ماهیت تروریسم سایبری

بتول پاکزاد*

چکیده

در عصر اطلاعات مواجه با نوع جدیدی از تروریسم در فضای سایبر هستیم، به طوری که امروزه در پذیرش تروریسم سایبری به عنوان نوع جدیدی از تروریسم کمتر تردیدی وجود دارد. حضور تروریست‌ها در جهان مجازی یا سایبر گویای این است که این پدیده روز به روز در حال گسترش و تغییر چهره است. بهره‌گیری از فناوری‌های نوین در اقدامات تررویستی و یا هدف قرار دادن این فناوری‌ها توسط تروریست‌ها، سبب شده تا تروریسم سایبری هم در مجموعه جرائم تروریستی جایگاه ممتاز داشته باشد و هم در مجموعه جرائم رایانه‌ای. به این ترتیب تروریسم سایبری نه همچون یک نوع یا شیوه از اقدام‌های خشونت‌آمیز تروریستی است که بتوان به طور دقیق در زیر تروریسم جایش داد و نه ویژگی‌هایش محدود به ویژگی‌های جرائم سایبری است که آن را در این دسته نهاد. همین ابهام در جایگاه تروریسم سایبری سبب شده تا این پدیده به یک چالش و مسأله جدی هم برای تحقیق و هم برای سیاست‌گذاری در مقابله با آن تبدیل گردد. این تحقیق در صدد شناخت ماهیت متفاوت این پدیده جدید است.لازمه شناخت ماهیت آن آگاهی از مفهوم، ویژگی‌ها و گونه‌های آن می‌باشد. اگر چه در یک رویکرد حقوقی محض تروریسم سایبری فقط شامل اقدامات سایبری ضد سیستم‌ها و داده‌ها و اطلاعات با انگیزه-های سیاسی است یعنی تروریسم سایبری ناب، اما لزوم مبارزه با همه اشکال و تهدیدات ناشی از اقدامات تروریستی سایبری، به تروریسم سایبری مفهومی موسع داده و آن را شامل همه اشکال استفاده از اینترنت و فضای سایبر توسط تروریست‌ها نموده است، اعم از اینکه فضای سایبر افزار یا هدف اقدامات تروریستی باشد.

کلید واژگان

تروریسم سایبری، فضای سایبر، تروریسم، ماهیت.

---

* دانش‌آموخته دکتری حقوق جزا و جرم‌شناسی.

مقدمه

فضای سایبر[1] فضایی غیر مادی و ناملموس و بیکران است که از طریق اتصال شبکه‌های رایانه‌ای و از تجمیع فناوری‌های رایانه و فناوری اطلاعات و ارتباطات (ICT) [2] شکل گرفته است، با توجه به امکانات و ویژگی‌های فضای سایبر باید پذیرفت که جهان جدیدی در برابر جهانی که تاکنون می‌شناختیم، ظهور کرده است. پدیده تروریسم سایبری متعلق به این جهان پر از تارنما است. برای دانستن بستری که در آن تروریسم سایبری شکل می‌گیرد و خیره سرانه رشد می‌یابد، ابتدا باید بستر ارتکاب یا فضای سایبر و ارزش‌ها و هنجارهایی که در آن حاکم است را شناخت. این فضا دارای گستره‌ای جهانی و بدون مرز، پوشیده و پنهان، ناهنجارمند و کنترل‌ناپذیر است. ارزش‌ها و هنجارهای این فضا شاید از جهت عنوان با آنچه در فضای فیزیکی می‌بینیم، یکی باشد ولی از حیث کیفیت و ماهیت متفاوت است. یکی از برجسته‌ترین این ارزش‌ها امنیت است. امنیت فضای سایبر بر دو گونه است: امنیت درونی که متضمن حفظ استانداردهای حاکم بر فضای تبادل اطلاعات است بر سه پایه تمامیت داده و سیستم، محرمانگی و قابلیت دسترسی استوار است. امنیت بیرونی که متضمن نبود تهدید برای اشخاصی است که از شبکه‌های رایانه‌ای و اینترنتی بهره می‌گیرند. در کنار امنیت فضای سایبری، شاید تبادل و آزادی اطلاعات یکی از مهم‌ترین ارزش‌ها در فضای سایبر است. فضای سایبر ماهیتاً برای آزادی گردش اطلاعات شکل گرفته و محدودیت در این فضا معنا ندارد. با این حال تعارض ارزش‌ها در فضای سایبر همچون فضای بیرونی است و در این میان ارزش امنیت در برابر ارزش آزادی اطلاعات

---

۱ . در تعریف لغوی می‌توان گفت فضای سایبر یا Cyberspace واژه‌ای مرکب از دو کلمهٔ Cyber و نیز عبارت Space به معنای فضا است. واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و فناوری‌های ارتباطات بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود.
نگاه کنید به: http://www.techterms.org/definition/cyberspace

2. Information And Communication Technology.

قرار دارد به گونه‌ای که نقض هر یک احتمالاً در راستای دفاع از دیگری صورت می‌گیرد. ارزش‌های سایبری همچون ارزش‌های جهان واقعی با تهدیدات عدیده‌ای از جمله حملات تروریستی سایبری مواجه می‌شوند.

