جاسوسی رایانه‌ای ابزاری در حوزه جنگ نرم

(گونه شناسی، موانع حاکم بر تحقیقات و قوانین مترتب بر جاسوسی رایانه‌ای)

مسلم پیری زمانه*[۱]
داریوش پیری زمانه[۲]
کاوه قدمی[۳]
حمیدرضا بازگلی[۴]

چکیده:

در عصر حاضر جاسوسی و جمع آوری اطلاعات از طریق نیروی انسانی آموزش دیده یک امر سخت، وقت گیر، پر هزینه و خطرناک بوده و در صورت آشکار شدن و لو رفتن مأموریت هم برای کشور هدف و هم کشور مبدأ مسایلی را در سطح بین المللی به وجود می‌آورد، بنابراین کشورها در این راستا و با یک نگرش معقول، به این فکر افتادند که از راههای علمی، ساده و در نتیجه کم خطر (جاسوسی رایانه‌ای) برای جمع آوری اطلاعات از دیگر کشورها بهره برداری نمایند. در این مقاله سعی گردیده به دو سؤال ۱-

[۱]. دانشجوی دکتری مدیریت آموزشی دانشگاه علامه طباطبایی. نویسنده مسئول.
moslempiri62@yahoo.com
[۲]. کارشناسی ارشد حقوق جزا و جرم شناسی -دانشگاه پیام نور
Daryoosh.piri1981@gmail.com
[۳]. دانشجوی دکتری آموزش عالی دانشگاه علامه طباطبایی
kavehghadami@gmail.com
[۴]. دانشجوی دکتری مدیریت آموزشی دانشگاه آزاد
Hamidrezabazgoli@chmail.com

www.SID.ir

چیستی جاسوسی رایانه‌ای و ۲- انواع جاسوسی‌های رایانه‌ای شناخته شده و قوانین مرتبط با جاسوسی رایانه‌ای پاسخ داده شود. روش تحقیق به کارگرفته شده در این مقاله از نوع توصیفی و تحلیلی بوده و منابع جمع آوری اطلاعات از طریق مطالعات کتابخانه‌ای و اینترنتی می‌باشد. با توجه به مطالب مطرح شده می‌توان نتیجه گیری نمود که در دنیای پیشرفته امروزی با توجه به پیشرفت و توسعه فناوری‌های مختلف در عرصه‌های جاسوسی نیز انواع روش‌ها و تجهیزات به کار گرفته می‌شود و به طور کلی می‌توان اذعان داشت که در این عرصه از جنگ نرم، شیوه‌های جاسوسی هم در هدف و هم در مقاصد با روش‌های سنتی تفاوت ماهوی دارند.

کلید واژه‌ها: جنگ نرم، جاسوسی، جاسوسی رایانه‌ای، قوانین و مقررات

مقدمه:

تاریخ نشان می‌دهد که زندگی انسان بر روی زمین، به عنوان عضوی از جامعه‌ای که در آن زندگی می‌کند، مقتضی کسب اخبار قبلی درباره جایگاه کنونی و آینده وی بوده است. مطالعه رفتار انسانی نشان می‌دهد که انسان‌های نخستین نیز به اطلاعات گرایش داشته و به صورت ساده و ابتدایی آن را به کار بسته‌اند؛ و در حقیقت همان رفتارهای ساده و ابتدایی، به صورت گرایش به اطلاعات در روزگار نوین با ابعاد گوناگون نمود پیدا کرده است. از زمان‌های قدیم جاسوسی به عنوان ابزار قدرت نرم بین ملل مختلف وجود داشته است در زمان پیامبر اکرم (ص) افرادی به عنوان رابط و خبرچین به میان سپاه دشمن فرستاده می‌شدند تا اخبار و اطلاعات مربوط به تعداد و استعداد نیروها، محل استقرار و آرایش آنها را جمع آوری کنند. این شیوه را به طرق مختلف انجام می‌دادند مثلاً آن فرد فرستاده شده یا از افراد خودی بود که آموزش‌های لازم را دیده و بعد به میان سپاه دشمن فرستاده می‌شد یا اینکه از میان افراد دشمن انتخاب و جذب می‌شد از این روش‌ها امروزه نیز استفاده می‌شود. پیشرفت علم و تکنولوژی‌های جدید همواره یکی از دغدغه‌های بشر بوده است و تلاش مستمر دانشمندان و محققان برای دستیابی به فناوری‌های جدید هر روز دو چندان می‌شود اما از اتأثیرات مثبت این تکنولوژی‌ها که بگذریم نباید از آثار نامطلوب آن بر زندگی بشر غافل بود. حدود نیم قرن پیش، ابزاری بنام رایانه به جهانیان عرضه شد که با وجود قدرت محاسبه و پردازش بسیار کم آن نسبت به حساب‌های الکترونیکی کوچک امروزی، تحول عظیمی را نوید می‌داد (*casey- eoghan,2001*). عصر ارتباطات، همان عصری که در آن بسر می‌بریم، نماد شکوفایی استعدادهای بشری در پیشرفت و تکنولوژی و تبلور خلاقیت‌های مثبت و منفی انسانی است رایانه و اینترنت و دنیای مجازی یکی از هزاران ساخته دست بشر است که به منظور حل مشکلات و دستیابی آسان به اطلاعات و داده‌ها طراحی شده است و امروزه بدون وجود آن تقریباً هیچ کاری امکان‌پذیر نیست. یکی از این پیشرفت‌ها در عرصه جاسوسی است که شیوه‌های نوین و جدیدی نیز کشف شده است. به طوری که تقریباً می‌توان گفت در این عرصه‌ها هر چند وقت یک کشف جدید معرفی می‌شود. یکی از شیوه‌های

Archive of SID

www.SID.ir

جدید، جاسوسی از طریق رایانه یا جاسوسی رایانه‌ای می‌باشد. جاسوسی رایانه‌ای دارای ابعاد متفاوتی مثل بعد فنی و بعد حقوقی است که هر کدام از این ابعاد به طور کامل و دقیق در ذیل مورد بررسی قرار می‌گیرد.

با توجه به اینکه در حال حاضر به دلیل اینکه جاسوسی و جمع‌آوری اطلاعات از طریق نیروی انسانی آموزش‌دیده یک امر سخت، وقت گیر، پر هزینه و خطرناک از جهت آشکار شدن آن برای کشور مورد جاسوسی است (و باعث پیدایش تیرگی روابط سیاسی بین دو کشور می‌گردد) لذا کشورها در این راستا با یک نگرش معقول، به این فکر افتادند که از راههای علمی‌تر و ساده‌تر و در نتیجه کم خطرتر در راه جمع‌آوری اطلاعات از کشورهای دیگر استفاده کنند که امر جاسوسی از طریق رایانه از جمله این راهها است در حال حاضر تقریباً بیشتر کشورهای جهان از این شیوه نرم استفاده می‌کنند. اما در این میان وظیفه ما این است که این تهدیدات در حوزه جنگ نرم را به موقع بشناسیم و در رفع آن آماده، کوشا و پیگیر باشیم.

هدف:

بررسی جاسوسی رایانه‌ای به عنوان ابزار جنگ نرم و موانع حاکم بر تحقیقات و قوانین مترتب بر جاسوسی رایانه‌ای.

سؤالات تحقیق:

۱) آیا تعریف جاسوسی رایانه‌ای، یک امر اجمالی وکوتاه است یا اینکه برعکس وسیع و گسترده می‌باشد؟

۲) در صورت پیش بینی شدن موضوع جاسوسی رایانه‌ای در قانون جرائم رایانه‌ای نقاط قوت و ضعف آن کدامند؟

فرضیه‌های تحقیق:

۱- جاسوسی رایانه‌ای به عنوان ابزار جنگ نرم یک امر بسیار گسترده می‌باشد.

۲- با توجه به اینکه جاسوسی رایانه‌ای به عنوان ابزار جنگ نرم یک امر جدید می‌باشد، لذا قوانین مربوط به آن دارای نقاط ضعفی می‌باشد.

Archive of SID

www.SID.ir

روش تحقیق:

روش تحقیق توصیفی و تحلیلی و منابع جمع آوری اطلاعات به صورت کتابخانه‌ای و میدانی می‌باشد. در تحقیق حاضر از منابع کتابخانه‌ای، اینترنتی و همچنین تحقیق از مراجع رسیدگی کننده به صورت میدانی استفاده شده است. همچنین از مقالات موجود در مجلات معتبر، کتاب‌های اساتید معتبر و بنام، پایان نامه‌های کارشناسی ارشد و دکتری دانشجویان دانشگاه‌های معتبر و سایت‌های معتبر استفاده گردیده است.

