جرم و ارتباط از راه دور

تهیه و تنظیم: مؤسسه جرم‌شناسی استرالیا
مترجم: احسان زررخ
دانشجوی کارشناسی ارشد حقوق جزا و جرم‌شناسی
Email: e.zarrokh@gmail.com

اشاره

شـــرایط کنونی جهان پیرامون ما به گونه‌ای رقم خورده است که کار، تحصیل، تجارت و به طور کلی زندگی ما را با وسائل ارتباطی و مخابراتی پیوند زده است؛ به گونه‌ای که فکر زندگی بدون آن‌ها برای ما قابل تصور نیست. این پیشرفت خارق‌العاده در عرصه‌های مخابراتی و ارتباطی گذشته از جنبه‌های مثبتش، دارای جنبه‌های مخرب بسیاری است که می‌توان از آن‌ها به سیاه‌چاله‌های فضای مجازی تعبیر نمود.

مؤسســه جرم‌شناسی استرالیا که یکی از پیشـتازان عرصه جرائم دنیای مجازی اسـت در سـال ۱۹۹۶ میلادی اقدام به انتشـار تحقیقات خود در خصوص جـرم و ارتباطات نمود؛ هرچند که این گزارش تقریبا متعلق به یک دهه قبل اسـت لکن بـا تامل در آن درمی‌یابیم کـه بنیان‌های اصولی جرائم از راه دور همان است که در این مقاله بدان‌ها اشاره شده است؛ فلذا آشنایی با آن‌ها برای هر حقوقدانی که قصد ورود به این وادی را دارد لازم و ضروری است.

کلیدواژه: فناوری اطلاعات، جرم، مخابرات، قانون مجازات، مداخلات انتظامی

مقدمه

فناوری ارتباطات و مخابرات، فرصت‌های جزایی بی‌سابقه‌ای از حیث ابعاد و چهارچوب را فراهم آورد. انقلاب فناوری اطلاعات که ما در حال حاضر تجربه می‌کنیم شـاید قابل توجه‌ترین رشد و گسترش عصر ما به حسـاب می‌آید. تغییرات جدید و مورد انتظـار در فناوری مخابرات، در پرتو پیوستگی ارتباطات و محاسبات خسته‌کننده یقیناً تأثیر قابل توجهی بر جنبه‌هایی از زندگی داشته است؛ بانکداری، بورس سهام، کنترل حمل و نقل هوایی، تلفن‌ها، نیروی الکترونیکی و طیف وسیعی از سازمان‌های بهداشـت، رفاه و تعلیم و تربیت، به طرز گسترده‌ای به فناوری مخابرات و اطلاعات از حیث کار کرد آن‌ها نیاز دارند، که سبب شد ظرفیت آن‌ها برای عملکرد مؤثرتر افزایش یابد.

اما هماهنگ با این افزایش ظرفیت، آسیب‌پذیری نیز به دنبال آن مطرح شـد. این مسائل و این سیر حرکتی طرح تحقیقاتی جاری را در موسسه جرم‌شناسـی استرالیا خلاصه می‌کند و این موسسه درصدد کشف موارد خطر و اقدامات متقابل آن در جهت استفاده از مخابرات به عنوان ابزار و همچنین هدف جرم است.

اهداف نهایی مخابرات و طرح مطالعه جرم در موسسـه جرم‌شناسـی استرالیا برای شناسایی این موارد است:

اشکال جاری و بازده جرم‌خیزی مربوط به نظام‌های مخابراتی به عنوان ابزار و اهـداف فعالیت‌های مجرمانه، نقایص تشـکیلاتی و انتظامی که ارتکاب عمل نامشروع مورد بحث را تسریع می‌کند.

مشـکلاتی که در کارآگاهی، بازجویـی و تعقیب عمل مجرمانه بروز

می‌کند؛ ماحصل نوعی فرایند روشی قضائی و اقدامات متقابل است، که خطرات آتی عمل مجرمانه مورد بحث را بدون وارد آوردن خسارات جنبی به حداقل می‌رساند.

کار ما بالاخره به مباحثی منتهی می‌شود که شکل‌بندی انتظامی مناسب را برای مقابله با اشکال مختلف جرایم مربوط به مخابرات سامان می‌دهد.

تشکیلات آرمانی ممکن است با انتظارات ما متفاوت باشد – به فعالیت مورد بحث بستگی دارد – اما احتمالاً مجموعه‌ای از راه‌حل‌های بازاری، انتظامی و اجرایی قانون را در برخواهد داشت، این طرح همچنین مسائلی از رهیافت جهانی مخابرات را مورد بررسی قرار می‌دهد.

اگر بخواهیم از نظر تشکیلاتی صحبت کنیم، باید گفت که نظام‌های مخابراتی، جهان را مکانی کوچک‌تر کرده و کمتر کسانی اکنون می‌توانند این واقعیت را از نظر دور بدارند که تصمیمات مالی در لندن یا توکیو در حالی که تأثیرات محیطی دارند، سریعاً مسائل جهانی را به دنبال خواهند آورد. تصاویر با شکوهی که در هالیوود ساخته و پرداخته می‌شود شاخص‌های جدیدی را در روسیه به وجود می‌آورد. تصاویر هرزه نمایی که در دانمارک خلق و ابداع می‌شود برای جوانان پانزده ساله در استرالیا نیز قابل دسترسی است.

ابعاد بالقوه مربوط به ارتکاب جرم خارج از گستره صلاحیت، درگیری‌های جدی را برای بسیج موفقیت‌آمیز اقدامات مؤثر به دنبال دارد.