از میان گونه‌های تروریسم، یکی تروریسم هسته‌ای و دیگری تروریسم سایبری بیشتر بر پایه رویکرد پیشگیرانه و با طبع آینده‌نگری سر از قوانین در می‌آورند و از همین رو با آنکه پرونده جدی در ارتباط با اختلال در سیستم‌های رایانه‌ای و شبکه‌های مخابراتی به قصد خطر انداختن امنیت در ایران رخ نداده ولی قانون‌گذار ایران به جرم‌انگاری تروریسم سایبری دست زده است. هرچند مقنن ایران از این عنوان بهره نگرفته ولی محتوای آن را تا حدودی ذکر کرده است. فصل دوم قانون جرائم رایانه‌ای مصوب پنجم خرداد ۱۳۸۸ با عنوان جرایم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی پیش‌بینی شده است که مبحث دوم آن در ارتباط با تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی است. در ذیل این مبحث و در ماده ۱۱ آمده است: «هرکس به قصد خطر انداختن امنیت، آسایش و امنیت عمومی‌اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی‌به 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 خواهد شد.»

هر پدیده جدیدی که در علوم انسانی یا علوم تجربی مطرح می‌گردد، با چالش شناخت ماهیت (یعنی اینکه به چه نحو باید شناخته شود؟) مواجه است. تروریسم سایبری نیز به عنوان یک پدیده جدید باید ماهیتاً شناخته شود و چون هنوز سیستم تقنینی مسلم و شفاف درباره آن شکل نگرفته است، قاعدتاً با نسبیت تعریف مواجه است از این رو به جای تعریف باید با رهکارهای مختلف سعی کرد تا اطلاعاتی از ماهیت آن به دست داد. ماهیت تروریسم سایبری نیز بر طبق بررسی‌های همه جانبه مشخص می‌گردد و هرچند در اینجا قانون بیشترین تأثیر را دارد ولی این را نمی‌توان پذیرفت که تا پیش از پیش‌بینی قانون نمی-توان ماهیت یک جرم را شناخت، زیرا قانون تنها ماهیت را اعتباراً بیان می‌دارد در حالی که ماهیت به امور واقع در نزد جامعه است، یعنی این جامعه است که ابتدا بر ماهیت چیزی

صحه می‌گذارد و سپس آن را برای جرم انگاری به دست قانون‌گذار می‌دهد. در اینجا برای شناخت ماهیت از مفهوم شناسی،ویژگی‌ها و گونه‌ها کمک می‌گیریم.

گفتار نخست: مفهوم شناسی

در بررسی «تروریسم سایبری» اولین مشکل تعریف «تروریسم» و «تروریسم سایبری» است؛ اگر چه «تروریسم سایبری» مرکب از دو واژه «تروریسم» و «سایبر» است، اما برای تعریف آن و شناخت ماهیت آن ترکیب معانی این دو واژه به تنهایی کمکی نمی‌نماید، اما از آنجا که تروریسم سایبری به عنوان نوع جدید و به عبارتی نسل جدید از تروریسم موضوع این تحقیق است لازم است در ابتدا مفهوم و ویژگی‌های آن را بشناسیم.

بند یکم: تروریسم

ارائه تعریفی جامع و مانع از تروریسم [۳] بی‌نهایت مشکل است؛ تروریسم هم از دید مفهومی و هم از جهت مصداقی، نسبی و دگرگون پذیر است. جدا از این عقیده که «آنکه از دید یک شخص تروریست نامیده می‌شود از دید دیگری هواخواه حق و آزادی است»،[۴] از سویی انگیزه مرتکب و گرایش‌های عقیدتی و سیاسی نهفته در آن و از سویی دیگر تنوع و گسترده‌گی اقدامات تروریستی و تحول آن و به عبارتی ناروشن بودن رفتارها

---

۳ . از نظر لغوی واژه «تروریسم» از کلمه «ترور» أخذ شده است؛ ترور نیز از ریشه لاتین «terror»[۲] به معنای ترس و وحشت شدید است.نگاه کنید به:

Webster's Third New International dictionary Massachusetts Martin ,Webster inc, 1986, p.2361

در زبان فرانسه «ترور» را ابتدائاً ترس یا نگرانی شدید که اغلب از تهدید مبهم و نامأنوس و غیر قابل پیش-بینی ناشی می‌شود، تعریف کرده اند.[۴] ترور و تروریسم در غالب زبان‌های دنیا با همین واژه مورد استفاده قرار می‌گیرد.(اردبیلی، محمد علی، حقوق بین‌الملل کیفری، گزیده مقالات ۱، تهران، نشر میزان، ۱۳۸۳، ص ۱۹۵.)

4. Harvey W.Kushner, Encyclopedia of Terrorism, sage publication, In c,2003, p.359.

و مصداق‌های آن بر دشواری تعریف افزوده‌اند. «تروریسم پدیده‌ای است که به دلیل پیچیدگی و تأثیر سیاسی‌اش نمی‌تواند در یک تعریف واحد جمع شود».[5] قوانین داخلی و اسناد بین‌المللی به جای تعریف مفهومی یا توصیفی بیشتر به تعیین مصادیق رو آورده‌اند، یعنی یکسری افعال را تحت عنوان تروریسم گرد آورده‌اند؛ این نوع تعریف برای اهداف کاربردی بهتر می‌باشد. لازم به توضیح است؛ از نظر حقوقی آنچه قابلیت داشتن جایگاه حقوقی را دارد، *"اقدامات یا جرائم تروریستی"* است نه تروریسم؛ تروریسم یک واژه سیاسی و جامعه شناختی است که با توجه به ویژگی‌هایش قابلیت طرح در چارچوب جهت یافته و ضابطه‌مند حقوقی را ندارد. بدیهی است که اقدامات تروریستی دلالت بر نوع رفتار دارد و به معنای ارتکاب دو یا چند رفتار خشن یا تهدیدآمیز نیست و بلکه با یک رفتار نیز قابلیت ارتکاب دارد.