پیشینه تحقیق:

تلاش‌های اطلاعاتی پیش از میلاد مسیح میان بسیاری از ملت‌ها رایج بوده و مصریان قدیم در این زمینه ابتکارهای زیادی داشته‌اند. رونالدیش می‌نویسد: اسناد مصر قدیم نشان می‌دهد که آنان در زمینه کارهای اطلاعاتی اقدام‌های برجسته‌ای داشته‌اند، در سال‌های میان ۳۴۰۰ تا ۳۶۰۰ پیش از میلاد یکی از افسران اطلاعاتی مصر قدیم به نام توشا موفق گردید، دویست تن از لشگریان مسلح را درون کیسه‌های گندم، که با کشتی حمل می‌شد، به درون شهر محاصره شده یافا بفرستد. هنگامی که کشتی در بندر پهلو گرفت لشکریان بیرون آمده و بر شهر تسلط یافتند پس آن را به سپاه مصر که شهر را محاصره کرده بودند، تحویل دادند. چنانچه تلاش عناصر اطلاعاتی که درون کیسه‌های گندم به شهر رفتند نبود، سپاهیان مصری قدرت ورود به یافا را نداشتند

از نوشته سون تزو معلوم می‌شود که گردآوری اخبار چهارصد سال قبل از میلاد در میان چینی‌ها، رایج بوده است آنجا که می‌گوید: «چهار نوع مزدور وجود دارد: بومی، داخلی، دو جانبه و متحرک. دو نوع اول همان چیزی است که در زمان حاضر بر مزدوران منطقه‌ای که به نفع یک دولت و علیه دولت دیگر جاسوسی می‌کنند اطلاق می‌شود. تعبیر دو جانبه بر مزدوری از دشمن اطلاق می‌گردد که به اسارت در می‌آید و سپس از سوی کسانی که او را به اسارت گرفته‌اند، برای جاسوسی به کشور خودش فرستاده می‌شود اما مزدوران متحرک کسانی هستند که اخبار دروغ میان دشمن پخش کرده، به کشور خود باز می‌گردند (تزو، سون،۱۳۵۹).

داستان حضرت موسی (ع) در عهد عتیق نیز اشاره به مأموریت عناصر اطلاعاتی دارد پروردگار موسی بر وی فرمود مردان خویش را بفرست تا سرزمین کنعان را که به بنی اسرائیل بخشیده‌ام، جستجو کنند و به سوی هر قبیله‌ای رئیس آنان را بفرست موسی ۱۲ مرد، از آن جمله یوشع بن نون از قبیله افرایم را برای جاسوسی در سرزمین کنعان فرستاد و به آنان گفت: راه جنوب را در پیش گیرید، از فراز کوه‌ها حرکت کنید و زمین را زیر نظر بگیرید(محمدی، نوراله،۱۳۸۷).

عمربن ربیعه، سروس بن شیبان و صلیع بن عبدغنم را به لشکرگاه ابن زیاد، پادشاه شام فرستاد تا

Archive of SID

www.SID.ir

علیه او جاسوسی کنند (جواد علی، المفصل فی تاریخ العرب).

پیامبر اکرم (ص) در جنگ‌های بدر و خندق نیروهای اطلاعاتی‌اش را به کار گرفت و دوست داشت تا آنجا که امکان دارد اخبار دشمن را بداند (فجر الاسلام، احمد امین،۱۹۶۹).

تعاریف:

جاسوسی عبارت است از جمع آوری و تملک اطلاعات و تعلیمات و اسناد قابل استفاده یک کشور بر ضد امنیت خارجی آن کشور (رئه گارو، ژرژ،۱۳۴۸).

جاسوسی عبارت است از گردآوری پنهانی و غیر قانونی اطلاعات مرتبط با امور سیاسی و نظامی یک کشور یا اطلاعات متعلق به مردم آن (*De sola, Ralph, 1982*).

جاسوسی یکی از مصادیق بارز و قدیمی جرائم علیه امنیت است که معمولاً یک جرم سازمان یافته و در عین حال فر املی می‌باشد چرا که با ارتکاب آن اطلاعات حیاتی یک کشور در زمینه امور نظامی، امنیتی و سیاسی از طریق یک نظام سازمان یافته و با استفاده از منابع انسانی در اختیار کشور یا کشورهای دیگر قرار می‌گیرد (علی پور، حسن، ۱۳۸۸).

کار جاسوسی یک پازل دائمی است که از شکل‌ها و رنگ‌های مختلفی ساخته شده است و این رنگ‌ها و شکل‌ها به طور مداوم شکل می‌گیرند و از شکل می افتند. جاسوسی شامل جستجوی پایان ناپذیر برای یافتن قطعات جدا از هم است که تحلیل گران سرویس‌های مخفی آن‌ها را برای تکمیل پازل خود جمع می‌کنند. ولی درست وقتی که شما می‌خواهید یک جای خالی را با قطعات جدید پر کنید، پازل شکل عوض می‌کند مارانش در کتاب خود از جاسوسی به عنوان جنگ جهانی چهارم یاد می‌کند و می‌گوید: «جنگ جهانی چهارم یکی از آن‌هایی است که تا به حال هیچ برنده مشخص نداشته و در واقع هیچ طلسم پیروزی در آن موجود نیست اما آنچه که از قبل در خاطره‌ها و کابوس‌های زنده مانده‌اند؛ شکست‌ها هستند و اگر ما استراتژی خود را برای مبارزه در این درگیری عظیم تغییر ندهیم، همچنان از شکست‌های پی در پی رنج خواهیم برد، ما باید درک کنیم که به هیچ وسیله‌ای که تاکنون آن‌ها را به کار گرفته‌ایم، پیروزی به دست نمی‌آید. عده کمی از کسانی که کشور ما را رهبری کرده‌اند و در حقیقت تعداد کمی از آن‌ها که هر روز در خطوط مقدم جبهه هستند به درستی فهمیده‌اند که ما در یک سری نبردهایی که برای آن‌ها آمادگی کامل نداشتید گرفتار آمده‌ایم»(مارانش، کنت،۱۳۷۳).

جاسوسی دارای سه مرحله می‌باشد که عبارتند از: شناسایی و تعیین اطلاعات مورد نیاز، جمع آوری اطلاعات و بالاخره تجزیه اطلاعات جمع آوری شده که نهایتاً منجر به هدف اصلی جاسوسی

Archive of SID

www.SID.ir

یعنی ارائه اطلاعات به مسئولان یک دولت یا شرکت بیگانه جهت اتخاذ تصمیم است.[1]

انواع جاسوسی و راه‌های مقابله با آن‌ها

به طور کلی می‌توان جاسوسی را از دو بعد از نظر فنی مورد بررسی قرار داد:

۱. جاسوسی سنتی:

در زمان‌های قدیم پادشاهان حکام و فرماندهان نظامی افرادی را به عنوان عامل نفوذی به میان سپاه دشمن و رقیب خود می‌فرستادند تا از اوضاع نظامی و استعداد نیروهای دشمن اطلاعات را جمع‌آوری کند.

در جنگ‌های صدر اسلام نیز پیامبر اکرم (ص) افرادی را انتخاب می‌فرمودند که جهت جمع‌آوری اطلاعات از سپاه دشمن، موقعیت استقرار نیروهایشان، آرایش نظامی که گرفته‌اند خبرهایی جهت تصمیم گیری ایشان بیاورند. جاسوسی سنتی اغلب به صورت استفاده از نیروهای انسانی و عوامل نفوذی بود.

۲. جاسوسی مدرن و پیشرفته:

امروزه با پیشرفت علوم در عرصه‌های مختلف و مدرن شدن راههای ارتباطات، جاسوسی و شگرد آن نیز از این قاعده تبعیت می‌کند. مهم‌ترین موارد جاسوسی مدرن و پیشرفته به شرح زیر می‌باشد:

الف)- جاسوسی صنعتی ب)- جاسوسی تلفن همراه پ)- جاسوسی رایانه‌ای

در این مقاله به علت جلوگیری از پراکندگی مطلب از توضیح در خصوص جاسوس صنعتی و جاسوسی تلفن همراه صرف‌نظر نموده و به تشریح جاسوسی رایانه‌ای می‌پردازیم.

۳. جاسوسی رایانه‌ای:

هنگامی که از امنیت رایانه‌ها و شبکه‌های رایانه صحبت می‌شود، مباحث زیادی قابل طرح و بررسی می‌باشند، موضوعاتی که هر کدام به تنهایی می‌توانند در عین حال جالب، پر محتوا و قابل درک باشند. اما وقتی صحبت از کار عملی برمی‌آید قضیه تا حدودی 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

---

[1]. *world of criminal justic*

Archive of SID
www.SID.ir

علوم ارتباطات و اطلاعات را به خود مشغول ساخته بود، اینک ذهن اکثر انسان‌های کره خاکی را به خود مشغول کرده است. «کیث لیتل» تکنسین رایانه در آمریکا می‌گوید: هر روز تعداد بیشتری از مشتریان از او می‌خواهند برای حفظ حریم شخص 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)(نسیکی، کلو،۱۳۸۹).

