به نام خدا

سیر تطور تروریسم سایبری در حقوق کیفری ایران

مولفان:

میترا اردشیری - مینا اردشیری

انتشارات ارسطو

(چاپ و نشر ایران)

۱۴۰۰

فهرست مطالب

درامد :

امروزه تروریسم سایبری به یکی از چالش‌های عمدهٔ نظام‌های حقوقی، به خصوص نظام‌های کیفری تبدیل شده است. بزه تروریسم، دیگر از رویکردهای سنتی خود رنگ باخته و به سوی فناوری‌های نوین روی آورده است. در بیشتر کشورهای جهان به خصوص جوامع توسعه یافته، از تأسیسات رایانه‌ای و مخابراتی در انجام امور روزمره و اجرایی کشور مانند امور اعتباری و مالی، اتوماسیون‌های اداری، کنترل و نظارت‌های زیرساختی در حوزه‌های صنعتی، نظامی، بهداشتی،

و... استفاده می‌شود. زیرساخت‌های حیاتی و اطلاعاتی، به عنوان عمده‌ترین بزه‌دیدگان تروریسم سایبری، بیشترین جذابیت و مطلوبیت را برای تروریست‌های سایبری دارند. با نگاهی به افزایش رخدادها و حمله‌های سایبری علیه بیشتر کشورهای توسعه‌یافته و بروز خسارات شدید در زیرساخت‌های حیاتی، می‌توان به فاجعه‌آمیز بودن نتایج حملات تروریستی سایبری علیه سیستم‌ها و دارایی‌های پی برد که تأثیرات شدیدی بر امنیت فیزیکی، اقتصاد ملّی یا ایمنی همگانی خواهند گذاشت.

در سال‌های اخیر استفاده از این گونه حملات، علیه تأسیسات مهم و حیاتی دولت‌ها گسترش

یافته و به دلیل خصیصهٔ پنهان ماندن هویت بزهکاران مذکور، این گونه از تروریسم مورد توجه ویژهٔ اشخاص و دولت‌ها قرار گرفته است. با در نظر گرفتن وضعیت کنونی و بالا گرفتن تنش‌های سیاسی و اقتصادی میان دولت‌ها، حمایت ویژه از بزه‌دیدگان تروریسم سایبری ضروری است. بنابراین در این نوشتار سعی بر آن شده که به بیان و تشریح اقدامات اتخاذ شده در جهت حمایت از بزه‌دیدگان مذکور در حقوق کیفری ایران و اسناد بین‌المللی پرداخته شود؛ تا به خلأهای موجود در هر دو سطح داخلی و بین‌المللی، در زمینهٔ اهتمام به بزه‌دیدگان تروریسم سایبری پی برده شود.

تروریسم یکی از عوامل اصلی و همیشگی اثرگذار در تهدید امنیت ملّی کشورها در ابعاد مختلف داخلی و خارجی بوده است. هرچند تروریسم همواره و از گذشته‌های دور به عنوان یک عامل تهدیدکنندهٔ امنیت ملّی کشورها مطرح بوده؛ اما این پدید نیز در دنیای امروزی به یکی از مهم‌ترین دغدغه‌های امنیتی ملّت‌ها و دولت‌ها در سراسر جهان تبدیل شده و تحت تأثیر تحولات جهانی شدن، دچار دگرگونی و تغییرات اساسی شده است.

امروزه رایانه به عنوان یکی از وسایل معمولی و مرسوم در جامعه تبدیل شده است که از آن برای انجام امور روزمره مانند انتقال وجوه الکترونیکی، ذخیرهٔ حجم وسیعی از اطلاعات مانند

اطلاعات پزشکی، اعتباری و مالی، اتوماسیون‌های اداری، کنترل و نظارت‌های زیرساختی در حوزه‌های صنعتی، نظامی، بهداشتی، و... استفاده می‌شود. رایانه با توانایی‌های شگفت انگیزی همچون ذخیره‌سازی اطلاعات در حجم بالا، سرعت پردازش زیاد، دسترسی آسان، خستگی‌ناپذیری و محاسن بی‌شمار دیگر، امکانات زیادی را برای بشر به ارمغان آورده است که از جهت دیگر، سبب بروز جرایم نوینی شده که در مقایسه با جرایم کلاسیک خطرناک‌تر هستند. تروریسم نیز از مدرنیزه شدن دولت‌ها تأثیر پذیرفته و اعمال و اقدامات تروریستی نیز در این راستا، جنبه‌های نوینی به خود گرفته‌اند. این تغییر در شیوه‌های تروریسم، از شیوهٔ

سنتی به شیوه‌های الکترونیکی، به یکی از بزرگ‌ترین چالش‌های جوامع مدرن تبدیل شده است. اتصال هرچه بیشتر شبکه‌های رایانه‌ای گوناگون در سراسر جهان و قرار گرفتن حجم بیشتری از اطلاعات ارزشمند بر روی این شبکه‌ها، جذابیت رایانه‌ها و شبکه‌های رایانه‌ای را به عنوان اهداف حملات تروریستی هرچه بیشتر ساخته است.

آن دسته از تهدیدکنندگانی که در این نوشتار مورد توجه قرار گرفته‌اند، تروریست‌هایی هستند که صرف نظر از ماهیت و اهداف اقداماتشان، نتایج زیان‌باری به جای می‌گذارند. تروریست‌های سایبری به طور معمول، نقاط

حساس و حیاتی جوامع را هدف قرار می‌دهند تا اساسی‌ترین ضربات را به دشمنان خود وارد کنند. دغدغهٔ اصلی تمامی مخاطبان این تئاتر وحشتناک، خسارات سنگین و بعضاً جبران ناپذیر مالی و جانی است. اشخاص یا گروه‌های تروریستی سایبری با استفاده از امکانات نامحدود و در برخی موارد حتی رایگان، قادر خواهند بود در سرتاسر جهان با فشار دادن کلیدی فضای سایبر را به مخاطره بکشانند و به واسطهٔ استخدام نیروهای متخصص در زمینهٔ فناوری اطلاعات، از جمله، نفوذگران[۱]، کرکرها[۲] و با انتشار بدافزارهای مخرب رایانه‌ای در عرض چند ثانیه، هزاران سیستم‌های رایانه‌ای و مخابراتی در

۱- Hacker

۲- Cracker

جهان را آلوده نمایند. نتایج وحشتناک بر سیستم‌های رایانه‌ای و مخابراتی که در قالب جاسوسی رایانه‌ای، سرقت داده‌ها، تخریب برنامه و داده‌های رایانه‌ای ارتکاب می‌یابد، منجر به تخریب سخت افزارهای رایانه‌ای، مختل شدن خطوط نیرو، اختلال در سیستم‌های اورژانسی، و در برخی موارد منجر به صدمات شدید جسمانی و روانی در افراد جامعه می‌گردد. با نگاهی به افزایش رخدادها و حمله‌های سایبری علیه بیشتر کشورهای توسعه‌یافته و بروز خسارات شدید در زیرساخت‌های حیاتی، می‌توان به فاجعه‌آمیز بودن نتایج حملات تروریستی سایبری علیه سیستم‌ها و دارایی‌های پی برد که تأثیرات شدیدی بر امنیت

فیزیکی، اقتصاد ملّی یا ایمنی همگانی خواهد گذاشت.