انواع جرم

طیفی از انواع فعالیت‌های مجرمانه که با نظامات مخابراتی یا علیه نظامات مخابراتی صورت می‌گیرند به نحو عجیبی گسترده است.

برخی از این فعالیت‌های مجرمانه حقیقتاً از نظر ماهیت بدیع نیستند، بلکه از نظر میانجی بودن بدیع هستند.

فعالیت‌های مجرمانه دیگر من حیث‌المجموع معرف اشکال جدیدی از کارهای نامشروع هستند. اشکال منحصر به فرد زیرین و فعالیت‌های مجرمانه متضمن نظامات مخابراتی، ابزار یا اهدافی هستند که موضوع تحقیق و بررسی ما را به دنبال دارد، این موارد لزوماً به صورت متقابل نه استثنایی هستند و نه سیاهه کاملی را تشکیل می‌دهند، برعکس آن‌ها معرف پهنه‌های اولیه نگرانی‌های سیاست‌گذاران هستند.

سرقت خدمات مخابراتی[1]

از زمانی که در ربع قرن گذشته، مهاجمان نظام‌های مخابراتی را خارج از کنجکاوی مورد حمله قرار داده‌اند، خدمات مخابراتی در مقابل جرم سرقت آسیب‌پذیر بوده‌اند. از میان جهات و انگیزه‌هایی که محدود به نیت شیطنت‌آمیز ساده است آن انگیزه‌ها و جهاتی که سرقت خدمات مخابراتی را به عنوان شیوه زندگی و حرفه عمده جزایی انتخاب نموده‌اند، بیشتر محل بحث هستند. افرادی که خدمات را می‌دزدند درگیر چالش قابل ملاحظه‌ای با کارهای مخابراتی و فراهم‌کنندگان خدمات مخابراتی و عامه مردم هستند که همیشه متحمل خسارات ناشی از تقلب هستند. بازار خدمات سرقت شده مخابرات در واقع و نفس‌الامر وسیع است، کسانی هستند که به سهولت درصدد طفره رفتن یا تخفیف گرفتن در هزینه‌های تلفن هستند، افرادی هم هستند که مثل مهاجران غیرقانونی که به طور مشروع و بدون مخفی کردن پایگاه خود قادر به خرید خدمات مشروع مخابراتی نیستند.

افراد دیگری هم هستند که به خدمات مخابراتی دست می‌یازند برای اینکه داد و ستد نامشروع خود را با کمترین خطر کشف اعمالشان انجام می‌دهند. در سرتاسر جهان مبالغ بسیار زیادی توسط قربانیان این چنین اعمال نامشروع از دست می‌رود. همچنین مبالغ زیادی برای جلوگیری، شناسایی و تعقیب این جرایم صورت می‌گیرد.

توطئه‌های جزایی[2]

رکن اصلی توطئه جزایی متضمن یک یا چند نفر برای توافق و هماهنگی به منظور ارتکاب جرم جزایی است. تسهیلات جدید مخابراتی به صورت شفاف طرق و وسائل مختلفی را بیان می‌کند که از طریق آن افراد مجرم به این توطئه‌ها نائل آیند.

بروز شبکه‌هایی که توسط دستگاه‌های دادگستری غیرقابل دسترسی هستند از طریق کاربرد کلید ویژه و فناوری انتقال داده‌های بالای اطلاعاتی می‌توانند ظرفیت پیچیده تشکیلات خود را بالا ببرند، به طوری که به این حد بالای فعالیت نائل گردند.

در ساز و برگ‌های مخابراتی دلایل و اسنادی را به کار می‌برند تا کار تشکیلاتی نقل و انتقال مواد مخدر، قمار بازی، روسپیگری، پول شویی، هرزه‌نمایی کودکان و تجارت اسلحه را تسریع نمایند (درحوزه‌های قضائی که این چنین فعالیت‌ها کلاً نامشروع است).

سرقت مالکیت معنوی[3]

هر ساله به دلیل تخلفاتی که در حق‌التألیف صورت می‌گیرد میلیاردها دلار در جریان فروش و بهره‌های مالکانه از دست می‌رود.

سرعت و دقتی که در اینگونه کپی‌های با ظرافت انجام می‌گیرد، به طرز تأسف‌باری کپی به وسیله فناوری مدرن را در شبکه‌های دایر مخابراتی افزایش داده است. تخلف از حق‌التألیف ممکن است به سهولت و بدون هیچ مشکلی ادامه یابد و بتواند توسط هر کسی که قادر به کار در شاه راه مخابراتی است صورت گیرد. گسترش سریع و دسترسی همه جانبه در استفاده از فناوری‌های وسایل ارتباطی چندجانبه اکنون افق‌های فرصت برای سارقین مالکیت‌های معنوی ایجاد می‌کند.

انتشار و پخش مواد و مطالب مجرمانه[4]

مندرجات مطالبی که بعضی‌ها آن را قابل اعتراض می‌دانند به وفور در فضای سایبر وجود دارد. از میان سایر چیزها این امر متضمن مطالب صریح جنسی، تبلیغات نژادگرایانه و دستورات ساخت ابزار آتش‌زا و منفجره است.

نظام‌های مخابراتی همچنین برای ارتباطات تهاجمی، ارعاب، تهدید و ایجاد آزار در تلفن‌های سنتی مهجور و مکالمات آن در تجلی کارهای سایبر معاصر به کار برده می‌شود و در آن‌ها مصراً پیغام‌هایی برای گیرندگان ارسال می‌شود، که تمایلی به دریافت آن ندارند.