جاسوسی اینترنتی عموماً به صورت دستیابی به اطلاعات از طریق برنامه‌هایی معرفی می‌شود که از راه نصب نرم افزارها و یا حین گردش افراد در محیط وب وارد رایانه شخصی آنان شده و تا زمانی که کاربر به شبکه جهانی وصل است، اطلاعاتی را که روی هارد رایانه او ذخیره شده است، برای پایگاه‌های مطلوب خود می‌فرستند اما این تنها یکی از انواع جاسوسی الکترونیکی است نوع دیگر که امروزه تقریباً همه ما آن را می‌شناسیم و برای جلوگیری از بروز چنین خبر چینی‌هایی در رایانه‌های خویش انواع دیوارهای آتش و نرم افزار ضد جاسوسی را نصب می‌کنیم (خاکی، احمد،۱۳۸۷).

نرم افزار جاسوسی چیست؟

حتماً تا حالا پیش آمده است که در حال کار با اینترنت ناگهان پنجره‌های مختلف زیادی بدون درخواست شما باز می‌شوند که اصطلاحاً پنجره‌های باز شونده[1] نام دارند و وقت زیادی را باید برای بستن آنها صرف کنید. نرم افزار جاسوسی هر نوع فناوری یا برنامه روی رایانه شماست که اطلاعات را به طور پنهانی جمع آوری می‌کند. این نوع برنامه‌ها به تبلیغ- کنندگان یا به سایر گروه‌های علاقه‌مند فروخته می‌شوند. نوع اطلاعاتی که از رایانه شما جمع آوری می‌شود متفاوت است. بعضی از نرم افزارهای جاسوسی تنها اطلاعات سامانه شما را ردیابی می‌کنند مانند نوع اتصال شما به اینترنت و سامانه عامل رایانه شما بقیه نرم‌افزارهای جاسوسی، اطلاعات فردی شما را جمع‌آوری می‌کنند. نرم افزار جاسوسی بدون رضایت و اجازه کاربر نصب می‌گردد.

نصب نرم افزار جاسوسی روی رایانه شما می‌تواند با مشاهده یک وب سایت، دیدن یک ایمیل به فرمت *HTML* یا با کلیک کردن یک پنجره باز شونده (*popup*) آغاز شود.

نرم افزار جاسوسی هر نوع نرم افزاری است که اطلاعات را از یک رایانه بدون آگاهی کاربر به دست می‌آورد. انواع زیادی از این نوع نرم افزارها در اینترنت فعال هستند اما می‌توان آنها را به دو گروه تقسیم بندی کرد:

---

[1] . *popup windows*

Archive of SID

www.SID.ir

۱. نرم افزار جاسوسی خانگی[1]: این نرم افزار، نرم افزاری است که معمولاً به وسیله صاحبان رایانه‌ها برای آگاهی از تأثیرات اینترنت بر روی شبکه‌های رایانه خودشان، خریداری و نصب می‌گردد. مدیران از این نرم افزار برای آگاهی از فعالیت‌های آنلاین کارمندان استفاده می‌کنند. بعضی افراد نیز برای اطلاع از فعالیت‌های سایر اعضای خانواده از آن‌ها استفاده می‌کنند شخص سومی هم می‌تواند نرم افزار جاسوسی را بدون آگاهی صاحب رایانه نصب کند مجریان قانون از نرم افزار جاسوسی برای آگاهی از فعالیت مجرمان استفاده می‌کنند.

۲. نرم افزار جاسوسی تجاری[2]: نرم افزاری است که شرکت‌ها برای پیگیری فعالیت‌های وب‌گردی کاربران اینترنت استفاده می‌کنند این شرکت‌ها بیشتر اطلاعات به دست آمده را به بازاریان می‌فروشند و آنها کاربران را با تبلیغ خاص مورد هدف قرار می‌دهند منظور تبلیغاتی است که با علایق کاربر مطابقت دارد. و به احتمال زیاد برای وی جذاب است.

۳. اهداف نرم افزارهای جاسوسی: نرم افزار جاسوسی هر چه نباشد دست کم یک عامل آزاردهنده است که سرعت رایانه را کاهش می‌دهد، هارد رایانه را بی‌دلیل پر می‌کنند، و رایانه شما را به هدفی برای تبلیغ کنندگان تبدیل می‌کند. فراتر از آگاهی از اطلا عات خصوصی شما، نرم افزار جاسوسی می‌تواند به عنوان ابزاری برای جرائمی مانند تقلب در شناسایی استفاده می‌شود.

۴. چگونگی قرار گرفتن نرم افزار جاسوسی روی رایانه شما و روش مقابله با آن: تنها مسئله در مورد نرم افزار جاسوسی این نیست که چه مدت روی رایانه شما قرار داشته باشد و چه قصدی دارد، بلکه فهمیدن این که چگونه و از کجا این برنامه وارد رایانه شما شده است، در درجه اول قرار دارد. نرم افزارهای جاسوسی درست مانند علف‌های هرز که بدون سر و صدا هنگام قدم زدن در جنگل به جوراب شما می‌چسبند هنگامی که مشغول گشت و گذار در اینترنت هستید، خودش را مانند یک مسافر قاچاقی به رایانه شما می‌چسباند اما قبل از اینکه هر چیزی بتواند روی رایانه شما نصب گردد معمولاً باید روی چیزی کلیک یا برنامه‌ای را باز کنید. در زیر چند تا از معمول‌ترین روش‌های مورد استفاده برای فریب دادن کاربران برای نصب نرم افزارهای جاسوسی بیان شده است:

(۱)- باز کردن ایمیل.

(۲)- کلیک کردن روی پنجره‌های باز شونده فریبنده.

(۳)- دانلود رایگان برنامه‌ها، بازی‌ها، ابزارها و غیره.

(۴)- برنامه‌های اشتراک فایل.

(۵)- مشاهده وب سایت‌های غیر اخلاقی.

(۶)- نرم افزارهای اجرای فایل‌های صوتی و تصویری آنلاین.

---

[1] . *domestic SPY ware*

[2]. *Adware*

Archive of SID

انواع جاسوسی رایانه‌ای و اینترنتی:

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

۱. رایج‌ترین راه جاسوسی رایانه‌ای، کپی کردن فایل‌های داده است 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 عمدتاً به وسیله برنامه‌های کمکی یا به وسیله برنامه‌های خود ساخته، صورت می‌گیرد.

۲. نوع دیگر جاسوسی رایانه‌ای، جاسوسی شخصی سنتی است که آن هم به دو دسته جاسوسی شخصی سنتی و جاسوسی فنی سنتی تقسیم می‌شود: جاسوسی شخصی سنتی: روش‌های این نوع جاسوسی عبارت‌اند از رشوه دادن به کارمندان یا اخاذی از آن‌ها، فرستادن مأمور در قالب کارمند تازه وارد برای دوره‌های کوتاه کاری (این روش به سلام- خداحافظ معروف است) یا به وسیله مصاحبه با کارمندان شرکت مورد نظر که در جستجوی کار جدید به سراغ آگهی‌های دروغین می‌آیند و در ضمن مصاحبه وضعیت فعلی کارشان هم توصیف می‌کنند.

روش‌های فنی سنتی تحصیل اطلاعات ذخیره شده در کامپیوتر نیز بر مبنای سرقت فایل‌های داده، اتصال یک کابل مخفی به کامپیوتر مورد نظر، نصب بخش انتقال دهنده در سیستم کامپیوتر مورد نظر صورت گرفته است. روش دیگر سوء استفاده از داده‌هایی است که تاریخ اعتبار آن‌ها گذشته است شامل مواد:

(الف) جستجو در سطل زباله برای یافتن برگه‌های چاپ شده یا کاغذ کاربن‌هایی که در تهیه چند نسخه از یک نوشته به کار رفته است.

(ب) دیسک‌هایی که برای مبادله حامل‌های داده به کار رفته ولی محتویات آن‌ها کاملاً محو شده است. به این صورت که با استفاده از یک برنامه نرم افزاری خاص مثل (*recovery*) تمامی فایل‌های حذف شده بر روی یک دیسک بازخوانی شده و از آن سوءاستفاده می‌گردد.

(پ) برداشتن داده‌هایی که کارمند بعد از اتمام کارش در قسمت ذخیره داده‌های مورد نیاز برای مراجعه‌های بعدی بر روی کامپیوترش ذخیره می‌کند.

۳. برداشت داده از طریق فرکانس: دستیابی به میدان‌های الکترونیکی و فرکانسی تولید شده پایانه‌های رایانه‌ای و شنود و تحلیل و حتی ضبط آن‌ها با استفاده از امکانات استاندارد صوتی و تصویری که با قیمت ارزان به دست می‌آید به راحتی در یک ماشین نزدیک مرکز رایانه قابل

Archive of SID

www.SID.ir

جاسازی است.

