کلاهبرداری سایبری در حقوق کیفری ایران

(با تاکید بر جرایم اینترنتی و تروریسم سایبری در حقوق کیفری آمریکا)

مؤلف

عبداله شیرفردی

(مدرس دانشگاه)

انتشارات هوشمند تدبیر

سرشناسه	:	میرفردی، عبداله، ۱۳۶۱-
عنوان و نام پدیدآور	:	کلاهبرداری سایبری در حقوق کیفری ایران (با تاکید بر جرایم اینترنتی و تروریسم سایبری در حقوق کیفری امریکا)/ مولف عبداله میرفردی.
مشخصات نشر	:	تهران : هوشمند تدبیر، ۱۳۹۷.
مشخصات ظاهری	:	۳۴۸ ص.
شابک	:	۹۷۸-۶۰۰-۴۱۸-۱۷۹-۲ :
وضعیت فهرست نویسی	:	فیپا
موضوع	:	جرایم کامپیوتری -- قوانین و مقررات-- ایران
موضوع	:	Computer crimes -- Law and legislation-- Iran
موضوع	:	جرایم کامپیوتری -- قوانین و مقررات -- ایالات متحده
موضوع	:	Computer crimes -- Law and legislation -- United States
موضوع	:	تروریسم رایانه‌ای -- قوانین و مقررات -- ایالات متحده
موضوع	:	Cyberterrorism -- Law and legislation -- United States
موضوع	:	شبکه‌های کامپیوتری -- ایران -- تدابیر ایمنی
موضوع	:	Computer networks -- Security measures -- Iran
موضوع	:	شبکه‌های کامپیوتری -- ایالات متحده -- تدابیر ایمنی
موضوع	:	Computer networks -- Security measures--United States
موضوع	:	حقوق تطبیقی
موضوع	:	Comparative law
رده بندی کنگره	:	KMH ۲۰۱۸ ک۲/۱۳۹۷ م۹
رده بندی دیویی	:	۳۴۳/۵۵۰۹۰۴۴
شماره کتابشناسی ملی	:	۵۵۲۶۶۵۵

نام کتاب..... کلاهبرداری سایبری در حقوق کیفری ایران (با تاکید بر جرایم اینترنتی و تروریسم سایبری در حقوق کیفری آمریکا)

مولف..... عبداله میرفردی

نوبت چاپ..... اول ۱۳۹۷

تیراژ..... ۱۰۰ نسخه

ناشر..... انتشارات هوشمند تدبیر

مدیرمسئول نشر..... محمد قجر

قیمت..... ۱۸۰۰۰۰ ریال

شابک..... ۹۷۸-۶۰۰-۴۱۸-۱۷۹-۲

آدرس و شماره تلفن ناشر: تهران، خیابان انقلاب، بین خیابان دانشگاه و خیابان ابوریحان، پلاک ۱۱۷۶، طبقه‌ی اول

تلفن : ۶۶۴۷۹۶۶۵، ۶۶۴۷۹۶۷۵ و ۰۹۱۲۳۸۶۱۲۶۷

فهرست مطالب

عنوان | صفحه

پیشگفتار

متصل کردن رایانه های بی شمار در سراسر دنیا به یکدیگر منجر به پیشرفتهای حیرت‌آوری در زمینه های آموزشی، فناوری و اقتصاد شده است. نامه‌های الکترونیک یا ایمیل، به ما امکان می‌دهد که ظرف چند ثانیه با دیگران ارتباط برقرار کنیم."اتاق های گپ" و "گپ‌های مبتنی بر اینترنت" (IRC) به ما امکان می‌دهد که به وسیله صفحه کلید، بطور همزمان با افراد متعددی در سراسر دنیا ارتباط برقرار کنیم. اینترنت به خودی خود گستره‌ای از اطلاعات بسیار متنوع است و بهانه پیدا نکردن یک مفهوم در دائره المعارف را از دانش‌آموزان آینده سلب می‌کند اما در عین حال شبکه جهان گستر باعث شده است که انواع حیرت انگیزی از جرایم(رفتارهای کیفری) پدید آید، که برخی از این جرایم عبارتند از:

