صلاحیت فرامرزی بر جرایم سایبری با تأکید بر کیفرخواست امریکا

در پرونده گروه آی‌تی‌سک

مؤلفان: رضا خواجه نورالدینی

سیده پریسا میرابی

نشر راشدین

سرشناسه : خواجه نورالدینی، رضا، ۱۳۵۲ -
عنوان و نام پدیدآور : صلاحیت فرامرزی بر جرایم سایبری (با تاکید بر کیفرخواست امریکا در پرونده گروه آی‌تی‌سک)/ مولفین رضا خواجه‌نورالدینی، سیده‌پریسا میرابی.
مشخصات نشر : تهران : راشدین، ۱۳۹۷.
مشخصات ظاهری : ۱۳۷ص.
شابک : ۹۷۸-۶۰۰-۳۶۱-۵۶۷-۰
وضعیت فهرست نویسی : فیپا
یادداشت : واژه‌نامه.
یادداشت : کتابنامه:ص.۱۰۹-۱۱۱.
موضوع : شرکت آی تی سک
موضوع : جرایم کامپیوتری — ایالات متحده
موضوع : Computer crimes -- United States
موضوع : صلاحیت حقوقی — ایالات متحده
موضوع : Competent authority -- United States
موضوع : هکرها — ایران
موضوع : Hackers -- Iran
شناسه افزوده : میرابی، سیده پریسا، ۱۳۶۴ -
رده بندی کنگره : ۱۳۹۷ ۹خ۴چ/ HV۸۰۷۹
رده بندی دیویی : ۳۶۳/۲۵۹۶۸۰۹۷۳
شماره کتابشناسی ملی : ۵۳۷۳۹۶۲

انتشارات راشدین	
عنوان کتاب:	صلاحیت فرامرزی بر جرایم سایبری با تأکید بر کیفرخواست امریکا در پرونده گروه آی‌تی‌سک
مؤلفان:	رضا خواجه نورالدینی، سیده پریسا میرابی
صفحه‌آرا:	مونا اسماعیلی
طراح جلد:	علی زند
نوبت چاپ:	اول -۱۳۹۸
شمارگان:	۱۰۰۰
شابک:	۹۷۸-۶۰۰-۳۶۱-۵۶۷-۰
قیمت:	۲۰۰۰۰۰ ریال
نشانی:	میدان انقلاب ـ کارگر جنوبی- بن‌بست گشتاسب - پلاک ۴ واحد۶
تلفن/ نمابر:	۶۶۱۲۳۴۴۹ ـ ۶۶۴۰۸۲۲۴
پایگاه اینترنتی:	www.siteketab. com
پست الکترونیک:	rashed۱۸۲۹@yahoo. Com heydari_alireza۴۱@yahoo.com

دیباچه

درحالی که رشد سریع تکنولوژی برای بشریت سودمند است، تروریسم سایبری، به یکی از تهدیدات خطرناک جهانی تبدیل شده است. فقدان مرز و محدوده به شکل سنتی، اقدامات مجرمانه در این فضا، صلاحیت محاکم رسیدگی کننده را به چالش کشیده است. وقوع حملات سایبری روزافزون علیه کشورهای مستقل و زیرساخت های اطلاعات اساسی آنها، واکنش جهانی را ضروری می کنند. جامعه بین المللی همواره تلاش کرده است ازطریق انعقاد معاهدات دو یا چند جانبه، زمینه همکاری در رسیدگی به جرایم سایبری و تروریستی را فراهم کند؛ اما توافقنامه های منطقه ای و دوجانبه و قوانین داخلی برای جلوگیری از حملات سایبری کافی نیست. گرچه معاهدات بسیاری وجود دارد، اما هیچ یک از آنها مجوز قانونی لازم برای اعمال مجازاتها (مجازاتهای اصلی ، تکمیلی ، و تبعی)، تعقیب و رسیدگی فرامرزی را فراهم نمی‌کند. اکثر آن معاهدات به طور محدود و در سطح منطقه ای اعمال می شوند،که البته به منظور دستیابی به درک مشترک در کاهش تهدیدات تروریسم سایبری، باید راه حل های موجود ارائه شده در معاهدات بین المللی در نظر گرفته شوند تا پاسخ های موجود در برابر تهدیدهای سایبری فراملی بررسی شود. در حال حاضر، بسیاری از سازمان های بین المللی تلاش هایی را برای مبارزه با این تهدید انجام داده اند. سازمان ملل متحد و اینترپول با پیش بینی خطرات تروریسم در سطح جهان سعی می کنند از جرایم سایبری در سطح بین المللی جلوگیری کنند. مهمترین معاهده در این خصوص کنوانسیون جرایم سایبری است. گرچه کنوانسیون جرایم سایبری ورشو به عنوان یک تلاش منطقه ای در مبارزه با تروریسم سایبری در این مورد نقش مهمی ایفا می کند، و حتی تعدادی از کشورها که در خارج از

