سایبر تروریسم و جرایم سایبری در نظام حقوق بین‌الملل

بهزاد پورنقدی[1]

تاریخ دریافت: ۱۳۹۳/۰۹/۰۶

تاریخ پذیرش: ۱۳۹۳/۱۰/۱۸

چکیده

زمینه: *رشد سریع و در عین حال نامتوازن ساختار فضای سایبری، شبکه اینترنت و فضای مجازی را به یکی از فضاهای آسیب‌پذیر و خطرناک تبدیل کرده است که توجه جامعه جهانی و نهادهای امنیتی، انتظامی و قضائی را به‌طور نظام‌مند و هدفمند به‌منظور پیشگیری و مصون‌سازی این بستر از تهدیدهای موجود و پدیده نوظهور سایبر تروریسم را در فضای بین‌المللی می‌طلبد.*

روش کار: *با بررسی منابع، مقالات، کتاب‌ها، نتایج و مطالعات در حوزه جرایم سایبری، تروریسم بین‌المللی و سایبر تروریسم به روش غیر آزمایشی، مقایسه‌ای و کتابخانه‌ای، تهدیدها و مخاطرات سایبر تروریسم و ضرورت پیشگیری از جرایم سایبری در عرصه بین‌المللی مورد تحقیق و پژوهش قرار گرفته است.*

یافته‌ها: *سایبر تروریسم و جرایم سایبری بسیار خطرناک‌تر از تروریسم کلاسیک و جرایم سنتی هستند و تهدیدهای آن برای امنیت ملی کشورها به خطری بالقوه تبدیل شده که پیشگیری، کشف و مقابله با این پدیده جرم‌شناختی برای نهادهای پلیسی و امنیتی بسیار پیچیده و مشکل‌تر از جرایم سنتی می‌باشد.*

نتیجه‌گیری: *برنامه‌ریزی‌های جهانی و تصویب قوانین بین‌المللی، افزایش همکاری‌های فنی و آموزشی بین‌المللی، توجه ویژه به تصویب قوانین کارآمد و بازدارنده به عنوان راهکار پیشگیری از جرایم سایبری توسط نهادهای داخلی و همکاری فی مابین سازمان‌های امنیتی و پلیسی از جمله راهکارهای مبارزه با سایبر تروریسم می‌باشد.*

واژگان کلیدی: *سایبر تروریسم، حقوق و امنیت بین‌الملل، جرایم سایبری.*

[1] پژوهشگر دفتر تحقیقات کاربردی فرماندهی انتظامی استان سمنان، پست الکترونیک: behzad_pournaghdi@yahoo.com.

مقدمه

از اوایل دهه ۹۰ میلادی، پژوهش‌ها و بررسی‌های بسیاری در زمینه روان‌شناسی اینترنت و تاثیر آن بر سلامت و رفتار انسان و امنیت و ثبات داخلی کشورها انجام شده است. امروزه موضوع اینترنت[1]، مسئله مهمی برای بیشتر جوامع به‌ویژه کشورهای در حال توسعه و از جمله کشورهای اسلامی است. آگاهی از پیامدهای امنیتی فضای مجازی و درنظر گرفتن راهبردهای مناسب برای استفاده درست و پیشگیری یا کاهش مخاطرات و جرایم سایبری، اهمیت ویژه‌ای دارد. فراگیر شدن رسانه‌ها در آغاز قرن ۲۱ و موضوع جدی نقش اینترنت و شبکه‌های اجتماعی مجازی در شکل‌دهی به فرهنگ، هویت، باورها و ارزش‌های نظام اجتماعی، امنیت و ثبات داخلی کشورها از جمله ایران جایگاه مهمی دارد. بسیاری از کارشناسان و نظریه پردازان ارتباطات، اینترنت را گام مهمی در پیشرفت کشورهای درحال توسعه قلمداد می‌کنند (شجاعی، ۱۳۹۱). از طرفی نیز بستر اینترنت و فضای سایبری دارای کارمدهای منفی و فضایی آماده جهت وقوع انواع جرایم می‌باشد.

امروزه قدرت کشورها تنها به داشتن سلاح های نظامی و جنگی و بمب اتمی نیست، بلکه داشتن اطلاعات، پیشرفت در حوزه علم و دانش و نفوذ در فضای سایبری و فناوری اطلاعات میزان تشخیص قدرت آنهاست. تلاش دشمنان از طریق ابزارهای تکنولوژیک و فناوری اطلاعات و رسانه‌های ارتباطی برای مقاصدی همچون تهدید امنیت ملی از طریق ناسالم‌سازی فضای سایبری برای جوانان ایرانی و تولید و انتشار ویروس‌ها و بد افزارهای[2] رایانه‌ای همچون ویروس آزمایشگاهی استاکس‌نت[3] برای آسیب‌رسانی به تاسیسات هسته‌ای جمهوری اسلامی ایران، تهدید بیان خانواده، قبح‌زدایی و هنجارشکنی، ترویج فساد و تاسیس سایت‌های ضد اخلاقی و ضد ارزشی، ایجاد حس بی‌اعتمادی به مسئولین نظام، انتشار مطالب و اخبار کذب و گسترش شایعات سیاسی، اقتصادی، اجتماعی، نظامی، انتظامی و امنیتی، همچنین اعمال جاسوسی از طریق شبکه‌های اجتماعی مجازی صورت می‌گیرد (ساروخانی، ۱۳۹۱).

