فصـــــلنامه بیـــن المللـــــی قـــانـــون یـــار
License Number: 78864 Article Cod:Y8SH29A6412078 ISSN-P: 2538-3701

بررسی و تحلیل کیفری تروریسم سایبری
با مداقه در انواع و اقسام عملیات تروریسم سایبری

(تاریخ دریافت ۱۴۰۳/۰۱/۱۷، تاریخ تصویب ۱۴۰۳/۰۳/۲۰)

عطیه سلیم پور
پژوهشگر و مولف کتب حقوقی

چکیده

تروریسم سایبری یا سایبرتروریسم استفاده از اینترنت برای انجام اعمال خشونت آمیز، وحشت زا و خسارت ساز است که منجر به از بین رفتن یا تهدید به از دست دادن جان یا آسیب جسمی قابل توجهی، به منظور دستیابی به دستاوردهای سیاسی یا ایدئولوژیکی از طریق فضای مجازی می‌شود. با توجه به رشد روز افزون دانش بشری در زمینه فناوری اطلاعات و ارتباطات و همچنین درگیر شدن هر چه بیشتر جوامع به استفاده از این ابزارها و پیشرفت‌های دیگری که در اثر به کارگیری آنها حاصل شده به مراتب جوامع بشری آسیب‌پذیری‌های بیشتری پیدا کرده‌اند نقش مهم رایانه و اینترنت و ترغیب مجرمان و تروریست‌ها برای استفاده از آنها به عنوان یک ابزار مناسب برای حمله به اهداف‌شان غیر قابل انکار است. تروریسم سایبری از جدیدترین اشکال و شیوه‌های ارتکاب بزهکاری در جهان است که هدف از انجام این پژوهش تحلیل کیفری این موضوع و تشریح انواع و اقسام تروریسم سایبری در جهان می باشد. با توجه به اهمیت این موضوع در مقاله حاضر قصد داریم به بررسی و تحلیل کیفری تروریسم سایبری با مداقه در انواع و اقسام عملیات تروریسم سایبری بپردازیم. روش تحقیق از نوع تحلیلی-توصیفی بوده و ابزار گردآوری اطلاعات و داده ها فیش برداری و بهره از کتب و مقالات مرتبط با موضوع پژوهش است.

واژگان کلیدی: تروریسم سایبری، فضای مجازی، سایبر تروریسم، اقسام تروریسم

بخش اول: بررسی و شناخت فضای سایبر

فضای سایبر حاصل پیشرفت تکنولوژی بشر در زمینه دنیای دیجیتال و علوم رایانه‌ای است. این فضا در معنا در بر گیرنده ارتباطات انسان‌ها از طریق رایانه و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود یک ارتباط برخط (آنلاین) که کاربران با استفاده از امکانات فضای سایبر از قبیل اینترنت با ابزارهایی چون پست الکترونیک با یکدیگر ارتباط برقرار می‌کنند نمونه‌ای از فعالیت در حوزه فضای سایبر است. به بیان ساده‌تر در فرهنگ اصطلاحات فضای سایبر عبارت است از: «جهانی از محیط‌هایی همچون اینترنت که افراد در آن از طریق کامپیوترهای متصل به یکدیگر ارتباط برقرار می‌کنند. یکی از مشخصه‌های تعریف کننده فضای اینترنتی این است که برقراری ارتباط به دوری فاصله بستگی ندارد» (همان: ۱۰۰). امروزه هر جا سخن از فضای سایبری می‌شود اصطلاحاتی نظیر جرایم سایبری به طور اخص جنگ‌های اطلاعاتی دفاع سایبری و تروریسم سایبری به چشم می‌خورد. به طور غالب اصطلاح سایبر بیشتر برای توصیف هر چیزی به کار برده شده است که با شبکه‌ها و سیستم‌های کامپیوتری به طور ویژه در زمینه‌های امنیتی مربوط است. استفاده از فضای مجازی برای اولین بار توسط ویلیام گیبسون نویسنده داستانهای علمی - تخیلی در سال ۱۹۸۰ به ویژه در ادبیاتی که به جنگ الکترونیکی مشهور است به کار گرفته شده است (Gibson, ۱۹۸۵: ۶۹).

از نظر واژه‌شناسی نیز فضای سایبر با فضای مجازی واژه‌ای مرکب از دو کلمه cyber به معنای مجازی و غیر واقعی است که به عنوان پیشوندی برای توصیف شخص ایده و یا فضا که به دنیای رایانه و ارتباطات وابسته است استفاده می‌شود (مجیدی و همکاران، ۱۳۹۰: ۲) و کلمه space یعنی فضا تشکیل شده است. در فیزیولوژی نیز فضای سایبر عبارت است از به معنای مطالعه و مقایسه بین دستگاه عصبی خودکار مغز و اعصاب با دستگاه‌های الکتریکی و مکانیکی است (موسوی، ۱۳۹۰).

بخش دوم: بررسی ویژگی های جرم زای فضای سایبر

فضای سایبر محیط جدیدی را برای فعالیت بزهکارانه افراد فراهم آورده است. این محیط با ویژگی‌هایی که دارد بزه‌های رایانه‌ای را همراه با مزایای دیگر خود به همراه داشته است. با آشنایی در خصوص چگونگی ارتکاب و مشخصه‌های بزه‌های رایانه‌ای می‌توان به روش‌های پیشگیری و مقابله با بره‌های مذکور و جلوگیری از بزه‌دیدگی دوباره افراد پی برد. بنابراین در ذیل به عمده‌ترین مشخصه‌های بارز یزه‌های رایانه‌ای و مطلوبیت آنها برای بزهکاران از جمله تروریست‌های سایبری اشاره می گردد.