پولشویی الکترونیکی[5]

حالا برای مدتی نقل وانتقال وجوه از طریق الکترونیکی به مخفی کردن

1-**Theft of telecommunications services**

2-**Criminal conspiracie**

3-**Theft of intellectual property**

4- **Dissemination of offensive materials**

5-**Electronic money laundering**

و تحرک وجوه حاصل از جرم کمک می‌کند. فناوری‌های آشکار می‌تواند در حد وسیع به مخفی کردن وجوهاتی که ناشی از سوء استفاده است کمک کند. (Wahlert ۱۹۹٦)

نهادهای وسیع مالی تنها منابعی نیستند که قدرت وصول نقل و انتقالات وجوه الکترونیکی را با سرعت نور برای محاکم متعدد می‌فرستند.

گسترش و توسعه نهادهای غیررسمی بانکی و نظامات موازی بانکداری ممکن است باعث بشود که نظارت فائقه بانک مرکزی تغییر مسیر دهد، اما همچنین باعث تسهیل فرار از قانون در معاملات نقدی در خصوص شرایط تهیه گزارش برای کشورهایی باشد که این موارد را در خود دارند. بانک‌های سنتی زیرزمینی که در کشورهای آسیایی قرن‌هاست نشو و نما کرده‌اند برای استفاده از مخابرات ظرفیت بیشتری دارند، با ضرورت و ازدیاد فناوری‌های گوناگون، اقدامات متقابل سنتی تجارت الکترونیک در مقابل پولشویی ارزش محدود خود را به زودی آشکار خواهد کرد.

تخریب و وحشیگری الکترونیکی[6]

جامعه صنعتی غرب قبلا تا این حد وابسته به پردازش پیچیده اطلاعاتی و نظام‌های مخابراتی نبوده است. هر نوع خسارت و یا هر نوع مداخله در کار آن‌ها منجر به عواقب فاجعه‌آمیز خواهد شد (Hundley & Anderson ۱۹۹۵).

یک برنامه کامپیوتری در نوامبر ۱۹۸۸ وارد شبکه اطلاعاتی شد و به سرعت فعالیت ٦۰۰۰ کامپیوتر را در آمریکا مختل کرد. هزینه تخمینی تشخیص علت و تعمیر و بازسازی این نظام از میلیون‌ها دلار فراتر رفت. تشکیلات دفاعی ایالات متحده هدف شایع این اقدام بود. (US GAO ۱۹۹٦)

طراحان امر دفاع در سرتاسر جهان وسایل اطلاعاتی جهان را اساساً به منظور زیرساخت‌های فناوری اطلاعاتی تشکیلات دفاعی مهیا می‌کنند. (Stix ۱۹۹۵)

تشکیلات کامپوتری دانشگاهی به دلیل دسترسی آن‌ها به بازجویی‌ها و شایستگی بازجویی افراد صالح مورد هدف قرار گرفته است.

حداقل در یک مورد، حمله‌ای به یک کامپیوتر صورت گرفت و می‌خواست وضعیت هوا را پیش‌بینی کند که منجر به نابودی یک کشتی در دریا شد. (Cheswick & Bellovin ۱۹۹٤, p.۱۵)

تقلب در بازاریابی از راه دور[7]

استفاده از تلفن برای خرید و فروش‌های متقلبانه، تقاضاهای تلفنی به منظور صدقات و خیریه یا ملاقات، تماس سرمایه‌گذاری‌های میلیارد دلاری در یک سال صنعتی در ایالات متحده بوده است.

گسترش فعالیت تجاری در آمریکا و دنیا هماهنگ با فناوری‌های ارتباطی لازم خطر بیع و تجارت متقلبانه را ظاهرا افزایش می‌دهد، ما قبلاً ظهور داد و ستدهای متقلبانه و سرمایه‌گذاری در اینترنت و ضرورت‌های آن را مشاهده کردیم.

توسعه بازاریابی لباس الکترونیکی فرصت‌هایی را برای خطرات جدید در مورد افراد غیرمحتاط و غیردقیق فراهم می‌آورد.

6-**Electronic vandalism**
7-**Telemarketing fraud**

مداخله نامشروع و غیرقانونی[8]

توسعه مخابرات، فرصت‌های جدیدی برای رهیافت‌های زیرزمینی الکترونیکی است. ملاحظات الکترونیکی برای فعالیت‌های مربوط به نظارت بر کار، زمانی که یکی از زوجین که پایبند به قرارداد زوجیت نیست و نیز اشکال جدید جاسوسی‌های سیاسی و صنعتی طرفداران زیادی پیدا کرده است.

گسترش فناوری آسیب‌پذیری‌های جدیدی را با خود دارد، در حالی که با سخت‌افزارهای ساده کپی‌برداری می‌کنند و هر فردی می‌تواند در حالی که در خانه خود نشسته، ارتباطات بی‌سیم همسایه نزدیک خود را بازبینی کند؛ هر چند که علائم الکترومغناطیسی که به وسیله کامپیوتر حس می‌شود آن را مورد اختلال قرار دهد، در حالی که قوانین موجود مانع بازبینی تشعشعات کامپیوتری نخواهد بود.

نقل و انتقال متقلبانه وجوه الکترونیکی[9]

گسترش نقل و انتقال وجوه الکترونیکی این خطر را افزایش خواهد داد که داد و ستدهای ناشی از این امر را می‌توان از مسیر اصلی خود منحرف و مختل نمود. نظام‌های موجود از قبیل ماشین‌های پردازنده خودکار و نقل و انتقال وجوه الکترونیکی از ابتدا مأمن اهداف متقلبانه بوده و گسترش کارت‌های هوشمند و ذخیره‌ای و کارت‌های حافظه تصویری، بدون تردید سبب می‌شود تا برخی از افراد استعداد خویش را معطوف جعل و تحریف الکترونیکی کنند و راه دسترسی به نظامات امنیتی حاضر را فراهم سازند.