در حال حاضر ده‌ها هزار سایت جنسی در اینترنت وجود دارد که شمار آن‌ها هر روز نیز بیشتر می‌شود. اما تهدیدهای غیر اخلاقی اینترنت صرفاً نسبت به دسترسی سایت‌های جنسی محدود

---

[1] Internet
[3] Bad Ware
[4] StuxNet

نمی‌شود، بلکه امکانات متنوع اینترنت در دنیای فناوری اطلاعات، امکان برقراری هر نوع ارتباط فی مابین کاربران را فراهم می‌آورد و در بسیاری از موارد این ارتباطات می‌تواند ارتباطات شامل روابط نامشروع باشد. تلاش جامعه جهانی برای توسعه سازوکارهای بین‌المللی در راستای مبارزه با جرایم سازمان‌یافته ریشه در این حقیقت دارد که این نوع جرایم جدی‌تر و خطرناک‌تر شده‌اند. جنایات فراملی و جرایم سایبری، تهدیدی فراروی صلح و امنیت بین‌المللی است (گزارش مرکز پژوهش‌های مجلس شورای اسلامی، ۱۳۸۷).

بیان مسئله

انقلاب فناوری اطلاعات و ارتباطات به‌ویژه پیدایش و ظهور رسانه‌های الکترونیکی جدید، تمام قسمت‌های زندگی انسان‌ها را تحت تأثیر قرار داده است. فناوری‌های ارتباطی و اطلاعاتی در حوزه عملیات روانی نیز کاربرد فراوانی یافته‌اند. در واقع عملیات روانی و یا به تعبیر دیگر تأثیر و نفوذ در افکار و رفتار سایر دولت‌ها و ملت‌ها که کارگزاران، آن را در جهت اهداف و مقاصد خود پی‌ریزی می‌کنند، امروزه از طریق فناوری‌های ارتباطی و اطلاعاتی به خصوص رسانه‌های نوین روبه گسترش نهاده است (سوری، ۱۳۸۷). جمعیت کاربران جهان در سال ۲۰۱۲ میلادی بیش از دو میلیارد نفر بوده و کشور ایران در حال حاضر بیش از ۳۳ میلیون کاربر اینترنت دارد (پایگاه اینترنتی داده‌ها و آمار اینترنت، آمریکا، ۲۰۱۲). اهمیت و ضرورت فضای مجازی تا حدی است که مقام معظم رهبری حضرت امام خامنه‌ای (مدظله العالی) طی حکمی «شورای عالی فضای مجازی» را ایجاد کرده و اعضای آن را تعیین نمودند.

سایبر تروریسم یکی از روش‌های نوین حملات زیان‌بار و تهدید علیه امنیت ملی و منافع یک کشور در حوزه بین‌الملل است که به سرعت در حال رشد و گسترش می‌باشد. به دلایل مختلفی سایبر تروریسم برای تروریست‌های عصر حاضر جذاب‌تر از روش‌های کلاسیک است. مهمترین دلیلی که باعث جذابیت این روش می‌گردد، هزینه‌های اندک و بسیار پایین این روش در برابر روش‌های تروریستی سنتی است. در واقع در سایبر تروریسم تنها ابزاری که مورد نیاز است، یک رایانه شخصی متصل به اینترنت می‌باشد و نیازی به خرید اسلحه یا مواد منفجره نیست. همچنین تروریست‌ها مانند بسیاری از کاربران اینترنت از اسامی مستعار استفاده می‌کنند و به‌عنوان کاربر مهمان وارد سایت مورد نظرشان شده و به همین دلیل برای نیروهای پلیسی و امنیتی بسیار دشوار است که آنها را ردیابی کنند. سایبر تروریسم می‌تواند شبکه‌ها و رایانه‌های

دولتی یا سازمانی، افراد و کاربران عمومی، خدمات و شبکه حمل و نقل عمومی، خطوط هوایی، حرکت قطارهای شهری، نیروگاه‌های اتمی و برقی و غیره را مورد حمله قرار دهد که در نتیجه تعداد و تنوع این نوع حملات بسیار زیاد است. ویژگی دیگر سایبر تروریسم که باعث جذابیت آن برای تروریست‌ها شده، هدایت از راه دور این نوع جرایم است. همچنین سایبر تروریسم به سرمایه‌گذاری و فشار روانی کمتری نیاز دارد و با آموزش فیزیکی محدود و خطر دستگیری پایین‌تری توسط پلیس و نیروهای امنیتی مواجه است (برومند باستانی، ۱۳۸۷).