۴. استفاده از سیستم‌های مخابراتی: در این نوع، نفوذ به مراکز داده جهت دسترسی غیر مجاز به اطلاعات به روش‌های خاصی صورت می‌گیرد:

(الف) استفاده از گذر واژه (به ویژه اگر مدت زمان طولانی تغییر نکند).

(ب) استفاده از تماس‌های تلفنی دروغین.

(پ) شنود استراق سمع از طریق جمع‌آوری داده‌های سرگردان ارسالی از ماهواره‌ها یا ایستگاه‌های زمینی و نفوذ به کامپیوترهای حاوی داده‌ها.

۵. کسب اطلاعات از طریق:

(الف) معرفی برنامه‌هایی که از راه نصب نرم افزارها و یا حین گردش افراد در محیط وب وارد کامپیوتر شخصی آن‌ها شده و تا زمانی که کاربر به شبکه جهانی وصل است، اطلاعاتی را که روی هارددیسک او ذخیره شده است برای پایگاه‌های مطلوب خویش می‌فرستد. در تحقیقی که از یک میلیون کامپیوتر در سطح جهان به محل آمد مشخص شد که ۳۰ میلیون برنامه جاسوسی در آن‌ها به کار رفته است. با این وصف می‌توان گفت: در هر کامپیوتر حداقل ۳۰ نرم افزار جاسوسی هست که کلیه اطلاعات لازم را به مراکزی که آن‌ها را طراحی کرده‌اند ارسال می‌کند. بسیاری از برنامه‌های جاسوسی از طریق کلیک *ok* یا *NO* پیام‌های مزاحم به رایانه‌ها راه پیدا می‌کنند. سپس از یک کلیک، این نرم افزار اجازه نفوذ یافته و مستقیماً خود را در قسمت سخت افزار پنهان می‌نماید البته همه برنامه‌های جاسوسی آن قدرها مؤدب نیستند بعضی از این برنامه‌های جاسوسی، بدون هیچ مجوزی و تنها به خاطر ساختار قدرتمند خود می‌توانند حین دسترسی یک رایانه به اینترنت، به درون آن نفوذ کرده و به اجرای مقاصد خود بپردازند حتی پس از نصب این برنامه‌ها نیز تقریباً هیچ اثری در عملکرد دیده نمی‌شود تنها برخی از آن‌ها هستند که باعث کند شدن احتمالی سرعت رایانه یا معرفی برخی آدرس‌های غیر معمول می‌شوند اثرات این برنامه‌ها نیز جالب است. هر چند نرم افزارهای مذکور اکثراً در ظاهر، بی خطرند ولی حتی همین نرم افزارهای بی خطر نیز کارهای غیر قانونی انجام می‌دهند. ساده‌ترین حالت این است که تمامی عادات کاربر را شناسایی و در جمع آوری اطلاعات مربوط به عادات به شرکت‌های هدایتگر کمک می‌نماید. روش‌های مخرب نرم افزارهای جاسوسی، از سطح ورود به اطلاعات شخصی کاربر و استفاده غیر مجاز از آنها آغاز شده و به آسیب رسانی کامپیوترها می‌انجامد. برخی از آن‌ها جمع‌آوری کلیه اطلاعات شخصی آن‌ها را کپی برداری کرده و به اطلاع هدایتگرهای خود می‌رسانند.

(ب) بررسی ایمیل‌های شخصی و سازمانی.

(پ) گزارش عملکرد «وب گردی» کاربران وسرویس دهی ارائه دهندگان خدمات اینترنتی به

Archive of SID

www.SID.ir

شرکت‌ها و سازمان‌های ذی نفع از دیگر راه‌ها و انواع جاسوسی اینترنتی است.[1]

۶. استفاده از فلش: فلش ابزاری است که به عنوان محلی برای ذخیره اطلاعات و داده‌ها به کار می‌رود تفاوت اصلی ومزیت استفاده از این ابزار نسبت به سایر وسایل ذخیره کننده اطلاعات عبارت است از:

(الف) فلش نسبت به سایر وسایل ذخیره اطلاعات مثل لوح‌های فشرده این مزیت را دارا می‌باشد که فلش قابل برگشت می‌باشد یعنی اینکه بعد از ذخیره اطلاعات بر روی آن این امکان وجود دارد که به تعداد دفعات نا محدود اطلاعات را حذف و اطلاعات جدید بر روی آن ذخیره نمود.

(ب) مزیت دیگر فلش نسبت به سایر وسایل ذخیره اطلاعات مثل هارد های ذخیره اطلاعات این است که یک فلش به راحتی قابل حمل می‌باشد و آن را می‌توان در یک جای بسیار کم جاسازی نمود.

(پ) میزان قابلیت ذخیره سازی اطلاعات نسبت به ابعاد کوچک آن بسیار بالا و منحصر به فرد می‌باشد به طوری که در حال حاضر فلش‌هایی با ظرفیت ۶۴ گیگابایت نیز تولید می‌شوند البته فلشی با این ظرفیت جهت ارائه بازار به مشتریان می‌باشد و مسلماً فلش‌هایی که جهت مقاصد جاسوسی استفاده می‌شوند هم از نظر ابعاد و هم از نظر قابلیت ذخیره اطلاعات دارای ویژگی‌های بخصوصی می‌باشند.

با توجه به موارد فوق استفاده از فلش همیشه به عنوان یک ابزار مناسب مورد توجه جاسوسان می‌باشد این مسئله زمانی اهمیت پیدا می‌کند که مثلاً در یک مکان با درجه اهمیت بالای حفاظتی و امنیتی که هیچ کدام از رایانه‌ها به اینترنت متصل نیستند (که بتوان از طریق نرم افزارها و انجام عملیات هک، اطلاعات مورد نظر را برداشت نمود) با بهره گیری از افراد نفوذی یا به خدمت گرفتن کسانی که در آن اماکن مشغول به کار می‌باشند به همراه استفاده از ابزاری مطمئن و قابل حمل مثل فلش براحتی می‌توان به هدف دلخواه رسید.

اما اهمیت استفاده از فلش زمانی بیشتر و حساس‌تر می‌شود که با پیشرفت فناوری‌های امروزی انواع مختلفی از فلش‌ها ساخته شده است مثلاً نوعی از آن که جدیداً در دسترس جاسوسان قرار گرفته است دارای این نوع ویژگی می‌باشد که اگر حتی رایانه (شامل مجموعه *case*،*monitor*،...) خاموش بوده و هیچ گونه اتصالی به جریان الکتریسیته نداشته باشند اگر به *case* کامپیوتر وصل شود به اندازه حجم داخلی خود از اطلاعات موجود در هارد رایانه مزبور برداشت می‌نماید.

جرم جاسوسی رایانه‌ای:

[1] . *WWW. Ittink.blogfa.com*

Archive of SID

www.SID.ir

جاسوسی رایانه‌ای یکی از رایج‌ترین انواع جرائم رایانه‌ای محسوب می‌شود به علت ارزشمند بودن اطلاعات ذخیره شده در مراکز رایانه‌ای این جرم به طور ویژه‌ای برای مرتکب سودمند و برای شرکت متضرر از جرم، خطرناک است. در همه کسب و کارها هدف اصلی جاسوسی کامپیوتری «برنامه‌های کامپیوتری» است. ارزش این اهداف جدید جرم را می‌توان از این واقعیت دریافت که در سال ۱۹۸۵ فروش برنامه‌های کامپیوتری تقریباً ۵۵ میلیارد دلار برآورد شده است. در بخش تجاری هدف اصلی جاسوسی کامپیوتری بدست آوردن درآمدهای هنگفت از طریق فروش برنامه‌های ضد جاسوسی است.

