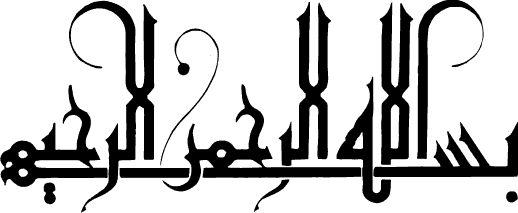
****

**عنوان:**

**جرایم سایبری**

**نام و نام خانوادگی:**

فهرست مطالب

[چکیده 1](#_Toc446613269)

[مقدمه 2](#_Toc446613270)

[جرایم سایبری 3](#_Toc446613271)

[تاریخچه جرایم سایبر 3](#_Toc446613272)

[ویژگی‌های سایبرسپیس 3](#_Toc446613273)

[تعریف محیط سایبر 4](#_Toc446613274)

[جرایم در سایبر اسپیس 5](#_Toc446613275)

[مجرمین سایبر 6](#_Toc446613276)

[1. کرکرها 7](#_Toc446613278)

[2. تفاوت هکرها و کرکرها 7](#_Toc446613279)

[3. فریک‌های تلفن 7](#_Toc446613280)

[بحران سازهای سایبر 8](#_Toc446613281)

[1. ویروس 8](#_Toc446613282)

[2. عنکبوت‌های موتورهای جستجو و پالس‌های الکترومغناطیس 9](#_Toc446613283)

[3. کرم ها 9](#_Toc446613284)

[4. بمب‌های منطقی 9](#_Toc446613285)

[انواع سایبرکرایم 9](#_Toc446613286)

[جرایم سنتی در محیط دیجیتال 10](#_Toc446613287)

[1. جاسوسی رایانه‌ای 10](#_Toc446613288)

[2. سابوتاژ رایانه‌ای 10](#_Toc446613289)

[3. جعل کامپیوتری 10](#_Toc446613290)

[4. افترا و نشر اطلاعات از طریق پست الکترونیک 11](#_Toc446613291)

[5. تطهیر نامشروع پول 11](#_Toc446613292)

[6. قاچاق مواد مخدر 12](#_Toc446613293)

[5. جرایم ناظر به کپی رایت و برنامه ها 13](#_Toc446613294)

[6. جرایم در تجارت الکترونیک 13](#_Toc446613295)

[جرم آینده، تروریسم سایبر 15](#_Toc446613296)

[پلیس سایبر 16](#_Toc446613297)

[امنیت سایبر 17](#_Toc446613298)

[لزوم وجود قانون جرایم رایانه ای (اینترنتی) 18](#_Toc446613299)

[نتیجه گیری 22](#_Toc446613300)

[منابع 24](#_Toc446613301)

# چکیده

در این مقاله از روشهای متعددی برای تحقیق استفاده شد اعم از کتاب، سایت‌های اینترنتی و هدف از انتخاب این موضوع آگاهی نداشتن جامعه در مورد یکسری جرم‌ها که به ظاهر ممکن است نوعی جرم به شمار نیایند و قابل لمس نباشند و به صورت مجازی و غیر قابل ملموس در محیط‌های مجازی صورت می‌گیرند، درست است که این جرم‌ها را با چشم نمی‌توان دید ولی در بعضی موارد ممکن است خطرات بیشماری را به وجود آورند که ممکن است سالیان سال نتوان آنها را جبران کرد، و هدف بررسی انواع جرمهایی که در محیط مجازی بوجود می‌آیند و آشنایی با آنها و چگونگی برخورد و هوشیار شدن اشخاص در حفاظت داده‌های خود، و تفاوت انتخاب این موضوع با سایر موضوع‌ها، ناشناس بودن این جرمها و آگاه ساختن دیگران از آن بود.

# مقدمه

جرایم سایبری، نوعی از جرایم [اینترنتی](http://fa.wikipedia.org/wiki/%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA%DB%8C) می‌باشند که شامل جرم‌هایی هستند که در محیط سایبر بوجود می‌آیند، که در این مقاله ما به تعریف محیط سایبر که یک محیط مجازی می‌باشد و به ویژگی محیط سایبر، بطوریکه کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی در سراسر دنیا دستیابی پیدا کنند و چگونگی ایجاد جرایم که در فضای سایبر کپی عین اصل می‌باشد و انواع مجرمین محیط سایبر شامل هکرها، کرکرها، فریک‌های تلفن و انواع جرم‌های ممکن با نام سایبرکرایم و در مورد جرم آینده با نام تروریسم سایبر که مانند تروریست‌های معمولی دارای انگیزه‌های سیاسی برای ارتکاب جرایم هستند و همچنین بحران سازهای سایبر شامل ویروسها، عنکبوتهای موتورهای جستجو و پالسهای الکترومغناطیسی، کرمها و بمب‌های منطقی و درمورد پلیس سایبر که مطابق با خاص بودن جرم‌های سایبر، نیاز به آموزش‌های خاص دارند و در آخر در مورد روشهای امنیت شبکه و داده‌ها می‌پردازیم.