۱- صرفه‌جویی در وقت و قابلیت تکرار فراوان

با گسترش تکنولوژی و فراگیر بودن دانش رایانه در سرتاسر جهان دسترسی مردم به سیستم‌های رایانه‌ای در سال‌های اخیر چندین برابر شده است. همین خصیصه فراگیر بودن باعث شده اغلب نیازهای روزمره با استفاده از فضای مجازی برطرف گردد. کسانی که قصد ارتکاب اعمالی را دارند که ضد هنجارهای جامعه و قانون هستند از طریق دنیای مجازی سریع‌تر و مطمئن‌تر به اهداف خود می‌رسند. به عنوان مثال با استفاده از چند کد دستوری می‌توان از حساب بانکی یک شخص وجهی را به حساب بانکی دیگر انتقال داد. اما اگر دنیای مجازی را با دنیای عینی مقایسه کنیم چه بسا عمل مذکور غیر قابل ارتکاب یا با گذشت زمان طولانی انجام می‌پذیرد. همین آسودگی و صرف زمان کمتر باعث تشویق جنایتکاران به ادامه و تکرار عمل مجرمانه خود می‌شود (جلالی فراهانی، ۱۳۸۵ الف: ۹۲).

۲- عدم آگاهی قربانیان از بزه‌دیدگی

در اکثر موارد بزه‌دیدگان جرایم رایانه‌ای از وضعیت خود که به عنوان مثال در اثر حملات سایبری سیستم رایانه به ویروس آلوده شده باشند یا در جایی که هکرها در سیستم نفوذ کرده باشند آگاه نیستند. این مسئله در ارتباط سازمان‌ها و شرکت‌ها به مراتب شدیدتر است زیرا کمتر از سیستم‌های تشخیص نفوذ استفاده می کنند (باستانی، ۱۳۹۰: ۳۵).

۳- سهولت در از بین بردن آثار وقوع جرم و بالا بودن رقم سیاه بزهکاری

کسانی که در این حوزه‌ها مرتکب جرم می‌شوند؛ دارای تخصص بالاتری بوده و از دانش کافی برخوردارند؛ لذا هنگام ارتکاب اعمال مجرمانه سعی و اقدام به حذف رد پاهای خود در محیط سایبری می‌کنند. هر چند با تکیه بر بعضی فناوری‌های نوین می‌توان اطلاعات را دوباره به دست آورد اما همین مهارت آنها باعث وقفه در عملیات‌های بازرسی و پیگیری تیم‌های متخصص می‌شود. نکته دیگری که در این جرایم از اهمیت بالایی برخوردار است حیثیت و وجهه‌ای است که افراد یا شرکت‌های معتبر و بانک‌ها با آن روبرو هستند که در اکثر جرایم به دلیل حفظ موقعیت و جلوگیری از تشویش اذهان مشتریان خود اقدام به گزارش این‌گونه جرایم نمی‌کنند که همین دلیل منجر به بالا رفتن رقم سیاه جرایم و عدم وجود آمارهای جنایی دقیق و در نهایت عدم برخورد مناسب از لحاظ قضایی با این گونه از بزهکاران باشیم (خداقلی، ۱۳۸۳: ۳۵).

۴- فراملی بودن و عدم نیاز به محل ارتکاب مشخص

جرم رایانه‌ای شکل تازه‌ای از جرمهای فراملی است و محدوده بالقوه آن به همان گستردگی سیستم‌های ارتباطی بین‌المللی وسیع‌تر می‌شود شبکه اینترنت و به طور کلی فضای مجازی این امکان را به محرمان می‌دهد که در هر کجا از دنیا که باشند و در هر زمان با استفاده از شبکه یکپارچه اینترنت به اهداف شوم خود برسند. به عنوان مثال در جرایم امنیتی و تروریستی که مجرمان در صدد انعکاس هر چه بیشتر اقدامات خود هستند فضای مجازی محیط مطلوبی برای این گونه اقدامات است؛ زیرا که هر اختلالی در آن به خوبی انعکاس جهانی داشته و به راحتی اعتبار یک کشور یا مجموعه خاصی را لکه دار می‌کند (رضوی، ۱۳۸۶: ۱۲۳).

۵- تنوع مرتکبان و گستردگی حجم خسارات حاصله

امروزه با همه گیر شدن اینترنت این فرصت برای همه افراد جامعه وجود دارد که با کمترین صرف وقت و با استفاده از نرم‌افزارهای آموزشی قابل دسترس انواع شیوه‌های نفوذ در سیستم‌ها را آموزش ببینند. بنابراین نمی‌توان گفت که در جامعه امروزی استفاده از

فضای مجازی و به تبعیت آن بزهکاران این حوزه افراد خاصی هستند. نکته دیگر این است که با توجه به گسترش دولت الکترونیک در سال‌های اخیر در ایران و کشورهای جهان ارتکاب جرم با استفاده از رایانه خسارات سنگینی را به حوزه‌های اقتصادی، امنیتی فرهنگی و... تحمیل می‌کند (وارن و هاچینسون، ۱۳۸۲: ۲۱).