با توجه به شیوع حملات سایبری در سرتاسر جهان، لزوم توجه به بزه‌دیدگان تروریسم سایبری در حقوق موضوعه و اسناد بین‌المللی دیده می‌شود. کشور ما نیز از حملات سایبری مستثنی نبوده به طوری که در سال‌های اخیر، به دلیل شدت گرفتن مخالفت‌های سران کشورهای اروپایی و غربی به ادامهٔ فعالیت‌های هسته‌ای در ایران، حملاتی به قصد مختل کردن این تأسیسات، از سوی برخی کشورها از قبیل اسرائیل و آمریکا صورت گرفته است. در خصوص موضع حقوق کیفری ایران در مقابله با تروریسم می‌توان گفت که قانون‌گذار

کیفری ایران فاقد جرم‌انگاری مستقل در مورد تروریسم و جرایم آن است و در واقع سیاست جنایی ایران مبتنی بر سیاست مصداقی است و می‌توان مواردی را که با مفهوم ترویسم منطبق است تشخیص داد. از جمله موارد جرم‌انگاری‌شده که می‌توان برای مقابله با تروریسم استناد کرد، محاربه است و البته عده‌ای معتقدند که با جرم‌انگاری عنوان فقهی محاربه می‌توان با تروریسم و اشکال آن مقابله کرد ولی آشکار است که با توجه به گسترش فن‌آوری‌های نوین و استفادهٔ گروه‌های تروریستی از آن، دیگر محاربه قادر نیست به تمامی این رفتارها پاسخ دهد. بنابراین با توجه به ماهیت و ابزارهای مورد استفاده توسط تروریست‌های

سایبری و خلاء ناشی از قوانین کیفری و غیرکیفری، تلفات و خسارت‌های زیان‌بارتری را نسبت به دیگر انواع تروریسم متحمل خواهیم شد. گستردگی فضای سایبر و به خدمت گرفتن آن توسط اکثر افراد جامعه و زیرساخت‌های کشور، طیف گسترده‌ای از مباحث را پیرامون بزه‌دیدگان این پدیده و چگونگی حمایت و جبران خسارت‌های وارد آمده به آن‌ها را چه در حقوق داخلی کشورمان و کشورهای دیگر و چه در سطح بین‌الملل شکل داده است.

در این میان آن چه از اهمیت ویژه‌ای برخوردار است، توجه به بزه‌دیدگان تروریسم سایبری است که به نوعی بزه‌دیدهٔ سایبری محسوب می‌شوند و

نمی‌توان همانند دیگر انواع بزه‌دیدگان تروریسم، به دلیل موقعیت و مکان بزه که در دنیای مجازی قرار دارند، با شیوه‌ای یکسان از آن‌ها حمایت نمود. بدین منظور در سال‌های اخیر، جرم‌شناسان خارجی و افراد دیگری به شاخه‌ای جدید از بزه‌دیده‌شناسی، به عنوان بزه‌دیده‌شناسی سایبری، به منظور تبیین نقش افراد جامعه و محیط سایبر در شکل‌گیری بزه‌های رایانه‌ای پرداخته‌اند. بر این اساس پرداختن به نیازهای بزه‌دیدگان تروریسم سایبری و همچنین اقدامات و روش‌های پیشگیری از این بزه به منظور حمایت بیشتر از بزه‌دیدگان ضروری به نظر می‌رسد. با توجه به مطالعات اولیه، این موضوع در حوزۀ جرم شناسیِ بزه‌دیده‌شناسی

و حقوق جزای اختصاصی جای می‌گیرد. بدین منظور در نوشتار حاضر، به تبیین تروریسم سایبری و روش‌های ارتکاب آن، بررسی قوانین موجود در زمینهٔ تروریسم سایبری در حقوق داخلی ایران و اسناد بین‌المللی، پیشگیری از وقوع تروریسم سایبری و حمایت از بزه‌دیدگانی که در اثر حملات تروریستی سایبری، خسارت و صدمه می‌بینند می‌پردازیم.

بنابراین مطالب این نوشتار بر اساس سه فصل بررسی می‌شوند. در فصل اول، به کلیات و مفاهیم رایانه‌ای و حقوقی مرتبط با موضوع مورد بحث پرداخته می‌شود. در فصل دوم، به طور تخصصی وارد موضوع بحث شده و به روش‌های پیشگیری از

وقوع تروریسم سایبری در راستای حمایت از بزه‌دیدگان تروریسم سایبری در حقوق کیفری ایران و اسناد بین‌المللی پرداخته می‌شود و در فصل سوم، به عنوان آخرین فصل این نوشتار، به انواع حمایت‌های موجود در حقوق کیفری ایران و اسناد بین‌المللی در زمینهٔ حمایت از بزه‌دیدگان تروریسم سایبری اشاره می‌گردد.

با توجه به رشد روز افزون دانش بشری در زمینهٔ فناوری اطلاعات و ارتباطات و همچنین درگیر شدن هرچه بیشتر جوامع به استفاده از این ابزارها و پیشرفت‌های دیگری که در اثر به‌کارگیری 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 غیرقابل انکار است. این تغییر در شیوه‌های تروریسم، از شیوهٔ سنتی به شیوه‌های الکترونیکی، به یکی از بزرگ‌ترین چالش‌های جوامع مدرن تبدیل شده است.