# جرایم سایبری

# تاریخچه جرایم سایبر

در اواسط دهه ۹۰با گسترش شبکه‌های بین‌المللی و ارتباطات ماهواره‌ای، نسل سوم جرایم کامپیوتری، تحت عنوان جرایم سایبری(مجازی)یا جرایم در محیط سایبر شکل گرفته ‌است .به این ترتیب جرایم اینترنتی را می‌توان مکمل جرایم کامپیوتری دانست، بخصوص اینکه جرایم نسل سوم کامپیوتری که به جرایم در محیط مجازی معروف است، غالبا از طریق این شبکه جهانی به وقوع می‌پیوندد.[۱]

# ویژگی‌های سایبرسپیس

کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند، بدون درنظرگرفتن اینکه این اطلاعات و خدمات در کدام نقطۀ دنیا واقع شده‌است. محیط سایبر زمینۀ فعالیتهای اقتصادی مهم و ابزار ضروری برای انجام کلیۀ معاملات تجاری و در سطح بین‌المللی بدون دخالت مستقیم بشر فراهم آورده ‌است. محدودۀ فعالیت کاربر به مرزهای فیزیکی یک خانه یا یک محل کار و حتی مرزهای یک کشور محدود نبوده و در یک سطح کم هزینه هر کاربر می‌تواند در هر زمانی و در هر مکانی با مردم در هر نقطه‌ای از جهان ملاقات کند و اطلاعات مبادله کند، بدون اینکه از محل واقعی و هویت فرد خبر داشته باشد.

از بعد اقتصادی سایبر سپس را می‌توان یک بازار واحد جهانی دانست که از ثمره‌های موفق جامعه مبتنی بر تکنولوژی مدرن اطلاعاتی می‌باشد که با روند توسعه آن روابط اجتماعی و سنتی و فرهنگی حاکم بر روابط افراد را در سطح ملی دچار تحول نماید.[۱]

# تعریف محیط سایبر

از لحاظ لغوی در فرهنگ ‌های مختلف سایبر به معنی مجازی و غیر ملموس می‌باشد، محیطی است مجازی و غیر ملموس موجود در فضای شبکه‌های بین‌المللی(این شبکه ها از طریق شاهراه ‌های اطلاعاتی مثل اینترنت بهم وصل هستند)که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگها، ملتها، کشورها و به طور کلی هرآنچه در کرۀ خاکی بصورت فیزیکی ملموس وجود دارد(به صورت نوشته، تصویر، صوت، اسناد) دریک فضای مجازی به شکل دیجیتالی وجود داشته و قابل استفاده و دسترس کاربران می‌باشند و به طریق کامپیوتر، اجزا آن و شبکه‌های بین‌المللی بهم مرتبط می‌باشند.[۱]

# جرایم در سایبر اسپیس

فضای سایبر هنوز در مراحل اولیه است. طبیعت این جرایم و سوءاستفاده‌های مرتکب شده در این دنیای مجازی جدید هیچ گاه در دنیای حقیقی دیده نشده است. امنیت نا کافی تکنولوژی همراه با طبیعت مجازی آن فرصت مناسبی را در اختیار افراد شرور قرار می‌دهد. نگران کننده‌ترین جنبۀ فضای سایبر انتشار سریع اطلاعات درآن می‌باشد، مثلا در لحظۀ کوتاهی قسمتی از اطلاعاتی که می‌تواند بطور بالقوه مورد سوءاستفاده قرار گیرد کشف می‌شود. در فضای سایبر برای جستجو و پیداکردن این جرایم مشکلات پیچیده تر می‌شود. در دنیای واقعی دزدی از بانک کاملا مشخص است چرا که بعد از سرقت در خزانه بانک پولی موجود نیست. ولی در تکنولوژی کامپیوتری شدن یک خزانه می‌تواند بدون هیچ علامتی خالی شود.