امروزه رسیدن به سه هدف امنیت، رفاه و آسایش از مهمترین وظایف دولت‌ها و نگرانی مسئولان جوامع می‌باشد. مواجهه با آینده یکی از مهمترین دغدغه‌های انسان امروز است، آینده‌ای که بر پایه رسانه‌های ارتباطی نوین استوار بوده و در فضایی مبتنی بر آن به بلوغ می‌رسد. جوامع بشری تاکنون دو دوره انقلاب کشاورزی و صنعتی را پشت سر گذاشته و هم‌اکنون در اواخر عصر فرا صنعتی یا عصر اطلاعات که بر پایه الکترونیک و رایانه‌ها استوار است، قرار دارند. این عصر، دوره ای است که در آن قدرت، ثروت و امنیت بر پایه دانش به وجود آمده و سرعت وجه مشخصه آن و اطلاعات به‌عنوان ارزشمندترین کالا محسوب می‌شود. «عصر اطلاعات» جهانی را ترسیم می‌نماید که بر پایه شبکه‌های رایانه‌ای و تعاملات کاربران در فضای سایبر شکل گرفته است. این جهان نوپا که به‌سرعت در حال بسط و گسترش بوده و تمامی شئون زندگی انسان‌ها را تحت تأثیر قرار داده است، بر پایه فناوری اطلاعات و رسانه‌های ارتباطی نوین استوار بوده و در فضایی غیر فیزیکی به رشد و توسعه خود ادامه داده و در حال تسخیر جهان واقعی می‌باشد که فضای سایبر[۱] یا فضای مجازی[۲] نام دارد.

فناوری اطلاعات[۳] و ابزار گسترده اینترنت توانایی و امکان انتقال متن، پست الکترونیک[۴]، تبادل اطلاعات و دسترسی به پایگاه‌های داده، دسترسی به تصاویر، پخش فیلم و موسیقی، چت و گفتگوی مجازی، شرکت در بحث‌های گروهی و امکانات دیگری را دارد که با عدم رعایت مسائل اخلاقی در کاربری این امکانات و دسترسی‌های غیر مجاز به اطلاعات و داده‌ها، پدیده‌های ضد امنیتی و غیر اخلاقی متعددی را به‌وجود می‌آورد که برخی از آن‌ها عبارت‌اند از: هک و نفوذ به رایانه‌های شخصی و اداری، سرقت و دزدی اطلاعات و داده‌ها، دسترسی غیر قانونی به منابع

---

[1] Cyberspace
[2] Virtual Space
[3] Information Technology (IT)
[4] E-Mail

اطلاعاتی و مالی، انتشار افکار و رفتارهای غیر اخلاقی و مخالف با هنجارهای جوامع بشری، سوء استفاده‌های جنسی، سوء استفاده‌های مالی و اطلاعاتی، دزدی هویت و ترویج فساد.

پدیده تروریسم با بسیاری از فعالیت‌های مجرمانه فراملی همچون جرایم سازمان‌یافته، قاچاق زنان و کودکان برای سوء استفاده جنسی، تجارت غیر قانونی اسلحه، پولشویی (خمامی زاده، ۱۳۸۲) و قاچاق مواد هسته‌ای و دیگر جرایم پیوند خورده است. تهدید به تروریسم و ارتکاب آن سبب تضعیف دولت‌ها و اقدامات صلح‌آمیز سازمان ملل متحد، ممانعت از رشد اقتصادی و اجتماعی و فرهنگی، ایجاد جنگ‌های داخلی و تقویت مالی تروریست‌ها (طیبی فرد، ۱۳۸۳) و اخلال در نظم و امنیت جوامع و کشورها می‌شود. در سال‌های اخیر قواعد ماهوی حقوق بین-الملل در مورد جرایم سازمان‌یافته فراملی توسعه یافته است (سلیمی، ۱۳۸۲: ۱۶۹). پدیده جهانی تروریسم سابقه‌ای طولانی در تاریخ بشر دارد و همواره در تمامی جوامع تروریسم وجود داشته و تنها تفاوت بین شکل‌ها و مظاهر عینی آن ناشی از روش‌ها، ابزارها و سلاح‌های مورد استفاده بوده است. به موازات تحولات تکنولوژیک در جهان و تغییر در نوع و ماهیت فعالیت‌های سیاسی، اقتصادی و نظامی هرچه سلاح‌های در دسترس تروریست‌ها توسعه می‌یابد، آثار مخرب آنها نسبت به جامعه بین‌المللی بیشتر می‌شود. با ظهور و گسترش فضای سایبری نوع جدید از تروریسم با عنوان سایبر تروریسم شکل گرفته است که قابلیت ارتکاب ترور در حوزه‌های بین-المللی و فراملی را به راحتی امکان‌پذیر می‌سازد. به همین دلیل امروزه بحث تروریسم و پیشگیری از جرایم سایبری بیش از هر زمان دیگری به موضوع امنیت بین‌المللی تبدیل شده است.

مفهوم‌شناسی سایبر تروریسم

تروریسم یعنی به‌کارگیری خشونت علیه اشخاص، دولت‌ها یا گروه‌ها برای پیشبرد زورمندانه اهداف سیاسی یا عمومی است (Antonio Cassese, 2001). سایبر تروریسم نیز در واقع همان تعریف را دارد با این تفاوت که این‌بار هدف متمرکز روی منابع موجود در فضای مجازی است. امروزه سایبر تروریسم خطرناک تر از تروریسم سنتی است این امر به دلیل رشد روزافزون ساختار اقتصادی و خدمات‌رسانی بسیاری از کشورها مبتنی بر فناوری‌های اطلاعاتی و ارتباطی می‌باشد. سایبر تروریسم را می‌توان این‌گونه تعریف کرد: «اقدامات برنامه‌ریزی شده و هدفمند با اغراض سیاسی و غیر شخصی که علیه رایانه‌ها و امکانات و برنامه‌های ذخیره شده درون آن‌ها از

طریق شبکه جهانی صورت می‌گیرد و هدف از چنین اقدامی نابودی یا وارد آوردن آسیب‌های جدی به آنهاست» (صدوقی، ۱۳۹۰).