اتصال هر چه بیشتر شبکه‌های رایانه‌ای گوناگون در سراسر جهان و قرار گرفتن حجم بیشتری از اطلاعات ارزشمند بر روی این شبکه‌ها، جذابیت رایانه‌ها و شبکه‌های رایانه‌ای را به عنوان اهداف حملات تروریستی سایبری هرچه بیشتر ساخته است. بنابراین روز به روز انگیزهٔ مهاجمین احتمالی برای آغاز حمله علیه اهداف سایبری افزوده

می‌گردد. انگیزه‌های اقتصادی، صنعتی و نظامی در این میان از همه چشمگیرتر به نظر می‌رسند. بارزترین ویژگی فضای سایبر، دسترس‌پذیر ساختن سریع با حداقل هزینهٔ کلیهٔ اطلاعات آنلاین است که بسیاری از نمونه‌های آن را در تارنماهای شبکه جهانی اینترنت شاهد هستیم. این دسترس پذیری، برای همگان فراهم آمده و هیچ گونه تبعیضی اعمال نشده است. با وجود این شرایط، به نظر می‌رسد در متزلزل شدن برخی مفاهیم حساس و اساسی، به ویژه امنیت، تردیدی باقی نمانده باشد. امنیت همانند فضای سایبر، آنقدر انعطاف پذیر است که در هر سطح و کیفیتی، معنا و کاربرد خود را حفظ می‌کند. آن دسته از تهدیدکنندگانی که

در این پژوهش مورد توجه قرار گرفته‌اند، تروریست‌هایی هستند که صرف نظر از ماهیت و اهداف اقداماتشان، نتایج زیان‌باری به جای می‌گذارند. معمولاً آن‌ها نقاط حساس و حیاتی جوامع را هدف قرار می‌دهند تا اساسی‌ترین ضربات را به دشمنان خود وارد کنند و با توجه به ماهیت شبکه‌های اینترنتی که در دسترس همگان قرار دارد، اهداف و نتایج فعالیت‌های خود را در عرض کوتاه‌ترین زمان در سطح جهان اطلاع رسانی کنند [۱].

۱- کلاریک، اندرو. ام، و یانچوسکی، لخ.، ترجمه: نژاد شلمانی، ابراهیم. (۱۳۸۹). **مقدمه ای بر جنگ سایبر و تروریسم سایبر**، چاپ اول. تهران: بوستان حمید

البته سهولت و کم هزینه بودن ارتکاب این اقدامات نیز از اهمیت قابل توجهی برخوردار است، لذا این گروه‌ها همواره به پیشرفته‌ترین ابزارها برای رسیدن به اهداف شوم خود مجهز هستند.

با اینکه پیشینهٔ اقدامات تروریستی به اندازهٔ عمر بشر طولانی است، اما نه تنها هیچ‌گاه دربارهٔ آن اتفاق نظر وجود نداشته، بلکه معانی بعضاً متعارضی به آن نسبت داده شده است. عده‌ای آن را تاکتیک و دیگران استراتژی دانسته‌اند. برخی آن را جنایت و گناهی نابخشودنی و گروهی وظیفهٔ الهی و واکنش موجه به ظلم و ستم برشمرده‌اند. در هر حال قدر مسلم این است که تروریسم ابزاری

برای رسیدن به هدف است. در این راستا کارشناسان، تروریسم را این گونه نموده است:
«ارتکاب هدفمند خشونت یا تهدید به آن، به منظور ایجاد وحشت و یا رفتار مقهورانه در قربانی و یا در ناظران آن عمل یا تهدید» [1]

اما دغدغهٔ اصلی تمامی مخاطبان این تئاتر وحشتناک، خسارات سنگین و بعضاً جبران ناپذیر مالی و جانی است، آن هم از جانب کسانی که به خوبی برای این نقش آفرینی کرده‌اند و حتی حاضرند برای رسیدن به اهدافشان، از ارزشمندترین سرمایه‌شان، یعنی جانشان بگذرند؛ لذا ایستادگی در برابر یا به حداقل رساندن

۱- طیب، علیرضا. (۱۳۸۴). **تروریسم، تاریخ، جامعه شناسی، گفتمان، حقوق**، چاپ دوم. تهران: نی.

خساراتشان، بدون برنامه ریزی اصولی و راهبردی نه تنها نتیجه بخش نیست؛ ممکن است منجر به تشدید این گونه اقدامات نیز بشود. آن چه در این راستا بیشتر مورد توجه قرار دارد، بزه‌دیده است. بزه دیده کسی است که: «به دنبال رویداد یک جرم آسیب و زیان و آزار می‌بیند»[1]

در این خصوص باید با همدردی و احترام و عزت و شرف انسانی با قربانیان جرایم تروریستی رفتار کرد. آن‌ها حق دارند به خاطر لطمه‌ای که دیده‌اند و به صورتی که در قانون مقرر شده است، به سازوکارهای اجرای عدالت و جبران غرامت فوری دسترسی داشته باشند. به این منظور که

۱- رایجیان اصلی، مهرداد. (۱۳۹۰) الف. **بزه‌دیده شناسی حمایتی**، چاپ دوم. تهران: دادگستر

قربانی بتواند به جبران غرامت خود دست یابد، باید سازوکارهای قضایی و اجرایی را نیز مقرر و تقویت نمود. تجربه در بسیاری از کشورها نشان داده است که یک راه مؤثر برای رسیدگی به نیازهای متعدد قربانیان جرایم تروریستی به خصوص این نوع خاص از تروریسم، وضع برنامه‌هایی است که حمایت اجتماعی، روان‌شناختی، عاطفی و مالی را فراهم سازند و در حیطهٔ نهادهای اجتماعی و عدالت کیفری به طور مؤثر به قربانیان کمک کنند.[1] بعضی کشورها علاوه بر مقرراتی که به قربانی اجازه می‌دهد علیه مرتکب جرم اقامهٔ دعوی کند، قوانینی را وضع کرده‌اند که حق قربانی برای

۱- نمامیان، پیمان. (۱۳۹۰). **واکنش‌های عدالت کیفری به تروریسم**، چاپ اول. تهران: میزان

جبران خسارت و شرکت در جلسات دادرسی را به رسمیت شناخته اند؛ این امکانات باعث بازشناسی درد و رنج قربانی می‌شوند .