۶- دارای حیثیت عمومی و خصوصی بودن

جرایم رایانه‌ای دارای هر دو خصیصه عمومی و خصوصی بودن هستند؛ به این صورت که از یک طرف در رابطه با دولت و فضای عمومی جامعه و از طرف دیگر به اشخاص حقیقی یا حقوقی خصوصی خسارت مادی و معنوی وارد می‌کنند.

۷- دشوار بودن تعیین صلاحیت کیفری

یکی از چالش برانگیزترین مشکلات در حوزه جرایم رایانه‌ای به خصوص در جرایمی که دارای خصیصه و منشأ فراملی هستند تعیین صلاحیت محاکم و دولت‌هایی است که با جرم در خاک آن کشور اتفاق افتاده با این که نتیجه جرم در کشور مزبور واقع شده است. جرایم سایبری با توجه به این که در سرتاسر جهان قابلیت ارتکاب را دارا هستند منجر به بروز مشکلاتی نظیر تعارض در صلاحیت محاکم می‌شود. (رضوی، ۱۳۸۶: ۱۲۵).

بخش سوم: بررسی انواع و اقسام بزه‌دیدگان تروریسم سایبری

بری کالین یکی از متخصصان حوزه سایبر، تروریسم سایبری را این‌گونه تعریف نموده است سوءاستفاده عمدی از سیستم شبکه با دستگاه‌های اطلاعاتی رایانه‌ای برای تحقق هدفی که مؤید با تسهیل کننده مبارزه با اقدام تروریستی است (بقایی‌هامانه و باقرپور اردکانی، ۱۳۸۴: ۳۵) بزه‌دیدگان تروریسم سایبری را می‌توان به دو دسته کلی اشخاص حقیقی و اشخاص حقوقی دسته‌بندی نمود:

الف) بزه‌دیدگان حقیقی تروریسم سایبری

این دسته از بزه‌دیدگان شامل افرادی می‌شود که کاربران فضای مجازی محسوب می‌شوند؛ و یا این که اشخاصی هستند که به تازگی وارد فضای سایبر شده‌اند. به عبارت دیگر بر اساس تئوری‌های فعالیت‌های روزمره یا سبک زندگی اشخاص افرادی که به طور

روزمره در اینترنت به سر می‌برند. بیشتر از سایرین در معرض بزه‌دیدگی قرار دارند (زررخ، ۱۳۹۰: ۱۴۷) نفوذگران با هکرهای تروریستی از شاخص‌ترین بزهکاران حوزه فضای سایبر هستند که با استفاده از دانش و مهارت خاص خود از نفوذپذیری و نقاط آسیب‌پذیر رایانه‌های افراد و شبکه‌ها در سطح وسیع سوء استفاده کرده و با به کارگیری بدافزارهای رایانه‌ای از قبیل تروجان‌ها ویروس‌ها و کرم‌های رایانه‌ای به تخریب سخت‌افزار و نرم‌افزارهای رایانه‌ای و یا اختلال در نرم‌افزارهای امنیتی اشخاص در سطح گسترده اقدام می‌کنند.

قربانیان تروریسم سایبری همانند دیگر انواع تروریسم از گستردگی و تنوع زیادی برخوردارند. به منظور درک بیشتر وضعیت قربانیان تروریسم سایبری می‌توان به نمونه‌ای از حملات سایبری در کشور آمریکا اشاره نمود که در سال ۲۰۰۳ با حمله علیه تأسیسات انتقال برق و نیروگاه‌های برخی از ایالات برق مناطق بسیاری از آمریکا قطع شد و سبب مختل شدن پایگاه نیروی هوایی «ادواردز» و آزمایشات بمب‌افکن‌های (B-۱ و B-۲) گردید (Colarik, ۲۰۰۶: ۱۸۵)با دقت و بررسی درباره رخدادهایی از این قبیل می‌توان به بحران بزه‌دیدگی ناشی از حملات تروریستی سایبری پی برد. کرم استاکس نت نمونه بارز تأثیر حملات تروریستی سایبری بر کاربران خانگی است؛ به طوری که با گذشت چند ماه از شناسایی این بدافزار در تأسیسات کشورمان خطر این جاسوس افزار به رایانه‌های خانگی رسید به همین دلیل مسئولان اعلام کردند که این کرم جاسوسی نه تنها تهدیدی برای سیستم‌های صنعتی کشور محسوب می‌شود بلکه تهدیدی برای بیش از یک سوم جمعیت کشور که کاربران اینترنت را تشکیل می‌دهند نیز هست؛ چرا که این کرم رایانه‌ای نقاط ضعفی را در رایانه‌های آلوده ایجاد کرده که امکان دسترسی به اطلاعات رایانه کاربران را از راه دور فراهم میسازد و کاربران خانگی و هم شرکت‌های دولتی و خصوصی نیز در معرض تهدید این بدافزار قرار دارند.