برای مثال سارق می‌تواند یک کپی دیجیتال کامل از نرم‌افزار بگیرد و نرم‌افزار اصلی را همان طور که دقیقا بوده باقی بگذارد. در فضای سایبر کپی عینا عین اصل است با کمی کار روی سیستم، سارق می‌تواند امکان هرگونه تعقیب و بررسی مثل پاک کردن اثر انگشت تغییر دهد.[۱]

# مجرمین سایبر

هکر: در دهۀ ۱۹۷۰ واژۀ هکر به شخصی اطلاق می‌شد که در برنامه نویسی بسیار ماهر و باهوش باشد. بعدها در دهۀ ۱۹۸۰ این واژه به معنی شخصی بود که در نفوذ به سیستم‌های جدید به صورت ناشناس تبحر داشته باشد. امروزه بیشتر با هدف ترساندن هکرها، رسانه‌ها و مقامات مسئول مانند آژانس‌های دولتی و ادارات پلیس، این واژه به هر شخصی که مرتکب یک جرم مرتبط با فناوری شود، اطلاق می‌کنند. این درست است که هکرهای کنجکاو میتوانند سهوا باعث زیان‌های قابل توجهی شوند، اما جستجو برای یافتن اطلاعات و آموزش، نه انتقام گیری یا صدمه زدن به دیگران، عاملی است که باعث می‌شود اکثر هکرها سرگرمی خود را به نحوی بیرحمانه دنبال کنند.

1. کرکرها: از سوی دیگر کرکرها هکرهای بدخواهی هستند. آنها به سیستم‌ها رخنه می‌کنند تا خرابکاری کنند، ویروس‌ها و کرمهای رایانه‌ای را منتشر کنند، فایلها را پاک کنند یا بعضی انواع دیگر ویرانی را ببارآورند. اختلاس، کلاهبرداری یا جاسوسی صنعتی(سرقت اطلاعات محرمانه یک شرکت)تنها بخش کوچکی از اهداف احتمالی کرکرها می‌باشد.
2. تفاوت هکرها و کرکرها: هکرها دریک مورد مهم با کرکرها تفاوت دارند، کارهایی که آنها انجام می‌دهند معمولاً از روی بدخواهی نیست. انگیزه بیشتر هکرها برای این کار، تمایل شدید به یادگیری نحوه کار سیستم رایانه، یافتن راهی برای ورود مخفیانه به آنها و پیداکردن سوراخ‌های امنیتی این سیستم هاست هیجان خواندن اطلاعاتی که می‌دانند اجازه دیدن آنها را ندارند یا انجام کاری که می‌دانند قانونی نیست به لذت دست زدن به چنین تجاربی توسط هکرها به عنوان سرگرمی می افزاید. آنها در فعالیت‌های خود معتقد به نگرش ببین اما دست نزن هستند.
3. فریک‌های تلفن: شکل دیگر از جرایم رایانه‌ای را «فریک‌های تلفن» مرتکب می‌شوند. فریک‌ها به جای دسترسی به سیستم‌های رایانه ای، از طریق خطوط تلفن در دنیای سایبر گشت می‌زنند. فریک‌ها از میان اولین هکرها دردهه۱۹۷۰ پدید آمدند. یکی از حوادثی که توسط فریک‌ها بوجود آمده بود در سال ۱۹۷۷ مربوط به اداره پلیس شهر نیویورک می‌شد، فریک‌ها به سیستم تلفن این اداره نفوذ کرده بودند و متن ضبط شده‌ای را که به تماس گیرندگان خوشامد می‌گفت تغییر داده بودند، در متن ضبط شدۀ جدید گفته می‌شد که افسران پلیس مشغول خوردن نان شیرینی و نوشیدن قهوه هستند و فرصت جواب دادن به تلفن‌ها را ندارند، این پیام به تماس گیرندگان توجه می‌کرد که در موارد اورژانس با شماره ۱۱۹ تماس بگیرند.[۱،۲]

