فهرست مطالب

مقدمه: [1]

امروزه فناوری اطلاعات صرف نظر از موقعیت جغرافیایی، در تمامی شئون زندگی وارد شده است و هریک از افراد، بسته به نیاز خود از مزایای این علم بهره مند می شوند. گرچه فضای سایبر همانند دیگر عناصر زندگی اجتماعی، از گزند یک پدیده بسیار انعطاف‌پذیر و لاینفک از اجتماع به نام جرم در امان نمانده است. دنیای ارتباطات و فضای سایبر، فرصتهای جدید و بسیار پیشرفته ای را برای قانون شکنی در اختیار کاربران خود قرار داده که امکان رفتارهای ضد اجتماعی و مجرمانه مهیا شده است.

به طور کلی، آنچه امروزه تحت عنوان جرم سایبر قرار می‌گیرد، دو طیف از جرائم است: گروه اول جرائمی هستند که نظایر آنها در دنیای فیزیکی نیز وجود دارد و فضای سایبر بدون تغییر ارکان مجرمانه‌شان، با امکاناتی که در اختیار مجرمان قرار می‌دهد، ارتکابشان را تسهیل می‌کند. جرائم تحت شمول این حوزه بسیار گسترده‌اند و از جرائم علیه امنیت ملی و حتی بین‌المللی نظیر اقدامات تروریستی گرفته تا جرائم علیه اموال و اشخاص را در برمی‌گیرند. اما طیف دیگر جرائم سایبر، به سوء استفاده‌های منحصر از این فضا مربوط می‌شود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست. جرائمی نظیر دسترسی غیرمجاز به داده ها 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.

جرائم رایانه‌ای ـ سایبری را در قالب سه نسل مورد بررسی قرار می‌دهند که قابل توجه می باشد:

نسل اول جرائم رایانه‌ای: همانگونه که از عنوان پیداست، این نسل به ابتدای ظهور سیستمهای رایانه‌ای، به ویژه زمانی که برای اولین بار در سطح گسترده‌ای در دسترس عموم قرار گرفتند، مربوط می‌شود. در آن زمان، عمده اقدامات غیرمجاز، به ایجاد اختلال در کارکرد این سیستمها و به تبع آن دستکاری داده‌ها مربوط می‌شد.

---

[1] مهرنوش ابوذری- استادیار و عضو هیات علمی دانشگاه تهران- گروه حقوق جزا و جرم شناسی

نسل دوم جرائم رایانه‌ای: این نسل از جرائم پل ارتباطی میان نسل اول و سوم بوده و دلیل بارز آن هم عمر بسیار کوتاه این نسل است که به سرعت با ظهور نسل سوم منتفی شد. این رویکرد که از اواخر نسل اول زمزمه‌های آن شنیده می‌شد، به دلیل محوریت یافتن داده‌ها اتخاذ گردید. دلیل آن هم این بود که در دوران نسل اول، سیستمهای رایانه‌ای به تازگی پا به عرصه گذاشته بودند و عمدتاً به شکل سیستمهای شخصی یا رومیزی بوده و به همین دلیل به تنهایی مورد توجه قرار گرفته بودند. اما به تدریج با توسعه و ارتقای فناوری رایانه و به کارگیری آن در بسیاری از ابزارها و به عبارت بهتر رایانه‌ای شدن امور، به تدریج ابزارهای رایانه‌ای جایگاه خود را از دست دادند و محتوای آنها یعنی داده‌ها محوریت یافت. بدیهی است در این مقطع مباحث حقوقی و به تبع آن رویکردهای مقابله با جرائم رایانه‌ای نیز تغییر یافت، به نحوی که تدابیر پیشگیرانه از جرائم رایانه‌ای با محوریت داده‌ها و نه واسطشان تنظیم شدند. حتی این رویکرد در قوانینی که در آن زمان به تصویب می‌رسید نیز قابل مشاهده است.

به این ترتیب، سیستمهای رایانه‌ای در صورتی در دوران نسل دوم، ایمن محسوب می‌شدند که داده‌های موجود در آنها از سه مولفه برخوردار بودند: ۱. محرمانگی: داده‌ها در برابر افشا یا دسترسی غیرمجاز حفاظت شده باشند؛ ۲. تمامیت: داده‌ها در برابر هرگونه تغییر یا آسیب حفاظت شده باشند؛ و ۳. دسترس‌پذیری: با حفظ کارکرد مطلوب سیستم، داده‌ها همواره در دسترس مجاز قرار داشته باشند.

هم اکنون، این سه مولفه در حوزه ی جرائم نسل سوم از جایگاه ویژه‌ای برخوردارند و حتی در اسناد قانونی به صراحت به آنها اشاره شده است.

برای مثال، عنوان اول از بخش اول فصل دوم کنوانسیون جرائم سایبر (بوداپست، ۲۰۰۱)، به جرائم علیه محرمانگی، تمامیت و دسترس‌پذیری داده‌ها و سیستمهای رایانه‌ای اختصاص دارد. در ذیل این عنوان، پنج مادّه به طور مفصل جرائم این حوزه را برمی‌شمرند که عبارتند از: دسترسی غیرقانونی، شنود غیرقانونی، ایجاد اختلال در سیستم و سوء استفاده از دستگاهها.

این دوره با وجود عمر کوتاه خود، تاثیر بسزایی در تحول نگرش به جرائم رایانه‌ای داشت. حتی می توان گفت، تقریباً از این زمان بود که اصطلاحاتی نظیر جامعه ی اطلاعاتی یا حقوق کیفری اطلاعات به طور رسمی در اسناد قانونی وارد شد.

نسل سوم جرائم رایانه‌ای: از اوایل دهه نود، با جدی شدن حضور شبکه‌های اطلاع‌رسانی رایانه‌ای در عرصه بین‌الملل و به ویژه ظهور شبکه جهانی وب که به فعالیت این شبکه‌ها ماهیتی تجاری بخشید، بحث راجع به ابعاد گوناگون فضای سایبر به ویژه مسائل حقوقی آن، وارد مرحله جدیدی شد. زیرا تا آن زمان شبکه‌های رایانه‌ای در ابعاد منطقه‌ای، محلی و در حوزه‌های محدودی نظیر سیستمهای تابلوی اعلانات که عمدتاً جهت بارگذاری و پیاده‌سازی برنامه‌ها، پیامها و همچنین ارتباطات پست الکترونیک به کار می‌رفتند به فعالیت می‌پرداختند.

بنابراین می توان گفت فضای سایبر، فرصت های تازه و بسیار پیشرفته‌ای را برای قانون شکنی در اختیار انسان می‌گذارد، هم‌چنین توان بالقوه ارتکاب گونه‌های مرسوم و کلاسیک جرایم را به شیوه‌های غیرمرسوم و بسیار جدید سوق می‌دهد تا مجرمان سایبری بتوانند در این کهکشان صفر و یک، هرآنچه می‌خواهند و در اندیشه دارند، به منصه ظهور برسانند. این امر، علوم مختلف و از جمله جرم‌شناسی را با تحول روبرو ساخت .

لذا با گسترش فرصت های فعالیت مجرمانه در فضای سایبر و نگرانی مردم از این جرایم، توجه اختصاصی حقوقدانان و جرم شناسان به جرایم ارتکابی در این فضا جلب شد و منجر به ایجاد حوزه مطالعاتی جرم شناسی سایبری گردید.

گرچه عده ای معتقدند حوزه سایبری وسیله ای نوین برای ارتکاب جرایم سنتی(جرایم ارتکابی در فضای واقعی) هستند و لذا آورده جدیدی نیستند که برایشان قائل به قانون جدید و مباحث نظری جدید باشیم اما عقیده غالب که با گذشت زمان و توسعه جرایم سایبری از حیث کمی و کیفی و تنوع انواع و اشکال، بر آن صحه گذاشته شده، قائل است اینترنت فضای جدیدی با ماهیتی کاملا متفاوت از فضای واقعی (جرایمی مانند هک کردن) خلق کرده است.

از این رو جرایم سایبری به علت مزایایی که مجرمان در آن می بینند، رو به گسترش است. ویژگی های مطلوب و مزایای حضور مجرمانه در فضای سایبر این است که از یک سو ارتکاب آنها آسان بوده و با کمترین ریسک از جهت احتمال دستگیری یا عدم موفقیت و شناسایی، به نتیجه مطلوب خود می رسند که با هویت و مکان ناشناس و چه بسا غیرقابل شناسایی، در دنیایی شناور و سیال به فعالیت مجرمانه و حیات خود ادامه می دهند که در اغلب موارد بزهدیده بر بزهدیدگی خود مطلع نمی شود یا بسیار دیر بر آن آگاهی می یابد و حتی در اغلب موارد غیرقانونی بودن آنها روشن نمی باشد. یک ویژگی خاص جرایم سایبری این است که وقوع می یابند بدون آنکه صحنه جرم داشته

باشند. به علاوه، مجرمان به دلیل عدم رویت فوری آثار و نتایج رفتار مجرمانه شان، راحت تر مرتکب جرم می شوند. این امر باعث سهولت از بین بردن آثار جرم می گردد. سرعت بالای ارتکاب جرم و قابلیت تکرار فراوان نیز از ویژگی های دیگر این جرایم می باشد. جرایم سایبری غالبا بسیار سریع به وقوع می پیوندند و از شروع جرم تا اجرای آن فاصله ای وجود ندارد. گاهی فاصله، تنها به اندازه فشردن یک کلید است. از سوی دیگر، جرایم سایبری معمولا ماهیت سریالی دارند و با یک بار ارتکاب، مجرم به اعمالش خاتمه نمی دهد. هم چنین این امر به ویژگی خاص این فضا نیز برمی گردد که داده ها در این فضا به سادگی گسترش یافته و به طور خودکار تکرار می گردند و محو آن به سادگی ممکن نیست. تعطیل ناپذیر بودن و امکان وقوع جرم در هر زمان شبانه روز و هر روز هفته، ویژگی دیگر این جرایم است که زمینه گستردگی وقوع آن و افزایش رغبت افراد در ارتکاب این جرایم را فراهم می آورد.