فصل اول:

مفهوم شناسی، تاریخچه، عناصر تروریسم سایبری

اقدام تروریستی سایبری را بیشتر در زمره بزه‌های رایانه‌ای می دانند[۱]، زیرا در بروز کنش تروریستی، همچون دیگر بزه‌های رایانه‌ای، رایانه و اینترنت هم

---

۱ - Lewis, Brian C; **Prevention of cyber crime admist international anarchy**, American criminal law review, vol ۴۱, ۲۰۰۴, p.۱۳۵۵

در نقش موضوع بزه نمود می‌یابد و هم افزار آن. در نگاه دیگر، بسیاری از بزه‌های رایانه‌ای به ویژه دستیابی غیرمجاز و خراب‌کاری، خود شیوه‌های ارتکاب تروریسم سایبری به شمار می‌رود؛ زیرا تروریسم سایبری از رخنه‌ی غیرمجاز به سیستم یا شبکه توسط خراب‌کاران رایانه‌ای می‌آغازد و به اخلال در سیستم‌های حیاتی و زیرساخت‌های اطلاعاتی و حتی پیامدهای فاجعه باری چون یورش‌های شیمیایی، میکروبی و هسته‌ای می-انجامد. این ادعا در پرتو این پرسش که « *چرا تبهکاران تروریسم رایانه‌ای (سایبر تروریسم) مرتکب جرایم رایانه‌ای نمی‌شوند*»[1]، شفاف‌تر می-

---

۱- فلمینگ پیتر و استول مایکل؛ **سایبر تروریسم: پندارها و**

شود و از همین جا روشن می‌گردد که تروریست-های رایانه‌ای، بزهکارانی نیستند که بتوان ارتکاب بزه‌های رایانه‌ای را از آنها چشم داشت. از این رو برخی تروریسم سایبری را در زیر بزه‌های رایانه‌ای جا نمی‌دهند؛ چون « *بزه چهره شخصی داشته و به شُوندهای(دلایل) فردی و شخصی ارتکاب می-یابد، ولی تروریسم جنبه سیاسی دارد و هرچند رفتارها و نشانه‌های آن با بزه جداناشدنی است ولی تنها با انگیزه‌های سیاسی ارتکاب می‌یابد.*»[1] ولی

واقعیت ها، برگردان اسماعیل بقایی هامانه و عباس باقر پور اردکانی، در مجموعه تروریسم ، گردآوری و ویرایش علیرضا طیب، نشر نی، چاپ دوم، ۱۳۸۴، ص ۱۵۶

۲-Brenner, Susan W; **Cybercrime, cyberterrorism and cyberwarfare**, International review of penal law: cybercrime, AIDP, volume ۷۷, ۲۰۰۶, p.۴۵۷

پیش از اینکه پیوند تروریسم سایبری با بزه رایانه-ای پیش آید، باید دانست هستیِ این گونه از تروریسم، خود گمان‌آور است؛ چه تروریست‌ها «*از اینترنت و رایانه برای تبلیغ و خبرپراکنی، گزینش نیروی انسانی، داده‌کاوی*[1] *و دیگر انگیزه‌ها بهره می‌جویند*»[2] وگرنه اقدام‌های برجسته‌ی تروریستی که دربردارنده خشونت و از بین بردن است، در فضای سایبر شدنی نیست.

مرتکب تروریسم سایبری با انگیزه‌های پیوندیافته با باورهای سیاسی، مذهبی، میهن‌پرستانه و مانند آن به اخلال در سیستم‌ها و شبکه‌های رایانه‌ای می-

---

۳- Data mining

۴- Walker, Clive; **Cyber-Terrorism: legal principal and law in the United Kingdom**, Penn state law review, volume ۱۱۰, ۲۰۰۵-۲۰۰۶, p.۶۳۴

کوشد و از این رو بر وارونه‌ی بزهکار رایانه‌ای، اقدام‌های آشوبگر و اخلال‌کننده‌ی آنها از پیش تصمیم‌گیری شده است. « *برعکسِ آنچه که بزهکار رایانه‌ای بزهش را پنهان نگه می‌دارد، تروریست رایانه‌ای افزون بر شناساندن خود، تلاش دارد خواسته‌های مذهبی، عقیدتی، سیاسی و اجتماعی خود را با پدید آوردن هراس در فضای سایبر یا از رهگذر آن پیش کشد.*»[۱]

واژه سایبر تروریسم از دهه هشتاد بر زبانها افتاد، ولی پیش از آن اقدام‌های تروریستی از رهگذر

۱- Matusitz, Jonathan A; **Cyberterrorism: A postmodern view of networks of terror and how computer security experts and law enforcement officials fight them**, UMI dissertation services, University of Oklahoma, ۲۰۰۶, p.۱۹ and ۲۰

رایانه رخ داده و به دهه هفتاد بر می‌گردد؛ « *زمانی که بریگاد سرخ طی این دهه در ایتالیا ۱۱ عدد از تاسیسات اصلی پردازشگرهای ارتباطی را تخریب کردند. میزان خسارت وارده پانصد هزار دلار تخمین زده شد. این گروه طی انتشار بیانیه‌ای استفاده روز افزون از رایانه را بخشی از یک توطئه جهت بیشینه کردن نظارت‌های اجتماعی برشمردند. به نظر این گروه ، رایانه‌ها به مثابه ابزاری جهت درگیری‌های طبقاتی به شمار می-رفتند و از این رو لازم بود تا این شبکه‌های نظارت مورد حمله قرار گرفته و از بین بروند.*»[۱]

۲- ماتئو وارن، ویلیام هاچینسون؛ **تروریسم شبکه‌ای**، برگردان غلامرضا رفعت نژاد، گزارش راهبردی، انتشارات پژوهشکده مطالعات راهبردی، ، ۱۳۸۲ ، ص ۶

به هر حال اقدام‌های تروریستی سایبری چهره نوین تروریسم است و بری کالین[1] که گفته می-شود واژه سایبر تروریسم را برای نخستین بار پیشنهاد داده، آن را این‌گونه تعریف کرده است: « *سوء استفاده عمدی از یک سیستم، شبکه یا مولفه اطلاعاتی رایانه ای برای تحقق هدفی که موید یا تسهیل کننده مبارزه یا اقدام تروریستی است.*»[2] برخی از نویسندگان نشانه‌ها و نتیجه‌های بیرونیِ کنش‌های تروریستی در فضای سایبر را نیز در تعریف خود گنجانده اند؛ به گفته کانوی[3] از نظریه-پردازان آمریکایی در زمینه تهدیدهای سایبری، «

۳- Barry Collin

۴- فلمینگ پیتر و استول مایکل، پیشین، ص ۱۵۳

۳ - Conway

تروریسم سایبری عبارت است از یورش عمدی و آگاهانه با انگیزه‌های سیاسی به وسیله گروه‌های فروملی یا عامل‌های پنهانی برضد اطلاعات، سیستم های رایانه ای، برنامه‌های رایانه ای و داده، که منتهی به خشونت بر ضد کسان غیر نظامی و دیگر هدف‌ها شود.»[۱]