# بحران سازهای سایبر

1. ویروس: ویروس‌ها یا برنامه‌های خود همانند ساز، برنامه‌هایی هستند که با هدف آلوده کردن سیستم‌های دیگر نوشته می‌شوند و معمولا از طریق یک دیسکت و گاهی از طریق اینترنت یا شبکه‌های پست الکترونیک سرایت می‌کنند. بعضی ویروسها ممکن است قادر به حمله به فایل‌های سیستم و ذوب کردن مادربورد یک رایانه، پاک کردن تمام داده‌های دیسک سخت و از کارانداختن رایانه باشند.
2. عنکبوت‌های موتورهای جستجو و پالس‌های الکترومغناطیس: که می‌توانند دیسک سخت یک رایانه را ذوب کنند.
3. کرم ها: میتوانند به یک سیستم دسترسی پیدا کنند اما نمی‌توانند در خارج از شبکه، برای مثال از طریق یک دیسکت، گسترش پیدا کنند. کرم‌ها در یک رایانه مقیم می‌شوند و فضای رایانه را اشغال می‌کنند تا آنکه رایانه کند شود یا از کار بیفتد.
4. بمب‌های منطقی: آنها تعمدا زیانبار ساخته می‌شوند اما مانند ویروس‌ها تکثیر نمی‌شوند. آنها طوری طراحی شده اند که طی یک دورۀ زمانی در رایانه غیرفعال باقی می مانند و سپس با سر رسیدن تاریخی که برنامۀ آنها مشخص شده است منفجر می‌شوند. اهداف این بمب‌ها متفاوت است.[۲]

# انواع سایبرکرایم

تنوع انواع جرایم ارتکابی در سایبرسپیس شامل جرایم نسل اول کامپیوتری (البته به شکل نوین) و یکسری جرایم بسیار جدید و بی سابقه می‌باشد.

# جرایم سنتی در محیط دیجیتال

* 1. جاسوسی رایانه‌ای: جاسوسی رایانه‌ای همانند جاسوسی کلاسیک ناظر به کسب اسرار حرفه ای، تجاری، اقتصادی، سیاسی، نظامی و نیز افشاء و انتقال و استفاده از اسرار است، فرد مرتکب جرم با دستیابی و فاش کردن این اسرار، ضرر سیاسی، نظامی، مالی، تجاری بمیکند. این جرم امنیت ملی را با مخاطره مواجه می‌کند.
  2. سابوتاژ رایانه‌ای: این جرم با جرم تخریب شباهت بسیاری دارد، هدف مجرم اخلال در نظام سیاسی و اقتصادی یک کشور و بالطبع اخلال در امر حکومت است. در واقع اصلاح، موقوف سازی، پاک کردن غیرمجاز داده‌ها یا عملیات کامپیوتر به منظور مختل ساختن عملکرد عادی سیستم سابوتاژ رایانه‌ای گویند.
  3. جعل کامپیوتری: وارد کردن، تغییر، محو یا موقوف سازی داده‌های کامپیوتری یا برنامه‌های کامپیوتری به منظور و اهداف سیاسی و اقتصادی صورت میگرد. جعل کامپیوتری جعل داده هاست. در جعل کامپیوتری عمل ارتکابی بر داده‌ها اثر میگذارد، با این تفاوت که داده، ماهیت اسناد عادی را ندارد.
  4. افترا و نشر اطلاعات از طریق پست الکترونیک: پست الکترونیک مرسوم‌ترین وگسترده‌ترین سرویس شبکه‌های کامپیوتری و بین المللی است، هر کاربر می‌تواند در شبکه‌های بین‌المللی از طریق یک آدرس مشخص الکترونیک شناخته شود که با دسترسی به رمز آن می‌توان به آسانی درآن تقلب کرد. این قابلیت پست الکترونیک می‌تواند ابزاری جالب برای نشر اطلاعات مجرمانه یا نشر اکاذیب و افترا به اشخاص باشد و احتمال کنترل اطلاعات برای تهیه کننده کاملا مشکل است و در عمل به خاطر تعداد بسیار زیاد پست الکترونیک ارسالی، اتخاذ تدابیر کلی و گسترده امنیتی مشکل بوده و تنها برای بخش کوچکی از داده‌ها میسر می‌باشد.
  5. تطهیر نامشروع پول: بدست آوردن پول از طریق غیر قانونی یا پول کثیف، به نحوی که قانونی یا پاک به نظر برسد، از جرایم کلاسیک بوده که در محیط سایبر به کمک اینترنت، پست الکترونیک و شبکه‌های بین‌المللی ارتباطی صورت می پذیرد، نحوۀ ارتکاب بدین نحو است که باندهای بزرگ نامشروع توسط پست الکترونیک یا اینترنت بدون هیچ کونه اثر و نشانی درخواست ارسال مبالغی پول به حساب شخص معینی را مینمایند و در تقاضای خود نحوۀ ارسال پول و دستمزد و مدت استرداد را بیان و در صورت قبول طرف نوع و نحوۀ تنظیمات لازم را اعلام می‌دارند و اصولا در زمان استرداد پول یک عنوان مشروع در تجارت الکترونیک را با منشا تجاری انتخاب وبا هدف خود هماهنگ می نمایند لازم به ذکر است غالب این درخواستها از افراد کشورهایی که از لحاظ تکنولوژی اطلاعاتی و ارتباطی و هماهنگی پلیسی در سطح بین‌المللی در درجۀ پایین تری قرار دارند انتخاب می‌شود.
  6. قاچاق مواد مخدر: با توجه به گسترش ارتباطات شبکه‌ای و در محیط سایبر و دسترسی آسان افراد به هم از طریق پست الکترونیک و اینترنت هرگونه قاچاق مواد مخدر اعم از خرید، فروش، پخش، توزیع یافتن واسطه ها و مصرف کنندگان از طریق شبکه‌های کامپیوتری انجام می‌شود. از ویژگیهای آن حذف و کمتر نمودن واسطه‌ها و توزیع کنندگان، گسترش دامنۀ فعالیت قاچاق چیان تا سطح بین‌المللی، اقدامات پلیس در خصوص کشف فروشندگان و خریداران مواد مخدر به سختی و در مواردی غیر ممکن می‌باشد و ضریب اطمینان قاچاق مواد مخدر از طریق ارتباطات کامپیوتری و شبکه‌ای بالاتر از نوع سنتی آن می‌باشد.