با این همه از توجه به تلاش‌های انجام شده برای تعریف توصیفی تروریسم نباید غافل شد. این تعاریف حداقل ویژگی‌هایی را که برای شکل‌دهی تروریسم مورد نظر بوده است آشکار می‌سازد. اشمید[6] و یانگمن[7] پس ازگردآوری ۱۰۹ تعریف از تروریسم تعریفی از تروریسم ارائه داده‌اند[8] و نهایتاً اذعان کرده‌اند که به هدف خود نرسیده‌اند. اما اهمیت کار

5. Council of Europe; The threat of cybercrime, Situation report, Council of Europe Publishing, 2005, p:171.

6 . Schmid.

7 . Jongman.

۸. این تعریف بیان می‌دارد که «تروریسم شیوه‌ای از اقدامات خشونت‌آمیز تکراری است که موجد احساس سردرگمی میان اضطراب و امید می‌شود و توسط فرد، گروه، یا عاملان دولتی (شبه) مخفی به دلایل ایدئولوژیکی، جنایی، یا سیاسی به کار گرفته می‌شود، که به موجب آن – برخلاف ترور (آدمکشی) – هدف‌های مستقیم خشونت، هدف‌های اصلی نیستند».

Alex P. Schmid & Albert J. Jongma; Political Terrorism: A New Guide To Actors, Authors, Concepts, Data Bases, Theories, And Literature ,North- Holland, Amsterdam, 1988, P. 5-6

آن‌ها در شناسایی عناصر مشترک تعاریف بوده است که ما را به ویژگی‌های اصلی تروریسم رهنمون می‌کند. آن‌ها سه عنصر مشترک را شناسایی کردند: ایجاد ترس یا وحشت در جمعیت مورد هدف (هراس افکنی)؛ استفاده از خشونت یا تهدید به خشونت و انگیزه سیاسی.[9] این عناصر به عنوان ارکان اصلی تروریسم شناخته می‌شوند.

هراس افکنی مهم‌ترین ویژگی اقدامات تروریستی است، به طوری که بعضی این ویژگی را تنها رکن اصلی در تعریف تروریسم می‌دانند و بیان می‌دارند که «تروریسم یعنی ایجاد وحشت».[10] از نظر حقوقی، موضوع و هدف اصلی تروریسم امنیت است که با ایجاد ترس و وحشت در مردم تحقق می‌یابد. *البته ممکن است موضوع اقدامات تروریستی منقسم به موضوع رفتاری و موضوع غایی گردد. موضوع رفتاری یا هدف مستقیم رفتارهای خشونت‌بار تروریست‌ها افراد یا اموال است اما موضوع نهایی یا هدف نهایی تروریست‌ها امنیت ملی است.*[11]

استفاده از خشونت یا تهدید به آن غالباً به عنوان رکن مادی اقدامات تروریستی مطرح می‌شود؛ خشونت، معادل واژه Violence در زبان انگلیسی است؛ با دقت در معانی و تفاسیری که تا به حال از خشونت به عمل آمده، معلوم می‌گردد که مفهوم خشونت و رفتار خشن، امری نسبی است که متناسب با زمان و مکان تغییر ماهیت و معنی می‌دهد. برای تحقق تروریسم ضرورتی ندارد که خشونت به صورت فیزیکی باشد بلکه خشونت روانی

9. Merari, A;Terrorism as a Strategy of Insurgency, Terrorism and Political Violence, Volume5, 1993,No.4, http://www.st-ndrews.ac.uk/academic/intrel/research /cstpv/pdffiles/ TerrorismStrategy.pdf.

۱۰ . آزمایش، دکتر سید علی؛ نگرشی نو به مفهوم تروریسم بین‌المللی، مجله پژوهش، حقوق و سیاست،دانشگاه علامه طباطبایی، دانشکده حقوق علوم سیاسی، شماره چهارم بهار و تابستان ۱۳۸۰، ص ۱۷۸.

۱۱ . نگاه کنید به: عالی پور حسن؛ توازن میان امنیت ملی و آزادی فردی در مقابله با جرائم تروریستی، رساله دکترای حقوق جزا و جرم شناسی، دانشکده حقوق دانشگاه شهید بهشتی، بهمن۱۳۸۷، ص۸۴ .