منطقه قرار دارند، آن را تصویب نموده و عضو این کنوانسیون شده اند؛ با این حال، معروف ترین معاهده در زمینه جرایم سایبری، تروریسم سایبری را شامل نمی شود. تروریسم سایبری یک جنایت بین المللی است و قوانین داخلی از آن جمله قانون مبارزه با تامین مالی تروریسم (۱۳۹۴/۱۱/۱۳) و مجازات جرایم ضد امنیت داخلی و خارجی کشورها (ماده ۷۲۹ و ۴۹۸ قانون مجازات اسلامی ۱۳۹۲/۲/۱) به تنهایی قادر به مقابله با چنین حملاتی نیست؛ بنابراین آنها نیاز به پاسخ فراملیتی و جهانی دارند. جرایم تروریست سایبری ماهیتاً منجر به پیچیدگی های قانونی می شود و تعقیب و تحقیق و پیگرد قانونی را دشوار می سازد. عدم هماهنگی در قانون گذاری در میان کشورها به مشکلاتی در زمینه تعقیب و پیگرد قانونی منجر می گردد. از آنجایی که اعمال صلاحیت (شخصی، سرزمینی، جهانی، واقعی و ...) همه موارد تروریسم سایبری را پوشش نمی دهد، بهترین کار در بدو امر الحاق یک پروتکل ویژه مربوط به تروریسم سایبری است. همچنین، از آنجایی که قوانین ملی به تنهایی نمی توانند نقش بازدارنده یا مبارزه با این نوع جرایم را داشته باشند؛ به یک سازمان بین المللی برای جلوگیری و دفاع از افراد، شخصیت ها، گروه‌ها و اهداف مورد حمایت حقوق بین المللی در برابرحملات تروریستی سایبری نیاز است که باید از طریق همکاری های چند ملیتی وسازمان های بین المللی برای مقابله با جنایات تروریستی از آن بهره برد.

علیرضا دیهیم

شهریورماه ۱۳۹۷

فهرست مطالب

مقدمه ۹
کلیات ۱۳
فصل اول: جرایم سایبری و صلاحیت فرامرزی آن ۱۹
● بخش اول- جرایم سایبریی ۲۱
جرم آینده، تروریسم سایبری ۲۲
مباشران داخلی جرایم سایبری ۲۳
ویژگی‌های جرایم سایبری ۲۳
حملات سایبری، شیوه‌های تشخیص و جلوگیری از آن ۲۵
● بخش دوم - مفهوم صلاحیت بین فرامرزی و مبانی اعمال صلاحیت در جرایم سایبری ۲۷
صلاحیت جهانی ۲۷
اصل صلاحیت جهانی قوانین کیفری ۲۸
محدودیت‌های اعمال صلاحیت جهانی توسط محاکم ملی ۲۹
چالش‌های ماهوی، سیاسی ۲۹
مفهوم صلاحیت دادگاه‌ها و سیر تکامل آن ۳۱
اصل صلاحیت سرزمینی ۳۳
اسناد بین‌المللی ناظر بر صلاحیت سرزمینی ۳۳
قوانین و مقررات ملی ناظر بر صلاحیت سرزمینی ۳۳
اعمال صلاحیت بر مبنای اصل تابعیت ۳۵
اسناد بین المللی مرتبط با اعمال صلاحیت بر مبنای تابعیت ۳۵
رویکرد قوانین و مقررات داخلی به اعمال صلاحیت بر مبنای تابعیت ۳۵
سایر مبانی اعمال صلاحیت ۳۵
اقدامات سازمان ملل متحد در تبیین جرایم سایبری فراملی ۳۷
قانون مصونیت دولت‌های خارجی ۳۹
اصلاحیه‌ی ۱۹۹۶ قانون مصونیت دولت‌های خارجی ۴۰
●بخش سوم اصول حاکم بر اعمال صلاحیت دادگاه ها در رسیدگی به جرایم سایبری ۴۱
چگونگی صلاحیت محاکم در جرایم سایبری ۴۱
صلاحیت دادگاه‌ها در جرایم سایبری ۴۳
تعارض صلاحیت‌ها در رسیدگی به جرایم سایبری ۴۳