بنابراین با پشت سر گذاشتن تجربه مواجهه با بدافزار استاکس نت می‌توان به درگیر بودن بزه‌دیدگان حقیقی در حملات سایبری و جایگاه آنها در میان بزه‌دیدگان حملات

تروریستی سایبری پی برد. با نگاهی به قوانین کشورهای مختلف و کنوانسیون‌های بین‌المللی در مورد محافظت از سیستم‌ها و دستگاه‌های رایانه‌ای و مخابراتی اغلب رفتارهای جرم‌انگاری شده حول دو محور اختلال یا تخریب تأسیسات مذکور است. بدین منظور هر گونه اختلال یا تخریب به وسیله دستکاری نفوذگران و کرکرها در داده‌ها که منجر به تخریب یا اختلال سخت‌افزار با نرم‌افزاری تأسیسات رایانه‌ای و مخابراتی اشخاص شود بزه‌دیدگی اشخاص حقیقی را نیز در پی خواهد داشت. بنابراین خسارت‌های تحمیل شده فقط اختصاص به منابع رایانه‌ای ندارد؛ بلکه ممکن است به دنبال وقوع حادثه، در شخص قربانی اثرات جسمی یا روانی بروز نماید در خصوص بزه‌دیدگان تروریسم سایبری ذکر این نکته ضروری است که اختلال تخریب یا تلفات ناشی از حملات تروریستی سایبری یا تهدید به این حملات باید در سطح کلان وقوع یابد تا تحت عنوان بزه‌دیدگان آن محسوب شوند (جلالی فراهانی، ۱۳۸۵ الف: ۹۵) در میان انواع بزه‌دیدگان تروریسم سایبری به نظر می‌رسد که کاربران خانگی و کارکنان تأسیسات زیر ساختی مبتنی بر فناوری اطلاعات بیشترین آسیب‌پذیری را در مقابل حملات سایبری از یک طرف به دلیل عدم آشنایی کافی با اصول امنیت شبکه و رایانه بی تجربه بودن آنها و فقدان دسترسی به امکاناتی از قبیل اینترنت برای بروز رسانی وضعیت ایمنی رایانه‌های شخصی متحمل می‌شوند و از طرف دیگر به دلیل توقف امور اجرایی و تخریب زیر ساخت‌های کشور شهروندان بیشترین خسارت را در جنبه‌های مختلف اقتصادی امنیتی بهداشتی مخابراتی و انرژی تجربه می‌کنند.

علاوه بر کاربران خانگی و کارکنان دسته‌ای دیگر از بزه‌دیدگان حقیقی افرادی هستند که با استفاده از تلفن‌های همراه به فعالیت‌های روزمره خود می‌پردازند گوشی‌های تلفن همراه نوینی چون ای پدا و به طور غالب گوشی‌هایی که دارای سیستم عامل آندروید ۲ هستند امروزه در میان مردم از محبوبیت ویژه ایی برخوردار هستند و قابلیت این را دارند که مانند یک رایانه شخصی به کاربران خدمات ارائه دهند. این افزایش محبوبیت منجر به جذب بزهکاران سایبری و به خصوص تروریست‌های سایبری به فناوری‌های مذکور شده

است به طوری که در سال ۲۰۱۲ تعداد بد افزارهای کشف شده‌ای که به منظور حمله به گوشی‌های تلفن همراه برنامه نویسی شده‌اند نسبت به سال ۲۰۱۰ چهار برابر افزایش داشته است. بدافزارهای مذکور قادر هستند که با دور زدن حالت مبتنی بر امضاء در نرم‌افزارهای پویشگر خود را به نرم‌افزارهای معتبر الصاق کرده و بین گوشی‌های تلفن همراه منتشر شوند، بر اساس تحقیقات صورت گرفته مهم‌ترین تهدیدات سایبری گوشی‌های همراه در سه ماه اول سال ۲۰۱۲ عبارت‌اند از: تروجان‌های پیامک نرم‌افزارهای جاسوسی ابزارهای نفوذ و برنامه‌های کاربردی آلوده هستند. نفوذگران و کرکرها در بسیاری از مواقع از گوشی‌های تلفن همراه به عنوان ابزاری برای دستیابی به شبکه‌های مخابراتی و آلوده کردن آنها اقدام می‌کنند و به سادگی می‌توان با روش‌های مذکور به انواع شبکه‌ها و رایانه‌ای حساس دسترسی پیدا کرد بد افزارهای مذکور در اغلب موارد از طریق استفاده و دریافت موسیقی یا متن از شبکه‌های اجتماعی از قبیل تویتر، مای اسپیس و فیس بوک وارد گوشی‌های همراه شده و موجب کشیده شدن نفوذگران تروریستی به دستگاه‌های مربوطه می‌شوند.

ب) بزه‌دیدگان حقوق تروریسم سایبری

عمده‌ترین و گسترده‌ترین بزه‌دیدگان تروریسم سایبری زیر ساخت‌های حیاتی و اطلاعاتی مهم کشور هستند. منظور از شبکه‌های حیاتی شبکه‌هایی هستند که در صورت اخلال به مدت هر چند کوتاه یا عملکرد نادرست زندگی روزمره مردم و یا عملکرد عادی دستگاه‌های اجرایی کشور و مأموریت آنها را مخدوش می‌کند جذاب‌ترین هدف برای حملات تروریستی سایبری و تروریسم سنتی، اقدام به تخریب یا اختلال در تأسیسات و داده‌های رایانه‌ای و مخابراتی سازمان‌هایی است که قسمت بزرگی از امور اجرایی کشور و فعالیت‌های شهروندان به آنها وابسته است. انتخاب چنین اهدافی نیز به دلیل جلب توجه عموم جامعه و به خصوص جامعه جهانی به اقدامات و خواسته‌های آنان است.