هم می‌تواند موجب تحقق اقدامی تروریستی شود. تروریست‌ها با استفاده از خشونت و ابزارهای فیزیکی و روانی سعی دارند تا در جامعه ترس ایجاد کنند.[۱۲]

باید توجه داشت خشونت در تروریسم موضوعیت ندارد زیرا آنچه اهمیت دارد نتیجه استفاده ازخشونت یعنی ایجاد ترس و وحشت است. بنابراین تحقق عینی خشونت در ارتکاب یک اقدام تروریستی ضرورت ندارد. وسیله خاص نیز موضوعیت ندارد، با این حال تحقق برخی از مصادیق جرم تروریسم نیاز به استفاده از وسایل خاص دارد؛از جمله، اقدامات تروریستی با به کارگیری مواد انفجاری و تروریسم هسته‌ای. بنابراین *تحقق جرم تروریسم ممکن است از طریق سیستم‌های رایانه‌ای و با ایجاد اختلال در شبکه‌های اطلاعاتی و سیستم‌های کنترل حمل و نقل زمینی، هوایی و دریایی و یا خارج کردن کنترل سلاح‌های کشتار جمعی عملی شود.*

انگیزه سیاسی، یک عنصر مهم در تروریسم است؛ «هدف تروریست‌ها استفاده از ترس یا نگرانی شدید برای وادار ساختن اهداف اصلی خود به انجام رفتاری یا اتخاذ ایستارهایی است که با نتیجه (سیاسی) مطلوب ارتباط دارد.»[۱۳] *برخی بدون وجود انگیزه سیاسی هیچ اقدامی را تروریستی نمی‌دانند.*[۱۴] *مفهوم «اهداف سیاسی» مفهوم گسترده‌ای است که اهداف اعتقادی و مذهبی و قومی را نیز در بر می‌گیرد.*[۱۵]

در بند C ماده۱ بخش ۱ قانون تروریسم انگلستان مصوب ۲۰۰۰[۱۶] *صراحتاً انگیزه سیاسی، مذهبی یا اعتقادی را از شرایط ارتکاب جرم تروریستی قلمداد نموده است و در*

12. Oots, K.; Bargaining with Terrorist: Organizational Consideration, Terrorism,vol. 13, 1988, p.145-158.

۱۳ . میرمحمد صادقی، حسین؛ تروریسم رسانه‌ای، مجموعه مقالات همایش تروریسم و دفاع مشروع از منظر اسلام و حقوق بین‌الملل، روزنامه رسمی،۱۳۸۱، ص ۱۷۵.

14. Ruby, C.L.; The Deffinition of Terrorism, In Analyses of Social Issues and Public Policy, 2002, pp.9-14.

15 . Ibid، pp 9-14

16 . The UK- anti terrorism act 2000.

قانون ضد تروریسم انگلستان در سال ۲۰۰۸ انگیزه "نژادی" نیز به این بند اضافه شده و مجموعاً دایرهٔ اهداف سیاسی را گسترش داده‌اند.[۱۷]

بند دوم : تروریسم سایبری

همانند تعریف *"تروریسم"*، عبارت *"تروریسم سایبری"* معانی متفاوتی را برای افراد گوناگون دارد و جهت پوشش دادن دامنه وسیعی از فعالیت‌ها به کار برده شده است. این عبارت با ترکیب واژه‌های فضای سایبر و تروریسم، در دهه ۱۹۸۰ توسط بری کلین[۱۸] ابداع گردید و آن را این‌گونه تعریف کرد: «سوء استفاده عمدی از یک سیستم، شبکه یا مؤلفه اطلاعاتی رایانه‌ای برای تحقق هدفی که مؤید یا تسهیل‌کننده مبارزه یا اقدام تروریستی است».[۱۹] ازآن زمان تاکنون تعاریف مختلفی از این واژه ارائه شده است، درتعاریف متعدد ارائه شده دو رویکرد قابل بررسی هستند.

الف) تعریف عینی

منظور از تعریف عینی تروریسم سایبری، نمود خارجی آن به عنوان یک اقدام ناهنجار و ضد ارزش در فضای سایبر است. تعریف عینی معادل تعریف بر اساس اجزای رکن مادی است و از این منظر تعریف عادی نیز می‌توان گفت. بر این اساس تعریف تروریسم سایبری بیشتر سه معیاری بوده و بر اساس معیارهای موضوع، وسیله و نتیجه صورت می‌گیرد. این تعریف به جهت دوره زمانی به نخستین سال‌های طرح عنوان « تروریسم سایبری» بر می‌گردد و از این رو رویکردش نزدیک به خود تروریسم است؛ یعنی تروریسم سایبری رفتاری است که با انگیزه سیاسی از طریق سامانه‌ها یا شبکه‌ها علیه

17. The UK –Counter-Terrorism Act 2008.

۱۸ . محقق ارشد مؤسسه حفاظت اطلاعات در کالیفرنیا.

19 . Barry Collin; The Future of Cyber terrorism, Crime and Justice International, 1997, pp. 15–18.

سامانه‌ها و داده‌ها ارتکاب می‌یابد و نتایج بیرونی به بار می‌آورد. از آنجا که در ابتدای طرح تروریسم سایبری نسبت به موجودیت آن و رابطه‌اش با خود تروریسم تردید وجود داشت، در برداشت‌های اولیه بر وقوع نتایج و آثار زیان‌بار در محیط خارج از سایبر تاکید می‌شد ولی باید گفت که معیارهای فوق در تعاریف ارائه شده کم و بیش، اضافه و کم می‌شوند.