انجام اقدام تروریستی بر ضد شبکه‌ها، سیستم‌ها و اطلاعات یا بهره‌گیری از فضای سایبر برای تروریسم در جهان فیزیکی، به چهار دلیل برای تروریست‌ها مهم است: « *پایین بودن هزینه‌های*

---

۱ - Ozeren, Suleyman; **Global response to cyberterrorism and cybercrime: A matrix for international cooperation and vulnerability assessment**, UMI dissertation services, university of north texas, august ۲۰۰۵, p.۲۸

ارتکاب از فراهم ساختن رایانه گرفته تا طراحی برنامه های آماده سازی خدمات دروغین، دشواری در ردیابی یا دستگیری مرتکب، نبودِ رویارویی حضوری به دلیل نبود محدوده‌ای مشخص برای انجام اقدام تروریستی و دست‌آخر بودِ هدف‌ها و قربانیان گوناگون در یک زمان.»[۱] از همین رو محدوده‌ی اقدام‌های تروریستی سایبری به اندازه‌ای گسترده است که رایانه در جهت ارتکاب آنها، هم نقش‌افزار را دارد و هم نقش هدف یا موضوع. رایانه زمانی افزار بزه است که تروریست‌ها از رهگذر آن مرام و هدف‌های خود را تبلیغ می‌کنند یا با کمک

---

۱ - Nigel, Phair; **Cybercrime; the reality of the threat**, E-security Publishing, Canberra, ۲۰۰۷, p. ۱۴۶

آن شیوه‌ی انجام اقدام‌های تروریستی را می‌آموزانند. در اینجا اقدام‌های تروریستی سنتی با کمک رایانه ارتکاب می‌یابد؛ برای نمونه « *عبدالله قریشی یکی از هواخواهان اسامه بن لادن، در سال ۲۰۰۰ گروه خادمان بن لادن(OLB) را در اروپا بنیاد نهاد که کار اصلی این گروه طراحی و راه انداختن پایگاه‌های اینترنتی برای آفرینش اطلاعاتی پیرامون ساخت جنگ‌افزار، افزارهای انفجاری دستی و نیز تبلیغ و آگاهی‌رسانی برای گروه القاعده بود.*»[۱]

---

۱ - Colarik, Andrew M; **Cyber terrorism**: political and economic implication, Idea Group Publication, ۲۰۰۶, p.۵۱

رایانه هنگامی به عنوان موضوع یا هدف اقدام تروریستی مطرح می‌شود که اطلاعات یا سیستم‌ها یا شبکه‌ها در پی یورش مجازی تروریست‌ها دچار آشفتگی شده یا از میان بروند. اقدام‌های تروریستیِ سایبریِ محض، یعنی جایی‌که فضای سایبر خود موضوعِ مستقیم بزه است، ممکن است به صورت-های گوناگونی انجام یابند. برجسته‌ترین روش، به نام *عامل تشدید کننده وضعیت(یا ضریب افزاینده نیرو)*[1] است که کنش‌های تروریستی سایبری به دنبال اقدام‌های خرابکارانه سنتی انجام می‌شود؛ « *مانند یورش دیجیتالی به زیرساخت‌های ارتباطاتی حیاتی به دنبال یک بمب‌گذاری یا حمله*

---

۱ - Force Multiplier

شیمیایی.»[۱] روش دیگر، هدف قرار دادنِ سیستم یا شبکه، ناتوان‌سازی از رهگذرِ پخش ویروس‌ها، کرم‌ها یا دیگر نرم‌افزارهای پخش‌کننده در فضای سایبر است که گفته می‌شود با این روش، « *خسارتی بالغ بر پانزده هزار میلیون دلار بر اقتصاد جهانی وارد می شود.*»[۲] مهمترین بخش از یورش-های ویروسی از طریق پست‌های الکترونیکی آلوده انجام می‌گیرد که اندازه آنها روز به روز در حال افزایش است. کرم‌ها نیز همانند ویروس‌ها توانایی مختل کردن سیستم را دارا هستند؛ برای نمونه، «

---

۱ - Podesta, John D and Goyle, Raj: **Lost in cyberspace? Finding American liberties in a dangerous digital world**, Yale law and policy review, volume ۲۳, ۲۰۰۵, p.۵۱۷

۲ - Embar-Seddon,Ayn; op.cit, p.۱۵

کرم رایانه‌ای نیمدا که به دلیل تأثیرگذاری مخرب بالای آن و همچنین برخورداری از قابلیت‌های دیگر، مانند ویروس تروجان به کرم چهارسر معروف است. معروفیت این کرم رایانه‌ای بیشتر به زمان انتشار آن مربوط می‌شود که درست یک هفته پس از واقعه یازدهم سپتامبر ۲۰۰۱ منتشر شد و خسارات زیادی را به ویژه به سیستم‌های رایانه‌ای ایالات متحده، بریتانیا و هنگ‌کنگ وارد آورد. با این‌حال، دادستان کل امریکا، جان اشکرافت اظهار داشت دلیلی مبنی بر ارتباط این کرم با حملات یازدهم سپتامبر در دست نیست.»[1]

---

۱ - جلالی، امیرحسین؛ **تروریسم سایبری**، فصلنامه تخصصی فقه و حقوق؛ شماره ۱۰؛ پاییز ۱۳۸۵، ص ۹۶

رخنه‌گری غیرمجاز به سیستم رایانه‌ای[۱] و انجام رفتارهای بزهکارانه در آن[۲] از دیگر روش‌های شناخته شده برای ارتکاب اقدامات تروریستی است. در این روش مرتکب با نفوذِ فنی (هک) یا با نفوذِ شفاهی (مهندسی اجتماعی[۳]) بخش‌های آسیب-پذیر سیستم یا شبکه را شناسایی کرده تا در زمان مناسب آن را از کار بیندازد یا اطلاعات را دگرگون سازد یا از بین ببرد و یا اینکه مانع دسترسی به داده یا سیستم و در نتیجه کارآیی آنها شود. جدا از مهندسی اجتماعی، هک صرف رخنه‌ی غیر مجاز به سیستم است که در گام نخست چهره کیفری

---

۱ - Hacking
۲ - Cracking
۳ Social engineering

ندارد اما خرابکاری رایانه‌ای[1] چهره کیفری هک است که مرتکب با قصد ربایش داده یا دگرگون ساختن آن یا جابجایی اطلاعات، به اقدام‌های بزهکارانه دست می‌زند و از این رو تروریست سایبری شخصی است که « *با انگیزه‌های سیاسی و اجتماعی، مهارت‌های هک را به خدمت می‌گیرد.*»[2]