زیرا همانطور که می‌توان از کارت‌های تلفن مجدداً استفاده نمود، می‌توان از کارت‌های هوشمند نیز مجدداً استفاده نمود، که این خود مستلزم طراحی مهندسی ویژه است.

انتقال وجوهات در داخل کشور بین چند حساب و پرداخت وجوه معاملات، خسارات زیادی را از طریق سرقت و تقلب و وجوه حاصله الکترونیکی با مقیاس بسیار وسیع ایجاد کرده، به طوری که آن‌ها را در شبکه‌های اطلاعاتی بین‌المللی مورد استفاده قرار داده و فرصت‌های جدیدی را برای ارتکاب جرم فراهم آورد.

به مرحله اجرا در آمدن درگیری و چالش[10]

ابعاد مشکل

متأسفانه جرایم مربوط به مخابرات را برخلاف سرقت‌های بانکی یا تصادفات مرگبار نمی‌توان در ابعاد کمی گنجاند.

بعضی از جرایمی که به کمک نظامات مخابراتی با تمهیدات متقلبانه قبلی انجام می‌شود یا علیه نظامات مخابراتی صورت می‌گیرد هر گز کشف نمی‌شوند، حتی نمی‌توان آن‌ها را با قربانیان این جرم کشف کرد.

از میان این جرایم بعضی‌ها به این دلیل از مقامات پنهان می‌مانند که در صورت افشای آن باعث بی‌آبرویی یا آسیب‌های تجاری قربانیان آن می‌شود.

ارزیابی عددی هم فریبنده است، چیزی که ممکن است مسئله بی‌اهمیت یا جزئی هم باشد می‌تواند در عمل و نفس‌الامر انعام و بخشش آدم با اهمیتی باشد. آقای استول در سال ۱۹۹۱ در جستجوی اشتباه حسابرسی ۰/۵۷ دلار در حساب کامپیوتری بود که منجر به افشای باند جاسوسی بین‌المللی شد.

8-**Illegal interception**
9-**Electronic funds transfer fraud**
10-**The Enforcement Challenge**

حتی توصیفات کیفی نیز ممکن اســت سر از اوهام درآورد، بسیاری از مردم صرف نظــر از مکالمات تلفنی تمایل دارند که کارهای خود را تکمیل نمایند. در این میان جنایتکاران مخابراتی نیز مستثنی نیستند، در حالی که بعضی‌ها می‌خواهند نام و نشــان آن‌ها افشــاء نگردد ولی بقیه می‌خواهند که هویت آن‌ها آشــکار شــود و این افراد اغلب می‌خواهند فعالیت‌های خود را با زیور بیآرایند. از اینرو شکاف عمده‌ای بین آن‌هایی کــه فقط کار می‌کنند و آن‌هایی که کار خــود را به زبان می‌آورند و بین آن‌هایی که فکر می‌کنند کار خود را انجام داده‌اند وجود دارد.

سازمان‌های اجرایی قانون از طرفی می‌خواهند عظمت و ابعاد مشکل را بیش از آنچه که هست نشان دهند تا از این طریق بتوانند پایگاه‌های مسئولیتی خود را حفظ کنند و یا گسترش دهند. سایر بازیگران که انگیزه‌های تجارتی قابل بحث برای افزایش حجم مشکل دارند، شامل صاحبین وسایل ارتباط جمعــی خبری و صاحبان صنایع امنیتی هســتند. صرف نظر از کراهت و بی‌میلی قربانیان جرایم مذکور کــه نمی‌خواهند موضوع را گزارش دهند، مرموز بودن فناوری و پیچیدگی‌های آن اغلب کشــف و افشای مرتکبین آن را بی‌نهایت مشــکل می‌ســازد. از سوی دیگر کسانی که سعی دارند بر هویت خود نقاب بزنند اغلب می‌توانند از طریق اختفاء یا تشکیل شبکه‌های چندگانه در کشــور، خرده‌فروشان و واســطه‌های بی‌نشان سپری در برابر بازرسی‌های کلی بسازند. بعضی جرایم منجر به کشف یا خسارت نمی‌شود مگر آنکه مدت زیــادی از بروز آن بگذرد. درحالی که جرایم دیگر هرگز کشف نخواهند شد، مانند انتشار یک ویروس رایانه‌ای و یا درج یک بمب هوشــمند و انفجار آن، که در این موارد ممکن اســت بین آن‌ها زمان قابل ملاحظه‌ای سپری شود.

مسائل خارج از قلمرو ارضی[11]

یکــی از جنبه‌های پر معنای جرایم مربوط به مخابرات جهانی بودن آن اســت، در حالی که جرم بین‌المللی به هیچ وجه یک پدیده متحدالشــکل جدید نیســت، ولی جهانی شــدن مخابرات و ارتباطات آسیب‌پذیر بودن انســان را در مقابل جرایم ارتکابی خارج از کشــور به طور قابل توجه‌ای افزایش داده است. نظریه زندگی در جهان بدون حدود و ثغور بیشتر درباره مجرمین حقیقت دارد تا دســتگاه‌های اجرایی قانون و این مضمون و معنا تأثیری عمیقی بر کشف جرم، بازجویی، تحقیق و تعقیب مجرمین می‌گذارد؛ از اینرو در رابطه با تعقیب جرایم مخابراتی که از جنبه بین‌المللی برخوردار هســتند، دو مشــکل بروز می‌کند: اول تعیین اینکه کدام دادگاه صلاحیت رسیدگی به جرم ارتکابی را دارد. دوم تحصیل دلیل و تضمین اینکه مجرم را می‌توان یافت و در نزد دادگاهی محاکمه کرد. هر دو این سوالات مسائل حقوقی پیچیده‌ای را از لحاظ صلاحیت و استرداد مجرم بیان می‌کند.