فصل دوم: بررسی کیفرخواست گروه آی‌تی‌سک و مبانی جرایم آن ۴۵
● بخش اول - کیفرخواست ایالات متحده آمریکا در پرونده گروه آی تی سِک ۴۷
دلایل صدور کیفرخواست ۴۷
بیان تاریخچه‌ی موضوع پرونده‌ی مطروحه گروه آی‌تی‌سک ۴۸
● بخش دوم: دیدگاه‌ها و اظهارنظرهای حقوقی کیفرخواست در ایالات متحده ۵۸
اداره امور اجتماعی وزارت دادگستری ۵۸
بازگرداندن رایانه‌های هک شده توسط طرح DDos ۶۲
نفوذ در سد بومن ۶۲
دیدگاه اف بی آی ۶۳
اظهار نظر پریت بهارار ۶۵
اظهار نظر جیم کامی ۶۶
اظهارنظر مایکل سولمیر ۶۷
قابلیت‌های فعلی و خط سیر آینده ۶۸
پیشنهادات برای منطقه و منافع آمریکا ۶۹
توصیه هایی برای دولت آمریکا و متحدانش ۶۹
● بخش سوم نقد حقوقی پرونده در دو دیدگاه عرف و رویه‌های قضایی و حقوق نوشته ۷۴
مسئله اول – تعیین محل ارتکاب جرم سایبری ۸۵
مسئله دوم – شناسائی تابعیت شخص مرتکب ۸۶
مسئله سوم – حل تعارض صلاحیت‌ها ۸۷
فرجام سخن ۸۹
پیوستها (متن کیفرخواست) ۹۵
واژه نامه ۱۰۹
منابع ۱۳۱
Abstract ۱۳۶

مقدمه

در عصر انفجارتکنولوژی و پیامدهای آن، بناچار قوانین حقوقی کشورها دستخوش تغییرات همسو با آن می‌شوند ، در این راستا و با ظهور فضای مجازی (سایبری) تغییرات حقوقی خاصه قوانین کیفری بین‌المللی می‌بایست تغییر داده شود زیرا جرایم آنلاین خارج از مرزها اتفاق می‌افتد، و ممکن است حملات سایبری خارج از مرزهای یک ایالت و یا کشور صورت بگیرد، در نتیجه صحنه‌های جرم از طریق دو یا چند کشور، گاهی اوقات در بیش از یک قاره صورت می‌پذیرد. راه حل‌های مربوط به مشکلات مطرح شده باید از طریق قوانین بین‌المللی یا از طریق تصویب ابزار قانونی مناسب بین‌المللی مورد توجه قرار گیرد. اولین و مهم‌ترین بخش از قوانین که دستخوش این دگرگونی شده است قلمرو سرزمینی یا اصل سرزمینی بودن جرایم و مجازات‌ها است. این اصل از قدیمی‌ترین اصول در تعیین صلاحیت کیفری و سازگار با اصل حاکمیت دولت‌ها و به عنوان یکی از مقتضیات حقوق بشر و آزادی انسانها است که در پرونده لوتوس مورد تایید دیوان بین‌المللی دادگستری و حمایت اشخاصی چون ولتر، منتسکیو، روسو و بکاریا قرار گرفته است.

با توجه به این موضوع که تعیین هویت یک تبهکاری سایبری و محل حمله آنها در فضای سایبر بسیار دشوار است، و یک مهاجم سایبری می‌تواند منوهای گریز از قبیل جعل یا استفاده از آدرس‌های آی پی ناشناس یا پنهان را اجرا کند و احتمال شناسایی مرتکبین حملات سایبری با هر سطح معقول اطمینان به شدت کاهش یافته است، اقدام به اعمال صلاحیت فراسرزمینی و محاکمه غیابی افراد در دادگاه‌های داخلی امری نامشروع و مخالف قواعد آمره بین‌المللی است. در حمله سایبری استونی، کارشناسان مطمئن نبودند که آیا می‌توانند هویت هکرها را شناسایی کنند، و یا نامهای افراد را کشف کنند. بعضی از مقامات استونی ادعا کردند که دولت روسیه مسئول حمله بوده است، اما روسیه به شدت این ادعاها

را رد کرد.