اقدام‌های تروریستی سایبری روی‌هم‌رفته به چهار شیوه انجام می‌شوند: « *الف- یورش به اطلاعات که همان دگرگونی یا از میان بردن محتوای فایل-های الکترونیکی، سیستم‌های رایانه‌ای یا محتویات گوناگون موجود در آنها است. ب- یورش به زیرساخت که بر پایه آن، مرتکب، سخت‌افزارها،*

---

۱ - Cracking
۲ - Embar-Seddon,Ayn; op.cit

پایگاه‌های عملیاتی یا برنامه‌های محیط رایانه را مختل می‌کند یا از بین می برد. ج- معاونت فنی در ارتکاب که عبارت است از به کارگیری ارتباطات الکترونیکی برای فرستادن نقشه‌ها و طرح‌ها به منظور انجام یورش‌های تروریستی یا تحریک به انجام آنها یا توسل به سایر تسهیلات. د- افزایش یا ارتقای منابع مالی که به موجب آن تروریست‌ها با بهره‌گیری از اینترنت برای خشونت سیاسی یا دیگر رفتارها، به گرفتن کمک‌های مالی افراد یا سازمان-ها می‌کوشند.»[۱]

۱- Ballard, James David and Hornik, Joseph G and Mckenzie, Douglas; **Technological facilitation of terrorism**, in Cyberterrorism, edited Alan Oday, Ashgate publishing company, ۲۰۰۴, p.۵۹

رکن روانی اقدام‌های تروریستی نیز همچون روش ارتکاب آنها گوناگون بوده و تروریست‌ها با انگیزه-های چندی در فضای سایبر حضور می‌یابند که از جمله آنها می‌توان به « *طرح‌ریزی (مانند گرد-آوری اطلاعات، تجزیه و تحلیل آنها و تجهیز به نرم‌افزار پیشرفته و کمک‌رسان)، تامین یا تراکنش-های مالی (همچون به دست آوردن کمک‌ها و بخشایش‌های هواخواهان، انتقال پول، پولشویی)، هماهنگی برای اجرای عملیات (مانند فرستادن نشانه‌ها یا رمزهای عملیات و بسیجیدن نیروها)، اقدام‌های سیاسی (مانند بازگویی قصدها و هدف-های سیاسی) و تبلیغ و آموزش انگشت نهاد.*»[۱]

---

۱ - Cohen, Fred; **Terrorism and cyberspace**, in Cyberterrorism, edited Alan Oday, Ashgate

گابریل وایمن[1] پژوهشگر اسرائیلی، برای نشان دادن اندازه و شیوه‌های بهره‌گیری از فضای سایبر می‌گوید: «*گروه‌های مسلمان در ابتدای فعالیت روی اینترنت دوازده سایت داشتند اما این تعداد در انتهای سال ۲۰۰۳ به ۴۰۰ سایت افزایش یافت. وی نشان داده که چگونه طراحان یازهم سپتامبر از اینترنت برای یافتن اطلاعات ارزشمندی به منظور هواپیماربایی از قبیل چگونگی سوخت گیری، تعداد مسافران ثبت شده و مانند آن بهره برداری کرده اند.*»[2]

---

publishing company, ۲۰۰۴, p.۱۵۰-۱۵۱

۱- Gabrielle Weiman

۱- بازگفت از کلهر، رضا؛ **جهاد مجازی: ماهیت و چالش ها**، فصلنامه مطالعات منظقه ای جهان اسلام، شماره ۳۲، سال هشتم، ۱۳۸۶، ص۳۱

اقدامات تروریستی سایبری هر چند به طوری که به چشم آید، رخ نداده ولی نمونه‌هایی از آن مانند خاموشی برق در ایالات متحده در سال ۲۰۰۳ در اثر دستکاری در سیستم رایانه‌ای اداره برق هشداری است برای آینده که تروریستها با انگیزه-های گوناگون می‌توانند وارد سیستم رایانه‌ای جاهای حساس مانند کارخانه‌های داروسازی، بیمارستانها، سازمان‌های مربوط به آب و برق و مانند آن در سیستم‌ها و شبکه‌ها، آشفتگی و پریشانی پدید آورند که چه بسا نشانه‌های وخیمی از جهت سلامت و بهداشت همگانی به همراه داشته باشد. به همین دلیل دولتها جدا از جرم-انگاری (مانند استرالیا که در ماده ۴۷۷ از قانون

جرایم سایبری مصوب ۲۰۰۱ در سرلوحه بزه های برجسته و خطرناک سایبری به ارتکاب آگاهانه رفتارهایی چون رخنه‌گری غیر مجاز، تغییر داده و اختلال در سیستم بر ضد سلامت و بهداشت عمومی و دولت پرداخته است.[1] و یا پاکستان در

۲- در بخش مزبور آمده است: هر کس به طور عمد و با آگاهی از سیستم ها و داده‌های مرتبط با بهداشت عمومی یا دولتی یا سرزمینی مرتکب یکی از جرایم زیر شود به مجازات جرایم مهم (از ۵ سال حبس تا ابد) محکوم خواهد شد:

۱- الف- چنانچه شخص به داده های نگهداری شده در سیستم مرتبط با بهداشت عمومی یا داده‌های دولتی به طور غیر مجاز دست یابد یا ب – به طور غیر مجاز آنها را تغییر دهد یا ج- یا بدون مجوز باعث اختلال در سیستم ارتباطی شود.

۲- چنانچه شخص بدون مجوز به خدمات ارتباطی و مخابراتی دست یابد یا آنها را تغییر دهد یا موجب اختلال در آنها شود. برای جرایم موضوع این بخش پاسخدهی (مسوولیت) مطلق پیش‌بینی شده است.

سال ۲۰۰۸) چاره‌اندیشی‌های ویژه‌ای برای مبارزه با اقدام‌های تروریستی سایبری در دستور کار قرار داده‌اند.