1. جرایم ناظر به کپی رایت و برنامه ها: هرگونه تکثیر، ارسال، انتقال، در اختیار عامه گذاشتن، پخش گسترده، توزیع، فروش و استفادۀ غیر مجاز از برنامه‌های کامپیوتری سرقت نرم‌افزار گویند.
2. جرایم در تجارت الکترونیک: شامل کلاهبرداری در تجارت، تعریف کلی و کلاسیک کلاهبرداری عبارتست از «تحصیل مال دیگری با استفاده از وسایل متقلّبانه» شخصی در نقطه‌ای نامعلوم با وارد شدن به شبکۀ بین‌المللی (مثل اینترنت)و معرفی خود به عنوان تاجر و صاحب یک شرکت معتبر در یک سایت تجاری و ارائۀ نهادی مشابه ادارۀ ثبت اسناد که این نهاد عهده دار ثبت داده‌های تجاری و تجار است تا بدین ترتیب تاجر مجوز ورود به عرصۀ تبادلات الکترونیک را کسب نماید وهم چنین نهادی که در تجارت الکترونیک به معنای زیرساخت کلید عمومی است. اساس تجارت الکترونیک و از محورهای عمده و مهم آن داشتن این نهاد برای تجار می‌باشد (تماما غیرواقع و کذب)، اظهار می‌دارد که کالایی را با قیمت معین، نوع و تعداد مشخص در اختیار داشته و قابل عرضه به مشتریان می‌باشد از طرفی خریدارانی که در فضای شبکه‌ها مشغول تجارت الکترونیک( خرید و فروش) می‌باشند پس از دریافت پیام، نسبت به برقراری ارتباط شبکه ای(که غالبا به صورت پست الکترونیک یا ارسال درخواست هر طریق شبکه می‌باشد قبول (خرید) خود را اعلام و مقداری از کالای مورد نظر را درخواست می‌کنند. شخص فروشنده پس از جلب اعتماد طرف مقابل، نسبت به اعلام شماره حساب یا شماره کارت اعتباری خود برای دریافت وجه اقدام مینماید. خریدار نیز پس از پرداخت وجه (غالبا به صورت پرداختهای الکترونیکی) منتظر دریافت کالا می‌باشد در صورتیکه شخص فروشنده قبلا با عملیات‌های متقلّبانه و نفوذ توانسته بوده که نهادهای نامبرده را به صورت غیرواقع برای خود اختیار نماید و بدین وسیله مبلغی را من غیرحق کسب نماید.