لذا نکته قابل توجه، تفاوت در علل وقوع جرایم سایبری و ضرورت توجه چندجانبه به این جرایم است. از همین رو، برنامه‌هایی که به منظور پیشگیری از جرایم سایبری ارائه می‌شوند باید به این امر توجه داشته باشند. نکته دیگر ، قابلیت اعمال برخی نظریات جرم‌شناسانه مربوط به جرایم فضای سنتی بر جرایم این فضای نوین و جستجوی نظریه‌های جدید در تبیین جرایم سایبری است .

شکل گیری جرم شناسی سایبری یک تبیین میان رشته ای از جنبه های عملی و مباحث نظری در باب جرایم سایبری را با شناخت علوم رایانه ای فراهم می کند. به دلیل رشد روزافزون اینترنت و علوم کامپیوتری فناوری اطلاعات، باعث شده جرم شناسی سایبری به تدریج از یک مطالعه حاشیه ای به یک شاخه اصلی و با اهمیت در جرم شناسی تبدیل شود.

بحث جرم شناسی سایبری در سال ۲۰۰۷ توسط جایشانکار مطرح شد. در سال ۲۰۰۸ ایشان نظریه ای را در تبیین منسجم جرم شناسی سایبری به نام « نظریه جابجایی مکانی» مطرح کرد و در این نظریه جرایم در فضای سایبری را توضیح داد. جرم شناسی سایبری مطالعه عوامل ایجاد جرم در فضای مجازی و تاثیرات آن بر دنیای حقیقی و راهکارهای پیشگیری از حدوث اینگونه جرایم می باشد.نظریه جابجایی مکانی یا انتقال فضا، تفسیری درباره ماهیت رفتار اشخاصی است که رفتار هنجار و ناهنجار خود را در فضای فیزیکی و سایبری نشان می دهند. این نظریه اختصاصا برای جرایمی که با استفاده از اینترنت واقع می شوند، شکل گرفته است و بیان می دارد که مردم هنگامی که به دنیایی با ویژگی های مطلوبشان وارد می شوند، ممکن است به گونه متفاوتی رفتار کنند که سبب گرایش افراد به ارتکاب جرم و همچنین بزهدیدگی آنان گردد.

لازم به ذکر است در بحث جرم شناسی جرایم سایبری مطالعات اندکی صورت گرفته است که این امر می تواند به دلیل سرعت تغییرات فناوری و نیاز به مشارکت و حضور فعال در فضای سایبری برای تبیین آن و دشواری هایی در رسیدن به یک توافق جامع در هنجارهای رفتاری فضای سایبر است. کمااینکه رقم سیاه بزهکاری در این جرایم نیز بسیار بالا می باشد. در اثر عواملی همچون عدم آگاهی و شناخت کامل بزهدیدگان این جرایم، ترس از لطمه به اعتبار شرکت و از دست دادن اعتبار سرمایه گذاران، عدم تخصص ضابطان قضائی در شیوه کشف و تعقیب این جرایم و فقدان امکانات کافی در این خصوص، مشکلات فنی خاص در کشف و اثبات آنها رقم سیاه در جرایم سایبری بسیار بالاست. لذا متخصصان، اطلاعات موجود در زمینه جرایم سایبری را مانند کوه یخ می دانند.

در واقع، این واقعیت را باید پذیرفت که هنوز برداشت عمل مجرمانه در بسیاری از فعالیت‌های سایبری که فی‌الواقع جرم هستند، نمی‌شود. لذا نقش فرهنگ‌سازی در اینجا پررنگ می‌گردد. می‌توان گفت برای برقراری امنیت و کاهش جرایم در فضای سایبر، سه مولفه قابل توجه هستند: حاکمیت، پلیس، مردم. در جرایم سایبری، نقش حاکمیت به دو دلیل عمده بسیار برجسته می‌گردد. نخست آنکه، مجرمان بابت اعمالشان احساس شرمساری نمی‌کنند زیرا عملشان را جرم نمی‌دانند. در برخی موارد، مشاهده شده فرد به دلیل احساسات میهن پرستانه اش اقدام به برخی جرایم سایبری نموده است، مانند هک کردن سایت‌های دولتی کشورهای متخاصم . این امر، می تواند نتایج بسیار مخرب و خطرناک برای کلیت جامعه و امنیت ملی به بار آورد و چه بسا دامنه جنگی گسترده را فراهم نماید.

عامل دیگر، مباحث مربوط به تبادلات مالی و گسترده شدن بانکداری الکترونیک بدون توجه به فراهم آوردن بسترهای فرهنگی در این زمینه و آگاهی رساندن مناسب به مردم می‌باشد.

لذا حتی گاه مردم از اینکه بزهدیده یک جرم سایبری شده‌اند، ناآگاه هستند .این ناآگاهی، دامن خانواده ها را نیز می گیرد. فقر علمی خانواده‌ها در این زمینه و پیشرو بودن فرزندانشان امری است که منجر به عدم نظارت شایسته والدین بر فعالیت فرزندانشان در این فضا می گردد. این خانواده‌ها که با سفر چندروزه فرزندانشان با دوستان خود مخالفند، به یک‌باره فرزند خود را برای سفری جهانی در کنار هزاران غریبه در دنیای سایبر رها می سازند که این امر می تواند افزایش جرایم سایبری –خواه در بزهکاری این نوجوانان و خواه در بزهدیدگی آنان- را در پی داشته باشد.

ویژگی های خاص این فضا و ناآگاهی مردم و نبود زیرساختهای فرهنگی لازم برای حضور در این فضا، عنصری تشویق کننده برای مجرمین گشته است که علاوه بر مجرمان خاص فضای سایبر، مجرمان

فضای واقعی نیز دامنه جرایمشان را از فضای واقعی به دنیای سایبر انتقال داده اند و به نوعی پدیده « کوچ مجرمانه » شکل گرفته است. ارتقاء سطح اطلاعات جامعه نسبت به فضای مجازی و اطلاع رسانی در زمینه جرایم سایبری و راههای مقابله با آن، ارتقاء سطح باورهای اخلاقی خصوصا در بین نوجوانان و جوانان نمونه‌هایی از پیشگیری از شکل گیری جرایم در فضای مجازی است.

هم چنین از آنجا که خسارات وارده بر اثر جرائم سایبری به مراتب گسترده‌تر و جبران ناپذیرتر درمقایسه با جرائم سنتی است، و با توجه به تهدیدات و آسیب های این محیط علیرغم مزایای فراوان آن، لازم است به خوبی بر آن اشراف داشته و این تهدیدات مستمرا شناسایی شوند تا بتوان در عصر حاضر با افزایش ادراک از تأثیر و کاربرد فضای سایبر بر ماهیت جرم و انحراف، بهتر مقابله نموده و از بروزشان پیشگیری نمود.

کتاب حاضر از آثار نوین و ارزشمند در حوزه تبیین جرایم سایبر از منظر جرم شناختی و نقش آن در دستاوردهای علمی علوم جنائی مدرن می باشد که پیرامون ماهیت جرایم سایبری و بررسی اقسام آن شامل هک کردن، حملات اتوماتیک کامپیوتری و آسیب رسانی بدافزارها، دزدی دیجیتالی، کلاهبرداری اینترنتی، جرایم جنسی رایانه ای، آزار و اذیت آنلاین و مزاحمت سایبری، ترور سایبری، نقش ادله اثبات و جرم یابی دیجیتال و چشم انداز آینده جرایم سایبری مباحثی ارزشمند و بسیار جدید و به روز را مطرح نموده است که قطعا از آثار قابل استناد و ارجاع در حوزه شناسایی جرایم سایبری و جرم شناسی سایبری می باشد.

فصل اول: تکنولوژی و جرایم سایبری

اهداف فصل :

- ✓ توضیح اینکه چگونه تکنولوژی رفتار بشری را تحت تاثیر قرار داده است
- ✓ شناسایی تفاوت فی مابین انسان‌های متولد در عصر دیجیتال و انسان‌های متولد در دوره‌های قبل
- ✓ بحث در مورد سه طریقی که به واسطه‌ی آن‌ها تکنولوژی میتواند توسط افراد مورد سواستفاده واقع شود
- ✓ فهم مدارک بدست آمده از کامپیوترها و تکنولوژی‌های دیجیتالی و ارزش آن‌ها در نظام تحقیقات جزایی
- ✓ توضیح انواع مختلف جرایم مجازی که روزانه در سراسر جهان رخ میدهد.