تفاوت بین عنوان‌های جاسوسی رایانه‌ای و اینترنتی:

با عنایت به اینکه دو عنوان جاسوسی رایانه‌ای و جاسوسی اینترنتی دقیقاً نمی‌توانند بر هم منطبق باشند، تفاوت‌هایی بین آن‌ها وجود دارد جاسوسی رایانه‌ای یکی از جرائم رایانه‌ای است که قدمتی دیرینه دارد و در امتداد تلاش‌های نظامی و سیاسی برای کسب اطلاع از طرف مقابل به هنگام جنگ یا هر رقابت دیگری به وجود آمده است اما با راه اندازی شبکه اینترنت این جرم هم ماهیتی متناسب با قالب فضای مجازی یافت و با تغییر و پیدایش روش‌های جدید که نتیجه فضای مجازی و خصوصیات آن بود به نوع نوینی از جاسوسی یعنی اینترنتی یا سایبر تبدیل شد. اساساً باید بین جاسوسی رایانه‌ای و جاسوسی اینترنتی تمایز قائل شد چرا که هم ماهیتاً و هم از لحاظ روش‌های مورد استفاده با هم متمایزند. در جاسوسی رایانه‌ای به طور عمده از روش‌هایی مانند کپی کردن فایل‌ها، جاسوسی سنتی، برداشت از طریق فرکانس و استفاده از سیستم‌های مخابراتی استفاده می‌شود ولی در جاسوسی اینترنتی از نصب نرم افزارهایی که در حین اتصال کاربر به شبکه بر رایانه او (با اجازه یا بی‌اجازه کاربر) نصب می‌شود. بررسی ایمیل‌های شخصی از طریق هک کردن رمزهای آن، مشاهده دقیق عملکرد کاربران و سرویس دهندگان اینترنت استفاده می‌شود. تفاوت اصلی و بنیادی جاسوسی رایانه‌ای و جاسوسی اینترنتی در این است که جاسوسی رایانه‌ای نیاز به استخدام مزدور دارد و بدون نیاز عضو واسط نمی‌توان به کسب اطلاعات نائل گردید اما در جاسوسی اینترنتی از استخدام مزدور بی نیاز می‌باشند و بعضی مواقع با اجازه خود کاربر وارد رایانه او می‌شوند.[۱]

مقایسه جاسوسی و خیانت به کشور: قانونگذار جمهوری اسلامی ایران جرم مستقلی را به عنوان خیانت به کشور جرم انگاری ننموده است در تعریف خیانت به کشور می‌توان گفت، خیانت به کشور عبارت است از سوء قصد بر ضد امنیت کشور به وسیله ایجاد ارتباط با کشور دیگری که دارای سلطه و استقلال است (رئه گارو، ژرژ،۱۳۴۸). لذا در تعریف جرم خیانت می‌توان گفت: خیانت به

۱. همان سایت

Archive of SID

www.SID.ir

کشور فعل عمدی یک فرد ایرانی و خارجی در خدمت دولت ایران است که منافع یک قدرت بیگانه را در زمان صلح یا جنگ به زیان مملکت، تأمین نموده و امنیت کشور را به خطر می‌اندازد. مرز بین بزه جاسوسی وخیانت به کشور تابعیت، «ملیت» است. بدین معنا که چنانچه یک فرد بیگانه در یک کشور مبادرت به جمع آوری اطلاعات و اسناد به کشور متبوع خود یا یک کشور دیگر ویا شخصی بیگانه یا مرجعی غیر ذیصلاح باشد جاسوس تلقی می‌شود اما در صورتی که این مرتکب از اتباع کشور دارنده اطلاعات باشد اقدامات صورت پذیرفته توسط وی خیانت به کشور محسوب می گردد و او به عنوان خیانت به کشور قابل مجازات است (گلدوزیان، ایرج، ۱۳۸۰).

روش ارتکاب جرم جاسوسی رایانه‌ای:

در خصوص روش ارتکاب جرائم رایانه‌ای و جرم جاسوسی کامپیوتری وسرقت نرم افزار باید گفت که رایج‌ترین روش برای به دست آوردن داده‌ها، کپی کردن فایل‌های داده است. در زمینه برنامه‌هایی که به تعداد انبوه تولید و به فروش می‌رسند کپی کردن برنامه‌ها روش معمول و سریع است که با این وجود در صورت وجود برنامه‌های ویژه ،کپی کردن ممکن است بسیار دشوار شود. در خصوص برنامه‌هایی که به تعداد انبوه تولید نمی‌شود کپی کردن عمدتاً به وسیله برنامه‌های کمکی یا به وسیله برنامه‌های خود ساخته (که بعضاً در غالب برنامه‌های اجرایی معمولی جا زده می‌شوند) یا به وسیله زیر برنامه‌های اسب تروآ که به برنامه‌های ممتاز اجرایی نفوذ می‌کنند، صورت می گیرد (زیبر، اولریش،۱۳۸۳).

ممکن است جاسوسی از طریق ارسال پیام‌های ناخواسته الکترونیکی واقع شود. پیام‌های ناخواسته هم می‌توانند حامل نرم افزارهای جاسوسی باشند و هم ممکن است شرایط تخلیه اطلاعاتی دریافت کننده پیام ناخواسته را فراهم سازند و ساده‌تر از همه جاسوسی رایانه‌ای ممکن است با فریب یا تحریک متصدی حفظ اطلاعات رایانه‌ای طبقه بندی شده از طریق بهره گیری از مسائل شخصی یا عاطفی صورت گیرد (*morris- Sheridan,2004*).

اینترنت در ایران: برای درک آسیب پذیری های ساختار رایانه‌ای در ایران ناگزیر از ارائه چشم انداز وورد اینترنت به ایران و نحوه رشد وگسترش آن هستیم. در سال ۱۳۸۶ طبق اعلام رسمی وزارت ارتباطات و فناوری اطلاعات بیش از ۴/۷ میلیون نفر کاربر اینترنت در ایران وجود دارد که در مقایسه با سال ۱۳۸۱ که رقم ۱/۸ میلیون نفر بود، از رشدی بیش از ۲۰۰ درصد برخوردار بوده است (ضیایی پور، حمید،۱۳۸۶).

موانع حاکم بر تحقیقات در جرم جاسوسی رایانه‌ای:

Archive of SID
www.SID.ir

الف)- اصل صلاحیت: «نخستین مسئله‌ای که در تحقیق اهمیت دارد بحث صلاحیت است لذا در صورتی که مراجع رسیدگی کننده خود را صالح ندانند مکلف به صدور قرار عدم صلاحیت هستند. صلاحیت عبارت است از استعداد یک مرجع معین برای رسیدگی به یک دادرسی مشخص. وقتی مرجعی این استعداد را داشته باشد می گوییم صلاحیت دارد. به بیان دیگر صلاحیت کیفری عبارت است از: شایستگی و اختیاری است که به موجب قانون برای مراجع جزایی و رسیدگی به امور کیفری واگذار شده است. اهمیت صلاحیت به خاطر تقسیم کاری است که باید وجود داشته باشد.

با توجه به ماهیت جرم جاسوسی رایانه‌ای که کاملاً با جرم‌های دیگر مثل کلاهبرداری و سرقت متفاوت است زیرا این جرم در فضای سایبر و مجازی به وقوع می‌پیوندد و در نتیجه به عنوان مثال محل ارتکاب این جرم معلوم نیست که بتوان صلاحیت رسیدگی را به یکی از مراجع واگذار نمود. پس می‌توان اصل صلاحیت را به عنوان یکی از موانع در تحقیقات این جرم بیان نمود. در جایی که جرم سایبر به طور عام و جرم جاسوسی رایانه‌ای به طور خاص بر داده‌ها ارتکاب یافته تعیین محل ارتکاب جرم، کاری بس دشوار به نظر می‌رسد. چگونه می‌توان یک رخداد غیر فیزیکی و مجازی را در دنیای فیزیکی و در بعد مکانی جستجو کرد. برای نمونه کاربری در ایران با مخاطب خود در شهر فرانکفورت ارتباط اینترنتی برقرار می‌کند این تماس با نفوذ غیر مجاز در بانک داده‌های شخصی مخاطب خود در شهر فرانکفورت است، با جاسوسی از داده‌های او، اطلاعات مورد نیاز خود از مخاطب را دریافت کرده سپس با تخریب اطلاعات باقی مانده بانک اطلاعات وی را ترک می‌کند. در این نمونه ساده محل ارتکاب این جرم‌ها کجاست؟ زیرا مرتکب در ایران با استفاده از برنامه‌های خاص نرم افزاری اقدام به نفوذ غیر مجاز به سامانه‌های مخاطب خود در شهر فرانکفورت کرده در همین حین مرتکب جرم‌های دیگری نیز بر داده‌های کاربر فرانکفورتی است و کاربر مذکور در رایانه خود نتیجه این افعال مجرمانه را به شکل بروز اختلال در برنامه‌ها و سامانه‌های خود مشاهده می‌کند. این‌ها همه در حالی است که در واقع پایگاه داده‌ها در شهر تورنتوی کانادا واقع است و اگر سرقت، تخریب (یا جاسوسی) و هر گونه جرم علیه داده‌ها رخ داده باشد در واقع آن پایگاه داده‌ها مورد حمله قرار گرفته و کاربر آلمانی فقط نمایشی از آن را مشاهده خواهد کرد. ملاحظه می‌شود جرم محیط سایبر برخلاف جرم سنتی که در مکان‌های مشخصی یا محصوری اعم از یک اتاق، ساختمان یا یک طبقه رخ می‌دهد ممکن است در چند گوشه کره زمین رخ دهد.