# جرم آینده، تروریسم سایبر

والتر لاکور یک متخصص تروریسم در مرکز مطالعات استراتژیک و بین المللی اشاره می‌کند که یک مقام رسمی سیا ادعا کرده است که می‌تواند با یک میلیارد دلار و ۲۰ هکر قابل، ایالت متحده را فلج کند. لاکور یادآوری می‌کند که اگرچه هدف تروریست‌ها معمولاً قتل سران سیاسی، گروگان گیری یا بعضا حمله ناگهانی به تسهیلات دولتی یا عمومی است، اما صدمه‌ای که ممکن است به وسیلۀ حمله الکترونیکی به شبکه‌های رایانه‌ای وارد آید می‌تواند بسیار غم انگیزتر باشد و اثرات آن تا مدت‌ها باقی بماند. لاکور معتقد است که تروریسم رایانه‌ای ممکن است برای تعداد کثیری از مردم بسیار ویران کننده تر از جنگ‌های بیولوژیک یا شیمیایی باشد. از اقدامات سایبر ترور ارتباط بین تروریست‌ها از طریق شبکه‌های بین‌المللی و تبادل افکار و اعمال مجرمانه در سطح بسیار پیچیده است که از ویژگیهای این نوع ارتباط عدم توانایی پلیس در کنترل و شنود این ارتباطات می‌باشد. اما آیا واقعاً تروریسم سایبر امکان پذیر است؟ در سال ۱۹۹۱ حین جنگ خلیج فارس که میان عراق و ائتلافی از چند کشور به رهبری ایالت متحده در گرفت، یک جوان ۱۸ ساله فلسطینی، متهم به نفوذ به رایانه‌های پنتاگون شد. این مرد جوان ظاهرا به اطلاعات سری مربوط به موشک پیتریوت دسترسی پیدا کرده بود که یک سلاح کلیدی آمریکا برای دفاع در مقابل حمله موشکهای اسکاد عراق محسوب می‌شد. در نفوذ دیگری در همان جنگ چندین نوجوان هلندی به رایانه‌های نظامی، زمینی، هوایی و دریایی ایالت متحده در۳۴ سایت مختلف نفوذ کردند، نفوذ کنندگان در یکی از حملات خود به داده‌های بسیار حساسی درباره پرسنل نظامی، نوع و میزان تجهیزات نظامی فرستاده شده به خلیج فارس، اهداف موشکها و توسعۀ سیستم‌های تسلیحاتی دست یافتند، در واقع این نوجوانان کرکرهایی بودند که تنها به خواندن این فایلها اکتفا نکردند بلکه اطلاعات مربوط به تحرکات ارتش و توانایی موشک‌ها را سرقت کردند و در اختیار عراقی‌ها قراردادند.[۱،۳]

# پلیس سایبر

بعضی از افسران پلیس از دهه۱۹۷۰ در زمینه جرایم سایبر آموزش دیده اند و تخصص پیدا کرده اند. جرایم سایبر ممکن است در هر جایی اتفاق بیفتد و غالبا قابل ردیابی نیستند. بیشتر ادارات پلیس محلی فاقد پرسنل ماهر یا بودجه لازم برای مبارزه با جرایم سایبر هستند به ویژه به این دلیل که این پرونده‌ها ممکن است در آن واحد به حوزه‌های قضایی متعددی مربوط شوند. بنابراین چه کسی مسئول مبارزه با جرایم سایبر خواهد بود؟ علاوه برآنچه پلیس رایانه‌ای نامیده می‌شود، شهروندانی نیز وجود دارند که به صورت شخصی به جلوگیری از جرایم سایبر و شناسایی مجرمان کمک می‌کند. هنوز هم مباحثات زیادی درمورد روشهای مورد استفاده توسط مقامات رسمی، در اجرای قوانین مبارزه با جرایم سایبر وجود دارد. پلیس تا چه حد مجاز است که در تحت پیگرد قراردادن و دستگیری مجرمان سایبر به ویژه هکرها پیش رود؟ پلیس تا چه حد اجازه دارد که به حریم خصوصی الکترونیک شهروندان پا بگذارد؟ چگونه باید میان حقوق افراد و نیاز مقامات دولتی برای تحقیقات و تشکیل پرونده تعادل برقرار کرد؟ ولی با این وجود پلیس توانسته بسیاری از هکرهای بدخواه را شناسایی کند و در یافتن مجرمان سایبر موفق باشد.[۲]

# امنیت سایبر

با وجود تبادل عظیم اطلاعات حیاتی و یا خصوصی از طریق اینترنت باید دید اینترنت تا چه حد برای ارسال داده‌های حساس، مطمئن است. و امنیت شبکه‌ها وقتی داده‌ها درآن جریان پیدا می‌کنند چگونه است؟ چرا که با وجود جریان داده‌ها روی اینترنت بسیار طبیعی است که فکر کنیم گوش دادن و گرفتن اطلاعات حساس موجود می‌تواند کار ساده‌ای باشد. اما رمز گذاری روی داده ها (غیر قابل فهم یا غیر قابل خواندن داده ها)لایه سوکت‌های امن به عنوان استاندارد ایمنی و رمز عبور معتبر، جداسازی داده‌ها روی کامپیوترهای متعدد و تفکیک پایگاه داده‌ها (جدا نگه داشتن اطلاعات مشتریان)روش‌های پیشرفته در ایمنی داده‌ها می‌باشند. که می‌توانند از دستیابی هکرها به داده‌ها جلوگیری کنند.[۲،۳]