مقدمه

اینترنت، کامپیوترها، و تکنولوژی‌های موبایل بطور چشمگیری شکل جامعه مدرن را از نو ساخته‌اند. گرچه درک این امر دشوار است، کمتر از دو دهه پیش بیشتر افراد یک دستگاه تلفن یا کامپیوتر شخصی نیز نداشتند و این وسایل هنوز تاحدی تجهیزات گران قیمتی محسوب می‌شدند. افراد نمی‌توانستند تایپ کنند، و ایمیل چیز عجیبی بود. ارتباطات اینترنتی بواسطه مودم‌های شماره گیری یا کابلهای اترنت کار می‌کرد و مردم برای هر ساعت دسترسی به اینترنت هزینه پرداخت می‌کردند. سیستم‌های بازی‌های کامپیوتری از گرافیک ۱۶ بیتی استفاده می‌کردند و به تجهیزات دیگر متصل نمی‌شدند. سیستم‌های موقعیت یابی جهانی(GPS) فقط در کاربردهای نظامی استفاده می‌شدند. امروزه، بیشتر کارهای دنیا به کامپیوترها، اینترنت، و تکنولوژی‌های سلولی وابسته است. امروزه افراد لپ تاپ دارند و به وای فای متصل می‌شوند ، تلفنهای همراه ممکن است از اینترنت استفاده کنند و بازی‌های ویدئویی بصورت شبکه ایی بهم متصل شوند. بعلاوه، مردم چندین حساب ایمیل برای کارهای شخصی و تجاری خود دارند، درست مانند پروفایلهای شبکه ایی در صفحات مختلف اینترنتی. تلفنهای همراه، بخصوص متون به اولین روش برقراری ارتباط برای اکثر مردم تبدیل شده‌اند. در واقع افراد زیر سن بیست سال بطور منظم متنهای بیشتری را نسبت به گروه‌های سنی دیگر ارسال می‌کنند و ترجیح می‌دهند تا بیشتر متن ارسال کنند تا تماس تلفنی داشته باشند. افراد نیز بطور مکرر کالاهای را بصورت اینترنتی خریداری می‌کنند و بطور فزاینده ایی بجای رسانه‌های چاپی سنتی از خواندن الکترونیکی برای کتابها، روزنامه‌ها استفاده می‌کنند.

جالب است که درنظر بگیریم دنیا و رفتارهای انسانی بسرعت بواسطه استفاده از تکنولوژی تغییر کرده‌اند. در واقع، در حال حاضر ۲,۱ میلیارد کاربر اینترنتی در سرتاسر دنیا وجود دارد و ۲۴۵ میلیون نفر از آنها در امریکا زندگی می‌کنند. ایالات متحده امریکا دومین پرجمعیت ترین کاربران اینترنتی در سرتاسر دنیا را بعد از چین تشکیل می‌دهند. درمقابل، باتوجه به بررسی‌های سال ۲۰۱۳ بریتانیا ۳۶ میلیون کاربر اینترنتی دارد.

تکثیر این تکنولوژی به تغییرات متمایزی در چگونگی مشارکت افراد در سرتاسر دنیا منجر شده است. امروزه مردم به شکل دیجیتالی خرید می‌کنند، ارتباط برقرار می‌کنند و اطلاعات خود را به اشتراک می‌گذارند که قبلا یک امر غیرممکن بود. تغییرات دیگر رفتاری، با رویارویی با تکنولوژی‌ها و نوآوری‌های مربوطه بوجود آمده است. در واقع، جامعه شناس هوارد ادوم به این فرایند باعنوان

techicways[۱] اشاره کرده است، روشهایی را مشخص می‌کند که الگوهای رفتاری در پاسخ به نوآوری‌های فنی تغییر می‌کنند. از دیدگاه اودوم، راه‌های فنی جایگزین الگوهای رفتاری موجود می‌شود و تغییرات بنیادین را در جامعه ایجاد می‌کند. برای مثال، اگر یک فرد ۳۰ ساله بخواهد با افراد دیگر ارتباط برقرار کند، ممکن است با او تماس بگیرد، یا درصورت امکان اورا ببیند یا در غیراینصورت یک نامه از طریق پست برایش ارسال کند. اما امروزه آن فرد یک پیغام می‌فرستد، یک ایمیل می‌نویسد، یا از طریق فیسبوک به او یک پوک می‌دهد تا برایش نامه ایی را پست کند.

تاثیرات راه‌های فنی در تمام گروه‌های آماری در جامعه مدرن دیده می‌شود. برای مثال، در ۲۰۱۱ ، ۷۱درصد از امریکایی‌ها از سایتهایی استقبال می‌کردند که ویدئوها در آن به اشتراک گذاشته می‌شد ، بویژه امریکایی افریقایی‌ها و کاربران اسپانیایی که بسیاری از آنها به افزایش دسترسی به ارتباطات اینترنتی گسترده و استفاده از تلفنهای هوشمند و وسایل موبایلی نسبت پیدا می‌کنند. در بریتانیا ۴۲ درصد از منازل در ۲۰۱۳ فیبرهای نوری یا اتصالات کابلهای اینترنتی دارند، به این معنا که ارتباط سرعت بالا تاحدی رایج است. در ۲۰۱۱ ، بیش از ۸۰ درصد از افراد بزرگسال در ایالات متحده از تلفن استفاده می‌کردند و تقریبا یک سوم از آنها تلفن هوشمند داشتند که می‌تواند برای چک کردن ایمیل را ارتباطات دیگر استفاده شود. ۶۱ درصد افراد در بریتانیا در سال ۲۰۱۳ تلفن هوشمند داشتند که می‌توانستند از طریق آن به اینترنت دسترسی داشته باشند.

در بیشتر روشهای مشابه، تکنولوژی تاثیر زیادی بر جمعیت جوانی که هرگز زندگی بدون اینترنت و ارتباطات بواسطه کامپیوتر(CMCs) مانند ایمیل و متن را تجربه نکرده بودند داشت. بعلاوه، تحقیقات اخیر با استفاده از یک نمونه از جوانان ایالات متحده نشان داد که ۷۵ درصد از جوانان لپ تاپ یا کامپیوتر دارند و ۱۵ درصد از آنها هردو را دارند. علارغم این ۹۳ درصد از جوانان بین سنین ۱۲ تا ۱۷ سال از اینترنت استفاده می‌کنند، به این معنا که تقریبا تمام آنها در اینترنت حضور دارند. علاوه براین، نه تنها جوانان حضور دارند بلکه حضور مداوم دارند-۸۸ درصد از کودکان حداقل یکبار در هفته آنلاین می‌شوند. یک بررسی مشابه نشان داد که ۴۹ درصد از کودکان بطور متوسط برای پنج یا هفت روز در هر هفته آنلاین هستند.

---

[۱] راه های فنی

تکنولوژی نه تنها رفتارهای جوانان را بلکه شکل و مدل رفتار آنها را نیز تغییر داده است. اکثر مردم که در اواسط دهه ۸۰ متولد شده‌اند هرگز بدون کامپیوتر ، اینترنت یا تلفن‌های همراه نبوده‌اند. در نتیجه آنها دنیای بدون این وسایل را نمی‌شناسند و نمی‌دانند دنبال بدون این منابع چگونه خواهد بود. بنابراین پرسکی(۲۰۰۱) استدلال کرد که این جوانان بومی‌های دیجیتال هستند ، بدین وسیله آنها به دنیایی آورده شدند که دیجیتال بود و زمانهای زیادی از زندگی آنها را به محیط دیجیتالی اختصاص می‌داد و از منابع تکنلووژی در زندگی روزمره آنها استفاده می‌نمود. برای مثال، افراد بین سنین ۱۸ تا ۳۴ امروزه منابع تکنولوژی خود را دارند ودرمیان کاربران اینترنتی در ایالات متحده هستند. در واقع، ۸۷ درصد از نوجوانان امریکایی از اینترنت استفاده می‌کنند، و ۶۶ درصد از بزرگسالان نیز این وضعیت را دارند. این به معنای ۱۸ میلیون جوان آنلاین بطور روزانه است و از CMC از روشهای مختلف استفاده می‌کنند، که شامل ۸۹ درصد از جوانانی است در زمان آنلاین بودنشان ایمیل ارسال می‌کنند یا دریافت می‌کنند و ۸۱ درصدشان بازی‌های اینترنتی انجام می‌دهند. بطور مشابه ۹۴ درصد از افراد بین سنین ۱۶ و ۲۴ در بریتانیا یک موبایل همراه دارند. بعلاوه افراد بین سنین ۱۸ و ۳۴ تقریبا ۴۹ درصد از کل جمعیت کاربران فیسبوک را در ایالات متحده تشکیل می‌دهند.

در مقابل، مهاجران دیجیتالی آنهایی هستند که پیش از ایجاد تکنولوژی‌های دیجیتالی و اینترنتی بدنیا آمدند. این افراد نیاز داشتند تا با محیط دیجیتال تطبیق یابند، که با سرعت بالاتری از آماده شدنشان تغییر می‌کند. این برای بسیاری از افرادی که در دهه‌های پیش از ایجاد و ظهور این تکنولوژی‌ها بدنیا آمدند صادق است. درنتیجه ، آنها ممکن است کمتر تمایل داشته باشند تا فورا با این منابع تطبیق یابند و یا به روشهای مختلفی از آنها استفاده کنند. برای مثال، تنها ۴۵ درصد از بزرگسالان در ایالات متحده بالای سن ۶۵ لپ تاپ دارند. بعلاوه ممکن است درکِ برخی از منابع برای مهاجران دیجیتال دشوارتر باشند، مانند فیسبوک، که نیاز دارد تا کاربران بطور منظم درباره خودشان و علایقشان صحبت کنند و میزان خصوصی بودن ارتباطشان با دیگران را تمام کنند. در واقع افراد ۵۵ ساله و پیرتر تنها ۱۳ درصد از جمعیت فیسبوک را در ایالات متحده تشکیل می‌دهند. در ایالات متحده افراد دارای سن ۴۵ سال یا بیشتر بطور متوسط بیش از ۱۴ متن را در هر روز دریافت نمی‌کنند درحالیکه آنهایی که بین سنین ۱۸ تا ۲۴ هستند بطور متوسط ۱۰۹,۵ پیغام در روز دریافت می‌کنند. بطور مشابه، تنها ۱۷ درصد از افراد سن ۶۵ سال یا بیشتر در بریتانیا از موبایل

استفاده می‌کنند. بنابراین مهاجران دیجیتال الگوهای متفاوت تری از اتخاذ و استفاده از تکنلووژی‌ها با بومیان دیجیتال دارن.