حتی اگر کســی قادر باشــد که قانــون حاکم در این مــورد را بیابد، مشــکلات دیگری در خصوص به کار بردن قانون مطرح می‌شــود. در مــورد وحدت صلاحیت در کشــوری مثل نیوزلند که یک قانون و یک دســتگاه قانونی وجــود دارد، باز هم در قانون حاکــم و به کار بردن آن مشکل حادث می‌شود.

لذا در نظامات فدرالی مثل استرالیا، آمریکا و کانادا اجرای قانون استرداد مجرمین کاری بس دشوار است.

اعمال مجرمانه‌ای که در سراسر دنیا بروز می‌کنند مشکلات فزاینده‌ای را مطرح می‌کنند؛ از سوی دیگر فرمانروایان سیاسی و حاکمان کشورها در داخل کشور خود نظارت بر رفتار و جریان‌ها را مشکل می‌بینند چه رســد به خارج از کشورشــان. در نتیجه تثبیت و تنظیم قوانین در داخل برای این نوع جرایم ثابت شــده است که تناسبی ندارد. (Post ۱۹۹۵)

اجرای قانون خارج از قلمرو ارضی اغلب ممنوع است، و نیز همکاری در مرزهــای بین‌المللی برای اجرای این چنین مواردی مســتلزم تلفیق ارزش‌ها و اولویت‌هاست، که هر چند سیطره جهانی دارند ولی همیشه در دسترس نیستند.

گاهی تصاویر، ایده‌ها، انگاره‌ها و رویه‌ها که در یک کشور و در یک مکان کاملاً مطلوب و پذیرفتنی است در کشور دیگر منفور و نامطلوب است.

مقامات صلاحیتدار یک دادگاه که در افشــای آثار الحادی چون رمان سلمان رشدی یا در رابطه با استقلال تبت از طریق الکترونیک هیچ رنج و زحمتی متحمل نمی‌شوند و هیچ زمان یا تلاش زیادی صرف نمی‌کنند تا به مقامات دادگاه‌های صلاحیتدار که قربانی این چنین مواردی هستند کمک کنند.

تقریباً ســه دهه طول کشیده تا توافق اتفاق آراء معتدلی در خصوص کمک متقابل بین‌المللی در توسعه مبارزه علیه نقل و انتقال مواد مخدر و پولشویی حاصل شود.

حتی در آن کشورهایی هم که اصولاً با میثاق کنار آمده‌اند اجرای بالفعل این امر خیلی مشکل است (Nadelmann ۱۹۹۳) مشکلات مشابهی در رابطه با حق تفسیر آثار بین‌المللی و ترتیبات بانکی وجود دارد.

ســایر مسائل که بازرسی و تحقیقات پیچیده و سازمان یافته و صرف وقت زیادی را به دنبال دارد، حجم مواد و مطالبی را که ادله اثبات جرم در آن گنجانده شــده و اطلاعات افزونی که در این باره جمع می‌شود یا این امر را به طور کلی غیرقابل حصول می‌داند، یا دسترسی به آن تنها با تلاش بسیار و پرهزینه میسر خواهد بود.

مشکلات دیگری در اجرای حاکمیت ملی و فرماندهی سیاسی روی ســرمایه و اطلاعات منعکس می‌شــود. مســاله صلاحیت محاکم برای انتقال‌دهنده اطلاعات بر روی دستگاه کامپیوتر مطرح است. اگر روزنامه مالی بر روی خط شبکه‌ای که در آلبانی منتشر می‌شود حاوی پیش‌بینی سفته بازی متقلبانه شرکتی باشد که سهامش در بازار بورس استرالیا خرید و فروش می‌شود، بگوئید جرم در کجا اتفاق افتاده است؟

طیف وسیع اقدامات متقابل[12]

با در نظر گرفتن مشــکلات فوق‌الاشعار مناســب است که در مورد تمامی نهادها، ابزارها و وسائلی که غیرقانونی بودن مسائل مطروحه را در برمی‌گیرد فکر کنیم. کیفیت گوناگون مخابراتی مربوط به غیرقانونی بودن یک عمل، در مقابل یک راه حل منفرد مقاومت می‌کند. در واقع هر کدام از این اشکال اساسی، نامشروعیت و غیرقانونی بودن که در بالا شرح آن رفت به قدری پیچیده است که اگر اساساً راه حلی هم وجود داشته باشد این راه حل مجموعه‌ای از ابزار و تجهیزات را به دنبال خواهد داشت.

بــه طور کلی این ترکیب از راه‌حل‌ها متضمن عناصر حفاظت شــخصی به وســیله قربانیان مورد نظر اعمال نامشــروع مخابراتی است و راه‌حل‌های تجاری- بازاری را نیز در برمی‌گیرد و همچنین ابتکارات خود سامانی که مورد نظر مقررات و آئین‌نامه‌ها هستند و نیز موارد ریز را نیز شامل می‌شود. اجرای قوانین و مداخله منظم دولت و همکاری اشخاص ثالث در تولید، نظارت به وسیله افراد به خصوص و گروه‌های شهروند در همین راستاست.