بر اساس آیین‌نامه اجرایی بند ۱۱ ماده ۱۲۱ قانون برنامه پنج ساله چهارم توسعه کشور، مراکز و تأسیساتی که ممکن است هدف بالقوه‌ای برای دشمنان تلقی گردند به سه دسته

تقسیم می‌شوند که عبارت‌اند از: مراکز حیاتی مراکزی که دارای گستره فعالیت ملی هستند و وجود و استمرار فعالیت آنها برای کشور حیاتی است و آسیب یا تصرف آنها به وسیله دشمن باعث اختلال کلی در اداره امور کشور می‌گردد. مراکز حساس یعنی مراکزی که دارای گستره فعالیت منطقه‌ای هستند و وجود و استمرار فعالیت آنها برای مناطقی از کشور ضروری است و آسیب یا تصرف آنها به وسیله دشمن باعث بروز اختلال در بخش‌های گسترده‌ای از کشور می‌گردد. مراکز مهم یعنی مراکزی که دارای گستره فعالیت محلی هستند و وجود و استمرار فعالت آنها برای بخشی از کشور دارای اهمیت است. و آسیب یا تصرف آنها به وسیله دشمن باعث بروز اختلال در بخشی از کشور می‌گردد.

بخش چهارم: نگاهی اجمالی به انواع عملیات تروریسم سایبری

بر اساس مطالعات پریچارد و مک دونالد در زمینه تروریسم سایبری در خصوص طبقه‌بندی تروریسم سایبری و افعال مرتبط با آن تروریسم سایبری را به هفت گروه تقسیم کرده‌اند که در ذیل به (Janet and Laurie; ۲۰۰۴: ۲۸۴) بیان مختصر آنها پرداخته می‌شود.

بند اول: جنگ اطلاعاتی

جنگ اطلاعاتی مفهومی نزدیک با تروریسم سایبری دارد؛ اما در برخی ارکان تشکیل‌دهنده این بزه تفاوت‌هایی وجود دارد که می‌توان تفاوت آن را با تروریسم سایبری روشن نمود. در تعریف جنگ اطلاعاتی آمده است اقدامات لازم جهت حفظ یکپارچگی سامانه‌های اطلاعاتی خودی در مقابل بهره‌برداری آلوده شدن و تخریب و از طرف دیگر تلاش برای بهره‌برداری آلوده کردن و همچنین تخریب سامانه‌های اطلاعاتی دشمن و انجام پردازش‌های لازم جهت به دست آوردن برتری اطلاعاتی در مواقع اعمال فشار است (رنجبر و همکاران، ۱۳۸۶: ۲۶) تقسیم‌بندی‌های متفاوتی از جنگ اطلاعاتی ارائه شده که بیشتر در ابعاد نظامی به مسئله پرداخته‌اند؛ از جمله یکی از متخصصین این امر به نام لیبسکی با تأکید بر واژه‌شناسی نظامی جنگ اطلاعاتی را به هفت گونه تقسیم کرده است: «نبرد فرماندهی و کنترل جنگ جاسوسی جنگ الکترونیکی جنگ روانی نبرد نفوذیاب‌ها،

جنگ اطلاعاتی اقتصادی و جنگ سایبر (Kenneth& Boulton; ۲۰۰۶: ۷۷) آن‌چه در جنگ‌های اطلاعاتی از اهمیت زیادی برخوردار است برتری اطلاعاتی است و سعی می‌شود با تهاجم اطلاعاتی به فرآیندهای اطلاعاتی دشمن و خرابکاری در آنها دسترسی به نیروهای اطلاعاتی خودی محروم شود. به طور کلی قابلیت‌های جنگ اطلاعاتی از نقطه نظر دفاعی به پنج گروه تقسیم شده است عملیات روانی، فریبکاری نظامی جنگ جاسوسی عملیات شبکه کامپیوتری و جنگ الکترونیکی (Cox; ۲۰۰۵: ۸۸۶).

نکته قابل توجه در تمایز تروریسم سایبری با جنگ اطلاعاتی این است که نبرد سایبری عبارت است. از این که جنگ اطلاعاتی فقط علیه داده‌های اطلاعاتی صورت می‌گیرد و تخریب سخت‌افزاری، مانند. تروریسم سایبری در آن وجود ندارد همچنین در نبرد اطلاعاتی نیروهای نظامی دو کشور درگیر هستند در صورتی که در تروریسم سایبری اشخاص و گروه‌های غیر دولتی در دو طرف نبرد سایبری قرار دارند.

بند دوم: جنگ سایبری

اصطلاح جنگ سایبر برای اولین بار توسط دکتر توماس رونا در سال ۱۹۷۹ به کار گرفته شد. جنگ سایبر عبارت است از اقداماتی که شامل استفاده از حملات سایبری به وسیله کشورها یا گروه‌های (Andrew lewis; ۲۰۱۰: ۱) برانگیخته سیاسی که به منظور دستیابی به اهداف سیاسی انجام می‌شود جنگ سایبری را به سه گونه تقسیم‌بندی کرده‌اند جنگ اطلاعاتی علیه داده‌های افراد، جنگ اطلاعاتی علیه داده‌های شرکت‌ها با سازمان‌ها جنگ اطلاعاتی جهانی که به منظور حمله علیه سیستم‌های حیاتی کشورها ارتکاب می‌یابد. نمونه‌ای از جنگ‌های سایبری اخیر می‌توان به هک شدن تارنمای شرکت ارتباطاتی (SK) کره جنوبی در ژوئیه ۲۰۱۱ اشاره نمود که در طی آن اطلاعات شماره تلفن، پست‌های الکترونیک و آدرس منزل ۳۵ میلیون نفر دزدیده شد. همچنین در اکتبر ۲۰۱۱ دولت آمریکا پذیرفت که کنترل هواپیمای جاسوسی خود را در یک حمله سایبری از سوی ایران از دست داده است. در سال ۲۰۱۲ هم اطلاعات کمیسیون دو جانبه اقتصادی بین چین و