موضوع یا همان چیزی که قانون کیفری از آن دفاع کرده است، عموماً بهترین روش شناخت جرائم در حقوق کیفری است. موضوع جرم چیزی است که رفتار مجرمانه بر آن واقع می‌شود و به تعبیر دیگر موضوع جرم ارزش یا مرتبط با ارزشی است که قانون‌گذار در صدد حمایت از آن است. بر این اساس تعریف تروریسم سایبری راحت جلوه می‌نماید و آن اینکه هر اقدام غیرقانونی که بر ضد فضای سایبر ارتکاب یابد(به ضمیمه انگیزه سیاسی) تروریسم سایبری خواهد بود. با این حال در کنار هدف، وسیله نیز نقش مهمی در معرفی تروریسم سایبری دارد. در واقع از نگاه وسیله یا چیزی که جرم از طریق آن واقع می‌شود، باید گفت که تروریسم سایبری به رفتارهای غیر قانونی بر دولت یا حاکمیت سیاسی از طریق فضای سایبر است. البته در تعاریف اولیه در کنار هدف یا موضوع، به وسیله نیز تأکید می‌شده است؛ همان‌طور که در تعریف بری کلین که نخستین بار تروریسم سایبری را تعریف نمود مشاهده می‌شود. برخی تروریسم را در معنای مضیقی تعریف کرده‌اند؛ مانند تعریف گابریل ویمن که بر اساس آن، «استفاده از ابزارهای شبکه رایانه‌ای جهت آسیب رساندن یا از کار انداختن زیر ساختارهای ملی حیاتی (مثل انرژی، حمل و نقل، فعالیت‌های دولت)». وی در تعریفی دیگر چنین آورده است: «جرائم سایبری و تروریسم سایبری همانند نیستند استفاده تروریستی از رایانه‌ها به عنوان یک تسهیل‌کننده اقدامات، اعم از این برای تبلیغات، عضوگیری، استخراج اطلاعات، برقراری ارتباط یا مقاصد دیگر باشد، تروریسم سایبری نیست».[۲۰]

20. Weimann, Gabriel; Cyberterrorism: The Sum of All Fears? 28 Studies In Conflict & Terrrrorism , 2005,P. 129, 130, Weimann, Gabriel, Cyberterrorism: How Real is the Threat? U.S. INST.OF PEACE Dec. 2004.

حتی در بررسی تعاریف مضیق ارائه‌شده از تروریسم سایبری اختلاف نظر مشاهده می‌شود؛ در برخی تعاریف سیستم‌های رایانه‌ای و شبکه‌ها وسیله ارتکاب هستند و در برخی هدف حمله و برخی نیز معتقدند هم به عنوان وسیله و هم به عنوان هدف باید باشند.

علاوه بر وسیله و هدف در تعریف عینی، معیار نتیجه نیز لحاظ شده است، نتیجه زمانی تحقق می‌یابد که حمله‌ای رایانه‌ای منتهی به نتایجی ویران‌کننده شود که در مقایسه با تروریسم سنتی برای ایجاد ترس کافی باشد. در این رویکرد برخی مانند دنینگ که از نخستین نظریه پردازان جنگ اطلاعات وتروریسم سایبری است، بر تحقق نتیجه فیزیکی تأکید دارند و معتقدند حمله به سیستم‌های رایانه‌ای باید منتهی به ورود خسارات مادی و فیزیکی یا حتی مرگ اشخاص شود.:«تروریسم سایبری همگرائی تروریسم و فضای سایبری است و عموماً به معنای تهاجم غیرقانونی و تهدید به تهاجم علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن‌ها، به منظور ارعاب یا اعمال زور بر دولت یا ملتی جهت پیشبرد هدف‌های سیاسی یا اجتماعی است. به علاوه، در توصیف تروریسم سایبری، تهاجم باید منجر به تعرضی علیه شخص یا اموال شود، یا حداقل سبب صدمه‌ای شود که ایجاد ترس نماید».[۲۱]در تعاریف دیگر نیز بر نتیجه فیزیکی تأکید شده است. در طرح کنوانسیون بین‌المللی برای افزایش حمایت در برابر تروریسم و جرم سایبری، طبق ماده ۱ پیش نویس، «تروریسم سایبری به معنی استفاده عمدی یا تهدید به استفاده از خشونت، تخریب یا اختلال علیه سیستم‌های سایبری، بدون اجازه قانونی، زمانی که محتمل است چنین استفاده-ای منتهی به مرگ یا آسیب جسمی به فرد یا افرادی، خسارت اساسی به اموال فیزیکی، بی نظمی مدنی یا صدمه اقتصادی مهم شود».[۲۲] تعریف ارائه‌شده از سوی مرکز حفاظت از

---

httP. //www.usip/Org/pubs/ specialreports /srl 19.html.

21. Dorothy Denning, Cyber terrorism ,2000, http://www.cs.georgetown.edu/-den ing/ infosec/ cyberterror.html.

22. Council of Europe;OpCit, p:171.

زیرساختارهای ملی در آمریکا چنین است:"ارتکاب اقدامی جنایی با استفاده از امکانات رایانه‌ای و ارتباطات راه دور که منجر به خشونت، تخریب، و یا قطع خدمات شود تا از طریق ایجاد اغتشاش و بلاتکلیفی در درون جمعیتی مشخص موجد ترس و وحشت گردد، با هدف تأثیرگذاشتن بر دولت یا مردم که مطابق بر برنامه کاری سیاسی، اجتماعی، یا ایدئولوژیکی خاصی است.[۲۳]