11-**Extraterritorial issues**

12-**The Range of Countermeasures**

خودیاری[13]

با توجه به اینکه مشخص شـده ظرفیت دولت‌ها برای نظارت و کنترل جرائم مربوط به مخابرات محدود است، بنابراین اولین سیر دفاع و مقابله در اجرای رفتار محتاطانه به وسیله قربانیان مورد نظر قرار دارد؛ درست در حالی که اولین اقدام در کنترل سرقت با کیفیت مشدد و شکستن حرز، قفل و کلید نمودن درها و پنجره‌هاسـت، در همان حال اصول اساسی امنیت اطلاعات را باید مورد احترام قرار داد. خواه خطر مورد بحث تقلب یا ناخواسـته در معرض مسـائل قابل اعتراض قرار گرفتن باشد، افراد و سازمان‌ها می‌توانند اقدامات مشابهی برای دفاع از خود اتخاذ نمایند. در اجرای یک احتیاط ساده مثل استفاده از روش‌های محدود کردن دسترسی به نظامات کامپیوتری در بسیاری از موارد کفایت می‌کند. این امر منجر شده تا امنیت کامپیوتری به یکی از صنایع پیشرفته جهان بدل شود. علاوه بر رویه‌های مدیریتی مستحکم‌تر و معرفی مسیرهای ظریف‌تر و احراز صحت روش‌ها و برنامه‌های فناوری جدید از قبیل ابزار امنیتی حیات‌سـنج و برنامه‌های کشف بی‌نظمی، باعث می‌شود که ایمنی نظامات کامپیوتری بالا رود.

بعد از بروز حادثه اولین خط سیر ترمیم خرابی در خود قربانی نهفته است. مسـیر عادی ارائه طریق در پرونده‌های تخلفات مالکیت معنوی یا افتراء در دعاوی مربوط به خسـارت محاکم حقوقی است. اخیراً یک نفر سـخنران دانشگاهی در استرالیای غربی به موجب حکم دادگاه پس از اینکه موضوع مداخله وی در شاهراه اطلاعاتی به عنوان قربانی اثبات گردید خسارت معتنابهی به موجب حکم دادگاه دریافت کرد.[14]

در این موارد وقتی کسانی خدماتی را فراهم می‌کنند، بهتر است از نوع و مندرجات مسائل مضر اطلاع داشته باشند، زیرا آن‌ها نیز مسئول شناخته می‌شـوند. در این شـرایط خطر قانونی کمک می‌کند که سطح بازرسی دقیق را که ممکن است به طرق دیگر حادث نشود بسیار بالا ببریم.

راه‌حل‌های تجاری

خود بازار می‌تواند فرآورده‌هایی را ارائه دهد که به ابتکار عمل فرد در مقابل خلاف‌های مخابراتی کمک کند، مثلاً مشـکل دسترسی به مطلب و مواد مجرمانه در شاهراه اطلاعاتی را در نظر بگیرید؛ طیف وسیعی از نرم‌افزارهای تجارتی با قابلیت بالا وجود دارند که دسترسی به سایت‌های معینی را محدود می‌کنند؛ به علاوه بازاری در حال گسترش برای فراهم آوردن خدمات اختصاصی با حجم مناسـب برای خانواده‌ها با تضمین عاری بودن از اعمال جنسی، خشونت و تحقیر در حال بروز است.

مضافاً اینکه به احتمال قوی یک بازار در حال گسـترش برای کنترل خسارت بر خدمات در هنگام هجوم و حمله به نظام‌های مخابراتی وجود دارد. سازمان‌های قربانی جرم در خصوص افزایش سیستم ایمنی و ذخیره مجدد عملیات عادی نگرانی بیشتری دارند تا بسیج کردن قانون و حقوق و در مراحل دیگر جلب توجه عامه برای آسیب‌پذیری خودشان؛ گسترش دسته‌های جوابگویی به موارد اضطراری کامپیوتری و دادن بودجه صنعتی و کمک در اجرای قانون باعث تحقق این اهداف می‌شود.

ظرفیت تجارتی اینترنت که واسـطه مسلم تجارت در زندگی امروز ماست از نظر کارآفرینان در سرتاسر جهان دور نیفتاده است. فناوری‌های گسـترده تجاری در صـدد فراهم آوردن اعتمادی هسـتند که به عنوان پی‌بنای تجارت و کاهش خطر سوء استفاده به حداقل، ضرورت دارند.

بعضی مواقع مشـکلات را می‌توان به راه‌حل‌هایی کشانید، مثلاً یک ویروس کامپیوتـری را در نظر بگیرید که عاملین نظام‌های مورد حمله آن در سرتاسـر دنیا هستند. به عنوان یک اقدام متقابل در مقابل سرقت نرم‌افزار یک بمب هوشمند می‌تواند در فراورده‌های نرم‌افزار تجاری جای داده شود و هدف آن فعال کردن این مرحله است، وقتی که برای بار دوم از آن نرم‌افزار نسخه‌برداری می‌شود.

نیروهای بازاری هم می‌توانند سـفارش و دسـتور ثانوی برای کنترل نفوذها ایجاد کنند. به محض اینکه تشـکیلات بزرگ شروع به ارزیابی آسیب‌پذیری خودشان نسبت به سرقت الکترونیک یا آوارگی آن نمایند، می‌توان از آن‌ها انتظار داشـت که خود را در مقابل خسارت‌های بالقوه بیمه کنند. شرکت‌های بیمه‌گر در صورتی که احتیاط‌های مناسب و لازم ایمنی را از طرف قرارداد بیمه خودشـان مطالبه نمایند، خیلی به نفعشان خواهد بود؛ در واقع آن‌هائی که می‌خواهند بهای بیمه را ارزیابی و تعیین کنند بیشتر بستگی به رویه‌های ایمنی بیمه‌گذار آتی دارد.