تکثیر تکنولوژی در جامعه مدرن تاثیر زیادی بر رفتار انسانی دارد . دنیا حول استفاده از CMCها ساخته می‌شود و روشی را تحت تاثیر قرار می‌دهد که ما با دولت ها، تجارتها و دیگران در ارتباط هستیم. بعلاوه استفاده از تکنولوژی نیز شکافی میان نسلها ایجاد می‌کند ، براین اساس که افراد از تکنولوژی در زندگی روزمره اشان استفاده می‌کنند. در عوض افراد رفتارشان را به روشهای مختلفی تطبیق می‌دهند که مزایای اصلی طراحی و کاربرد کامپیوترها و اینترنت را تخریب می‌کند.

۱-۱ تکنولوژی بعنوان فضایی برای جرم

انقلاب رفتار انسانی بعنوان نتیجه نوآوری‌های فنی فرصتهای نابرابری را برای جرم و سو استفاده‌ها فراهم کرده است. در طی سه دهه گذشته، افزایش اساسی در استفاده از تکنولوژی در جرایم خیابانی و کاربردهای جدید تکنولوژی برای ایجاد شکلهای جدید جرایم بوده است که قبلا وجود نداشت. وب جهانی و اینترنت نیز حوزه ایی برای افرادی ایجاد می‌کند که در جرم مشارکت داشته‌اند تا اطلاعاتی را نشر دهند یا ارتباط برقرار کنند که در دنیایی واقعی ممکن نیست. در نتیجه حیاتی است که چگونگی تغییر اینها و معنایشان برای تخلف در قرن بیست و یکم را درک کنیم. سه روش مهم هستند که ممکن است تکنولوژی‌های کامپیوتری و سلولی از سوی متخلفان مورد سواستفاده قرار گیرند:

۱- بعنوان میانجی برای ارتباط و توسعه زیرساختارهای آنلاین
۲- بعنوان مکانیزمی برای مورد هدف قرار دادن منابع حساس و مشارکت در جرم و انحراف
۳- بعنوان وسیله ایی فرعی برای آسان کردن تخلف و ارائه شواهدی از فعالیتهای کیفری بصورت آنلاین و آفلاین

۱-۲ تکنولوژی بعنوان میانجی ارتباطی

رسانه‌های تلفنی، اینترنتی و دیجیتالی می‌توانند بعنوان ابزارهایی برای ارتباط بین افراد در شکل سریع در سرتاسر دنیا استفاده شوند. کامپیوترها ، تلفنها، و تجهیزات فنی می‌توانند با کمترین هزینه و بطور ناشناس مورد استفاده قرار گیرند. برای مثال، خرده فروشان مهم و مغازه‌ها تلفنهایی را می‌فروشند که

می‌توان بدون ارتباط بواسطه اسپرینت یا واریزن از آنها استفاده کرد. توانایی استفاده از تلفن به تعداد دقایق خریداری شده بستگی دارد و می‌تواند پس از استفاده مورد رسیدگی قرار گیرد.

در عوض، بزهکاران می‌توانند از این وسایل برای ارتباط با دیگران و به اشتراک گذاشتن اطلاعاتی استفاده کنند که ممکن است مورد علاقه آنها باشد. برای مثال، مشتریان استفاده از روسپی گری از چت روم‌ها[1] برای بحث درمورد سکس استفاده می‌کنند. این مبادله اطلاعات دست اول به سختی در دنیای واقعی اتفاق می‌افتد، همانطور که هیچ نشانه ایی وجود ندارد که نشان دهد کسی به روسپی گری علاقه دارد یا مطلب در مورد آن را دیده است. بعلاوه میزان بالایی از ننگ اجتماعی و شرم و حیا درمورد پرداخت پول در ازای رابطه جنسی وجود دارد، بنابراین احتمال ندارد که کسی بخواهد همچین رابطه ایی را عمومی کند. ماهیت ناشناس بودن در اینترنت به افراد اجازه می‌دهد تا درمورد موارد این چنینی بدون خطر و آسیب صحبت کنند.

ماهیت توزیعی اینترنت و CMC به افراد اجازه می‌دهد تا با افرا و گروه‌هایی که ویژگی‌های مشترک دارند و رفتارها ، نظرات و ارزشهای یکسان دارند ارتباط برقرار کنند. درنتیجه، تکنولوژی به ایجاد زیرساختارهایی بین افراد براساس رفتارهای مشترک و ایده آلهای یکسان کمک می‌کند، و این بدون توجه به انزوای اجتماعی و یا جغرافیایی صورت می‌پذیرد . از یک دیدگاه ایدئولوژیک یا جامعه نگرانه، زیرساختارها گروه‌هایی هستند که ارزشها، هنجارها، سنتها و مراسم خود را دارند که آنها را از فرهنگها جدا می‌کند.

شرکت کنندگان در این زیرساختارها قوانین خود را دارند تا روشهایی را بسازند که می‌توانند از آن طریق با اعضای دیگر زیرساختارها و گروه‌های مختلف در جامعه ارتباط برقرار کنند. بعلاوه ، عضویت در یک زیرساختار با ایجاد باورها، اهداف، و ارزشهایی که فعالیتها را توجیه می‌کنند رفتارهای فردی را تحت تاثیر قرار می‌دهند. برای مثال، یک زیرساختار ممکن است بر توسعه و تکامل مهارتها و توانایی‌هایی تاکید کند که ممکن است در فرهنگ عمومی بی ارزش باشد، مانند توانایی استفاده از زبانهای برنامه نویسی و کار با سخت افزارها و نرم افزارها میان هکرهای کامپیوتری. اعضای یک زیرساختار نیز گویش و شعارهای خود را برای برقراری ارتباط با دیگران و حفاظت از بحثهای خود دارند. استفاده از این زبان می‌تواند بعنوان نمایش عملی عضویت در هر ساختاری باشد. بنابراین

---

[1] چت روم: (Chat) همانگونه که در لغت می دانید به معنای گفتگو است و روم (Room) به معنای اتاق می باشد. ترکیب این دو کلمه مفهوم اتاق های گفتگو یا همان چت روم ها را به وجود می آورد.

زیرساختار روشهایی را در اختیار اعضا قرار می‌دهند که از طریق آن شـهرت و وضـعیت و انسجامشـان با ارزشها و باورهای گروه را تنظیم می‌کنند.

میلیاردها زیرساختار در جامعه مدرن وجـود دارد ، بسـیاری از آنهـا شـامل تجـارب اینترنتـی و غیـر اینترنتی هستند . با این وجود تمام آنها منحرف کننده نیستند و شـما مـی‌توانیـد بطـور همزمـان در چند مورد از آنها عضویت داشته باشید. برای مثال ممکن است به زیرساختارهای طرفـداران تـیم‌هـای ورزشی تعلق داشته باشید(فوتبال، بسکتبال، یا هر ورزش دیگری) تنها اگر"۱) از تماشـای آنهـا لـذت ببرید. ۲) آمار بازیکنان مورد علاقه اتان را بدانید.۳) رویدادهای تاریخی در فصلهای پیشـین تیمتـان را بدانید. و۴) درمورد فردی که بهترین بازیکن است صحبت کنید. زیرساختارهای مشابه بـرای باغبـانی، اتومبیلها، فشن و فیلمها و رفتارهای دیگر نیز موجود هستند. یافتن کسانی که علاقه‌هایی مشـابه شـما دارند می‌تواند برایتان سودمند بادش که به شما اجاره می‌دهد تا به روشی با دنیای علاقمندی هایتـان در ارتباط باشید.

در اکثر این روشها، زیر ساختارها می‌توانند بصورت آفلاین برای آنهایی که به شکلهای خاصـی از جـرم و انحراف علاقمند هستند ظهور کند. تکنولوژی به آنها اجازه می‌دهد تا بـدون تـرس از طـرد شـدگی اجتماعی باهم درارتباط باشند، و حتی به افرادی که درمورد رفتارهایی کنجکاو هستند اجازه می‌دهـد در محیط آنلاین بدون ترس از شناسایی درموردش اطلاعات بدست آورند. تکنولوژی‌هـای جدیـد نیـز امکان شکل گیری و مشارکت در زیرساختارهای چندگانه را با دستیابی بیشتر از حالت آفلایـن فـراهم می‌کنند. در واقع، افراد می‌توانند با دانش زیرساختاری بواسطه ایمیل یا CMCهـای دیگـر در ارتبـاط باشند مانند تکنیک‌های تخلف که ممکن است خطر شناسایی آنها از قربانیان را کـاهش دهـد. بخـاطر استفاده غالب از تکنولـوژی بعنـوان ابـزاری بـرای برقـراری ارتبـاط بـا دیگـران ایـن کتـاب بـر نقـش زیرساختارهای آنلاین برای آسان کردن جرم و انحراف در محیطهای واقعی تمرکز خواهد داشت.

۱-۳ تکنولوژی بعنوان هدف یا ابزاری برای مشارکت در جرم

دومین راهی که تکنولوژی می‌تواند از طریق آن دچار سواستفاده قرار گیرد بسیار حیلـه گرانـه اسـت- بعنوان منبعی برای افراد برای حمله آنلاین و آفلاین به افراد، تجارتهـا و دولتهـا. بسـیاری از وسـایل د زندگی روزمره ما قابلیت برقراری ارتباط اینترنتی را دارند، از دستگاه‌های پهـش mp3 تـا کامپیوترهـا. این تکنولوژی‌ها شامل بیتهای حساس به اطلاعات هستند ، که عبارت است از عادات خرید کـردن مـا

برای نام کاربری و رمز ورود برای حسابهای بانکی و ایمیلها است. از آنجائیکه این وسایل می‌توانند با یکدیگر ارتباط برقرار کنند، افراد بواسطه روشهای مختلف هک کردن کامپیوترها می‌توانند به این اطلاعات دست یابند.