این رویکرد که در واقع نخستین رویکرد به تروریسم سایبری بوده است با توجه به ذهنیت موجود از تروریسم شکل گرفته و متأثر از آن است؛ در این دیدگاه تروریسم سایبری صرفاً تکنیک یا شیوه جدید اقدام تروریستی است، یعنی اقدامات تروریستی سنتی در دنیای واقعی از طریق حمله به سیستم‌های رایانه‌ای کنترل‌کننده خدمات یا فعالیت‌ها در دنیای سایبر صورت می‌گیرد. ایراد دیگر بر این رویکرد این است که در اینجا از فناوری‌های اطلاعاتی و ارتباطاتی فقط به عنوان وسیله برای ارتکاب حمله تروریستی استفاده شده است و به جای شیوه سنتی مثل بمب‌گذاری‌ها و.... از شیوه‌های فنی و رایانه‌ای برای اختلال، تخریب سیستم رایانه‌ای استفاده شده که نتیجه آن ورود صدمه فیزیکی است. ایراد مهم دیگر این است که اصولاً جرائم ترویستی مقید به نتیجه نیستند، حال چگونه در تروریسم سایبری تحقق نتیجه فیزیکی لازم وضروری انگاشته شده است. حقوق‌دانان ومتخصصین دیگری نیز رویکرد نتیجه محور نسبت به تروریسم سایبری داشته‌اند؛ اما بر نتیجه فیزیکی تأکید ندارند مثلاً زیبر که بدون ارائه تعریف از تروریسم سایبری برای تحلیل حمله‌های تروریسم سایبری قائل به سه نتیجه است:

۱. اختلال در داده‌ها یعنی تخریب، تغییر، حذف یا غیر قابل دسترس کردن آن‌ها؛

۲. خسارات دیجیتالی (غیر ملموس) یا خسارت فیزیکی؛

23.Garrison, L. and Grand, M.;Cyber terrorism: An evolving concept, 2001, NIPC Highlights, http://www.nipc.gov/publications/highlights/2001/highlight-01-06.htm

۳. اجرای اهدف سیاسی، مانند ترساندن مردم، مجبور کردن دولتی به اینکه به شیوهٔ خاصی عمل کند یا تغییر ساختار سیاسی.[۲۴]

به عقیده او، با تحقق اولین سطح نتیجه تروریسم سایبری تحقق می‌یابد و سطوح بالاتر نتیجه می‌تواند در نوع مجازات و یا تشدید آن مؤثر واقع شود.

تعاریف دیگری نیز وجود دارد که برتحقق نتیجه تأکید دارند اما نه نتیجه فیزیکی، بلکه صرف ایجاد اختلال یا تخریب در داده‌ها یا سیستم‌های رایانه‌ای با جمع سایر عناصر می‌تواند تروریسم سایبری باشد؛ از جمله در، قانون جزای فرانسه ماده۱-۴۲۱ بند ۲ جرائم مربوط به انفورماتیک که در کتاب سوم قانون جزای فرانسه ذکر شده‌اند را عمل تروریستی قلمداد نموده است، بنابراین مواردی مانند دستیابی غیر مجاز به تمام یا بخشی از یک سیستم پردازش خودکار داده‌ها، ۲ – ایجاد مانع در کارکرد یک سیستم پردازش خودکار داده‌ها ۳ – دسترسی متقلبانه به داده‌ها یا حذف یا تغییر داده‌های محتوا؛ اقدام تروریستی قلمداد شده است.بنابراین اقدامات تروریستی سایبری صرف‌نظر از نتیجه فیزیکی جرم انگاری شده‌اند.[۲۵]

همچنین قانون تروریسم استرالیا عملی که صرفاً موجب اختلال یا توقف یا تخریب سیستم الکترونیکی شود، اقدام تروریستی قلمداد نموده است(در قانون تروریسم؛ اصلاحیه قانون امنیت سال ۲۰۰۲).[۲۶]

در جرم انگاری تروریسم سایبری در پاکستان نیز که از جمله معدود کشورهایی است که صراحتاً تحت عنوان تروریسم سایبری جرم انگاری نموده است،[۲۷] نتیجه فیزیکی از شرایط تحقق تروریسم سایبری نمی‌باشد.

---

24. Sieber. Ulrich; Cyber terrorism –The use of the Internet for terrorist purposes, Council of Europe Publishing, 2008, P.76.

۲۵ . قانون جزای فرانسه،ترجمه محمد رضا گودرزی، و لیلا مقدادی، معاونت حقوقی و توسعه قضایی، ۱۳۸۶، ص ۲۹۹ .

26. Kerr,Kathryn ;Putting Cyberterrorism Into Context;24 October 2003: http://www.auscert.org. au/render.html? cid=2997&it=3552.

رویکرد اخیر به نظر با ماهیت تروریسم سایبری سازگارتر است، زیرا مقید کردن حمله‌های سایبری تروریستی به تحقق نتیجه فیزیکی ایراداتی اساسی دارد. اولاً: دلیلی برای این محدودیت و مقید کردن وجود ندارد. ثانیاً: استفاده از خشونت یا نتایجی مانند مرگ اشخاص یا تخریب اموال به دلیل پیامدهای آنها در ایجاد رعب و هراس، مورد توجه بوده-اند؛ از این رو میزان ترس و وحشت یک جامعه با ویژگی‌های خاص همان جامعه باید

---

۲۷ . تروریسم سایبری – هر شخص، گروه یا سازمانی که با قصدی تروریستی، از هر طریق ممکن رایانه یا شبکه رایانه‌ای یا سیستمی الکترونیکی یا دستگاهی الکترونیکی را به کار می‌گیرد، به آن دسترسی می‌یابد یا موجب دسترسی به آن می‌شود، و به این وسیله به طور آگاهانه اقدامی تروریستی را انجام می‌دهد یا شروع به انجام اقدامی تروریستی می‌کند، آن شخص، گروه یا سازمان مرتکب جرم تروریسم سایبری می-شود.