واژه سایبر تروریسم نخستین بار از سوی «کالین باری»[1] در سال ۱۹۸۰ مطرح شد و تعریف جامع‌تری از سوی «دوروتی دنینگ»، استاد علوم رایانه‌ای دانشگاه جرج تاون ارایه شده است: «سایبر تروریسم بیشتر به معنای حمله یا تهدید علیه رایانه‌ها، شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آن‌ها است، هنگامی که به‌منظور ترساندن یا مجبور کردن دولت یا اتباع آن برای پیشبرد اهداف سیاسی یا اجتماعی خاص اعمال می‌شود. در تروریسم کلاسیک مواد منفجره و سلاح‌های گرم اصلی‌ترین ابزار تروریسم کلاسیک وجود دارند، اما مهم‌ترین ابزار سایبر تروریست‌ها رایانه است. «در واقع آن‌ها ترجیح می‌دهند به جای بمب از بایت استفاده کنند». اساسی‌ترین روش‌های سایبر تروریسم عبارت است از: «هک کردن، انتشار ویروس‌های رایانه‌ای، جاسوسی الکترونیک، دزدی هویت و تخریب یا دستکاری اطلاعات و یا حامل داده‌های الکترونیکی. دلایلی که سبب جذابیت سایبر تروریسم برای تروریست‌ها می‌شود عبارت‌اند از:

۱. سایبر تروریسم ارزان‌تر از روش‌های تروریستی متداول و کلاسیک است. تنها ابزاری که نیاز است یک رایانه شخصی متصل به شبکه اینترنت است. همچنین نیازی به خرید اسلحه نیست و می‌توان ویروس‌های رایانه را طراحی و تولید نمود و از طریق خطوط تلفن، کابل و ارتباط بی‌سیم آن‌ها را ارسال کرد (Shinder,Debar Littlejohn, 2002).

۲. سایبر تروریسم ناشناخته‌تر از روش‌های تروریسم کلاسیک است. مانند بسیاری از کاربران اینترنت، تروریست‌ها نیز از اسامی و هویت مستعار استفاده می‌کنند و برای نیروهای نظامی و امنیتی بسیار دشوار است که هویت واقعی تروریست‌ها را ردیابی و کشف کنند. همچنین در فضای مجازی موانع فیزیکی مانند ایست بازرسی، مرز و یا گمرک وجود ندارد.

۳. تنوع و تعداد حملات بسیار زیاد است. سایبر تروریسم می‌تواند شبکه‌های دولتی یا رایانه-ای دولتی، خدمات عمومی، خطوط هوایی خصوصی و... را مورد حمله قرار دهد. تعداد زیاد و پیچیدگی حملات احتمالی به تروریست‌ها کمک می‌کند تا نقاط ضعف و آسیب‌پذیر را برای حمله پیدا کند. مطالعات نشان می‌دهد شبکه‌های برق و خدمات اضطراری در برابر حملات سایبر آسیب‌پذیر هستند.

---

[1] Callin Barry

۴. سایبر تروریسم را می‌توان از راه دور هدایت کرد، این ویژگی جذابیت زیادی برای تروریست‌ها دارد. سایبر تروریسم، آموزش فیزیکی اندکی را می‌طلبد، سرمایه‌گذاری و فشار روانی کمتر و خطر دستگیری کمتری دارد و امکان می‌دهد تا سازمان‌های تروریستی عضوگیری کنند و اعضا را در اختیار داشته باشند. سایبر تروریسم توانایی زیادی دارد تا تعداد زیادی از مردم را به خود جذب کند، از این‌رو پوشش خبری و رسانه‌ای بیشتری را ایجاد می‌کند.

جرایم سایبری در عرصه بین‌الملل

فضای سایبر شامل جرایم نسل اول رایانه‌ای و هم‌اکنون شاهد جرایم بسیار جدید و بی‌سابقه در سطوح مختلف بین‌المللی می‌باشد.

جاسوسی رایانه‌ای: جاسوسی رایانه‌ای همانند جاسوسی کلاسیک ناظر به کسب اسرار حرفه‌ای، تجاری، اقتصادی، سیاسی، نظامی و نیز افشاء و انتقال و استفاده از اسرار است. مُجرم با دستیابی و فاش کردن این اطلاعات، اهداف خرابکارانه سیاسی، نظامی، اقتصادی، تجاری، اجتماعی، امنیتی و انتظامی دارد. وقوع و ارتکاب این نوع جرایم در فضای سایبری، امنیت ملی و حتی ثبات نظم و امنیت بین‌المللی را با مخاطره و تهدید مواجه می‌کند.