درحالیکه که هک کردن افراد ماهری را با درک بالایی از تکنولوژی می‌طلبد، اقدام ساده می‌تواند حدس زدن رمز ورود ایمیل یا کامپیوتر یک فرد باشد که می‌توان این را بعنوان هک کردن درنظر گرفت. دستیابی غیر مجاز به اطلاعات شخصی افراد می‌تواند نکته کلیدی در تعریف هک کردن باشد، همانطور که یک فرد تلاش می‌کند تا به سیستم‌های امنیتی یا داده‌ها دسترسی یابد. در عوض، آن اطلاعات مانند فردی که با دیگری صحبت می‌کند یا موسسه مالی که آنها برای خرید استفاده می‌کنند، می‌تواند برای آسیبهای دیگر مورد استفاده قرار گیرد. در واقع، تحقیقات بر دانش آموزان کالج حاکی از اینست که بین ۱۰ تا ۲۵ درصد از دانشجویان دوره کارشناسی سعی کرده‌اند تا رمز ورود دیگری را حدس بزنند. بنابراین اطلاعاتی که می‌تواند درمورد فعالیتهای آنلاین ما مطرح شود می‌تواند توسط دیگران مورد استفاده قرار گیرد.

بطور مشابه، برخی از هکرها وبسایتها و منابعی را درنظر می‌گیرند تا باعث آسیب یا تعریف پیغامهای سیاسی شوند. اغلب، هکر و جامعه فعال از تخریب وب استفاده می‌کنند تا پیغامی را منتشر کنند و باعث آسیب شوند. تخریب وب یک اقدام آنلاین محسوب می‌شود که مجموعه قوانین موجود html را برای صفحه وب را با یک تصویر و پیغامی جایگزین می‌کند که آنها می‌فرستند. برای مثال، یک شخص ممکن است سعی کند تا وبسایت کاخ سفید را هک کند و مطالبی را جایگزین کند که دیگران آنرا ببینند. گرچه این برای مالک سایت جالب نیست، در صورتی بدخواهانه تر می‌شود که تخریب گر تصمیم بگیرد کل مطالب اصلی را از بین ببرد.

تخریبها ابزار منظمی برای هکرهای سیاسی هستند تا نظراتشان را توضیح دهند، و حول رویدادهای اجتماعی داغ مورد استفاده قرار گرفته‌اند. برای مثال، هکرهای ترکیه کمپین گسترده ایی از تخریب وب را پس از انتشار کارتونی آغاز کردند که تصویری از حضرت محمد (ص) را با بمبی در دامنش نشان می‌داد. بسیاری از مسلمانان عمیقا از این تصویر رنجیده خاطر شدند، و هکرهای ترک شروع به تخریب وبسایتهایی دانمارکی کردند، که این کارتون را منتشر کرده بود. این تخریبها در جهت حمایت از مذهب اسالمی و تعریف خشونت علیه ایمان آنها بود که در رسانه‌های جمعی به نمایش

گذاشته شده بود. بنابراین، عاملانی که انگیزه داشند کسانی بودند که قصدشان آسیب به نظری بود که ممکن است منابع مختلفی را بعنوان یک هدف ببینند.

۱-۴ تعریف سواستفاده و استفاده نادرست از کامپیوتر

از زمانی که تکنولوژی می‌تواند بعنوان راه برقراری ارتباط و هدفی برای حمله درمقابل اهداف دیجیتال و زیرساختارها مورد استفاده قرار گیرد ، توصیف عامل ایجاد سو استفاده و استفاده نادرست از تکنولوژی ضروری می‌شود. برای مثال، عبارت انحراف به رفتاری اشاره دارد که ممکن است غیر قانونی بود، گرچه خارج از هنجارهای رسمی و غیر رسمی یا باورهای فرهنگ ارجح است. شکلهایی از انحراف هستند که به هنجارهای جامعه گرایی و موضوعات اجتماعی بستگی دارند. برای مثال، در حالیکه ممکن است استفاده از فیسبوک و نوشتن متن در کلاس غیرقانونی نباشد، اما مزاحم است و عموما مدیر یا معلم از این کار راضی نیست. در سینما و مجامع عمومی نیز این قضیه صادق است. از اینرو استفاده از فیسبوک در شرایط و موقعیتهای خاص می‌تواند بعنوان یک امر مخرب در نظر گرفته شود، اما ممکن است غیرقانونی نباشد. این فعالیتی که توسط تکنولوژی بوجود آمده است ممکن است با عنوان انحراف سایبری مورد اشاره قرار بگیرد.

یک نمونه مناسب دیگر از انحراف سایبری در ایجاد و استفاده از پورنوگرافی مطرح است. اینترنت دیدن تصاویر پورن و ویدئوهای آن را برای افراد آسانتر کرده است، در ست همانطور که این امکان را فراهم کرده است تا از طریق دوربینهای تلفن همراه و وبکم‌ها و عکسهای دیجیتالی ظهور این اتفاق را ساده کرده است. هرفرد بالای ۱۸ سالی این اجازه را دارد تا به تصاویر پورنوگرافی در این فیلمها و رسانه‌ها دسترسی یابد. اگر جامعه بزرگتر دیدگاهی را مطرح کند که پورنوگرافی از نظر اخلاقی اشتباه است، پس دیدن مطالب ممکن است بعنوان امری منحرف کننده در نظر گرفته شود. از اینرو مشارکت در این فعالیتها قانونی نیست؛ در عوض نقض سیستم‌های هنجاری و باورها را نقض می‌کند و یک رفتار منحرف کننده ایجاد می‌کند.

فعالیتهایی که مقررات قانونی را نقض می‌کند از انحراف بسوی اقدامات کیفری تغییر می‌یابد. در زمینه پورنو گرافی ، اگر فردی در ایالات متحده زیر سن ۱۸ باشد، از نظر قانونی اجازه ایجاد یا دیدن این تصاویر را ندارند. از اینرو چنین اقدامی بعنوان یک جرم در نظر گرفته می‌شود زیرا تحریمات قانونی را در پی دارد. مقررات کیفری در امریکا در هردو سطح ایالتی و فدرال تخلفات بسیاری را در

دنیای واقعی می‌شناسد. اتخاذ و استفاده سریع از تکنولوژی به منظور آسان سازی فعالیتهای کیفری به ایجاد بندهای مختلفی به منظور دسته بندی این رفتارها منجر شده است. بطور خاص، جرم کامپیوتری و سایبری چند دهه قبل برای اشاره به روش منحصربفردی ظهور پیدا کرد که می‌گفت تکنولوژی برای آسان کردن فعلیتهای کیفری استفاده می‌شود. جرایم سایبری به جرایمی اشاره می‌کند که در آن متخطی از دانش خاصی در زمینه سایبری استفاده می‌کند. در حالیکه جرایم کامپیوتری به این دلیل اتفاق می‌افتند که متخطی از دانش خاصی درباره تکنولوژی کامپیوتری استفاده می‌کند. در روزهای اولیه کامپیوتری شدن، تفاوت به این دو بند برای روشن کردن اینکه تکنولوژی چطور وارد تخلفات شد کمک کننده بود. اینکه تقریبا تمام کامپیوترها امروزه به اینترنت متصل می‌شوند نیاز به جدا کردن این دو اقدام را کاهش داده است. بعلاوه، آنها تقریبا در هردو حوزه‌های علمی و رسانه ایی بعنوان مترادف استفاده می‌شوند. درنتیجه، این کتاب از عبارت "جرم سایبری" برای اشاره به جرایم مختلفی استفاده می‌کند که بواسطه استفاده از محیطهای آنلاین و تعداد بالای کامپیوترها و موبایلهایی اتفاق می‌افتد که به اینترنت متصل هستند.

ماهیت بدون مرز اینترنت پاسخ قضایی به جرم و انحراف را دشوار می‌کند چون راه‌هایی که کشورها از طریق آن بعنوان یک اقدام تعریف می‌شوند عموما افراد را از دسترسی به مطالب اینرتنتی منع نمی‌کند. با استفاده از نمونه‌های پورنوگرافی، تولید و دستیابی به این مفاد در ایالات متحده و اکثر کشورهای دنیا قانونی است. کشورهای اسلامی مانند ایران و عربستان قانونی بودن دسترسی به پورنوگرافی را بدلیل باورهای مذهبی اشان ممنوع کرده‌اند. کشورهای دیگر مانند سوئد، محدودیتهایی در تولید مفاد پورنوگرافی دارند ، مانند تصاویر حیوانات یا عمل جنسی بین حیوان و انسان. گرچه تولید و دیدن این مفاد در ایالات متحده و اکثر کشورها غیر قانونی است ، افراد در سرتاسر دنیا می‌تواند به خشونت، رابطه جنسی حیوانی یا مفاد غیر عادی دسترسی داشته باشند، با وجود اینترنت بدون توجه به اینکه قانون کشورشان در این رابطه چیست. بنابراین محدود کردن و اجرای قوانین داخلی بر رفتار افراد بدلیل دسترسی اشان به اینترنت و مفاد این چنینی دشوار است .

فصل مشترک جرم سایبری و انحراف سایبری نیز به ظهور مشکل تروریسم سایبری وابسته است. این عبارت در اواسط دهه ۱۹۹۰ بعنوان تکنولوژی ایی ظهور یافت که نقش مهمی در تمام جوانب جامعه داشت. هیچ تعریف واحد قابل قبولی برای تروریسم سایبری وجود ندارد که بواسطه آن بسیاری از افراد این رفتار را بعنوان استفاده از تکنولوژی یا کامپیوتر بعنوان راه ارتباطی برای ایجاد

آسیب یا تغییرات اجتماعی استفاده کنند. گرچه چند رویداد از تروریسم سایبری وجود دارد که در دو دهه پیش رخ داده است، حضور تکنولوژی می‌تواند به گروه‌های افراط گرا مانند القاعده اجازه می‌دهد تا سیستم‌های نظامی شامل اطلاعات حساس، سیستم‌های خدمات مالی مانند تجارت تولید بچه، شبکه‌های قدرت، ایستگاه‌های سوئیچینگ، و زیرساختارهای مهم دیگر که برای حفظ خدمات بنیادین ضروری هستند را مورد هدف قرار دهند. بزهکاران نیز می‌توانند با استفاده از تاکتیکهای مشابه این اهداف را مورد حمله قرار دهند و جداسازی اقدامات جرم سایبری و ترور سایبری را از یکدیگر دشوار کنند.