ب)- تفتیش و توقیف در محیط سایبر: اختیار بازرسی و ورود به اماکن مستلزم آن است که بتوان داده را توقیف یا تصرف کرد. از لحاظ بررسی داده‌های رایانه‌ای که به طور دائم در محیط مادی حامل داده ذخیره می‌شوند محدودیت‌های کلی اختیارات بازرسی و توقیف، در مورد بازرسی و توقیف موضوعات مربوط به سوابق امر یا کشف حقیقت در اکثر کشورها مسائل جدی به وجود نمی‌آورد زیرا حق ضبط و بازرسی در محیط‌های مادی حامل داده در مورد حافظه‌های داخلی، واحد

Archive of SID

www.SID.ir

پردازش مرکزی، شامل حق بازرسی داده نیز می‌شود. در زمینه بازرسی و توقیف در شبکه‌های رایانه‌ای نیز مسائل خاصی مطرح می‌شود. در اینجا سؤالی پیش می‌آید که حق بازرسی و توقیف تأسیسات رایانه‌ای خاص تا چه حد شامل حق بازرسی بانک‌های اطلاعاتی می‌شود که در دسترس تأسیسات مزبور قرار دارد، اما در مکان‌های دیگر مستقر است؟ مجرمان به طور معمول به منظور جلوگیری از پیگرد قانونی اطلاعات خود را در سامانه‌های رایانه‌ای ذخیره می‌کنند که در جایی دیگر مستقر شده‌اند. در زمینه بازرسی و توقیف پایگاه داده‌ها از طریق سامانه‌های مخابراتی بین المللی، مسائل خاصی در ارتباط با حقوق بین الملل عمومی مطرح می‌شود. در سامانه‌های بین المللی نفوذ مستقیم در بانک‌های داده‌های خارجی به وسیله مقامات تعقیب و تحقیق معمولاً تجاوز به حاکمیت کشوری محسوب می‌شود که اطلاعات در آن ذخیره شده است. اما ممکن است موارد استثنایی خاصی در سطح بین المللی بیابید که در آن دستیابی مستقیم به بانک‌های داده‌های خارجی از طریق شبکه‌های مخابراتی می‌تواند مجاز محسوب شود و از روال طولانی معاضدت دو جانبه پرهیز شود.

پ)- ضرورت حمایت از حریم خصوصی افراد: اطلاعات شخصی افراد با آگاهی یا بدون آگاهی آن‌ها با اهداف اولیه گوناگون ذخیره، نگهداری و استفاده می‌شوند، گاهی ارائه خدمات به افراد در ارگان‌ها و سازمان‌های مختلف و یا حتی استفاده از خدمات قابل ارائه از سوی آنها مستلزم ثبت اطلاعات شخصی آن‌ها است. در تحقیقات مقدماتی در جرائم سایبری (خاصه جاسوسی رایانه‌ای) جهت جمع‌آوری اطلاعات از متهمین، باید رایانه آن‌ها و یا وسایل الکترونیکی که مختص آن‌ها می‌باشد مورد بازرسی و بازدید قرار گیرد با توجه به اینکه بعضاً این احتمال قریب وجود دارد که افراد و اشخاص اطلاعات فوق‌العاده شخصی خود، خانواده و بستگان نزدیکشان را در آن ذخیره کرده باشند لذا باید توجه داشت که در تحقیقات از آن‌ها در این مورد با مشکل برخورد می‌کنیم و باید آن را مد نظر داشت»(زندی، محمدرضا،۱۳۸۹).

بررسی قوانین مرتبط با جاسوسی رایانه‌ای:

در باب عنوان جاسوسی رایانه‌ای قوانین متنوعی وجود ندارد فقط در قانون جرائم رایانه‌ای در ماده ۳، ۴ و ۵ به این موضوع پرداخته است، اما قانون مجازات اسلامی و قانون جرائم نیروهای مسلح از جنبه پرداختن به موضوع جرم جاسوسی به قانون جرائم رایانه‌ای شباهت‌ها و تمایزهای قابل تأملی دارد لذا در اینجا به بررسی این ۳ قانون درباره موضوع فوق می‌پردازیم:

الف) مواد قانون جرائم رایانه‌ای (ق.ج.ر)[1]:

لایحه جرائم رایانه‌ای به شماره چاپ ۱۲۲ که جهت رسیدگی به کمیسیون قضایی و حقوقی

۱. قانون جرائم رایانه‌ای

Archive of SID
www.SID.ir

مجلس شورای اسلامی به عنوان کمیسیون اصلی ارجاع شده بود در جلسه‌ای در تاریخ ۱۳۸۷/۵/۷ با حضور کارشناسان ذیربط مطرح گردید و پس از بحث و تبادل نظر کلیات آن عیناً مورد تصویب قرار گرفت. با تصویب این قانون در سال ۸۸ دیگر لازم نیست قضات جرائم ارتکابی رابا مواد قانونی قبل تطبیق دهند (دینداری، مرتضی،۱۳۸۹). در ماده ۳ و ۴ و ۵ لایحه فوق که بعداً قانون گردید به عنوان جاسوسی رایانه‌ای پرداخته است.

ماده ۳ ق.ج.ر: هر کس به طور غیر مجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سامانه‌های رایانه‌ای مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد:

الف- دسترسی به داده‌های مذکور یا تحصیل آن‌ها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از بیست میلیون (۲۰/۰۰۰/۰۰۰ ریال) تا شصت میلیون (۶۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات.

ب- در دسترس قرار دادن داده‌های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

پ- افشا یا در دسترس قرار دادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آن‌ها، به حبس از پنج تا پانزده سال.

تبصره ۱: داده‌های سری داده‌هایی است که افشای آن‌ها به امنیت کشور یا منافع ملی لطمه می زند.

تبصره ۲: آیین نامه نحوه تعیین و تشخیص داده‌های سری و نحوه طبقه‌بندی و حفاظت آن‌ها ظرف ۳ ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارتخانه‌های دادگستری، کشور، ارتباطات و فناوری اطلاعات ودفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیئت وزیران خواهد رسید.

ماده ۴ ق.ج.ر: هر کس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدابیر امنیتی سامانه‌های رایانه‌ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (۱۰/۰۰۰/۰۰۰) ریال تا چهل میلیون (۴۰/۰۰۰/۰۰۰ ریال) یا هر دو مجازات محکوم خواهد شد.

ماده ۵ ق.ج.ر: چنانچه مأموران دولتی که مسئول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سامانه‌های مربوطه هستند و به آن‌ها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آن‌ها قرار گرفته است بر اثر بی احتیاطی، بی مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل‌های داده یا سامانه‌های مذکور شوند، به حبس از یک روز تا دو سال یا جزای نقدی از پنج میلیون ۵/۰۰۰/۰۰۰ ریال تا چهل میلیون ۴۰/۰۰۰/۰۰۰ ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.

Archive of SID

www.SID.ir

ب) مواد قانون مجازات اسلامی (ق.م.ا) ۱:

ماده ۵۰۱ ق.م.ا: هر کس نقشه‌ها یا اسرار یا اسناد و تصمیمات راجع به سیاست داخلی یا خارجی کشور را عالماً و عامداً در اختیار افرادی که صلاحیت دسترسی به آن‌ها را ندارند قرار دهد یا از مفاد آن مطلع کند به نحوی که متضمن نوعی جاسوسی باشد، نظر به کیفیات و مراتب جرم به یک تا ده سال محکوم می‌شود.

ماده ۵۰۲ ق.م.ا: هر کس به نفع یک دولت بیگانه و به ضرر دولت بیگانه دیگر در قلمرو ایران مرتکب یکی از جرائم جاسوسی شود به نحوی که به امنیت ملی صدمه وارد نماید به یک تا پنج سال حبس محکوم خواهد شد.

ماده ۵۰۳ ق.م.ا: هر کس به قصد سرقت یا نقشه برداری یا کسب اطلاعات از اسرار سیاسی یا نظامی یا امنیتی به مواضع مربوطه داخل شود و همچنین اشخاصی که بدون اجازه مأمورین یا مقامات ذی‌صلاح در حال نقشه برداری یا گرفتن فیلم یا عکس‌برداری از استحکامات نظامی یا اماکن ممنوعه دستگیر شوند به شش ماه تا ۳ سال حبس محکوم می‌شوند.

ماده ۵۰۵ ق.م.ا: هر کس با هدف بر هم زدن امنیت کشور به هر وسیله اطلاعات طبقه بندی شده را با پوشش مسئولین نظام یا مأمورین دولت یا به نحو دیگر جمع‌آوری کند چنانچه بخواهد آن را در اختیار دیگران قرار دهد و موفق به انجام آن شود به حبس از دو تا ده سال و در غیر این صورت به حبس از یک تا پنج سال محکوم می‌شود.