سابوتاژ رایانه‌ای: این جرم با جرایم تخریب شباهت بسیاری دارد و هدف مجرم اخلال در نظام سیاسی و اقتصادی یک کشور و بالطبع اخلال در امر حکومت آن کشور است. در واقع اصلاح، موقوف سازی، پاک کردن و تغییرات غیرمجاز داده‌ها و یا عملیات رایانه‌ای به‌منظور مختل ساختن عملکرد عادی سیستم را سابوتاژ رایانه‌ای می‌گویند.

جعل رایانه‌ای: وارد کردن، تغییر، محو یا موقوف سازی داده‌های کامپیوتری یا برنامه‌ها و نرم-افزارها با انگیزه و اهداف سیاسی و اقتصادی و امنیتی صورت می‌گردد. در مبحث یکم از فصل دوم قانون جرایم رایانه‌ای مصوب خرداد ماه ۱۳۸۸ مجلس شورای اسلامی؛ جعل رایانه‌ای به این شکل تعریف شده است:

الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانه داده به آنها.

ب) تغییر داده‌ها یا علایم موجود در کارت‌های حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانه داده‌ها یا علائم به آنها (قانون جرایم رایانه‌ای، ۱۳۸۸).

پول‌شویی در حوزه بین‌الملل: به دست آوردن پول و کسب ثروت از طریق غیرقانونی و نامشروع یا پول کثیف به‌نحوی که قانونی و پاک به‌نظر برسد، از جرایم کلاسیک بوده که در محیط سایبر به کمک اینترنت، پست الکترونیک و شبکه‌های بین‌المللی ارتباطی صورت می‌پذیرد. نحوه ارتکاب جرم به این شکل است که باندهای بزرگ فساد و کلاهبرداری به‌طور نامشروع توسط پست الکترونیک و یا شبکه مجازی اینترنت و بدون هیچ‌گونه هویت و نشانی، درخواست ارسال مبالغی پول به حساب شخص معینی را می‌نمایند و در تقاضای خود نحوه ارسال پول و دستمزد و مدت استرداد آن را بیان و در صورت پذیرفتن قربانی، چگونگی و شیوه تنظیمات لازم را اعلام می‌دارند و اصولاً در زمان استرداد پول یک عنوان مشروع در تجارت الکترونیک را با منشاء تجاری انتخاب و با اهداف مجرمانه خود هماهنگ می‌سازند. بیشترین بزه‌دیدگی و جرایم ارتکابی در حوزه سایبری و بین‌المللی از کشورهایی بوده که از لحاظ فناوری اطلاعات و ارتباطات و توانمندی پلیس سایبری در سطح بین‌المللی از درجه پایینی برخودارند.

قاچاق مواد مخدر: با توجه به گسترش ارتباطات شبکه‌ای و در محیط سایبر و سهولت برقراری ارتباطات کاربران از طریق پست الکترونیک و اینترنت، هرگونه قاچاق مواد مخدر اَعم از خرید، فروش، پخش، توزیع و حتی پیدا کردن واسطه‌ها و مصرف کنندگان از طریق فضای سایبری انجام می‌شود. از ویژگی‌های این روش: حذف واسطه‌ها و توزیع کنندگان غیرضروری، گسترش دامنه فعالیت قاچاقچیان تا سطوح بین‌المللی، دشواری پلیس و نهادهای انتظامی و امنیتی در خصوص کشف و دستگیری قاچاقچیان است.

سایبر تروریسم: «والتر لاکور» یک متخصص تروریسم در مرکز مطالعات استراتژیک و بین‌المللی به این موضوع اشاره می‌کند که یک مقام رسمی سازمان CIA ادعا نموده می‌تواند با مبلغ یک میلیارد دلار و تعداد ۲۰ هکر حرفه‌ای، ایالت متحده آمریکا را فلج کند. لاکور یادآوری می‌کند اگرچه هدف تروریست‌ها معمولاً ترور سران و رهبران سیاسی، گروگان‌گیری و یا حمله ناگهانی به تاسیسات دولتی، نظامی، پلیسی و یا عمومی است، اما تهدیدهایی که ممکن است به‌وسیله حمله‌های سایبر تروریسم به شبکه‌های رایانه‌ای وارد گردد، بسیار خطرناک‌تر از حملات

تروریستی سنتی و کلاسیک است. لاکور معتقد است که تروریسم رایانه‌ای برای تعداد کثیری از مردم بسیار ویران کننده‌تر از جنگ‌های بیولوژیک و یا شیمیایی است. از اقدامات سایبر تروریسم، ارتباط بین تروریست‌ها از طریق شبکه‌های بین‌المللی ارتباطات و تبادل اطلاعات و آموزش سریع و آسان اعمال مجرمانه در سطوح بسیار پیچیده جهانی است که از ویژگی‌های این نوع ارتباطات، عدم توانایی و یا دشواری پلیس در کنترل و شنود این ارتباطات و جرایم می‌باشد.