به منظور دسته بندی کردن این پدیده ، درنظر گرفتن هردو انگیزه حمله کننده و حوزه آسیبهای تحمیلی مهم است. برای مثال، اقدامات کیفری اغلب افرادی را مورد هدف قرار می‌دهند و ممکن است بخاطر اهداف اقتصادی و ... انگیزه داشته باشند، درحالیکه حملات تروریستی اغلب انگیزه‌های سیاسی دارند و نه تنها برای آسیب رساندن یا کشتن فرد استفاده می‌شوند بلکه برای ایجاد ترس در جمعیتهای بزرگتری نیز استفاده می‌شوند. علاوه براین، ارتباطاتی که از طریق اینترنت ممکن هستند فصل مشترک جالبی بین ترور سایبری و انحراف سایبری ایجاد می‌کنند. برای مثال، اعضای افراط گرایی و گروه‌های انزجار، به تالارهای وب و بلاگهایی نیاز دارند تا پستها و دیدگاه هایشان را درمعرض دید عموم در سرتاسر دنیا قرار دهند. قوانین یک کشور مشخص ممکن است اجازه چنین زبانی را ندهد، همانطور که در آلمان پست کردن مفاد مربوط به نازی‌ها غیرقانونی است. در ایالات متحده چنین سخنانی تحت حمایت اولین اصلاحات قانون اساسی قرار می‌گیرد؛ از اینرو، استفاده از تالارهای آنلاین برای توضیح نظری که تحت حمایت جامعه نیست اقدام منحرفانه محسوب می‌شود تا یک رفتار غیرقانونی. بنابراین، ترور، جرایم سایبری، انحراف همگی بهم وابسته هستند و بنابر ماهیت محیطهای آنلاین عوامل مشترکی را به اشتراک می‌گذارند.

۱-۴-۱ چه چیزی جرم سایبری یا انحراف را جذابتر می‌کند؟

افزایش جرم سایبری، جرم سایبری، و ترور سایبری سوالات بسیاری را در این باره مطرح کرده است که چرا برخی از مردم در اقدامات اشتباه در محیطهای مجازی استفاده می‌کنند. چندین عامل منحصربفرد وجود دارد که ممکن است موجب تخریب آنلاین شود ، بطور خاص در دسترس بودن تکنولوژی در دنیای مدرن. ابتدا حضور تکنولوژی دسترسی به ابزارهای ضروری برای تخلف را برای افراد آسان می‌کند. قیمت لپ تاپ و کامپیوترها در دهه پیش به طور چشمگیری کاهش داشته است

و دستیابی به این تجهیزات را ساده کرده است. برای مثال قیمت لپ تاپ از مقدار متوسط ۱۶۴۰ دلار در سال ۲۰۰۱ به ۱۰۰۰ دلار در سال ۲۰۰۵ رسید. این کاهش قیمت به همین صورت ادامه داشت و حالا این وسایل با کامپیوترهای کوچکتر قابل حمل در رقابت هستند، مانند تلفنهای هوشمند وای پدها، که می‌توانند بواسطه تکنولوژی‌های سلولی به اینترنت متصل شوند. در نتیجه، متخلفان می‌توانند بسرعت از هر جایی بواسطه این منابع به اطلاعات دستیابی پیدا کنند. اگر یک شخص نتواند این وسایل را بخرد، می‌تواند همیشه بطور رایگان یا با هزینه کم از کامپیوترها در کافی نت‌ها و کتابخانه‌های عمومی استفاده کند. بنابراین موانع کمی برای جهانی شدن تکنولوژی کامپیوتری وجود دارد.

بعلاوه، گستره پهناوری از جرایم سایبری وجود دارند که می‌توانند بسته به مهارتهای فنی فرد اجرا شوند. برخی از این اشکال جرم سایبری هستند که به مهارت و حرفه ایی بودن در این زمینه نیاز دارد، گرچه تخلفات ساده می توانند با سرمایه گذاری کمی روی متخلف اجرا شوند. برای مثال، هرکسی می‌تواند موسیقی یا فیلمهای غیراورجینال را از محیطهای آنلاین دانلود کند یا پستهای جنسی بگذارد. تکنولوژی بعنوان تقویت کننده در کامپیوترها و CMCها استفاده می‌شود و به فرد اجازه می‌دهد تا در جرایمی مشارکت داشته باشد که افراد یا طرح‌های پیچیده ایی را درگیر می‌کند تا قربانیان را مورد هدف قرار دهد. برای مثال، اگر یک بزهکار تلاش کند تا یک فرد را در دنیای واقعی بدزد، آنها باید بدلیلی دشواری در ایجاد ترس و مدیریت گروه ها، افراد را مورد هدف قرار دهند . متخلف نیز باید سعی کند تا پیشرفت را تعیین کند ، تنها اگر فردی که او تلاش در دزدینش دارد پول، جواهر یا کالاهای ارزشمند دیگری داشته باشد.

در محیطهای آنلاین، متخلفان می‌توانند هزاران قربانی را بطور همزمان مورد هدف قرار دهند. برای مثال، افراد بطور منظم ایمیلهای ناخواسته که اسپ نامیده می‌شوند را از طریق ایمیل آدرسهایی که در وبسایتهای عمومی قرار دارد به هزاران قربانی می‌فرستند. برای مثال، دانشگاه‌های عمومی اغلب آدرس پروفسورها، معلمان، و کارکنان را روی وبسایتشان قرار می‌دهند. در عوض ، افراد می‌توانند این آدرسها را در فهرست اسامی خود کپی کنند و از آنها برای ارسال پیغام‌های اسپ مختلف استفاده کنند. در واقع، یکی از رایج ترین اشکال پیغامهای اسپم در نیجریه وجود دارد که فرستنده ادعا می‌کند بانکدار، وکیل یا پادشاه خارجی است که نیاز دارد تا برای حمل پولی از کسی کمک بگیرد. آنها اطلاعاتی را از ایمیل گیرنده درخواست می‌کنند، مانند نام، آدرس، شماره تلفن، و حساب بانکی بنابراین می‌توانند

اطلاعات را براحتی مورد سو استفاده قرار دهند و از حساب آنها دزدی کنند. از آنجائیکه برخی از مردم در این دام می‌افتند، ارسال هزاران پیغام مانند این می‌تواند تضمین کند حداقل یک نفر پاسخ می‌دهد. بنابراین فریبکاران احتمال موفقیت خود را از این طریق افزایش می‌دهند.

خطرِ شناسایی از اجرای قانون در محیطهای آنلاین نسبت به دنیای واقعی بسیار کمتر است. متخلفان در دنیای واقعی باید گام‌های مخالفی بردارند تا این احتمال که هویت واقعی اشان می‌تواند تعیین شود را کاهش دهند. برای مثال، دزدان ممکن است از ماسک‌هایی استفاده کنند تا صورت خود را بپوشانند. ممکن است آنها نیز از تغییر قیافه یا تغییر صدا استفاده کنند. قربانیان می‌توانند اطلاعاتی درمورد متخلفان را از طریق دوربین و فیلمبرداری از آنها نگه دارند و این کار را برای متخلف سخت می‌کند.

این موضوعات در محیطهای آنلاین اتفاق نمی‌افتد، پس برای متخلفان پنهان شدن پشت هویت واقعی اشان بسیار آسان می‌شود. ماهیت ناشناخته اینترنت این امکان را به افراد می‌دهد تا جنسیت، سن، نژاد خود را به روشهای مختلفی پنهان کنند. یک پروفایل در شبکه‌های اجتماعی مانند فیسبوک یا حساب ایمیل می‌تواند با استفاده از اطلاعات اشتباه از طریق گوگل، یاهو، یا هاتمیل ایجاد شود. این حساب اشتباه می‌تواند برای ارسال پیغام‌های تهدید آمیز به دیگران استفاده شود تا کمک کند هویتشان پنهان بماند. بطور مشابه، منابع فنی مختلفی برای مخفی کردن موقعیت فرد از دیگران طراحی می‌شوند. برای مثال، سرورهای پروکسی می‌توانند برای مخفی کردن موقعیت کامپیوترها استفاده شوند. برای مثال اگر سعی کنیم تا از طریق یک کامپیوتر و با استفاده از یک پروکسی به گوگل دسترسی پیدا کنیم، این دستور بواسطه سرویسی که درخواست را می‌سازد مسیری می‌سازد و اطلاعات را به ما برمی گرداند. در عوض، سرورها در گوکل کامپیوتر مارا بعنوان کامپیوتری که درخواست می‌دهد ثبت نمی‌کنند بلکه آنرا با سرور پروکسی همراه می‌کنند. برخی از متخلفان حتی می توانند به وب و ایمیل خود بواسطه کامپیوتر مردم مسیر دهند تا احتمال دستگیری خود را کاهش دهند.