خودسامانی[15]

یک شـیوه خود سامانی هم می‌تواند به وسـیله کارپردازان مخابراتی و فراهم‌آورنـدگان خدمات مخابراتی اعمال شـود، در حالی که حجم وسـیع عبور و مرور مانع بازرسـی دقیق کلیه مندرجات آن می‌شـود؛ فراهم‌آورندگان تعهدات اکنون تعهدات کتبی و امضاء شـده را از طرف مقابل به عنوان شـرط ارائه خدماتی عنوان می‌کنند که اسـتفاده‌کننده از ارتـکاب فعالیت‌های غیرقانونی خودداری نمـوده و همچنین از طیف وسیع موارد نقض معاهده‌نامه بکاهد. زیر پا گذاشتن این تعهدات منجر به پایان دادن به خدمات خواهد بود.

با توجه به اینکه گروه‌های گوناگون صنعتی با تهدید به اقدامات قوی اقدام به تحمیل مقررات بر ارتباطات اطلاعاتی می‌کنند، لذا این گروه‌های صنعتی رمزهای کاری خودشـان را گسترش می‌دهند تا از احتمال سوء استفاده از فضای سایبر و دستگاه هوشمند بکاهند.

همکاری شهروندان در تولید[16]

هر شـهروندی درباره دسترسـی به مطالب نامطلوب نگران است و این امر منجر به بازبینی و نظارت در فضای هوشـمند می‌شود. دو مورد از برجسـته‌ترین تشکیلات این نظارت عبارتند از مرکز سیمون ویزنتال (Simon Wiesenthal) کـه خـط نظارت آن در راسـتای مقابله با پیام‌های ضدصهیونیستی و نژاد پرستانه صرف می‌شود و دیگری دستگاه فرشتگان قیم و ناظر (Guardian Angels) هستند که منادیان هوشمند آن داوطلبانی را اسـتخدام می‌کنند که به گونه‌ای بر فضای سـایبر فائق آمده در جستجوی طیف اعمال غیرقانونی باشند، که شامل مواردی چون برهنه‌نمایی کودکان، هرزه نمایی، تحقیر، اهانت و امثال آن است.

تمامی اطلاعاتی که از این داوطلبان اخذ می‌شود برای مراجع و مقامات اجرایی قانون در پرونده‌های فعالیت‌های جزایی و نیز برای فراهم آوردن نرم‌افزار در زمینه نقض رفتار ارسال می‌شود.

گروه‌هایی که حامی حقوق افراد هستند، چنین شبکه‌هایی را تشویق می‌کنند که برای ایمنی کودکان و رفتار دوستانه با آن‌ها این عناوین را ثبت

13-**Self-help**

14-(Rindos v. Hardwick, Supreme Court of Western Australia, 31 March 1994)

15-**Self-regulation**

16-**Citizen co-production**

کننـد، به طوری که والدین آن‌ها بتوانند نرم‌افزار تجاری موجود را برای هدایت فرزندانشان به کار گیرند.

اجرای سنتی قانون[17]

اجرای قانون با بسیاری از ملاحظات مالی، فنی و خارج از قلمرو ارضی به صورتی که فوقاً شرح آن رفت محال می‌گردد. مع‌الوصف روش‌ها و رویه‌ها در حال گسترش هستند و برای تحقیق و بازجویی از جرایم مربوط به مخابرات دست در دست هم می‌دهند. مشکلات امر به صورتی است که اجرای قراردادی این موارد هدفشان صرفاً محدود به نقض جدی تعهدات باشد.

علی رغم چالش‌ها و درگیری‌هایی که در فضای سـایبر وجود دارد، شـاهراه‌های وسـیع اطلاعاتی مانع اجرای قانون می‌شوند، هر چند که قدرت بالقوه آن‌ها را باید تمیز بدهیم. انتظار می‌رود اسـتفاده از فناوری برای روابط عمومی توسـط دسـتگاه‌های عمومی به منظور جلوگیری از جـرم و نیز مبادله اطلاعات برای پیشـگیری و بازپرسـی جنایی در سـال‌های آتی به صورت تأسف‌باری گسـترش یابد. قبلاً تصاویری را در شبکه‌های اینترنتی به نمایش گذاشتند که منجر به دستگیری افرادی شـد که سـازمان اطلاعات مرکزی آمریکا (F.B.I) بـه دنبال آن‌ها بود.

عواقبی که مورد نظر نبوده[18]

خط سیر اعمال نامشروع مخابراتی، شامل تعارض‌ها و تضادهاست. بسـیاری از راه‌حل‌های ظاهری، مثل شمشیر دولبه می‌مانند که عواقب نامطلوب داشـته و حتی در برخی موارد وخامت آن بیش از مشـکلات اساسی است. همچنان که در پهنه‌های انتظامی و پهنه‌های عمومی هر فرد باید دفاع ویژه‌ای در مقابل اعمال نامشروع مخابراتی انجام دهد که صدمه‌ای بیشـتر از آنچه که مورد نظر بوده به بارمـی‌آورد. (Grabosky 1995)

بر همین منوال ممکن است چیزهایی به بار بیاورد که ما آن را نتایج و پیامدهای ممنوعه می‌دانیم، تلاش‌های رسمی برای سد کردن دسترسی به یک سایت اطلاعاتی معین اضطرار و فوریت الهام گرفتن از سایت‌های مرتبط را در محاکم مشروع‌تر می‌نماید، مراجعی که برای افزایش موارد دسترسـی به مطالب مورد بحث به کار گرفته می‌شوند. تلاش‌هایی که به کار می‌روند برای کتمان و مخفی کردن سـایت‌های اطلاعاتی کانادا، سـایت‌هایی که تبلیغات نئونازی‌ها را منتشر می‌کردند و حتی اطلاعات مضری درباره محاکمه جنایی در حال اجرا می‌دادند، که اقدامات صورت گرفته در این قسمت به صورت منحصر به فرد، ناموق از آب درآمدند.