اقدامات قانونی و پیشگیری از سایبر تروریسم

روش‌های قانون‌گذاری و اقدامات قانونی برای مبارزه با سایبر تروریسم و پیشگیری از وقوع جرایم سایبری به دو حوزه ملی و فراملی (بین‌المللی) تقسیم می‌شود. روش‌های قانون‌گذاری ملی، فراسرزمینی و مختلط ناشی از پذیرش دکترین اثرگذاری در حاکمیت بر فضای سایبر است اما روش‌های خودانتظامی و بین‌المللی ناشی از پذیرش دکترین میراث مشترک بشریت در حاکمیت بر فضای سایبر است (ضیایی، ۱۳۸۸).

قانون‌گذاری ملی:

قانون‌گذاری ملی، احاله قدرت به قانون‌گذاران داخلی کشورها است و هر کشور دارای حکومتی بوده که به‌طور مستقل حق وضع قوانین در این رابطه را خواهد داشت. به‌عنوان مثال کشور آمریکا تعدادی قانون کیفری تصویب نموده که در آن نقض توافقات بین‌المللی مرتبط با ارتباطات رادیویی و یا تلگرافی را جرم انگاری کرده است. در کشور آمریکا اختلال همراه با سوء نیت خاص در وظایف فراملی و ماهواره‌ای در سطح بین‌المللی همچون کلاهبرداری تلگرافی جرم تلقی شده است. این روش تبعات نامطلوبی به دنبال دارد. با تکیه بر قانون‌گذاری ملی نمی‌توان از جرم انگاری کلیه جرایم علیه بشریت در فضای سایبر و حوزه بین‌المللی اطمینان خاطر داشت. (Graham J. H. Smith, op. cit., p. 533). همچنین در کشور ایران نیز در خرداد ماه سال ۱۳۸۸ مجلس شورای اسلامی قانون جرایم رایانه‌ای را به تصویب رسانده که بخشی از این قانون جنبه پیشگیرانه در مقابل وقوع جرایم سایبری دارد، اما با گذشت زمان و پیشرفت فناوری اطلاعات و ارتباطات، این قانون کارکردهای پیشگیری از جرم خود را از دست داده که در این خصوص نیازمند بازنگری و بروزرسانی توسط قانون‌گذار می‌باشد.

قانون‌گذاری فراملی[1]

در شیوه قانون‌گذاری فراملی، کشورها موظف به وضع قوانین ملی با آثاری بین‌المللی هستند، چنان‌که در صلاحیت جهانی به وضع چنین مقرراتی می‌پردازند. این روش نیز معضل چند کیفری را به دنبال دارد، خصوصاً آن که نه دولت‌ها و نه افراد نمی‌دانند کدام قانون را باید پاس بدارند و در نهایت مجبور خواهند بود مضیق‌ترین قانون را رعایت کنند (حافظی و خرم آبادی، ۱۳۹۰: ۴۱).

اقدامات پیشگیری از جرم و روش خود انتظامی[2]

برخی حقوق‌دانان بین‌المللی معتقد هستند حقوق حاکم بر فضای سایبر از جمله حقوق بشر، می‌باید در پروسه تبادلات کاربران آن ایجاد گردد. همان‌طور که حقوق تجارت بین‌الملل طبق عرف موجود میان بازرگانان ایجاد شده است (حسن بیگی، ۱۳۸۹). در این دیدگاه اینترنت به‌عنوان تابع حقوق بین‌الملل، واضع و مجری حقوق بشر خواهد بود. ویژگی این روش در مؤثر بودن قواعد آن است، زیرا این قواعد توسط جامعه‌ای ایجاد می‌شود که قرار است آن را اجرا نماید و همچنین دیگری در تخصصی بودن آن است زیرا این قواعد توسط جامعه‌ای ایجاد می‌شود که نسبت به مقامات بیرونی از تخصص بیشتری در زمینه فضای سایبری برخوردار است (Henry H. Perritt, JR 1999, p. 423).

نظام قانون‌گذاری بین‌المللی

در مناسب‌ترین روش با انعقاد کنوانسیون‌های بین‌المللی، موضوع حقوق بشر در فضای سایبر را به‌عنوان یکی از شاخه‌های حقوق بین‌الملل شاهد خواهیم بود. این روش که بسیاری از معایب روش‌های قبلی را نیز به همراه ندارد، تنها با مانع تعارض منافع دولت‌ها روبه‌رو است. به این معنا که دولت‌هایی که از نظر تکنولوژیک پیشرفته‌تر بوده و تأمین کننده خدمات اینترنتی هستند، روش قانون‌گذاری ملی یا فراملی را ترجیح می‌دهند. این در حالی است که کشورهای ضعیف‌تر که از نظر فناوری اطلاعات و ارتباطات در حوزه فضای سایبری از دیگر جوامع عقب‌تر هستند، علاقه‌مند به بین‌المللی شدن این حقوق خواهند بود. اولین تلاش برای مقابله با جرایم سایبری و

---

[1] Exterritorial
[2] Self-regulating

پیشگیری از سایبر تروریسم در عرصه بین‌المللی به اواخر قرن بیستم باز می‌گردد. زمانی که به پیشنهاد دادستان آمریکا «تلی کوساک[1]»، پلیس بین‌الملل در سال ۱۹۸۱ هماهنگ‌سازی قانون‌گذاری‌های داخلی پراکنده در مورد جرایم سایبری را در دستور کار خود قرار داد. در سال ۱۹۹۷ گروه هشت کشور صنعتی، کارگروه پیشگیری از جرایم فناوری برتر را تشکیل دادند و تعداد ۱۰ قانون در مبارزه با جرایم رایانه‌ای را وضع کردند.