ماده ۵۰۶: چنانچه مأمورین دولتی که مسئول امور حفاظتی و اطلاعاتی طبقه بندی شده می‌باشند و به آن‌ها آموزش لازم داده شده است در اثر بی مبالاتی و عدم رعایت اصول حفاظتی توسط دشمنان تخلیه اطلاعاتی شوند به یک تا شش ماه حبس محکوم می‌شوند.

پ) مواد قانون مجازات نیروهای مسلح در مواد ۲۴ و ۲۵ و ۲۶ و ۲۷ و ۲۸ به عنوان جاسوسی اختصاص دارد (ق.م.ن.م) ۲:

ماده ۲۴ ق. م. ن. م: افراد زیر جاسوس محسوب و به مجازات‌های ذیل محکوم می‌شوند:

الف- هر نظامی که اسناد یا اطلاعات یا اشیای دارای ارزش اطلاعاتی را در اختیار دشمن و یا بیگانه قرار دهد و این امر را برای عملیات نظامی یا نسبت به امنیت تأسیسات، استحکامات، پایگاه‌ها، کارخانجات، انبارهای دائمی یا موقتی تسلیحاتی، توقف‌گاه‌های موقت، ساختمان‌های نظامی، کشتی‌ها، هواپیماها یا وسایل نقلیه زمینی نظامی یا امنیت تأسیسات دفاعی کشور مضر باشد به مجازات محارب محکوم خواهد شد.

---

۱. قانون مجازات اسلامی

۱. قانون مجازات نیروهای مسلح

Archive of SID

www.SID.ir

ب- هر نظامی که اسناد یا اطلاعات برای دشمن یا بیگانگان تحصیل کرده، به هر دلیلی موفق به تسلیم آن نشود به حبس از سه تا پانزده سال محکوم می‌گردد.

پ- هر نظامی که اسرار نظامی، سیاسی، امنیتی، اقتصادی و یا صنعتی مربوط به نیروهای مسلح را به دشمنان داخلی یا خارجی یا بیگانگان یا منابع آن تسلیم و یا آنان را از مفاد آن آگاه سازد به مجازات محارب محکوم خواهد شد.

ت- هر نظامی که برای به دست آوردن اسناد یا اطلاعات طبقه‌بندی شده، به نفع دشمن و یا بیگانه به محل نگه داری اسناد یا اطلاعات داخل شود، چنانچه به موجب قوانین دیگر مستوجب مجازات شدیدتری نباشد به حبس از دو تا ده سال محکوم می‌گردد.

تبصره: هر نظامی که عالماً یا عامداً فقط به صورت غیر مجاز به محل مذکور وارد شود به حبس از شش ماه تا ۳ سال محکوم می‌گردد.

ث- هر بیگانه که برای کسب اطلاعات به نفع دشمن به پایگاه‌ها، کارخانجات، انبارهای تسلیحاتی، اردوگاه‌های نظامی، یگان‌های نیروهای مسلح، توقف‌گاه‌های موقتی نظامی، ساختمان‌های دفاعی نظامی و وسائط نقلیه زمینی، هوایی و دریایی وارد شده یا به محل‌های نگهداری اسناد یا اطلاعات داخل شود، به اعدام و در غیر این صورت به حبس از یک تا ده سال محکوم می‌گردد.

تبصره ۱: هر کس در جرائم جاسوسی با نظامیان مشارکت نماید به تبع مجرمان اصلی نظامی در دادگاه‌های نظامی محاکمه و به همان مجازاتی که برای نظامیان مقرراست محکوم می‌شود.

تبصره ۲: معاونت در امر جاسوسی و یا مخفی نمودن و پناه دادن به جاسوس جرم محسوب و مرتکب به تبع مجرمان اصلی نظامی در دادگاه‌های نظامی محاکمه و در مواردی که مجازات محارب و یا اعدام است به حبس از ۳ سال تا پانزده سال محکوم می‌گردد.

ماده ۲۶ ق.م.ن.م: هر نظامی که اسناد و مدارک، مذاکرات، تصمیمات یا اطلاعات طبقه‌بندی شده را در اختیار افرادی که صلاحیت اطلاع نسبت به آن‌ها را ندارند، قرار دهد یا به هر نحو آنان را از مفاد آن مطلع سازد به ترتیب ذیل محکوم می‌شود:

الف- هر گاه اسناد، مذاکرات، تصمیمات یا اطلاعات عنوان به کلی سری داشته باشد به حبس از سه تا پانزده سال.

ب- هر گاه اسناد، مذاکرات، تصمیمات یا اطلاع عنوان سری داشته باشد، به حبس از دو تا ده سال.

پ- هر گاه اسناد، مذاکرات، تصمیمات یا اطلاعات عنوان خیلی محرمانه داشته باشد به حبس از ۳ ماه تا یک سال.

تبصره ۱: هر گاه اسناد، مذاکرات، تصمیمات یا اطلاعات محرمانه داشته باشد، از طرف فرمانده یا رئیس مربوط تنبیه انضباطی خواهد شد.

Archive of SID

ماده ۲۷ ق.م.ن.م: هر نظامی که بر اثر بی احتیاطی یا بی مبالاتی یا سهل انگاری یا عدم رعایت نظامات دولتی موجب افشای اطلاعات و تصمیمات یا فقدان یا از بین رفتن اسناد و مدارک مذکور درماده ۲۶ قانون (ق.م.ا) شود با توجه به طبقه‌بندی اسناد افشا شده به ترتیب زیر محکوم می‌شود:

الف- چنانچه اسناد، مذاکرات، اطلاعات یا تصمیمات، عنوان به کلی سری داشته باشد به حبس از شش ماه تا دو سال.

ب- چنانچه اسناد، مذاکرات، اطلاعات یا تصمیمات عنوان سری داشته باشد به حبس از ۳ ماه تا یکسال.

پ- چنانچه اسناد، مذاکرات، اطلاعات یا تصمیمات، عنوان محرمانه داشته باشد به حبس از دو ماه تا شش ماه.

تبصره: هر گاه اسناد و مدارک، مذاکرات، اطلاعات یا تصمیمات عنوان محرمانه داشته باشد از طرف فرمانده یا رئیس مربوط تنبیه انضباطی خواهد شد.

ماده ۲۸ ق.م.ن.م: هر نظامی که پس از آموزش لازم در مورد حفظ اطلاعات طبقه بندی شده، در اثر بی مبالاتی و عدم رعایت اصول حفاظتی، توسط دشمنان و یا بیگانگان تخلیه اطلاعاتی شود، به یک تا شش ماه حبس محکوم می‌گردد.

جاسوسی رایانه‌ای از نظر کشور آمریکا وشورای اروپا:

با توجه به اینکه در کشورمان ایران هیچ تعریفی از جرائم رایانه‌ای نشده است چه در قانون تجارت الکترونیک و چه در قانون جدید جرائم رایانه‌ای هیچ تعریفی از این مفهوم ارائه نشده است. اما در قانون کشور آمریکا یک تعریف نسبتاً جامع از جرائم رایانه‌ای به طور کلی ارائه شده است که به این طریق می‌باشد: «هر اقدام غیر قانونی که با یک رایانه یا به کارگیری آن مرتبط باشد را جرم رایانه‌ای می گویند».[1]

با توجه به تعریف فوق از جرائم رایانه‌ای در کشور آمریکا می‌توان این نتیجه کلی را گرفت که جاسوسی رایانه‌ای نیز در غالب یک اقدام غیر قانونی است که به وسیله رایانه انجام می‌شود و یا در ارتباط با آن می‌باشد. پس می‌توان برداشت نمود که جاسوسی رایانه‌ای نیز در قانون این کشور پیش بینی شده است.

از نظر شورای اروپا جاسوسی رایانه‌ای یعنی تفتیش و بررسی ابزارهای لازم یا افشای داده در حال انتقال یا استفاده از اسرار تجاری یا بازرگانی بدون حق یا بدون هیچ توجیه قانونی دیگر با قصد خواه

[1] . www.Imj.ir

Archive of SID
www.SID.ir

ضرر اقتصادی به شخص وخواه به قصد کسب یک منفعت اقتصادی غیر قانونی برای خود یا دیگران می‌باشد (خداقلی، زهرا،۱۳۸۳).