# لزوم وجود قانون جرایم رایانه ای (اینترنتی)

حقوق مالکیت فکری به عنوان حق کنترل نسخه برداری از روی اثر و سایر کاربردهای آن برای مدت زمانی محدود در نظام های حقوقی کشورهای مختلف و در سطح بین الملل شناخته شده است. با ظهور رسانه های جدید و گسترش شبکه های رایانه ای و اینترنت، فرصت های تازه ای هم در کنترل اطلاعات و بیان و هم فرار از این کنترل را فراهم کرده و از طرف دیگر صاحبان اثر را به کنترل انحصاری اثر خود برانگیخته و مردم را نیز به دسترسی آزاد و گسترده تر آن دعوت کرده است.

امروزه تولیدکنندگان محتوا به یک سری بنگاه های خاص محدود نیستند و هر فرد می تواند انواع رسانه ها از جمله رادیو اینترنتی، پادکست و برنامه های تصویری ایجاد کند. مهمترین جرم های اینترنتی در جهان انتشار اخبار کذب، ارسال مطالب، تصاویر و فیلم های مستهجن، آموزش و تبلیغ تروریسم، هتک حرمت افراد، استفاده از فضای متعلق به دیگران، ارسال پیام های مخرب، اخلال دسترسی به دیگران، دین زدایی، حک و ویروسی کردن سایت ها و ... می باشند.

لذا می بینیم که با توجه به پیشرفت علم و گستردگی کاربرد اینترنت در جهان امروز، در بسیاری از کشورهای جهان مقررات و شرایط ویژه ای برای حمایت از حقوق کاربران اینترنتی وضع شده است و این مقررات پیش از آن که جنبه کنترل و نظارت توسط دولت ها را داشته باشد، به طور خاص در زمینه حمایت از کاربران اینترنت و شهروندان آن کشورهاست.

برخی نویسندگان مانند سوزان برنر، حقوقدان آمریکایی معتقدند که پدیده رایانه ها یا اینترنت نیاز به قوانین مجزا و قانونگذاری جدید ندارند و اصلاح و تغییر قوانین سنتی جزایی پاسخگوی نیازها در برابر جرایم رایانه ای – سایبر است. این نویسندگان معتقدند همان گونه که با اختراع تلفن و به وجود آمدن جرایمی مانند مزاحم تلفنی یا (Tele Crime) ایجاد نشده است، استفاده از فضای سایبر نیز صرفا یک فناوری جدید برای ارتکاب جرم است. در مقابل حقوقدانانی مانند دان پارکر معتقدند به دلایل زیر وضع حقوق جزای مستقل برای جرایم رایانه ای ضرورت دارد:

1- دنیای مجازی به طور سمبلیک، دنیای جدید است که باید از طریق قانونگذاری مستقل مانند دنیای واقعی آن را به نظم در آوریم.

2- مجرمان سایبر از لحاظ جرم شناسی از مجرمان عادی متفاوتند و مجازات ها و درمان های متفاوتی را نیاز دارند.

3- ضررهای ناشی از جرایم سایبر بسیار بیشتر از جرایم عادی است.

4- مشکلات ناشی از کشف جرم و تعقیب متهمان و به مجازات رساندن آن ها و خاصیت بین المللی این جرایم به آن ها ماهیتی متفاوت از جرایم سنتی می بخشد.

نکته اساسی در جرایم اینترنتی حذف مکان در قلمرو مکان فیزیکی و محدود حاکمیت سیاسی است. امکان دارد جرم در محدوده خارج از جغرافیا و قلمرو حاکمیت کشور انجام شود و جرم انگاری لازمه نادیده گرفتن اصل صلاحیت سرزمینی و توسعه مرزهای جغرافیایی است.