اختلاس ، کلاهبرداری یا جاسوسی صنعتی (سرقت اطلاعات محرمانه یک شرکت) تنها بخش کوچکی از اهداف احتمالی هکرها می باشد . جاسوسی سایبر همانطور که بین شرکت ها وجود دارد، میان کشورها نیز در جریان است . بنابراین امنیت ملی ما را با مخاطره مواجه می کند . تروریسم های سایبر ، توسعه رایانه ای وحشتناک دیگری است که قادر است میلیون ها انسان را در سراسر دنیا تهدید کند. هیچ بحثی در این نیست که آنچه هکرها انجام می‌دهند هر قدر که غیر قانونی است، مخاطره آمیز نیز می باشد. فریک‌های تلفن. شکل دیگری از جرایم رایانه ای را " فریک های تلفن" مرتکب می شوند. فریک ها بجای دسترسی به سیستم های رایانه ای ، از طریق خطوط تلفن در دنیای سایبر گشت می زنند . فریک ها از میان اولین هکرها در دهه ۱۹۷۰ پدید آمدند. اما خود رایانه ها تنها یک ابزارند. این افراد هستند که مرتکب جرایم سایبر می شوند و مردم نیز مانند فایل‌های رایانه ای می توانند به عنوان منابع اطلاعات حفاظت شده یا حساس مورد استفاده قرار گیرند . نکته خوبی که در این میان وجود دارد آن است که مردم نیز می توانند از جرایم سایبر جلوگیری کنند. هرقدر ما بیشتر درباره انواع مختلف جرایم سایبر و ابزارهایی که برای جلوگیری از آن ایجاد شده است بدانیم ، امنیت بیشتری خواهیم داشت. اصطلاح جرم رایانه ای تمام جرایم را شامل می شود که بوسیله یک رایانه ، درون یک فضای سایبر و علیه یک رایانه ارتکاب می یابد . بعضی از این جرایم کاملاً جدید هستند در حالیکه جرایم دیگر، جرایم قدیمی تری هستند که از رایانه به عنوان ابزار استفاده می کنند. رشد دائم و تنوع بی پایان جرایم سایبر ، تدوین قوانینی با احاطه مناسب بر جرایم سایبر جدید را دشوار ساخته است . بعضی جرایم مانند اختلاس ، کلاهبرداری و جعل سند توسط سایبر و جاسوسی سایبر نسبتاً جدید هستند . برای این جرایم جدیدتر ، نص قوانین موجود گاهی اوقات اجازه تحت پیگرد قرار دادن آنچه بطور وضوح جز رفتار کیفری محسوب می‌شود را نمی دهد .

یکی از مهم ترین و پیچیده ترین جرایم مالی ، جرم کلاهبرداری خصوصا کلاهبرداری های اینترنتی است که هرروزه به صورت متنوع و تکامل یافته در جوامع مختلف از جمله کشور ما شایع است. آنچه جرم کلاهبرداری را از سایر جرایم علیه اموال متمایز می سازد ، این است که در اکثر این جرایم ، مال بدون رضایت یا آگاهی صاحب مال و یا حتی گاه به دلیل توسل مجرم به زور و اعمال خشونت آمیز ، از قربانی جرم به مجرم منتقل می گردد ، در حالی که در جرم کلاهبرداری ، فرد کلاهبردار به گونه ای عمل می کند که مالک یا متصرف مال ، فریب خورده و از روی میل و رضایت به امید کسب ثروت و منفعت، مال خود را اختیار مجرم قرار می دهد. اغفال و فریب قربانی جرم ، نیاز به انجام مانورهای متقلبانه و عملیات اجرایی خاصی از سوی مجرم دارد. ممکن است جرم کلاهبرداری توسط افرادی که دارای مناصب اجتماعی ، اقتصادی و یا حتی دولتی هستند صورت گیرد. به همین دلیل جرم کلاهبرداری را از زمره «جرایم یقه سفیدها» محسوب کرده اند. در واقع این جرم بیش از آن که جرم فقرا و نیازمندان باشد ، جرم ثروتمندان محسوب می گردد.