اروپا در گذر از ساختار سنتی به یک جامعه اطلاعاتی تحولات عظیمی را در تمامی ابعاد زندگی انسانی، پشت سر گذاشته است. کمیسیون اروپایی در دسامبر ۱۹۹۹ برای اولین بار طرح اروپایی الکترونیکی را به اجرا درآورد تا اطمینان یابد که اروپا می‌تواند از منافع فناوری‌های دیجیتال بهره‌برداری کرده و جامعه اطلاعاتی در تمام ابعاد جامعه شیوع یافته است در ژوئن ۲۰۰۰ شورای اروپا (فیرا) طرح اقدام جامعه اروپای الکترونیکی را پذیرفت و خواستار اجرای آن تا قبل از پایان سال ۲۰۰۲ شد. در این طرح تأکید بسیاری بر اهمیت امنیت شبکه و لزوم مقابله با جرائم اینترنتی شده است اتحادیه اروپایی اخیراً اقداماتی علیه نشر مطالب غیر قانونی و زیان آور، حفظ حقوق مالکیت معنوی و اطلاعات شخصی، ترویج تجارت الکترونیک، استفاده از امضاهای الکترونیکی و ارتقای امنیت معاملات انجام داده است. در آوریل ۱۹۹۸، این کمیسیون نتایج مطالعه‌ای را که در مورد جرائم مربوط به رایانه صورت گرفته بود به شورای اروپا داد در اکتبر ۱۹۹۹ شورای اروپا اعلام نمود که موضوع جرائم مربوط به فناوری‌های پیشرفته را باید در زمره اقداماتی که حصول توافق پیرامون تعاریف و مجازات‌های مشترک لازم است، قرار داد. پارلمان اروپایی، همچنین خواستار ارائه تعاریف قابل پذیرشی از جرائم مرتبط با رایانه و وضع قوانین مؤثر مشابه به ویژه در بخش حقوقی جزای ماهوی شد (ضیایی پور، حمید، ۱۳۸۶).

نحوه کشف و رسیدگی به جرائم رایانه‌ای در رویه قضایی ایران:

با توجه به ماهیت جرائم رایانه‌ای این جرائم ممکن است به دو طریق کشف گردند:

الف)- کشف توسط مراجع، سازمان‌ها و ارگان‌های ذیربط: سازمان‌ها و ارگان‌ها با توجه به استفاده مداوم از رایانه و سیستم‌های نرم افزاری ممکن است با این موارد رو به رو شوند به عنوان مثال ممکن است یک سازمان دولتی رایانه‌هایش مورد هجوم هکرها و یا اطلاعات آنها مورد سرقت و یا جاسوسی از طرف دیگران قرار گیرد.

ب)- با شکایت شاکی خصوصی: این حالت در مواقعی است که از یک رایانه شخصی اطلاعاتی که شخصی است سرقت یا شنود شود و توسط فرد به مراجع شکایت تنظیم گردد. بعد از گزارش به مرجع قضایی، عمل در دستور کار یکی از ارگان‌های پلیس به اسم پلیس فتا قرار می‌گیرد.

نتیجه‌گیری:

در پاسخ به سؤالات مطرح شده در مقدمه می‌توان گفت:

Archive of SID

www.SID.ir

در پاسخ به سؤال اول: دید و نگاه به جاسوسی رایانه‌ای به عنوان ابزار جنگ نرم می‌باشد، همان‌طور که در متن ملاحظه گردید می‌توان آن‌را به دو قسمت تقسیم بندی کرد. ۱- حالت و بخش بررسی فنی جاسوسی رایانه‌ای: در این بخش دریک نگاه سطحی به امر جاسوسی رایانه‌ای این امر به ذهن متبادر می‌شود که با استفاده از رایانه بخواهیم جاسوسی نماییم ولی با بررسی فنی و علمی که داشتیم امر جاسوسی رایانه‌ای یک علم بسیار گسترده و دارای ابعاد بسیار وسیع بوده و از تنوع خاصی برخوردار است. به عنوان مثال جاسوسی از طریق انواع فلش هاو .... شامل این نوع جاسوسی می‌شود.۲- حالت و بخش بررسی حقوقی جاسوسی رایانه‌ای: آن چیزی که درباره جاسوسی رایانه‌ای و بررسی حقوقی آن در زمینه‌ها و جنبه‌های مختلف وجود دارد خیلی فراتر از چند ماده ساده می‌باشد؛ به این معنی که دامنه این جرم خیلی گسترده می‌باشد به عنوان مثال در بخش‌های کشف جرم، دادرسی، تحقیقات مقدماتی، نحوه انجام و عنصر مادی و.... کاملاً با جرائم کلاسیک متفاوت است.

با توجه به مطالبی که در باب جاسوسی صورت گرفت می‌توان نتیجه‌گیری نمود که در دنیای پیشرفته امروزی با پیشرفت و توسعه فناوری‌های مختلف در عرصه‌های جاسوسی نیز انواع روش‌ها و تجهیزات به کار گرفته می‌شود و به طور کلی هم شیوه‌های جاسوسی تفاوت دارد و هم هدف و مقاصد آن‌ها. همان‌طور که دراین مقاله بحث شد بعضی از جاسوسی‌ها از پیشرفت‌های صنعتی است برخی از تلفن‌های همراه و بعضی نیز رایانه‌ای که جزو مدرنترین انواع جاسوسی می‌باشند.

در پاسخ به سؤال دوم: ایرادات و معایب موجود در ماده ۳ و ۴ و ۵ قانون جرائم رایانه‌ای شرح داده شده است. فقط باید عنوان کرد که این مواد دارای ایراداتی هستند و به خصوص در بخش دادرسی و تحقیقات مقدماتی نیز این جرم ویژه می‌باشد و با جرائم کلاسیک کاملاً متفاوت است. هر چند قانونگذار تمام سعی خود را نموده که حداقل ایراد موجود باشد ولی با این اوصاف اشکالاتی مثل این‌که چرا با وجود این‌که درجه اهمیت «به کلی سری از سری» بالاتر است ، در ماده ۳ قانون جرائم رایانه‌ای صرفاً داده‌های سری را مشمول این ماده دانسته است.

منابع

- احمد امین، فجرالاسلام(۱۹۶۹)، بیروت،چاپ دهم،ص ۱۱۳.
- تزو، سون(۱۳۵۹)، هنر جنگ. ترجمه حسن حبیبی، انتشارات قلم.
- جواد علی، المفصل فی تاریخ العرب قبل الاسلام در العلم الملاکیین.بیروت، چاپ اول ،جلد ۵، ص ۴۰۸.
- خداقلی، زهرا(۱۳۸۳)، جرائم کامپیوتری. انتشارات آریان.
- دیندار، مرتضی(بهار ۸۹)، مسولیت کیفری اشخاص حقوقی در قانون جرائم رایانه‌ای.

Archive of SID
www.SID.ir

دانشگاه علامه طباطبایی، دانشکده حقوق و علوم سیاسی.

- دزیانی، محمد حسن(۱۳۸۴)، شروع جرائم کامپیوتری- سایبری، خبرنامه انفورماتیک، شماره ۹۳.

- رئه گارو، ژرژ(۱۳۴۸)، مطالعه نظری و عملی در حقوق جزا. ترجمه ضیاء الدین نقابت، انتشارات ابن سینا، جلد ۳.

- زیبر، اولریش(۱۳۸۳)، جرائم رایانه‌ای. ترجمه محمدعلی نوری،انتشارات گنج دانش.

- ضیایی پور، حمید(۱۳۸۶)،جنگ نرم ۱. موسسه فرهنگی مطالعات وتحقیقات بین المللی ابرار معاصر ایران.

- عالی پور، حسن(۱۳۸۸)، جرائم ضد امنیت ملی. معاونت حقوقی وتوسعه قضایی قوه قضائیه مرکز مطالعات توسعه قضایی.

- گلدوزیان، ایرج(۱۳۸۰)، حقوق جزای اختصاصی (جرائم علیه تمامیت جسمانی، صدمات معنوی، اموال ومالکیت، امنیت و آسایش عمومی). چاپ هشتم، انتشارات دانشگاه.

- مارانش، کنت(۱۳۸۹)، جنگ جهانی چهارم.ترجمه سهیلا کیانتاژ، انتشارات اطلاعات.

- محمدی، ابوالحسن(۱۳۸۲)، قواعد فقه. انتشارات دانشگاه تهران.

- محمدی، نوراله(۱۳۸۷)، مبانی جاسوسی در قانون مجازات اسلامی. پایان نامه کارشناسی ارشد،ص۱۱.

- نسیکی، کلو(۱۳۸۹)، آموزش هک. مترجم الهام بشیری، انتشارات بیشه.

- قانون جرائم رایانه‌ای.

- قانون مجازات اسلامی.

- قانون مجازات نیروهای مسلح.

- eoghan, casey. (2001). "digital evidence and computer crime" academic press, p. 31.

- ralf, De sola. (1982). "crime dictionary, facts on file" new York

- Sheridan, morris. (2004), "the future of net crime" now- part1- threats and challenge, home office online report.

Archive of SID

www.SID.ir

- derba, shinder. (2002) “scene of the cyber crime- computer forensics” hand books, synngress publication.
- Philips, shirelle. (2002) “world of criminal justice” volume1, gale group, Thomson learning, p.260
-
- www.ittink.blogfa.com/post-28.asp
- www.pegahhawzeh.com
- www.Sid.ir
- http://www.ulead.com
- www.itiran.com
- http://www.itnewsway.com

Archive of SID

www.SID.ir