تاریخچه مشخصی از جرم اینترنتی و کامپیوتری وجود ندارد. ولی به هر حال این دسته از جرایم را باید زاییده و نتیجه تکنولوژی ارتباطی و اطلاعاتی دانست. در ابتدا جرم اینترنتی و کامپیوتری منحصر به جعل اسکناس و چک، اسناد و بلیط های شرکت های اتوبوسرانی و جعل اسناد دولتی می گردید. چنانچه اولین جرم رایانه ای در ایران در 26 خرداد 1378 به وقوع پیوست که مربوط به جعل چک های تضمینی مسافرتی بود و در آن زمان هنوز تفاوت و تمایز چندانی بین جرم اینترنتی و رایانه ای نبود. اما هم اکنون با گسترش روز افزون اینترنت و دسترسی تقریبا همگانی به آن، جرایم اینترنتی نسبت به جرایم رایانه ای شکل متمایزی را به خود می گیرند. چنان که شاید یکی از مهمترین و خبرسازترین پرونده ها، توزیع سی دی ها یا تصاویر مستهجن به نمایش در آمده در سایت های مختلف از افراد مشهور از جمله بازیگران یا مردم عادی است. در قسمت دوم این مقاله به بررسی انواع جرائم رایانه ای و نحوه برخورد با آنها در کشور های مختلف خواهیم پرداخت.

# نتیجه گیری

در این مقاله ما در مورد محیط سایبر، چگونگی بوجود آمدن این جرمها در این محیط، عوامل بوجود آورندۀ این جرمها، انواع مجرمین و چگونگی برخورد با مجرمان و امنیت محیط شبکه‌ها بحث کردیم. هدف ما از این است که بتوانیم برای شبکه‌ها و محیط‌های اینترنتی خود امنیتی بوجود بیاوریم و از این جرایم جلوگیری کنیم که بهترین راه برای جلوگیری از وقوع اکثر جرایم رایانه‌ای یا غیر رایانه‌ای به آگاهی ما بستگی دارد. اگر تعداد بیشتری از مردم از اشکال و روش‌های فعلی جرایم سایبر آگاهی یابند، تعداد قربانیان کاهش خواهد یافت.

صدها شرکت مشاور امنیت رایانه در سطح جامعه و در تمام جهان پدید خواهد آمد وبا برطرف کردن ضعف‌های سیستم‌های رایانه‌ای و نرم‌افزارها، حفاظت بیشتری پدید خواهند آورد. هم چنین استفاده از روش‌های رمز گذاری روی داده ها، لایه سوکت‌های امن، جداسازی داده ها، میتواند روشهای مفیدی برای جلوگیری از دستیابی هکرها به داده‌ها شود. و در آخر اینکه محتمل بودن جرایم سایبر سیاسی با افزایش مهارت تعداد بیشتری از افراد در برنامه نویسی و نفوذ به سیستم‌های رایانه افزایش می‌یابد، اما تروریسم و جاسوسی رایانه‌ای تنها تهدیدهایی برای شبکه‌های رایانه‌ای نیستند!!جرایم سایبر می‌تواند امنیت و خلوت افراد را نیز همانند امنیت جامعه به خطر بیندازد.

# منابع

1. برومند باستانی «جرائم کامپیوتری و اینترنتی» انتشارات بهنامی، تهران،۱۳۸۳
2. Gina.De.Angelis،Cyber Crimes ،Chelsea House Publisher.۲۰۰۰
3. دکتر ابراهیم حسن بیگی «حقوق و امنیت در فضای سایبر» موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار، تهران،۱۳۸۴
4. قانون مجازات اسلامی، قانون تجارت الکترونیک، قانون مطبوعات، قانون حمایت از حقوق مولفان و مصنفان و هنرمندان و قانون جرایم رایانه ای.
5. ماهرخ دانش کیا، گسترش جرایم اینترنتی و رایانه ای، نشریه صدای عدالت، 1383.
6. علیرضا اکبری، فصلنامه کتاب (حق مولف در اینترنت)، ش 65، بهار 1385.
7. یکتا معظمی به راهنمایی حسین آقایی نیا، رویکردهای حقوقی نسبت به مفهوم جرم رایانه ای ( از دیدگاه بین المللی و ایران )، پایان نامه کارشناسی ارشد دانشگاه تهران-دانشکده حقوق و علوم سیاسی، 1383.
8. عبد الصمد خرم آبادی به راهنمایی حسین آقایی نیا و استاد مشاور : محمد آشوری و سید علی آزمایش، جرایم فناوری اطلاعات، پایان نامه دکترای تخصصی دانشگاه تهران-دانشکده حقوق و علوم سیاسی، 1384.