آمریکا توسط نفوذگران هندی هک شد که در طی آن دسترسی به اطلاعاتی شامل تبادلات پست‌های الکترونیک بین اعضای کمیسیون دو جانبه بوده است

بند سوم: جاسوسی سایبری

جاسوسی سایبری تابع روش‌های سنتی جاسوسی یعنی شناسایی اطلاعات مورد نیاز که به طور معمول اطلاعات مهم،حکومتی نظامی یا بازرگانی هستند دسترسی یا جمع‌آوری اطلاعات و افشاء یا در دسترس قرار دادن اطلاعات به اشخاص غیر مجاز به طور معمول با انگیزه‌های سیاسی، اقتصادی، نسبت به داده‌های محرمانه در حال انتقال یا ذخیره شده در سیستم‌های رایانه‌ای و مخابراتی انجام می‌شود (ماه پیشانیان، ۱۳۹۰: ۱۰۳) جاسوسی رایانه‌ای یا سایبری یکی از مراحل اولیه و ضروری تروریسم سایبری برای مرتکبان آن است با این توضیح که اشخاص تروریست از جمله نفوذگران، برای طرح‌ریزی حملات سایبری نیازمند اطلاعات مربوط به زیر ساخت‌های حیاتی یا اطلاعاتی هستند تا با استفاده از اطلاعات کسب شده و نحوه پیکربندی سیستم‌ها به عملیات‌های غیر قانونی علیه داده‌ها و سیستم‌های رایانه‌ای و مخابراتی اقدام کنند.

بند چهارم: خرابکاری سایبری

خرابکاری رایانه‌ای عبارت است از عملیات‌های اخلال‌گرانه و تخریبی در داده‌ها یا برنامه سیستم‌های رایانه‌ای یا مخابراتی دولتی با افعالی از قبیل تغییر محو کردن متوقف ساختن، انتقال دادن و امثال آن با اهدافی معمولاً سیاسی یا اقتصادی (عالی‌پور، ۱۳۹۰: ۲۱۶) با مطالعه رفتار تروریست‌های سایبری می‌توان گفت که رکن رکین تروریسم سایبری در فعلیت بخشیدن به مقاصد تروریست‌های سایبری استفاده از خرابکاری رایانه‌ای و جاسوسی در عملیات‌های تروریستی است زیرا خرابکاری، دسته‌ای از اعمال غیر قانونی علیه سیستم‌ها و تجهیزات مخابراتی را شامل می‌شود که هم داده را در بر می‌گیرد و هم تجهیزات فیزیکی سخت‌افزار مربوطه را شامل می‌شود جاسوسی نیز مهم‌ترین بخش در پیاده کردن حملات سایبری است. آن چه در درجه اول تروریست‌های سایبری به آن نیاز دارند

اطلاعات در خصوص تجهیزات رایانه‌ای و مخابراتی و همچنین نفوذ در آنها و دسترسی به داده‌های حساس است.

بند پنجم: اختلال در زیرساخت‌ها

به طور کلی زیرساخت‌ها مجموعه‌ای از عناصر منسجم هستند که در صورت نابودی و اختلال در آنها امنیت فیزیکی، اقتصادی ملی یا ایمنی همگانی در معرض خطر قرار می‌گیرد (اسکندری، ۱۳۹۰: ۱۵). تروریست‌های سایبری به واسطه اخلال در زیر ساخت‌های از قبیل زیر ساخت‌های سرمایه‌ای تأسیسات و تجهیزات ساختمانها عوامل انسانی به اهداف خود دست می‌یابند.

بند ششم: دفاع سایبری

به مجموعه تدابیر امنیتی گفته می‌شود که با هدف ایمن‌سازی فضای سایبر در مقابل تهدیدات امنیتی و پیشگیری از بروز رخدادهای سایبری صورت می‌گیرد. دفاع در مقابل تروریسم سایبری می‌تواند. شامل آموزش سازو کار حقوقی و تقویت دفاعی باشد (سلامتی، ۱۳۸۷: ۱۵۷).