در سال‌های بعد نیز اسناد دیگری در سطح منطقه‌ای و سازمان ملل متحد در ارتباط با حملات سایبری و سایبر تروریسم تنظیم شد. کنوانسیون شورای اروپا درباره جرایم سایبری که در ابتدای ژوئیه سال ۲۰۰۴ لازم‌الاجرا شد نیز سازوکاری برای هماهنگ ساختن قوانین و حقوق داخلی کشورها مربوط به جرایم سایبری ابداع نمود. همچنین سران سازمان همکاری اقتصادی آسیا و اقیانوس آرام[2] از طریق قانون‌گذاری داخلی مطابق با مقررات اسناد حقوق بین‌المللی مانند کنوانسیون جرایم سایبری (بوداپست ۲۰۰۱) به توان اقتصادی خود جهت مبارزه با جرم سایبری قوت بخشیدند. به همین ترتیب سازمان کشورهای آمریکایی[3] در آوریل سال ۲۰۰۴ قطعنامه‌ای صادر کرد که در آن دولت‌ها باید «اجرای اصول کنوانسیون شورای اروپا مصوب ۲۰۰۱ را ارتقاء بخشند و امکان عضویت در این کنوانسیون را بررسی نمایند. بر اساس کنوانسیون شورای اروپا در مورد جرایم سایبری و قطعنامه مجمع عمومی سازمان ملل ما باید به هدف خود یعنی چارچوبی حقوقی و جهانی علیه جرم سایبری دست یابیم».

قطعنامه بعدی مجمع عمومی سازمان ملل متحد که به مبارزه با سوء استفاده مجرمانه از فناوری‌های اطلاعاتی می‌پردازد؛ در سال ۲۰۰۰ میلادی مورد پذیرش قرار گرفت. این قطعنامه غیر الزام‌آور و متضمن این بود که دولت‌ها باید تضمین دهند که حقوق و رویه آنها مأمن امنی برای کاربرانی که از فناوری اطلاعات سوء استفاده مجرمانه می‌کنند، ایجاد نمی‌کند. نظام‌های حقوقی و امنیتی و پلیسی می‌باید امنیت، تمامیت و سطوح دسترسی به اطلاعات و سیستم‌های رایانه‌های را از صدمات و تهدیدهای غیرمجاز حفظ نمایند و تضمین دهند که سوء استفاده مجرمانه از آنها مورد پیگرد و مجازات قرار می‌گیرد (جلالی فراهانی، ۱۳۸۵: ۱۰۹).

---

[2] Telly kossack
[3] APEC
[4] OAS

نتیجه‌گیری و پیشنهادها

مقاله حاضر در مورد پدیده جهانی سایبر تروریسم و جرایم سایبری، چگونگی به‌وجود آمدن این جرایم در فضای مجازی و راه‌های مقابله و پیشگیری از این نوع جرایم پرداخته است. تروریسم چالشی است که موجب جریحه‌دار شدن اذهان عمومی و مخدوش شدن نظم و امنیت در روابط بین‌الملل شده است. در طول چهل سال گذشته، حقوق بین‌الملل پیشرفت چشمگیری در مبارزه با این پدیده داشته است. تاکنون چندین سند بین‌المللی منطقه‌ای و جهانی در مورد تروریسم بین‌المللی به تصویب رسیده، در حالی که مسئله مبارزه با تروریسم هنوز معضلی برای پلیس ملی کشورها، پلیس بین‌الملل (اینترپل) و دادگاه‌های داخلی و بین‌المللی است. برای توسعه همکاری‌های بین‌المللی در خصوص مبارزه با تروریسم و به‌خصوص سایبر تروریسم لازم است تدابیر جدیدی در نظام‌های حقوقی داخلی کشورها و معاهدات و پروتکل‌های بین‌المللی اتخاذ شود و زیرساخت‌های حقوقی و اداری مقتضی برای پیشگیری و مبارزه با سایبر تروریسم ایجاد گردد.

پیشنهادهای کاربردی:

در ادامه این بخش، راهکارهای کاربردی در خصوص افزایش همکاری‌های بین‌المللی برای مبارزه و پیشگیری از سایبر تروریسم ارائه می‌گردد:

۱- ایجاد معاهدات بین‌المللی و برگزاری نشست‌های تخصصی نهادهای امنیتی و پلیسی کشورها با محوریت پلیس بین‌الملل (اینترپل) در زمینه آموزش و ارایه راهکارهای مبارزه با سایبر تروریسم بین‌الملل.

۲- تدوین قوانین بین‌المللی برای مبارزه با جرایم سایبری و پیشگیری از سایبر تروریسم و الزام رعایت این قوانین از سوی کشورهای عضو و یا غیر عضو در جوامع بین‌المللی.

۳- توسعه و ارتقای امنیت ملی، ایمنی و پایداری در شبکه‌های ارتباطی و الکترونیکی موجود با تأکید بر فناوری‌های بومی.

