کشورهای بیشتری وارد صحنه کارزار 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 و رایانه است، عوامل جاسوسی رایانه‌ای و سایبری نقش پیاده نظام این جنگ پسامدرن را بازی می‌کنند. پس با عنایت بر اهمیت به سزای این تکنولوژی در تمامی ابعاد زندگی بشر و بقای دولت‌ها، گام نهادن در راستای ایمن سازی بنیادین این فضا و کاستن مخاطرات احتمالی آن نه تنها لازم بلکه واجب است. برای نمونه در کشور ما، ایران، تبصره ماده ۳۰ ق.ج.ر. قوه قضائیه را مکلف کرده تا قضاتی را که با امور رایانه‌ای آشنایی دارند را برای رسیدگی به این جرائم انتخاب کند. در این خصوص گفتنی است

قوه قضائیه از سال ۱۳۸۲ با برگزاری کلاس‌های آموزش ضمن خدمت قضات، دو عنوان درسی آموزشی در خلال برنامه‌های این دوره گنجانده که عبارتند از: «جرائم سایبری» برای قضات کیفری و دعاوی حقوقی (حقوق فناوری اطلاعات برای قضات حقوقی). در دوره جرائم سایبری کلیاتی در خصوص ادوار زمانی استفاده از رایانه و مسائل جزایی ناشی از آن، تقسیم بندی و شرح مختصر انواع جرائم سایبری و ماهیت آنها، آیین رسیدگی به این جرائم و صلاحیت سایبری مطرح می‌گردد. در مقابل در دوره دعاوی حقوقی به مسائلی از جمله قراردادهای انفورماتیک، مسئولیت مدنی در محیط دیجیتال و ... پرداخته می‌شود. در حال حاضر با عنایت به پیشرفت‌های لحظه‌ای در عرصه رایانه و فضای سایبر ضرورت این آموزش‌ها بیش از پیش مشخص شده و برای اجرای یک سیاست کیفری مؤثر جهت پیشگیری از جرائم رایانه‌ای به خصوص جاسوسی رایانه‌ای و اینترنتی، این آموزش‌ها باید در مقاطع مختلف زمانی تکرار و روز آمد شوند. یقینا أین قبیل قانون گذاری‌ها و اقدامات بنیادین، اگر مستمر باشند، می‌توانند در رسیدن به اصل قدیمی پیشگیری همواره بهتر و به صرفه تر از درمان است، مؤثر باشند. حال با توجه به مطالبی که گذشت، برای ارتقای سطح امنیت و کاستن از مخاطرات و جرائم برهم زننده امنیت از قبیل جاسوسی، در ذیل پیشنهاداتی ارائه می‌گردد تا شاید ما هم بتوانیم در برقراری بیشتر امنیت مؤثر باشیم. از آنجا که پلیس به عنوان ضابط دادگستری وظیفه کشف جرائم را بر عهده دارد، در کنار آموزش قضات و سایر مقدمات قضایی، آموزش و به روزرسانی اطلاعات پلیس نیز باید در سرفصل برنامه‌ریزی‌ها قرار گیرد.

- استمرار آموزش‌های عمومی در سطح کارمندان دولت و نظامیان و به روزرسانی اطلاعات آنها باید مد نظر قرار گیرد. - تا حد ممکن عدم ذخیره سازی داده‌ها و اطلاعات طبقه بندی شده و مهم به شبکه‌های رایانه‌ای به خصوص شبکه جهانی اینترنت
- عدم اتصال سیستم‌های رایانه‌ای دارای داده‌ها و اطلاعات طبقه بندی شده در رایانه‌ها و سایر سیستم‌های مخابراتی
- تشکیل هر چه سریع تر مراجع تخصصی قضایی و پلیس با عنایت به الزام قانونی ماده ۳۰ قانون جرائم رایانه‌ای و تقویت آنها.
- مسدود کردن درگاه‌های رایانه‌های حساس در ادارات به عنوان راهکاری سریع و کم هزینه و در عین حال مؤثر. در این روش تمامی درگاه‌های سیستم‌های رایانه‌ای از قبیل درایو CD، پورت‌های USB و از طریق رایانه سرور (شبکه) بسته شده و به این ترتیب کاربر رایانه نمی‌تواند هیچ داده و اطلاعاتی را وارد رایانه کرده و یا از آن خارج کند. در این حالت کاربر تنها