امروزه جرم کلاهبرداری به روش های سنتی و قدیمی آن محدود نمی گردد و دارای وسعت و پیچیدگی های فراوانی شده است. با پیشرفت علوم وتکنولوژی و تسهیل ابزارهایی ارتباطی ، راه های ارتکاب جرایم از جمله کلاهبرداری نیز به همان میزان پیشرفت کرده و موجبات تسهیل آن فراهم گشته است. به طوری که یکی از پیچیده ترین و مرموز ترین انواع کلاهبرداری در دنیای امروزه ، کلاهبرداری رایانه ای (الکترونیک) است که در کشورهای مختلف از جمله کشور ما سالیانه پرونده های زیادی از این نوع کلاهبرداری به مراجع قضایی ارجاع می گردد. البته کلاهبرداری دارای اشکال پیچیده و مختلفی است که به تفصیل به بررسی آنها پرداخته شده است. پیچیدگی های این جرم از یک سو و نداشتن آگاهی و اطلاعات لازم از جانب مردم ، باعث ایجاد مشکلات فراوانی برای جامعه شده است بنابراین لزوم وجود کتابی تخصصی و تفصیلی در مورد جرم کلاهبرداری در جهت آموزش به جامعه ضروری به نظر می رسد.

تروریسم سایبری یکی از پیچیده‌ترین و خطرناک‌ترین انواع جرایم اینترنتی است که در آن، مجموعه‌ای از برنامه‌ریزی‌ها و تهدیدها به وسیله اینترنت منجر به ایجاد آسیب و تخریب در جهان واقعی و از بین رفتن امنیت روانی و فیزیکی افراد جامعه می‌شود. به دلیل رشد روزافزون ساختار اقتصادی و خدمات‌رسانی بسیاری از کشورها، مبتنی بر فناوری‌های اطلاعاتی و ارتباطی، دنیای ما به قدری به دادوستد اطلاعات وابسته شده است، که اختلال یا وقفه در آن، چرخ صنعت و زندگی روزمره را از حرکت بازمی‌دارد. در این رابطه ایجاد خلل در رآکتورهای هسته‌ای، سیستم‌های اطلاعاتی فرودگاه‌ها و ترمینال‌ها و تأسیسات عمومی مثل برق، آب و فاضلاب، می‌تواند بسیار فاجعه‌آمیز باشد.

در حقوق کیفری آمریکا تروریسم سایبری، حاصل تلاقی تروریسم و فضای مجازی است. در این روش، تروریست‌ها با هزینه کم و با استفاده از یک رایانه شخصی متصل به اینترنت می‌توانند به اقدامات تروریستی دست بزنند. همچنین فضای مجازی این امکان را برای تروریست‌ها فراهم می‌کند که همانند دیگر کاربران اینترنت، به عنوان کاربر مهمان و با استفاده از اسامی مستعار وارد سایت مورد نظرشان شوند و با پنهان سازی هویت، دست به اقدامات تروریستی بزنند، بدین گونه امکان ردیابی آن‌ها برای نیروهای پلیس و امنیتی دشوارتر خواهد بود. مزیت دیگری که فضای مجازی، برای تروریست‌ها ایجاد کرده است، امکان هدایت از راه دور می‌باشد که آموزش فیزیکی، فشار روانی و خطر مرگ کمتری را به همراه دارد. اصولا ارائه یک تعریف جامع و قابل‌قبول در روابط بین‌الملل برای واژه «تروریسم» دشوار است.