جرایم سایبری برای عاملان براساس ملیتشان جذاب می‌شوند. از آنجائیکه افراد می‌توانند در سرتاسر دنیا قربانیان را مورد هدف قرار دهند، قانون داخلی یک تفاوت چشمگیر بر این هدف و دلیل هدف متخلف قائل هستند. بسیاری از کشورهای صنعتی قوانینی درمقابل جرایم سایبری دارند که خطر پیگیری و بررسی متخلفات را در صورت دستگیری افزایش می‌دهد. از اینرو مردمی که در کشور

حمله می کنند ممکن است احتمال پیگیری را افزایش دهند. با این وجود اگر یک کشور به شهروندانش اجازه ندهدتا در کشور دیگر جرمی کنند تا با پیگیری مواجه شوند ، پس عامل نمی‌توان بطور موفقیت آمیزی مورد پیگیری قرار گیرد. برای مثال معاهده ایی -نیست که به شهروندان روسی اجازه دهد تا در حملات درمقابل شهروندان ایالات متحده که در آنجا مورد پیگیری قرار می‌گیرد شرکت کنند . بزهکاران روسی نمی‌تواند بخاطر این تخلفات مجرم شناخته شوند و ممکن است عموما هیچ مجازاتی را متحمل نشوند. در عوض، بشدت دشوار است که مانع جرایم سایبری در کشورهای خارجی شد و ممکن است موجب تشویق حملات درمقابل کشورهای خاصی باشد.

درمقابل، برخی از کشورهای درحال توسعه، ممکن است قوانینی درمقابل سواستفاده از کامپیوتر نداشته باشند. اگر قوانینی وجود نداشته باشد، پس کشورها بعنوان دسته ایی از پناهگاه‌ها برای عاملان محسوب می‌شوند که درانجا می توانند تحریمات کمتری را متحمل شوند. این در ایجاد ویروس ILOVEYOU که در سرتاسر دنیا در سال ۲۰۰ منتشر شد مشهود است . این شکل از بدافزار هزاران کامپیوتر را مورد هدف قرار داد و بواسطه ایمیل منتشر شد، وبطور موثری اینترنت را در لحظه از کار می‌اندازد. برنامه در تاریخ ۴ می۲۰۰۰ در فیلیپین آغاز شد و در یک روز در سرتاسر دنیا منتشر شد . آن توسط یک دانش آموز فیلیپینی به نام اونل دی گوزامن، براساس برنامه ایی از مانیلا و علاقه او به هک کرد ساخته شد. در همان زمان هیچ قانونی درمقابل نوشتن بدافزارها در فیلیپین موجود نبود و امکان پیگیری گوزامن نبود. بنابراین عدم وجود قانون می‌تواند مقابله با جرایم سایبری را بطور بین المللی با مشکل مواجه کند.

بطور کلی، دسترسی جهانی به اینترنت مشکلات اساسی برای نهادهای اجرای قانون در کشور و کشورهای خارجی ایجاد کند. ساختار سیاست گذاری ها، بخصوص در امریکا، راهنمایی‌هایی را برای بررسی جرایم در داخل، ایالات و در سطح فدرال ایجاد می‌کند. تخلفهایی که در مرزهای قضایی روی می‌دهند مسئولیت دپارتمانهای پلیسی یا دپارتمانهای بخشداری هستند ، درحالیکه انهایی که در مرزهای ملی یا ایالتی هتسند توسط نهادهای ایالتی یا فدرال اداره می‌شوند. بسیاری از بزهکاران سایبری ممکن است در همان منطقه بعنوان قربانی نباشند، گرچه اگر در همان منطقه نیز باشند، ممکن است یک قربانی هیچ ایده ایی نداشته باشد که متخلف در کجا قرار دارد. این ابهامات چشمگیری درمورد نهاد یا ارتباط درست ایجاد می‌کند و میزان جرایم سایبری گزارش شده برای

اجرای قانون را کاهش می‌دهد. در واقع، این کم شماری با عنوان "تصویر تاریک" از جرم سایبری مورد اشاره قرار می‌گیرد، و در آن تعداد درست تخلفات ناشناخته هستند.

یک دلیل برای کم بودن گزارشات دشواری‌هایی است که در تعیین زمان دقیق روی دادن فعالیتهای غیر قانونی است. ممکن است افراد کاملا نا آگاه باشند که قربانی جرم سایبری هستند و وقتی بفهمند که دیر شده باشد. برای مثال، مشکلات سخت افزاری و نرم افزاری کامپیوتر ممکن است به خطا در تجهیزات منجر شود، یا نتیجه مستقیم فعالیتهای کیفری باشد که برای به تعویق انداختن آنها بوجود آمده است. بسیاری در محیطهای عمومی هستند که مهارتهای لازم برای تشخیص دلایل را ندارند و این تعیین زمان وقوع را دشوار می‌کند. از آنجائیکه بزهکاران سایبری تلاش می‌کنند تا قربانیان بیشتری بگیرند، شناسایی الگوها برای رفتارهای پرخطر آنلاین نیز دشوار می‌شود. در نهایت برنامه‌های نرم افزاری طراحی شده تحت حمایت برای کاهش خطر قربانی شدن افراد همیشه کار نمی‌کنند. تقریبا ۲۵ درصد از کامپیوترهای شخصی در سرتاسر دنیا از راه حلهای امنیتی مختلفی استفاده می‌کنند که نرم افزارهای بدخواهانه ایی دارند مانند ویروس، که روی حافظه اشان بارگذاری شده است.

شرم، حیا یا آسیب که ممکن است از قربانی سازی گزارش شده ناشی شود نیز احتمال اجرای قانون را کاهش می‌دهد. برای مثال، کلاهبرداری‌ها با ایمیل در نیجریه افراد بومی را مورد هدف قرار می‌دهد که باور دارند که هر ادعایی می‌تواند درست باشد. این گزارش که آنها فریب دیده‌اند ممکن است شرم آور باشد یا احتمال گزارش را کاهش دهد. در محیطهای کامپیوتری، موضوعاتی هستند که ممکن است احتمال گزارش در زمانی که جرم سایبری روی داده است را کم کند. برای مثال، ممکن است اگر مشتریان یک شرکت گزارش دهند که سیستم هایشان درمعرض آسیب هستند، شرکت مشتریانش را از دست بدهد. خجالت از دست دادن اطلاعات حساس ممکن است موجب پنهان کردن این جرم شود.

بطور کلی، تکنولوژی مزیتهای منحصربفردی برای متخلفانی دارد که لزوما در دنیای واقعی حضور ندارند. تکنولوژی بسرعت در دنیا حاضر می‌شود و به متخلفان اجازه می‌دهد تا به منابع دستیابی پیدا کنند. تعداد افراد آنلاین موجب فراوانی قربانیانی می‌شود که می‌توانند براحتی تحت تاثیر قرار بگیرند. تکنولوژی نیز افرادی را پیشنهاد می‌دهد که می‌توانند هویت خود را پشت نام‌ها و موقعیتهای اشتباه پنهان کند، و شناسایی افرادی که مسئول اتفاقات کیفری هستند را دشوار می‌کند. در نهایت

ساختارهای مختلفی قانونی و توافقات مشترک در سرتاسر دنیا پیگیری جرایم سایبری را دشوار می‌کند. درنتیجه افرادی که در جرایم سایبری مشارکت دارند با خطر کمتری در شناسایی روبرو هستند و ممکن است پاداشهای احساسی و مالی از جرایم سایبری را تجربه کنند.

۱-۵ تکنولوژی بعنوان یک اثبات

سومین و آخرین راهی که ممکن است تکنولوژی از آن طریق در تخلفات استفاده شود نقش تصادفی یا مشارکت در جرم است. در این مورد ممکن است کامپیوتر در ارتکاب جرم شرکت داشته باشد یا بعنوان وسیله ذخیره سازی استفاده شود. برای مثال، وجود پورنوگرافی کودک در لپ تاپ یا تلفنها نشان می‌دهد که تخلف صورت گرفته است . این اطلاعات، هرجایی که ذخیره شده باشند، شواهدی دیجیتالی محسوب می‌شوند، که بعنوان اطلاعاتی تعریف می‌شوند که در شکل باینری ذخیره و ارسال شده‌اند. شواهد دیجیتالی می‌توانند هرچیزی از تاریخچه بروزرها از ایمیل فرد ، چتها، و عکسها روی موبایل، وسایل GPS، و دوربینهای قرباین و متخلف باشد. کامپیوترها از لحاظ سنتی دیگر تنها وسایلی نیستند که می توانند ایمیل ارسال کنند ، چت کنند، و در اینترنت جستجو انجام دهند. تبلتها، موزیک پلیر ها، و وسایل دیگر می‌توانند به اینترنت متصل شده و شواهدی مبنی بر رفتارهای فردی را ایجاد کنند.

چندین نمونه ارزشمند وجود دارد که به روشن سازی شواهد دیجیتال و زمان دائمی شدنشان برای شکلهای مختلف جرم آنلاین و آفلاین کمک می‌کنند. برای مثال، BTK(Bind,Torture,Kill) (حصر، شکنجه، کشتن) یک قاتل زنجیره ای در کاناس بود، از سال ۱۹۷۴ تا ۲۰۰۵ که او دستگیر شد و و محکوم به ۱۰ قتل شد. قاتل در سالهای ۱۹۷۴ و ۱۹۹۱ ۱۰ نفر را در کاناس کشت و سپس به خواب رفت، گرچه بطور مداوم در رسانه‌ها نامه‌هایی را می‌نوشت و به پلیس می‌فرستاد. بررسی‌ها به نتیجه نینجامید و قاتلbtk نشان داد که او قتل دیگری را مرتکب شده بود که به او نسبت داده نشده بود.