قانونگذار ایران، هنوز به طور راستین اقدام تروریستی را به عنوان یک بزه جداگانه و ناوابسته از دیگر بزه های امنیتی، پیش بینی نکرده است؛ از این رو نمی توان چشم داشت که اقدام تروریستی سایبری که خود گونه ای از اقدام تروریستی است، را در قانون های کیفری جای داده باشد. با این حال ماده ۱۱ قانون جرایم رایانه ای ، بدون نام بردن از اقدام تروریستی یا تروریسم، بزهی را پیش بینی می کند که بسیار نزدیک به تروریسم سایبری است و آن اخلال رایانه ای همراه با قصد

است. همسان با این بزه، در مقرره های سنتی ایران، می توان به ماده ۶۸۷ قانون مجازات اسلامی انگشت نهاد. بر پایه این ماده، هر کس در وسایل و تاسیسات مورداستفاده عمومی از قبیل شبکه های آب و فاضلاب ، برق ، نفت ، گاز ، پست و تلگراف وتلفن و مراکز فرکانس و ماکروویو (مخابرات) و رادیو وتلویزیون ومتعلقات مربوط به آنها اعم ازسد و کانال وانشعاب لوله کشی ونیروگاههای برق وخطوط انتقال نیرو و مخابرات (کابلهای هوای یا زمینی یانوری) و دستگاههای تولید وتوزیع وانتقال آنها که به هزینه یا سرمایه دولت یا با سرمایه مشترک دولت و بخش غیر دولتی یا توسط بخش خصوصی برای استفاه

عمومی ایجاد شده وهمچنین در علائم راهنمایی و رانندگی و سایر علائمی که به منظور حفظ جان اشخاص یاتامین تاسیسات فوق یا شوارع و جاده ها نصب شده است ، مرتکب تخریب یا ایجاد حریق یا از کارانداختن یا هر نوع خرابکاری دیگر شود بدون آنکه منظور او اخلال در نظم وامنیت عمومی باشد به حبس از سه ماه تا ده سال محکوم خواهد شد.

ماده۱۱ قانون جرایم رایانه ای (ماده ۷۳۹ قانون مجازات اسلامی) پیش بینی می کند: « **هرکس به قصد خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری**

عمومی به کار می‌روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری مرتکب شود، به حبس از سه تا ده سال محکوم خواهدشد.»

۱-۱- رفتار : اخلال و تخریب

رفتارهای موضوع ماده ۷۳۹، همان رفتارهای پیش بینی شده در ماده های ۸ (حذف یا تخریب یا مختل یا غیرقابل پردازش کردن)، ۹(از کار انداختن و مختل کردن کارکرد) و ۱۰(مانع شدن از دسترسی) قانون جرایم رایانه ای (ماده های ۷۳۶ و ۷۳۷ و ۷۳۸ قانون مجازت اسلامی) است. بدین حال، از جهت رفتاری، بزه موضوع ماده ۷۳۹،

هیچ چیزی پیش بینی نکرده است و از جهت منطقی بهتر می بود که ماده ۷۳۹ که تنها بر قصد مرتکب و نیز گونه سامانه هایی که تهدید می شوند را سنجه ای برای افزایش کیفر بزهکار قرار می داد؛ زیرا بزه ها به رفتار شناخته می شوند و بزه موضوع ماده ۷۳۹ نیز رفتار جداگانه ای ندارد و برگرفته از همان رفتار بزه های دیگر است. نکته مهم در وابستگی رفتاری بزه موضوع ماده ۷۳۹ این است که در صورتی که این بزه رخ دهد، دیگر به جهت اینکه رفتار مرتکب که به طور جداگانه می تواند موضوع یکی از مواد سه گانه پیش گفته باشد، تعدد مادی یا معنوی در کار نیست. پس اگر مرتکب با قصد خاص پیش بینی شده در ماده

۷۳۹، اخلال یا تخریب یا ممانعت از دسترسی را بر روی سامانه های ارایه دهنده خدمات ضروری انجام دهد، تنها مرتکب بزه موضوع ماده ۷۳۹ شده است و گزاره های تعدد بزه جاری نیست؛ زیرا قانونگذار رفتار بزهی را با پیش بینی شرایط نوین برای بزه دیگر قرار داده است.

نباید پنداشت که رفتارهای تروریسم سایبری، تنها تخریب، اخلال و مانع دسترسی شدن است؛ بلکه تروریسم سایبری با رفتارهای چندگانه ای شناسانده می شود. پدیده تروریسم سایبری، در بستری بنیاد گرفته و پیشرفت کرده که خودِ قانونگذاری های کیفری و سیاست دولتها با برجسته کردن این عنوان به عنوان شاخه ای نوین

از تروریسم، زمینه ساز شکل گیری این بستر بوده اند. به راستی که برای دانستن بستر تروریسم سایبری باید از خود پدیده تروریسم آغاز کنیم.

خاستگاه تروریسم و علت های آن همواره چالش زا بوده است و با آنکه سیزده سند بین المللی برای پیکار با این پدیده آمده، ولی این چالش برطرف نگردیده است. پس از رخداد یازدهم سپتامبر ۲۰۰۱ که با بهره گیری از پیشرفت فضای مبادلات الکترونیکی همزمانی پیدا کرده بود، تروریسم به ویژه در قانون های داخلی کشورها، فراتر از اندازه عادی و بایسته پیش کشیده شد؛ با این حال تروریسم سایبری همواره در دل تروریسم پیش بینی می شد و جدا از اینکه خود تروریسم هنوز از

جهت هستی، گمان آور و ناپذیرفتنی بود ولی به دنبال تصویب پشت سر هم قانون های ضد تروریسم در بسیاری از کشورهای جهان، جای پایی گذاشت.

تروریسم سایبری در اندک زمانی برجسته و با رفتارهای چندی شناسانده شد. این چالش درباره خود تروریسم نیز بود. به راستی پیچیدگی بزه‌های هراس‌آور در حقوق کیفری از دید شمار رفتارهایی است که در زیر این دسته جا می‌گیرند؛ زیرا ریشه بزه‌های تروریستی به تروریسم بر می‌گردد که واژه-یی سیاسی- اندیشه ای است و برخی همین واژه را بی‌کم وکاست به درون گفتارهای حقوق کیفری آورده‌اند و چنین پنداشته‌اند که واژه "تروریسم"

خود عنوان مجرمانه‌ای که خواست حقوقدانان از برخی دهشت‌افکنی‌ها و دژرفتاری‌ها است را می-نمایاند. در حالی که در واژه "تروریسم" معناها و پندارهای سیاسی و گرایش‌های کیشی و اندیشه‌ای نهفته است و از این رو تروریسم در حقوق کیفری نمی‌تواند جایگاهی داشته باشد. سندهای بین-المللی مانند کنوانسیون بین‌المللی سرکوب رفتارهای دهشت‌افکنانه هسته‌ای ۲۰۰۵ ،گرایش در به کارگیری " اقدامات تروریستی" داشته اند تا به گونه‌ای بر رفتارهای سرزنش‌آمیز که در این دسته جا می‌گیرند، پافشاری کنند. ولی بر همین واژه‌ی " اقدامات تروریستی" این خرده را می‌توان گرفت که آیا چه رفتارهایی را دربر می‌دارد و