نتیجه گیری

در پایان مقاله حاضر و در جمع‌بندی و نتیجه‌گیری پایانی مطالب باید گفت در حقوق کیفری ایران همانند بزه تروریسم قواعد و مواد قانونی مشخص و معلومی در حقوق کیفری ایران حمایت از بزه‌دیدگان آن دیده نمی‌شود؛ بلکه در قوانینی از جمله قانون جرایم رایانه‌ای به خصوص ماده ۱۱ به طور مبهم و عام به بزهی پرداخته که با استفاده از تفسیر موسع می‌توان به جرم‌انگاری تروریسم سایبری استدلال نمود در خصوص بزه‌دیدگان مورد بحث، این نکته روشن است که بزه‌دیدگان سایبری یکی از بی‌دفاع‌ترین و بی‌گناه‌ترین اشخاصی هستند که در اثر فرایند بزه‌دیدگی متحمل خسارت‌های مادی عاطفی اجتماعی و در برخی موارد پزشکی می‌شوند، اما به دلیل برخی ویژگی‌های فضای سایبر چالش‌های تعقیب مجرمان و فقدان مقررات کافی نیازهای آنان بدون جبران باقی می‌ماند. بزه‌دیدگان تروریسم سایبری نیز به نوعی بزه‌دیده سایبری محسوب می‌گردند، بنابراین وضعیت کنونی نیازمند توجه قانون‌گذاران و سازمان‌های بین‌المللی در جهت حمایت از آنان است.

در حقوق کیفری ایران همه روش‌های پیشگیری از بزه‌دیدگی تروریست سایبری پذیرفته شده است. تروریست‌های فضای سایبر هرچند از انواع حملات و ترفندهای نوینی برای ضربه زدن به اهداف خود استفاده می‌کنند اما با نگاهی به گذشته و سیر وقوع حملات تروریستی سایبری می‌توان به این نتیجه رسید که اغلب اهداف آنها زیر ساخت‌های حیاتی کشور شرکت‌های تجاری تأسیسات وابسته به نهادهای دولتی و به طور کلی آن دسته از اهدافی را مد نظر قرار می‌دهند که طیف وسیعی از مردم یا سازمان‌های دولتی و بین‌المللی را شامل گردد؛ لذا در وهله اول به منظور پیشگیری از جرایم تروریستی سایبری با شناسایی ابزارها و شیوه‌های ارتکاب جرم از طریق فضای سایبر می‌توان به مقابله با آنها پرداخت. بنابراین بهترین راه مقابله با بحران ناشی از وقوع حملات تروریستی سایبری پیشگیری از آن است. در میان گونه‌های متفاوت پیشگیری از جرم پیشگیری وضعی از جرایم تروریسم سایبری مهم‌ترین نقش را دارد که این موضوع جای انجام یک کار پژوهشی در قالب کتاب یا مقاله ای مستقل را خواهد داشت.

منابع و مآخذ

الف) منابع فارسی

- آخوندی محمد (۱۳۸۳) قرار بازداشت موقت علوم جنایی مجموعه مقالات در تحلیل از دکتر محمد آشوری) چاپ اول تهران سمت ۸۴۰ صفحه
- اردبیلی، محمد علی (۱۳۸۱) مفهوم تروریسم گزیده مقالات همایش تروریسم از دیدگاه اسلام و حقوق بین‌الملل چاپ اول تهران مرکز مطالعات توسعه قضایی و دانشکده علوم قضایی و خدمات اداری، ۱۵۴ صفحه.
- اسکندی، حمید. (۱۳۹۰) دفاع سایبری و امنیت رایانه (۱) کلیات امنیت در فناوری اطلاعات چاپ اول، تهران: بوستان حمید ۱۰۴ صفحه.
- آقایی بهمن (۱۳۸۶) فرهنگ حقوقی بهمن چاپ سوم کتابخانه گنج دانش
- آیرم، منصور (۱۳۸۸) گزارش آشنایی با واحد اقدام ضد تروریسم سازمان امنیت و همکاری اروپا، فصلنامه سیاست خارجی، سال بیست و سوم شماره دو، صفحه ۶۰۸-۵۷۱
- محمد علی و تجیبیان، علی (۱۳۹۰) چالش‌های پیشگیری وضعی از جرم حقوقی دادگستری، سال ۷۵، شماره ۷۵ پاییز، صفحه ۱۷۳-۱۴۷
- باستانی برومند (۱۳۹۰) جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری چاپ سوم، تهران: بهنامی ۱۶۰ صفحه
- باطنی، زهره و پارجی،آبادی افسانه (۱۳۹۰) امنیت در تجارت الکترونیک و راهکارهای ارتقای آن اولین همایش منطقه‌ای رویکردهای نوین در مهندسی کامپیوتر و فناوری اطلاعات رودسر

- بزرگمهری، مجید (۱۳۸۷) تعریف سازمان ملل متحد از پدیده تروریسم مروری بر استاد مصوب و دیدگاه‌های صاحب نظران، فصلنامه مطالعات سیاسی پیش شماره ۲ صفحه ۳۲-۱۹
- تقی‌زاده انصاری، مصطفی (۱۳۸۸) سازمان جهانی پلیس جهانی اینترپل چاپ اول تهران خرسندی ۱۹۴ صفحه ۱۸
- جلالی فراهانی، امیر حسین و باقری اصل رضا (۱۳۸۷) پیشگیری اجتماعی از جرایم سایبری راهکاری اصلی برای نهادینه سازی اخلاق سایبری اطلاع‌رسانی و کتابداری ره‌آورد نور، شماره ۲۴، صفحه ۱۹-۱۰
- جلالی‌فراهانی، امیر حسین (۱۳۸۵) ب مراکز داده ضرورتی حیاتی مرکز پژوهش‌های مجلس شورای اسلامی شماره ۱۰۳۴ مهرماه صفحه ۲۸-۱
- جلالی‌فراهانی، امیر حسین (۱۳۸۴) پیشگیری از جرائم رایانه‌ای پایان‌نامه کارشناسی ارشد حقوق جزا و جرم‌شناسی، دانشگاه امام صادق ۲۴۱ صفحه
- جلالی، محمود (۱۳۸۴)، «تروریسم» از دیدگاه حقوق بین‌الملل با تأکید بر حادثه ۱۱ سپتامبر ۲۰۰۱ علوم انسانی نامه مفید، شماره ۵۲ صفحه ۸۰-۱۹
- حجتی اشرفی، غلامرضا (۱۳۹۶) قانون برنامه ششم توسعه هامش شده، تهران، گنج دانش، چاپ اول
- حسن بیگی ابراهیم (۱۳۸۵) حقوق و امنیت در فضای سایبر چاپ اول تهران مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران ۲۹۹ صفحه
- رایجیان، اصلی مهرداد (۱۳۸۳)، سه گفتار تطبیقی در بزه‌دیده شناسی داخلی منطقه‌ای و بین‌المللی، حقوقی دادگستری شماره ۴۶. صفحه ۱۹۲-۱۷۳