توضیح ۱ – برای اهداف این ماده، عبارت " قصد تروریستی" به معنای عملی است به قصد مضطرب کردن، به وحشت انداختن، مختل کردن، آسیب رساندن، ضرر زدن، یا انجام هر عمل خشونت آمیزی علیه بخشی از جامعه، دولت یا دستگاه‌های مربوط به آنها.

توضیح ۲ – برای اهداف این ماده، عبارت " اقدام تروریستی" شامل موارد زیر می‌شود و در عین حال محدود به آنها نمی‌شود:

(الف) تغییر به واسطه اضافه کردن، حذف کردن، یا تغییر دادن یا شروع به تغییر اطلاعات به نحوی که منجر به جراحت،بیماری، یا مرگ بخشی از جامعه شود؛

(ب) ارسال یا شروع به ارسال برنامه‌ای مضر به منظور اساساً از کار انداختن یا مختل سازی شبکه‌ای کامپیوتری که مورد استفاده دولت یا هر دستگاه دولتی است؛

(پ) کمک کردن به ارتکاب یا مبادرت جهت کمک کردن به ارتکاب هر نوع اقدام خشونت‌آمیز علیه استقلال و حاکمیت پاکستان، اعم از این که ارتکاب چنین عمل خشونت‌آمیزی واقعاً انجام شده باشد یا نشده باشد؛

(ت) سرقت یا کپی‌برداری، یا مبادرت به سرقت یا کپی برداری، یا به دست آوردن داده‌ها یا اطلاعات محرمانه ضروری برای ساخت هر نوع سلاح شیمیایی، بیولوژیکی، یا هسته‌ای، یا هر سلاح دیگر اتلاف جمعی. به موجب بند ۲ همین ماده مجازات مرگ یا حبس ابد را در مواردی که جرم تروریسم سایبری منجر به مرگ شخصی گردد را مقرر نموده است.

"prevention of the electronic crimes – Ordinance No. Iv Of 2008؛Published in the Gazette of Pakistan, Extraordinary, Part-I, Dated the31st May, 2008.

سنجیده شود مثلاً در جامعه‌ای که وابستگی به فناوری اطلاعات و ارتباطات زیاد است یک حمله سایبری (مانند حمله ممانعت از سرویس دهی) باعث اختلال شدید در سیستم‌های رایانه‌ای و ارائه خدمات عمومی می‌شود حتی چه بسا اهمیت آسیب‌ها وصدمات غیر فیزیکی ناشی از حمله‌های سایبری بیش از صدمات فیزیکی باشد.[۲۸] ثالثاً: در قوانین کیفری کشورهایی که تروریسم سایبری را جرم‌انگاری نموده‌اند مانند استرالیا، فرانسه، انگلستان، آمریکا و...، ایجاد اختلال در سیستم‌های رایانه‌ای به عنوان نتیجه جرم تروریستی کفایت می‌کند. رابعاً: به عقیده برخی چنانچه ما خود را در قلمرو آنچه که به عنوان تروریسم سنتی قلمداد می‌شود محصور کنیم در آن صورت با تمرکز به وقایع بسیار غیر محتملی که شامل بدترین سناریوها است خود را به خطر می‌اندازیم.[۲۹] تروریسم سایبری باید به گونه‌ای در نظر گرفته شود که در بردارندهٔ دامنهٔ کامل از تهدیدات، آسیب‌پذیری‌ها، خطرات و موضوعات فنی باشد.

ب) تعریف معنوی

منظور از تعریف معنوی یا انگیزه محور تروریسم سایبری، همچون خود تروریسم تأکید بر رکن روانی پدیده یا همان قصد و انگیزه مرتکب است. در تروریسم و به تبع آن در تروریسم سایبری، قصد خاص را می‌توان بر دو دسته تقسیم کرد: قصد مستقیم که

۲۸ . مانند حملات سایبری در ۲۷ آوریل تا ۱۸ مه ۲۰۰۷، به کشور استونی که از کشورهای پیشگام دارای دولت الکترونیکی است. در آن زمان استونی تحت حمله‌ای سایبری قرار داشت که نمونه‌ای از آن قبلاً در هیچ جای دنیا مشاهده نشده بود. این حملات وب سایت‌های اصلی دولتی و خصوصی را مورد هدف قرار دادند و به طور همزمان با به کارگیری دامنه وسیعی از فنون تهاجمی به زیرساختارهای اطلاعاتی مهم حمله ور شدند. نگاه کنید به:

Heise Security, Estonian DDoS- a final analysis.httP. //www.heise-security.co.uk/ news/ print/90461.

29. kerr, Op.Cit.