چگونه بزه‌های تروریستی در قانون‌های کشورها و نیز سندهای بین‌المللی این همه گوناگون و پرشمار است؟

پاسخ را می‌توان در دست‌درازی دولت در نهادهای قانونگذاری و داوری(قضایی) یافت. پس از فروکش کردن آتشِ جنگهای بین کشورها در سال‌های واپسین سده بیستم، برجسته‌ترین دشمن انسانی دولت‌ها، بزهکاران سازمان‌یافته داخلی و بین‌المللی بودند که به سان بازیگران بین‌المللی در برخی رویارویی‌ها، خود را هم‌اندازه و هم‌آورد دولت‌ها شناساندند تا جایی که نگرانی همه دولت‌ها را به دنبال داشته و در سال‌های کنونی، بیشترین تلاش‌های سیاسی و حقوقی در پیکار با سه پدیده-

ی اقدامات تروریستی، قاچاق و فساد که بیشتر سرشت سازمان یافته داشتند، به کار گرفته شد. در این میان چاره اندیشی‌های سیاسی از راهکارهای حقوقی پررنگ‌تر بود و در سایه سیاست دولت‌ها واژگان کارشناسی ناشده و خرده‌پذیری چون بزه-های سازمان‌یافته بر زبان ها افتاد در حالی که اینها از ریشه، جرم به شمار نمی‌روند. عنوان‌های دیگری مانند فساد و بزه‌های اقتصادی نیز در همه جا، همه گیر شد، در حالی که این دو عنوان بسیار پیچیده و سربسته بوده و فرآورده‌ی همان بزه‌های عادی و شناخته شده‌اند. اقدامات تروریستی نیز در چنین بستری پدید آمده و گسترانیده شد، به طوری‌که اقدامات تروریستی که امروزه بیشتر نام " بزه‌های

تروریستی" بر آن می‌نهند، از رفتارهای کم‌ارزشی مانند آموزش هراس‌افکنی یا ماندن در جایی‌که تروریسم را آموزش می‌دهند، آغاز می‌گردد و به رفتارهای بزرگ و اندوهباری مانند کشتار آدمیان پایان می‌یابد. بنابراین بزه‌های تروریستی نه تنها پراکنده و گوناگون شده‌اند که به راستی روشن نیست، اندازه و چارچوب آن کدام است؟ راستی آن است که بزه تروریستی یکی است و آن رفتارهای هراس‌آور با انگیزه سیاسی است و کم‌وبیشِ آن، پیش‌زمینه و نتیجه این رفتارها است ولی ساماندهی جهانیِ ابرقدرت‌ها به معنای تروریسم، جایگاه فراخ و پیچیده‌ای از این پدیده در حقوق کیفری پدید آورده است.

در یک بخش‌بندی گسترده، بزه‌های تروریستی را می‌توان در سه جهان بررسی کرد. جهان نخست همین جهان فیزیکی است که بزه‌های تروریستی در آن به چشم آمدنی‌اند و در جامه‌ی خشونت ورزیدن یا تهدید به آن نمود می‌یابند. جهان دوم جهان مجازی است که همان فضای سایبر یا فضای بنیاد گرفته از رایانه و اینترنت است. در این فضا دست‌یازی به خشونت، شدنی نیست، ولی هرگونه اخلال در شبکه‌های رایانه‌ای با اثرها و نشانه‌های خشونت‌آمیز در جهان فیزیکی همراه خواهد بود؛ از این رو ویژگی‌های تروریسم در فضای سایبر با جهان واقعی یکسان نیست. جهان سوم، جهان آینده است که پدید آمدن گونه‌های نوین و خطر-

آفرین تروریسم را هشدار می‌دهند، ولی هنوز به طور روشن رخ نداده‌اند. بزه‌های تروریستی جهان آینده مانند تروریسم هسته ای و مگایی بیشتر جنبه ذهنی داشته و بر پایه‌ی مفهومی پیشگیرانه پیش بینی شده اند.

تروریسم سایبری هم اکنون به اندازه ای فربه شده که با بیشتر بزه های رایانه ای را در برگرفته است. با بررسی قانون های ضد تروریسم، روی هم رفته ترویسم سایبری را می توان بر دو دسته بزه های افزار محور و بزه های هدف محور دسته بندی کرد. بزه های افزار محور، به رفتارهای بزهکارانه سنتی گفته می شود که گروه های تروریستی از فضای سایبر برای انگیزه ها و هدف های خود بهره می

جویند مانند تبلیغ اندیشه ها و آرمان های گروه، عضوگیری، تامین مالی و حتی تهدید دیگری یا ترساندن همگانی. این رفتار تنها با افزار رایانه انجام می شوند و به راستی تروریسم سایبری نیستند ولی در قانون های ضد تروریسم از آنها یاد شده و در ادبیات حقوقی نیز در زیر تروریسم سایبری آورده می شود. بزه های هدف محور همان رفتارهایی است که از سوی گروه های تروریستی بر ضد رایانه انجام می گردد. از آنجا که سنجه بزه تروریستی یا انگیزه سیاسی است یا پیوند یک رفتار با یک گروه تروریستی، همه رفتارهای نابهنجار رایانه ای مانند دسترسی غیرمجاز، شنود اطلاعات و جعل نیز می تواند در دل تروریسم سایبری جای

بگیرد ولی آنچه که مفهوم راستین تروریسم سایبری است، جایی است رایانه هدف است نه افزار و در جایی که هدف است باید تمامیت داده یا سامانه، موضوع رفتار تروریست ها قرار بگیرد، نه محرمانگی. بدین حال تنها تخریب داده و اخلال سامانه با انگیزه سیاسی می تواند اقدام تروریستی سایبری به شمار آید که با رفتارهایی مانند انتشار ویروس و دیگر نرم افزارهای زیان آور، دست اندازی به نام های دامنه، ممانعت از دسترسی به داده و سامانه، اخلال در زیرساخت های حیاتی، تحریف اطلاعات نهادهای خدمات رسان یا اخلال در عملکرد نهادهایی که خدمات ضروری به شهروندان می دهند، نمود می یابد. از همین نگاه است که