نتیجه‌گیری[19]

جرائم بین‌المللی که جنبه قراردادی بیشتری دارند چالش مشکلی را در اجرای قانون به دست می‌دهد، جرائم مربوط به مخابرات حتی چالش‌های بیشتری را به وجود می‌آورد، ممکن است در باره این سوال که آیا اساساً این عمل جزایی است یا نه و یا اینکه آیا اساساً این عمل را مرتکب شده یا نه یا اینکه چه کسی قربانی آن جرم است و چه کسی بازجویی در آن باره را می‌تواند انجام دهد و چه کسی بایستی حکم جزایی در آن مورد صادر کند و چه کسی او را باید مجازات کند، متفق‌القول نیستند.

یک کنـش بنیادین بین دسـتور غیرقانونی که اقتصادهای پیشـرفته جهان را مشـخص می‌کند با آرمان کنترل جنبه‌های نامطلوب مخابرات وجـود دارد. مـع الوصف حالتـی را می‌توان تصور کـرد که جنبه‌های نامنظـم آن حداقل در حال حاضر حاکم اسـت. خطر معتنابهی وجود دارد که مداخلات منظـم زودرس نه تنها توانایی نیل به آثار مطلوب را نداشته باشـد بلکه همچنین بر روی گسترش فناوری اثر منفی بگذارد.

مقررات بیـش از حد یا مداخلات انتظامـی زودرس خطر رکود در سـرمایه‌گذاری و ابـداع و اختراع را به دنبال دارد. با معین شـدن جنبه رقابتی روز افزون بازار جهانی، دولت‌ها مجبور می‌شوند بین دستورات پدرمآبانه و گسـترش رشـد اقتصادی و تجاری یکـی را انتخاب کنند.

چالشـی که رودرروی کسانی قرار دارد که می‌خواهند جرم مخابراتی را به حداقل برسـانند این اسـت که موازنه‌ای را فراهـم بکنند تا درجه تسـاهل‌پذیری و تحول‌پذیری از نظر عدم مشروعیت برای بهره‌برداری خلاق از فناوری ایجاد کنند. در این مرحله اولیه انقلاب فناوری برای افراد و گروه‌های ذی‌نفع و دولت‌هایی مفید خواهد بود، که اولویت‌های خود را سامان داده و اجازه بدهند این اولویت‌ها اثر خود را در بازار بگذارند.

بازارهـا می‌توانند راه‌حل‌های نهایی‌تـر و کاراتر را بیش از مداخلات دولت فراهم بکنند.

مخابرات به سختی اولین یا تنها برنامه مسلطی است که ماوراء نظارت و کنترل یک دولت منفرد، به تنهایی قرار داشته باشد. عبور مرور هوایی بین‌المللی، قانون دریا، نقل و انتقال وجوه و سایر مسائل محیط زیستی از قبیل شکاف در لایه اُزن و گرم شدن کره زمین، سایر تلاش‌های آشکار بین‌المللـی را می‌طلبد. یک جرم مخابراتی به شـیوه‌ای رخ می‌دهد که نامرتبط با آن‌هایی نیست که مسائل همراه بیرون از مرزهای یک کشور را در برمی‌گیرد یعنی بی‌شـباهت به مواد مخدر یا نیروی اتمی نیستند.

این مسأله که آیا تلاش‌های هماهنگ برای مبارزه با جرم مخابراتی به افقی موفق‌تر از آنچه که در سایر مسائل جهانی نائل آمده باشد یا خیر را در آینده خواهیم دید.

منابع

1. Cheswick, W.R. & Bellovin, S.M. 1994, Firewalls & Internet Security, Addison- Wesley, Reading, MA.

2.Grabosky, P. 1995, "Counterproductive regulation", International Journal of the Sociology of Law, vol. 23, pp. 347-69.

3. Hundley, R. & Anderson, R. 1995, "Emerging challenge: Security and safety in cyberspace", IEEE Technology and Society Magazine, vol. 14, no. 4, pp. 19-28.

4. Nadelmann, E. 1993, Cops across Borders: The Internationalization of U.S. Criminal Law Enforcement, Pennsylvania State University Press, University Park.

5. Post, David G. 1995, "Anarchy, State and the Internet: An essay on law-making in cyberspace", 1995 J.Online L, art.3, http: //warthog.cc.wm.edu/law/ publications/jol

6. Stix, G. 1995, "Fighting future wars", Scientific American, vol. 273, no. 6, pp. 74-80.

7. Stoll, C. 1991, The Cuckoo's Egg, Pan Books, London.

8. United States, General Accounting Office 1996, Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, GAO/AIMD-96-84, 22 May.

9. Wahlert, G. 1996, "Implications for law enforcement of the move to a cashless society", in Money Laundering, eds A. Graycar & P.N. Grabosky, Research and Public Policy Series No. 2, Australian Institute of Criminology, Canberra, pp. 22-8.

17-**Traditional enforcement**
18-**Unintended Consequences**
19-**Conclusion**