زیرا اعمال تروریستی در بسیاری از مواقع حالت دو وجهی دارد. یعنی ممکن است عمل یک فرد از نظر یک شخص تروریستی تلقی شود و از نظر دیگری شخص مزبور یک مبارز راه آزادی محسوب شود. با این حال برای تعریف تروریسم می‌توان به تعریفی که سازمان ملل متحد در سال ۱۹۹۲ منتشر کرده است، اشاره کرد که بیان می‌دارد: «روش اعمال نگرش از طریق خشونت که به وسیله بازیگران دولتی، گروه‌ها یا افراد (نیمه) مخفی که به دلایل سیاسی، جنایتکارانه یا شخصی اعمال می‌شود». در قوانین آمریکا «اقدام تروریستی» به معنی «تشکیل، معاونت یا مشارکت در یک عمل خشونت‌آمیز غیرموجه یا بی‌پروایانه با بی‌تفاوتی کامل نسبت به خطر کشتن یا ایراد صدمه شدید جسمانی به انسانی که در مخاصمات مسلحانه شرکت ندارند» به کار رفته است. این امکان وجود دارد که حملات تروریستی علیه یک دولت از سوی افرادی وابسته به دولت ها و کشورهای دیگرواقع گردد و یا ممکن است فرد بزه دیده از نقض قوانین بین المللی از سوی یک دولت در نهادهای بین المللی طرح شکایت کند. این مراجع در صورتی به شکایت رسیدگی می کنند که حداقل فرد شاکی تبعه ی دولتی باشد که آن دولت عضو اساسنامه یا کنوانسیون مربوط نهادهای بین المللی باشد. با عنایت به این مسئله مشاهده می شود که مبارزه همه جانبه علیه سایبر تروریسم در سطوح بین المللی با دشواری های قانونی و همکاری کامل کشورها و دولت ها همراه است .ازآنجاکه به موجب اصل حاکمیت ها، دادگاه داخلی یک کشور اصولاً نمی تواند علیه جرایم ارتکابی کشوری دیگرحکم صادر نماید و به دلیل فرامرزی و بین المللی بودن فضای سایبر و همچنین جرایم سایبری، بهترین روش برای مبارزه با سایبر تروریسم و جرایم سایبری رجوع به محاکم بین المللی و ایجاد همکاری های پلیسی و حقوقی در سطح بین المللی است.

یکی از تهدیدات امنیتی که همواره ملتها و دولتها را آزار داده، اقدامات تروریستی است که عمدتاً با پیامدهای بسیار زیانباری همراه هستند. بدیهی است «زیرساختهای حیاتی» از بهترین اهداف محسوب می‌شوند که با

توجه به الکترونیکی شدن آنها، نه تنها ارتکاب اقدامات تروریستی آسان‌تر شده، بلکه لطمات وارد شده بسیار سهمگین هستند. البته ماهیت «چند رسانه‌ای» فضای سایبر، به تروریستها امکان بهره‌برداریهای سوء دیگری را هم داده است. این نوشته بر آن است که با تبیین اجمالی مفهوم عام تروریسم سایبر به عنوان یک پدیدهٔ مجرمانه، راهکارهای حقوقی مقابله با آن و وضعیت کشورمان را بررسی نماید.

جمهوری اسلامی ایران که از بزرگترین قربانیان تروریسم می باشد مورد هجمه و حمله حملات سایبری نیز قرار دارد. استفاده گسترده از بدافزارهای خرابکاری و جاسوسی از نمونه های این حملات هستند. استفاده از انواع کدهای برنامه نویسی به قدری گسترده است که یقیناً از حد و اندازه حملات انفرادی یا حتی گروهی خارج بوده و پشتیبانی اطلاعاتی و تکنولوژیکی قدرت‌های بزرگ و صاحب تکنولوژی را می‌طلبد. به طوریکه گاهی خود دولت‌ها نیز از آماج حملات، نقش عامل را نیز بر عهده می‌گیرند و در برخی از موارد حاضر نیستند این ابزار یا علم را به هر دلیلی در دست گروه‌های مزدور قرار دهند. زیرا از یکسو ذات چنین تروریسمی نیز به دنبال پیوند با هزینه‌های سیاسی و حقوقی آن نیازی به برون‌سپاری دولت‌ها برای پنهان‌سازی نقش مستقیم دارد؛ به عبارت دقیق‌تر عدم امکان تشخیص دقیق مهاجمان و هویت واقعی آنها و مشکل بودن ارزیابی زمان و محل حملات و همچنین ضربه به زیرساخت‌های کشور هدف، از قبیل سیستم‌های مالی و بانکداری، کارخانجات و حتی شبکه های خدمت‌رسانی شهری از دلایل تمایل دولت‌ها در مدیریت و اجرای مستقیم این نوع هجمه‌ها است. از سوی دیگر نیز می‌توان به ارزش علمی و تکنولوژیکی این پدیده را درنظر گرفت که با برون سپاری آن به گروه‌ها و سازمان‌ها مزدور حتی می‌تواند در شرایطی مخل امنیت خود کشورهای صادر کننده و منافع آنها باشد.

عبداله میرفردی