سرانجام فردی به نام دیمیتری گالوشکویچ، مسئولیت حمله و مسدود کردن وب سایت نخست‌وزیر استونی و بعد از آن، اعضای جنبش جوانان تحت حمایت کرملین، مسئولیت این حملات را بر عهده گرفتند.

برای ایجاد اصل یکنواختی در صلاحیت کیفری در جرایم اینترنتی بین‌المللی، نیازمند فاکتورهای براساس اصول و قواعد بین‌المللی، دستوالعمل واضح و روشن سازمان ملل، شکل گیری یک رویه کلی بر اساس دستوالعمل است که این شیوه‌ها باید دارای تاییدیه قانونی جهانی باشند.

بسیاری از کشورها اقدام به تصویب قوانین جدیدی در این زمینه کرده‌اند، که از جمله آنها می‌توان به کشورهایی چون سنگاپور و مالزی اشاره کرد، که محل استقرار سیستم‌های رایانه‌ای را به عنوان محل ارتکاب جرم مجازی و یا ایالتهای آرکانزاس و کارولینای شمالی، محل حضور بارگذار و پیاده ساز شبکه‌ای را به عنوان محل ارتکاب جرم قلمداد کرده اند. البته می‌توان محل سرورها و فضای شبکه‌ای در چارچوب خدمات میزبانی، محل حضور مرتکب، ارتکاب بخشی از جرم یا نتیجه یا آثارآن در قلمرو حاکمیتی را ملاک اعمال صلاحیت قرار گیرد.

در سال ۲۰۱۶، دادستان عالی فدرال آمریکا ادعایی علیه هفت نفر از اتباع جمهوری اسلامی ایران مبنی بر حملات سایبری به اهدافی در خاک آمریکا مطرح نمود؛ که به ارائه کیفرخواستی به دادگاه نیویورک منجر شد. در این پرونده، آمریکا کارمندان شرکت‌هایی را معرفی می‌کند که همکاری تنگاتنگ با دولت جمهوری اسلامی ایران دارند و هرچند این افراد عاملان حملات سایبری به آمریکا هستند ولی مباشر اصلی آن را دولت ایران قلمداد می‌کند. بنابراین، اعمال دولت آمریکا مبنی بر محاکمه غیابی افراد، اصلاحیه قانون مصونیت حاکمیت خارجی ((FSIA ایالات متحده موسوم به اصلاحیه فلاتو که منجر به نقض قاعده «مصونیت دولت‌ها از تعقیب قضایی» و قاعده « عطف به ماسبق نشدن قوانین کیفری و حقوقی»، صلاحیت جهانی را به «یک فاجعه، کنترل نشده و در کاربرد آن مخرب فرآیندهای قانونی بین‌المللی »،که منجر به نقض حاکمیت و مصونیت دولتها و در نتیجه تیرگی روابط آنها در سطح بین الملل و نادیده گرفتن اصول اساسی منشور سازمان ملل خواشد شد.

آمریکا نه تنها شروع کننده حملات سایبری به ایران و سایر نقاط جهان بوده، بلکه همواره

تلاش کرده که با بزرگنمایی قدرت سایبری ایران، آن را خطری جدی علیه بشریت توصیف نماید و با این توجیه دست پیش نسبت به اقدام دفاع مشروع نماید

در این کتاب به پرونده « هکرهای گروه آی تی سک» که در سال ۲۰۱۶ در آمریکا مطرح شد و بیانگر نقض آشکار قواعد عرف بین‌المللی، قوانین و حاکمیت دولت‌ها است را مورد مطالعه قرار داده است.

هر چند که جامعه بین الملل نسبت به آن و حتی حملات پی در پی جبهه امریکایی، صهیونیستی، وهابی (که بارزترین آن حمله استاکس نت و ....)سکوت کرده است ولی جا دارد که جامعه حقوقی و در راس آن مدعی العموم به دفاع از حقوق حق کشور و به استناد مدارک موجود و حداقل با شیوه مهندسی معکوس از کیفرخواست صادر شده، بپردازد.

با امید به اینکه بابی گشوده شود که در آن از حقوق کشور جمهوری اسلامی ایران در حملات و تهدیدات سایبری و تروریستی دفاع لازم به عمل آید.