به داده‌های مجازی که از سوی مسئولان و به منظور انجام وظیفه روی سیستم او قرار داده شده، دسترسی خواهد داشت.

- بستر فرهنگی جامعه باید به گونه‌ای هدایت شود که هر کاربری بداند چگونه از رایانه و اینترنت استفاده کند تا اطلاعات مهم او حفظ شود. همچنین با توجه به گستردگی فضای مجازی و اینترنت، آموزش جنبه‌های مختلف آن از جمله کاربردها، آفت‌ها و سایر خطرها ضروری است. توجه به برخی نکات ساده مثل فاش نکردن گذرواژه‌های رایانه از الزامات است. در کل باید فرهنگ سازی‌ها مستمر و متناسب با زمان باشند.

- استفاده از تدابیر محدود کننده یا سلب کننده دسترسی می‌تواند راهکاری مفید باشد. این دسته از تدابیر در زمره مهم ترین تدابیر پیشگیرانه وضعی از جرائم سایبر قرار دارند. در این روش با نصب برنامه‌های خاص روی رایانه‌های شخصی و سیستم‌های ارائه دهنده خدمات شبکه‌ای از ورود یا ارسال برخی داده‌های غیر مجاز یا غیر قانونی جلوگیری می‌شود. این برنامه‌ها معمولا در سه قالب دیوارهای آتشین فیلترها و پراکسی‌ها هستند. این برنامه‌ها فهرستی از موضوعات مجاز یا غیر مجاز دارند و از ورودی‌ها و خروجی‌های غیر مجاز جلوگیری می‌کنند.

- به کار گیری تدابیر نظارتی خود راهی دیگر برای کنترل، پیشگیری و مبارزه با جرائم سایبری است. این اقدامات از دو بعد فنی و انسانی تشکیل شده است. در حالت فنی برنامه‌هایی روی سیستم نصب می‌شود و تمامی فعالیت‌های شبکه‌ای اشخاص، حتي ضربانی که بر روی صفحه کلیدشان زده اند یا نقاطی را که به وسیله موشواره روی آن کلیک کرده اند، ضبط می‌کنند و سپس مأمور مورد نظر (بعد انسانی) می‌تواند با بررسی این سوابق، موارد غیر قانونی را پیگیری و گزارش کند.

- راه دیگر، استفاده از تدابیر صدور مجوز است. در این روش از ورود اشخاص ناشناس یا فاقد اعتبار به یک سیستم رایانه‌ای با سایت جلوگیری می‌شود. نمونه ساده این اقدام به کار گیری گذرواژه است که از دیر باز متداول بوده است. به این ترتیب تنها کسانی حق بهره برداری از یک سیستم با سایت را خواهند داشت که پس از طی مراحل شناسایی و کسب اعتبار گذرواژه مربوطه را دریافت کنند.

- توصیه می‌گردد افراد و سازمان‌ها و ... برای انتقال فایل‌های خود از ابزارهای رمز کننده بهره گیرند. این ابزارها برنامه‌هایی هستند که به منظور انتقال ایمن محتوای ارتباطات رایانه‌ای

استفاده می‌شود. در این روش بر اساس کدهای خاصی متن اصلی به رمز نوشته تبدیل می‌شود و گیرنـــده در مقصد به وســـیله کلیـــدی که در اختیار دارد، آن را رمزگشـــایی می‌کند. مزیت این روش در این اســـت که با توجه به برنامه‌های متعددی که در فضای ســـایبر برای شـــنود و دســـتیابی به ارتباطات افراد وجود دارد بهره گیری از برنامه‌های رمزنگاری می‌تواند خطر این گونه تعرض‌ها را کاهش دهد.