سپس ، وقتی که قاتل پرسید که آیا هویتش براساس داده‌های دیسک قابل پیگیری است یا خیر پلیس شروع کرد به برقرار ارتباط مستقیم با btk. نهاد به اشتباه گفت که نمی‌توانستند اینکار را بکنند و BTK دیسکی برای آنها ارسال کرد که سندی در آن موجود بود که درمورد رفتارش توضیحاتی می‌داد. با استفاده از نرم افزار مناظره کامپیوتری تخصصی برای کمک به پردازش داده‌ها و شواهد روی دیسک، محققان موقعیت کامپیوتری که دیسک در آن باز شده بود را مشخص کردند،

همینطور توانستند فردی که آن سند را ایجاد کرده بود را نیز پیدا کنند. در عوض آنها توانستند اطلاعات دقیقی درمورد قاتل و شواهد کافی در مورد شرایط بدست آوردند که از طریق آن توانستند هویت اورا حدس بزنند که آیا او مردی بنام دنیز رادر بود. در نتیجه او دستگیر شد و ۱۰ حکم پی درپی گرفت که هر کدام برای یک قتل بودند.

شواهد دیجیتالی نیز از منابع آنلاینی بدست می‌آیند که ممکن است در وبسایتها و رسانه‌های اجتماعی دیده شوند. در واقع، شواهد دیجیتالی بدست آمده از سایتهای رسانه اجتماعی مانند فیسبوک و توییتر ، در اجرای قانون در چند دهه گذشته تاثیر گذار بوده‌اند. در پی خسارت کانادایی فرانسوی‌های ونکوور به برواین بوستون در فینال استنلی کاپ در۲۰۱۱، در ونکوور بین طرفداران آشوبی برپا شد که اتومبیلها را به آتش کشیدند و شیشه‌ها را شکستند و مغازه‌ها را به تارج بردند و بالای ماشینها به رقص درآمدند. در چند ساعت پس از این آشوب، پلیس بیش از ۳۵۰۰ ایمیل دریافت کرد که شامل ویدئو ها، تصاویر، لینکهای وبسایت برای سایتهای رسانه اجتماعی مختلف بودند. بعلاوه ، یک صفحه فیسبوک به نام " تصاویر آشوب ونکوور" ایجاد شد تا آنهایی که با تگ کردن تصاویر و ویدئوها در آشوبها مشارکت داشتند را دستگیر کند. بیش از ۱۰۰ نفر به کمک رسانه‌های اجتماعی دستگیر شدند.

با شکل گیری هر شکلی از شواهد دیجیتالی هویت احتمالی منابع و اطلاعات و موقعیتشان قابل شناسایی می‌شود. وسایل جانبی مختلف مانند درایو فلشها،سی دی‌ها و دی وی دی‌ها و حتی سیستم‌های بازی ممکن است شواهد دیجیتالی درخود داشته باشند که می‌توانند گردآوری شود. برخی از شرکتها رسانه‌های قابل پاک شدن را تولید می‌کنند که بسادگی تغییر می‌یابند، مانند عینک آفتابی یا یک مچ بند که یک درایو فلش دارند. با وسایل دیجیتالی ایی که بعنوان یک ابزار استفاده می‌شوند اجرای قانون و متقلبان باید ماهیت جرم دیجیتالی را بهتر درک کنند.

۱-۶ پاسخ اجرای قانون به جرایم سایبری

با درنظر گرفتن چالشهای تحمیلی توسط متخلفان حیاتی است که افراد بدانند در صورت قربانی شدنشان چه کسی با آنها ارتباط برقرار کرده است و چه نهادهایی وظیفه حمایت دارند. نهادهای سیاست گذاری و اجرای قانون دفاتر پیچیده ایی هستند که نقشهای مهمی دارند که به اصول قضایی محدود است. در بسیاری از موارد، موضوعات قضایی مانند این، به پیچیدگی شکلهای بسیاری از

جرایم سایبری وابسته هستند ، و جرایم سایبری را به قلمرویی از نهادهای اجرای قانون فدرال و ملی تبدیل می‌کنند تا به اجرای قانون داخلی.

مانند شکلهای سنتی جرم، بیشتر افراد ممکن است فکر کنند که اولین نهاد برای برقراری ارتباط که می‌تواند در زمینه جرایم سایبری به آنها کمک کند نهاد اجرای قانون داخل کشورشان است. اجرای قانون داخلی برای پاسخ به تماسهای مختلف، کمک به شهروندان، بررسی جرایم، دستگیری متخلفان، جلوگیری از جرایم، افزایش احساسات عمومی در زمینه امنیت، و پاسخ‌های عمومی به شهروندانی را برعهده دارد که در حوزه قضایی درخواستهایی را مطرح می‌کنند. در ایالات متحده، اکثر نهادهای اجرای قانون به تعداد کمی از جوامع روستایی و شهری با جمعیتهای زیر ۵۰۰۰۰ نفر خدمت رسانی می‌کنند. از ۲۰۰۸، حدود نیمی از نهادهای داخلی کمتر از ده مسئول قسم خورده داشتند؛ ۷۵ درصد از نهادها به کمتر از ۱۰۰۰۰ شهروند خدمت رسانی کرده بودند. در بریتانیا، نیروهای پلیسی مسئول سیاست گذاری در مناطق قضایی خاص و شکل دهی اکثریت نهادهای سیاسی هستند. درکانادا اکثر مراکز شهری مانند تورونتو یا مونترال نیز نیروهای خود را دارند که به جمعیت داخلی خدمت رسانی می‌کنند.

نهادهای اجرایی قانون در اکثر کشورها شامل ایالات متحده در حال حاضر نقش مهمی در جلوگیری و بررسی شکلهای جرایم سایبری ندارند. مسئول بررسی جرایمی هستند که قربانی یا متخلف در حوزه قضایی آنها سکونت دارد. برای مثال، اجرای قانون داخلی در ابتدا مسئول بررسی اکثر موارد در زمینه آزارهای اینترنتی بود. موارد مربوط به جرایم سایبری شخص محور مانند ایجاد و مصرف پورن کودکان، مانند درخواستهای جنسی و روسپی گری در امریکا، نیز ممکن است توسط نهادهای پلیسی داخلی مورد بررسی قرار بگیرد.

در طی دهه‌های گذشته، هردو مدیران سیاسی و علمی فهرستی از دلایلی را مطرح کرده‌اند که می‌گوید چرا جرایم سایبری چالشهای مهمی برای اجرای قانون داخلی ایجاد می‌کند و چرا بشدت درگیر نیستند. همانطور که می‌توان از لیست زیر دید، برخی از چالشها می‌توانند توسط ایجاد اولویت بر این تخلفات مطرح شوند. موارد دیگر می‌توانند بسادگی مطرح شوند. فهرست شامل موارد زیر است اما به آن محدود نمی‌شود:

- موضوعات قضایی ایجاد شده توسط قربانی و متخلفی که در یک کشور زندگی نمی‌کنند.
- نبود تعاریف استاندارد برای جرایم سایبری

- اعتراض عمومی در مقایسه با جرم سنتی، بویژه جرایم خشونت آمیز
- مشکل در بررسی جرایم نامرئی
- مشکل در دستیابی و حفظ تکنولوژی‌های مورد نیاز برای بررسی این منابع
- مشکل در آموزش و حفظ مسئولان آموزش دیده
- نبود حمایتهای پلیسی و حاشیه ایی برای بررسی جرایم سایبری

گرچه فهرست بالا درمورد دلیل اینکه چرا اجرای قانون داخلی توسط جرایم سایبری به چالش کشیده است قابل حل شدن نیست، دانشمندان و مدیران سیاسی استدلال کرده‌اند که اجرای قانون داخلی باید نقش بیشتری در بررسی جرایم سایبری داشته باشد. برخی استدلال کرده‌اند که واحدهای بررسی جرایم سایبری داخلی می‌توانند مستقیما به جرایمی پاسخ دهند که شامل شواهد دیجیتالی هستند تا کمک‌ها درسطوح ایالتی و فدرال و ملی را کاهش دهند. سرمایه ناکافی به واحدهای جرایم سایبری تخصصی کمی در سطح داخلی در ایالات متحده منجر شده است .

دانشمندان و منتقدان دیگر بر نیاز به بهبود ماموران در اقدام بعنوان اولین واکنشگر در صحنه‌های جرم در کامپیوترها و شواهد دیجیتالی تمرکز کرده‌اند. تقریبا هیچ اطلاعاتی نیست که نشان دهد مسئولان به تماسهای سایبری پاسخ می‌دهند. علارغم این، اسناد دولتی و راهنماهای آموزشی نشان می‌دهند که مسئولان دولتی انتظار این موارد را در آینده ندارند. برای مثال در امریکا، موسسه ملی قضایی(NIJ) دومین ویرایش از بررسی صحنه جرایم الکترونیکی: راهنمایی برای اولین واکنشگران را در سال ۲۰۰۸ منتشر کرد. این راهنما در ابتدا برای ماموران تهیه شد و اطلاعات پایه ایی و پیشرفته را درمورد چگونگی پاسخ به صحنه‌های جرم فراهم کرد. که شامل شناسایی، مصادره، ثبت، کنترل، بسته بندی و حتی انتقال شواهد دیجیتال بود. بعلاوه، دانشمندان و مدیران سیاسی بطور مشابه لزوم آموزش کامپیوترها به ماموران را مطرح کردند.آموزش کامپیوتر به ماموران به منظور اطلاع از امنیت و درک لغات مورد استفاده شاهدان ضروری است.

جالب توجه است که مشخص می‌شود ماموران پلیس خودشان نقش خود در برخورد با جرایم سایبری را مانند نقش دانشمندان و مدیران پلیسی نمی‌دانند. ماموران می‌دانند که نهادهای اجرای قانون عموما اولویت کمی بر جرایم سایبری قائل هستند مگر اینکه موضوع مربوط به سو استفاده از کودکان در پورنوگرافی باشد. نهادهای داخلی نیز ممکن است قابلیتهایشان برای بررسی شکلهای مختلف جرایم اقتصادی آنلاین را افزایش دهند اما توجه کمتری به تخلفات و مزاحمتهای کامپیوتری