۴- همکاری فنی و آموزشی بین دستگاه‌های امنیتی و انتظامی از جمله: پلیس فضای تولید و تبادل اطلاعات (فتا)، پلیس بین‌الملل (اینترپل)، مرکز بررسی جرایم سازمان‌یافته فرماندهی پدافند سایبری سپاه پاسداران انقلاب اسلامی، وزارت اطلاعات جمهوری اسلامی ایران، معاونت پیشگیری از جرم قوه قضائیه و سایر نهادها با یکدیگر.

۵- توسعه همکاری‌های فنی و آموزشی بین‌المللی در خصوص مبارزه با سایبر تروریسم.
۶- حمایت از خودکفایی تولیدات مجازی و برنامه ایجاد شبکه ملی اینترنت مبتنی بر مولفه-های امنیت، ایمنی، پایداری و متکی بر فناوری‌های بومی و توسعه توان کنترل و مدیریت فضای مجازی و برنامه‌های حراست، حفاظت و ضد جاسوسی و ضد تروریستی مراکز حساس در فضای سایبری.
۷- بازنگری و اصلاح قانون جرایم رایانه‌ای در مجلس شورای اسلامی و افزایش توان بازدارندگی و پیشگیری از وقوع جرم این قانون.
۸- آموزش کاربران فناوری اطلاعات و اطلاع‌رسانی عمومی در خصوص پیشگیری از جرایم سایبری.

فهرست منابع

- باستانی، برومند (۱۳۸۷). جرایم کامپیوتری و اینترنتی. انتشارات بهنامی، تهران.
- پایگاه اینترنتی «داده‌ها و آمار اینترنت» در آمریکا، ۲۰۱۲.
- جلالی فراهانی، امیرحسین (۱۳۸۵). صلاحیت کیفری در فضای سایبر. مجله فقه و حقوق، شماره ۱۱.
- جینا دی آنجلیز، جرایم سایبر. ترجمه سعید حافظی و عبدالصمد خرم‌آبادی (۱۳۹۰)، نشر دبیرخانه شورای‌عالی اطلاع‌رسانی.
- حسن بیگی، ابراهیم (۱۳۸۹). حقوق و امنیت در فضای سایبر. موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار، تهران.
- خمامی زاده، فرهاد (۱۳۸۲). مبارزه با پولشویی در بانک‌ها و مؤسسات مالی: نگاهی به قانون ضد تروریسم ایالات متحده آمریکا. مجله حقوقی بین‌المللی ج.ا.ا، شماره ۲۹.
- دفتر مطالعات حقوقی مرکز پژوهش‌های مجلس شورای اسلامی (۱۳۸۷). گزارش پژوهشی شماره مسلسل ۹۰۰۹.
- ساروخانی، محمدباقر (۱۳۹۱). جامعه شناسی ارتباطات. انتشارات اطلاعات. تهران.
- سلیمی، صادق (۱۳۸۲). جنایات سازمان‌یافته فراملی در کنوانسیون پالرمو و آثار آن. مجله حقوقی دفتر خدمات حقوقی بین‌المللی ج.ا.ا، شماره ۲۹.
- سندوز، یوس (۱۳۸۲). مبارزه علیه تروریسم و حقوق بین‌الملل: خطرات و فرصت‌ها. مترجم سواری، حسن، مجله حقوقی، دفتر خدمات حقوقی بین‌المللی ج.ا.ا، شماره ۲۹.
- سوری، جواد (۱۳۸۷). نقش فناوری‌های نوین ارتباطی در عملیات روانی. فصل‌نامه عملیات روانی، شماره ۱۲.
- صدوقی، مرادعلی (۱۳۹۰). فناوری‌های اطلاعاتی و حاکمیت ملی. دفتر مطالعات سیاسی و بین‌المللی، تهران.
- طبیبی فرد، امیرحسین (۱۳۸۳). مبارزه با تأمین مالی تروریسم در اسناد بین‌المللی. مجله حقوقی دفتر خدمات حقوقی ج.ا.ا، شماره ۳۲.
- کاستلز، مانوئل (۱۳۸۰). عصر اطلاعات و ظهور جامعه شبکه‌ای، ترجمه احمد علیقلیان و افشین خاکباز، تهران: انتشارات طرح نو.

- گروه تحقیق (۱۳۸۴). جهانی شدن ارتباطات و تهدیدهای امنیت ملی ما. فصل‌نامه راهبرد، شماره ۳۶.
- گزارش پژوهشی (۱۳۸۷). امنیت ملی ایران در تئوری و عمل. مرکز پژوهش‌های مجلس شورای اسلامی، دفتر سیاست خارجی، تهران.

- Antonio Cassese, Terrorism is also disrupting some Crucial Legal Categories of international Law, 12 European journal of international law, 2001.
- Errol P. Mendes, Democracy, Human Rights and the New Information Technologies in the 21st Century-The Law and Justice of Proportionality and Consensual Alliances, National Journal of Constitutional Law, no. 10, 1999, p. 363.
- Gina.De. Angelis, Cyber Crimes, Chelsea House Publisher, 2000.
- Henry H. Perritt, JR. Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism, Berkeley Technology Law Journal, vol. 12, 1999, p. 423.