نتیجه گیری

جاسوســـی رایانه‌ای یکی از جرائم رایانه‌ای اســـت که قدمتی دیرینه دارد و در امتداد تلاش‌های نظامی و سیاســـی برای کســـب اطلاع و آگاهی از طرف مقابل به‌هنگام جنگ یا هر رقابت دیگری به‌وجود آمده، اما با راه‌اندازی شبکه اینترنت این جرم هم ماهیتی متناسب با قالب فضای مجازی یافت و با تغییر و پیدایش روش‌های جدید که نتیجه فضای مجازی بود، به نوع نوینی از جاسوسی یعنی جاسوســـی اینترنتی یا ســـایبر تبدیل شد. اساساً باید بین جاسوســـی رایانه‌ای و جاسوسی اینترنتی تمایز قائل شـــد چراکه هم ماهیتاً و هم از لحاظ روش‌های مورد اســـتفاده، با جاسوســـی رایانه‌ای متفاوت اســـت. در جاسوسی رایانه‌ای به طور عمده از روش‌هایی مانند کپی کردن فایلها، جاسوسی سنتی، برداشت از افزارهایی که در خلال اتصال کاربر به شبکه بر رایانه ی او (با اجازه یا بی اجازه) نصب می‌شود، بررسی ایمیل‌های شخصی از طریق هک کردن رمزهای آن، مشاهده دقیق عملکرد کاربران و ســـرویس دهندگان اینترنت استفاده می‌شود. تفاوت اصلی و بنیادی جاسوسی رایانه‌ای با جاسوسی اینترنتی در این است که جاسوسی کامپیوتری نیاز به استخدام مزدور دارد و بدون عنصر واسط نمی‌توان به کسب اطلاعات نائل شد و قطعاً هزینه‌های مالی هم در بر دارد ولی با رشد اینترنت و فناوری و همچنین حرفه‌ای شدن ابزارها و روش‌های جاسوسی در فضای مجازی، جاسوســـان اینترنتی را از اســـتخدام مزدور و واســـط تا حد بسیاری بی نیاز کرده است و در بعضی موارد جاسوســـان خیلی راحت و با اجازه ی خود کاربران به سیســـتم او نفوذ کرده و به جمع آوری اطلاعات می‌پردازند. به عنوان یک نتیجه‌گیری کلی باید گفت لازم اســـت تدبیری اساســـی درباره جرائم مربوط به این حوزه اندیشـــیده شـــود. بااینکه در حال حاضر بسیاری از کشورها سعی کرده اند با وضع و اصلاح قوانین کیفری خود، امکان تعقیب و پیگرد و مجازات مجرمان سایبر را فراهم آورند، اما اجرای این قوانین با مشـــکلات عدیده‌ای مواجه بوده و همین امر باعث شـــده است بحث پیشـــگیری از جرائم ســـایبر اهمیت ویژه‌ای یابد. البته در این جا سه اصل مهم آزادی بیان، جریان

آزاد اطلاعات و حریم خصوصی نباید قربانی نظارت‌های بی مورد و اندیشـــه جرم انگارانه افراطی شود چون در حال حاضر کمتر کشوری را می‌توان یافت که در قانون اساسی یا قوانین عادی خود به این اصول نپرداخته باشـــد. قانون اساســـی کشور ما نیز، به این اصول توجه ویژه‌ای داشته است. در نهایت می‌توان گفت فناوری اطلاعات و ارتباطات موجب تغییر سریع ویژگی‌های سایر بخش‌ها از جمله حقوقی و قضایی شده که بیش تر به حفظ چارچوب‌های عمومی تمایل دارد، درحالی که جنس تکنولوژی، نوآوری اســـت که از طریق مرزشکنی اتفاق می‌افتد و شاید حضور این دو پدیده در کنار هم به معنای اصطکاک به نظر برسد؛ در این فضا جرم‌ها هم به تناسب رشد فناوری‌ها شکل جدیدتری به خود گرفتند، قضات و وکلا باید پاسخگوی تحولاتی باشند که تکنولوژی ایجاد کرده و در نتیجه باید خودشـــان را برای رویکرد پر شـــتاب آماده کننده و تجهیز نظام قضایی و آموزشی بیش از پیش مورد توجه قرار بگیرد.