- روزنهان دیوید ال و سلیگمن مارتین‌ای بی؛ ترجمه: سید محمدی، یحیی (۱۳۸۹) روان‌شناسی نابهنجاری؛ آسیب شناسی روانی، جلد اول، چاپ دوازدهم تهران، ساوانان، ۵۰۶ صفحه
- طیبی فرد، امیر حسین (۱۳۸۴) مبارزه با تأمین مالی تروریسم در اسناد بین‌المللی، دفتر خدمات حقوقی بین‌المللی جمهوری اسلامی ایران، شماره ۳۲، صفحه ۳۰۶-۲۵۹
- عقیری، آدینه (۱۳۷۷) جرایم کامپیوتری جلوه‌ای نوین از بزهکاری، پایان‌نامه کارشناسی‌ارشد، حقوق جزا و جرم‌شناسی، دانشگاه تهران، ۱۳۵ صفحه
- فلمینگ، پیتر و استول مایکل؛ ترجمه: بقایی هامانه، اسماعیل و پور اردکانی عباس باقر (۱۳۸۴) سایبر تروریسم پندارها و واقعیت‌ها، چاپ دوم، تهران، لی ۲۸۵ صفحه
- کاتوزیان، ناصر (۱۳۷۴) حقوق مدنی الزام‌های خارج از قرارداد ضمان قهری، جلد اول، چاپ اول، تهران: دانشگاه تهران ۳۰۰ صفحه
- مجیدی و همکاران (۱۳۹۰) امنیت فضای تبادل اطلاعات همایش منطقه‌ای چالش‌های جرایم رایانه‌ای در عصر امروز، صفحه ۱۶-۱
- نجفی ابرندآبادی، علی حسین (۱۳۸۲-۱۳۸۱) تقریرات درس جرم‌شناسی دوره کارشناسی ارشد، نیمسال دوم تحصیلی، مجتمع آموزش عالی قم تنظیم‌کننده سیدزاده مهدی ۱۵۶ صفحه
- والتز، ادوارد؛ مترجم: رنجبر و همکاران (۱۳۸۶) جنگ اطلاعات اصول و عملیات مؤسسه آموزشی و تحقیقاتی صنایع دفاعی، چاپ دوم، تهران: طرح فرا سازمانی فاوا نیروهای مسلح ۴۵۶ صفحه.

ب) منابع لاتین

- *Clarke, R., V., 1997, Situational Crime Prevention Successful Case Studies, Second Edition, London: Harrow and Heston Pub, p. 357 .*
- *Cox, S.J., 2005, Confronting Threat Through Unconventional Means: Offensive Information Warefare as a Covert Alterntive to Preemptive War. Houston Law Review, vol 42, numb (3), 910-881*
- *Dorothy E. Denning, 2007, A View of Cyberterrorism Five Years Later, Chapter 7 in Internet Security: Hacking, Counterhacking, and Society (K. Himma ed.), Boston: Jones and Bartlett Pub, pp.19-1*
- *Dunn. Myriam, Mauer, V., (eds.), 2006, International CIIP Handbook, ETH Zurich: Center for Security Studies, Vol. II., p.181*
- *Follmar Otto, Petra and Rabe, Heike. 2009, Human Trafficking in Germany. Berlin .p. 95.German Institute For human Rights Pub.*
- *Furnell, S., 2001, Cyber Crime: Vandalizing the Information Society, London. Addison Wesley Pub, p.256*
- *Garcia-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., Vazquez, E., 2009, Anomaly-based network intrusion detection: Techniques, systems and challenges, Computers & Security Volume 28, Issues 2-1, February-March, pp. 1028-18. Gibson, W., ۱۹۸٤, Neuromancer. New York: Ace Books Pub. P ۲۸۸.*
- *Mannelqvist, R, 2010- 1957 Civil Right, Stockholm Institute for Scandinavian Law, Stockholm University Pub, pp. 434- 424.*
- *Nicholson, A, Webber. S. Dyer, S, Patel.T, Janicke. H, 2012, SCADA security in the light of Cyber-Warfare, computers & security31, pp. 436- 118*
- *System Security Study Committee., Mathematics and Applications Commission on Physical Sciences., National Research Council., ۱۹۹۰ Computer at risk: Safe Computing p. 320. in the Information age, Washington: National Academy Press*