فهرست منابع

- جلالی فراهانی، امیر حسین(۱۳۸۵). صلاحیت کیفری در فضای سایبر، فصل نامه فقه و حقوق، سال سوم شماره ۱۱.

- رهامی، محسن(۱۳۹۳). جاسوسی رایانه‌ای در حقوق ایران و وضعیت بین‌المللی آن. مجله دانکده حقوق و علوم سیاسی، ۴۲ (۳).

- زیبـــر، اولریش(۱۳۹۰). جرائم رایانه ای، ترجمه ی محمـــد علی نوری و دیگران، تهران، انتشارات گنج دانش، چاپ دوم.

- زینلی، (۱۳۹۸). ابعاد و مؤلفه‌های خودحفاظتی در پیشـــگیری از جاسوســـی (کارکنان پلیس آگاهی ناجا)، مجله کارآگاه، دوره دوم، سال نهم، شماره ۳۳.

- شـــجوده(۱۳۹۸). سایبر تروریسم: پندارها و واقعیت‌ها، برگردان اسماعیل بقایی‌هامانه و عباس باقر پور اردکانی، در مجموعه تروریســـم، گردآوری و ویرایش علیرضا طیب، نشـــر نی، چاپ دوم.

- صبوری، رضا و ثقفی، کامیار(۱۳۹۸). بررسی جرائم سایبری حوزه اجتماعی و راهبردهای پیشگیری و مقابله با آن در جمهوری اسلامی ایران،https://civilica.com/doc/۱۱۸۷۶۸۹

- عابدینـــی، زین العابدین(۱۳۸۸). جرم در فضای مجازی، ضـــرورت آینده پژوهی، مجله کارآگاه، دوره دوم، سال سوم، شماره ۹.

- عرب زاده کفاش، آزاده و بیگزاده، علی(۱۳۹۹).پیشگیری کیفری در حوزه جرایم فناوری اطلاعات باتاکید بر پیشـــگیری از تروریســـم سایبری، نخســـتین کنفرانس ملی حقوق، فقه و فرهنگ،شیراز،https://civilica.com/doc/۱۰۱۸۹۲۱

- مرتضوی، سیدمرتضی و مظفری، محمدمهدی و کشاورز ترک، محسن(۱۴۰۰). سناریوهای پیشگیری از جرایم سایبری،چهارمین کنفرانس بین‌المللی سالانه تحولات نوین در مدیریت، اقتصاد و حسابداری،تهران،https://civilica.com/doc/۱۲۶۸۲۶۲

- نجفی ابرند آبادی، علی حسین(۱۳۹۶). پیشگیری عادلانه از جرم، علوم جنایی، مجموعه

مقالات در تجلیل از استاد آشوری، تهران، انتشارات سمت، چاپ هفتم.

- نیازپور، امیرحســـین(۱۳۸۲). پیشگیری از بزهکاری در قانون اساسی و لایحه پیشگیری از وقوع جرم، مجله حقوقی دادگستری، شماره ۴۵.

- وارن، ماتئو،هاچینسون، ویلیام(۱۳۸۲). تروریسم شبکه ای، برگردان غلامرضا رفعت نژاد، گزارش راهبردی، انتشارات پژوهشکده مطالعات راهبردی.