عبارت است از موضوع قصدی که مرتکب رفتارش را بر آن انجام می‌دهد مانند شهروندان و یا اموال که عموماً خشونت نسبت به آن‌ها واقع می‌شود. قصد نهایی عبارت است از هدفی که مرتکب با انجام خشونت یا تهدید یا سایر رفتارهای ذیل اقدامات تروریستی به دنبال آن است و همین قصد نهایی است که انگیزه تروریستی نامیده می‌شود. البته حالتی که مرتکب تنها قصد ترور یک شخصیت را داشته باشد در این حالت قصد مستقیم و نهایی یکی می‌شود.

همان طور که بیان شد در واقع بدون وجود این انگیزه،جرم تروریستی اصولاً تحقق نمی‌یابد و یکی از مهم‌ترین عوامل جدایی یک حمله تروریستی در جهان واقعی از یک حملهٔ غیر تروریستی صرفاً انگیزه است و این مهم نیست که نتیجه چقدر مهم باشد. یکی از عناصر اصلی در تروریسم سایبری نیز وجود انگیزه سیاسی، عقیدتی، مذهبی یا نژادی است و بدون وجود این انگیزه جرم تروریستی اصولاً تحقق نمی‌یابد؛ در واقع فارق اصلی تروریسم سایبری از جرائم سایبری انگیزه است؛ حمله‌ای با انگیزه سیاسی که منجر به مقدار قابل ملاحظه‌ای ترس و اضطراب در عامه مردم گردد، می‌تواند به عنوان تروریسم سایبری در نظر گرفته شود اگرچه ممکن است آن حمله منجر به مرگ یا صدمه فیزیکی نشود. [۳۰]

در بیشتر تعاریف مربوط به تروریسم سایبری، می‌توان نقش انگیزه سیاسی را دید وگرنه با حذف چنین شرطی، تروریسم سایبری عملاً همان رفتارهای مجرمانه رایانه‌ای مانند تخریب داده یا اخلال در سامانه و شبکه خواهد بود. پس تروریسم سایبری به جهت تعریف از خود تروریسم تبعیت می‌کند و تفاوتی با آن ندارد. در واقع تروریسم سایبری همچون تروریسم اصالت نداشته و در پیکره جرائم دیگر داخل شده و تنها روح یا عنصر روانی آن‌ها را متفاوت می‌کند.

30. Ozeren ,Suleyman; Global Response To Cyber terrorism And Cyber crime :A Matrix For International Cooperation And Vulnerability Assessment, Pro Quest Information and Learning Company, 2005,p.15.

البته در تعاریف معنوی یا انگیزه محور، از اجزای رکن مادی نیز یاد می‌شود ولی در اصل تأکید بر جنبه معنوی پدیده است. در تعریف ارائه شده در گزارش پارلمان انگلستان تروریسم سایبری به معنای « اختلال شدید سیستم‌های رایانه‌ای با انگیزهٔ سیاسی، مذهبی یا ایدئولوژیکی است»[۳۱] در این تعریف معیار اصلی و فارق تروریسم سایبری از جرم رایانه-ای، انگیزه است. یا در تعریف دیگری آمده است: «تروریسم سایبری، حمله‌ای با قصد قبلی و با انگیزه سیاسی علیه اطلاعات، سیستم‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده‌ها است که منجر به خشونت علیه هدف‌های غیرنظامی توسط گروه‌های فروملی یا سازمان‌های زیرزمینی می‌شود.»[۳۲] این تعریف در کنار ذکر انگیزه، همچنین هدف‌محور هم است و حتی دو گونه هدف پیش‌بینی کرده است: هدف مستقیم که همان اطلاعات و سیستم‌های رایانه‌ای است و هدف غیر مستقیم ولی غایی که شهروندان غیرنظامی و یا سازمان‌های سیاسی است.

شاید مختصرترین و مناسب‌ترین تعریف معنوی از تروریسم سایبری این باشد که «تروریسم سایبری عبارت است از هر اقدام غیر قانونی برضد سیستم‌ها و اطلاعات با انگیزه-های سیاسی».[۳۳] این تعریف بی‌جهت، دایره تروریسم سایبری را نمی‌گستراند؛ در پی نشان دادن اهمیت، اشخاص یا گروه‌هایی که به آن دست می‌زنند و نیز عواقب جرم نیست. تنها این معنا را به صورت کوتاه بیان می‌کند که تروریسم سایبری هر اقدام بر ضد سایبر بر پایه انگیزه سیاسی را گویند.در اینجا انگیزه در کنار هدف یا سیبل می‌نشیند و ماهیت این پدیده را نشان می‌دهد.

31. Feikert. Clare, Doyle. Charles; Anti-Terrorism Authority Under the Laws of theUnited Kingdom and the United States, CRS report for congress, September 7, 2006, httP. //www.fas.org/sgp/crs/intel/RL33726.pdf.

32. Pollitt, Mark.M; Cyberterrorism: Fact or Fancy? Proceedings of the 20th National Information Systems Security Conference, 1997, p.286.

33. Goodman, et all; Cyberspace as a medium for terrorists, Technological Forecasting & Social Change, volume 74, 2007, p. 194.

بنابراین تعریف معنوی در مقایسه با تعاریف دیگر، این مزیت آشکار را دارد که در عالم ثبوت، سبب تفکیک تروریسم از دیگر عناوین مجرمانه می‌شود ولی این ایراد بزرگ را هم دارا است که در عالم اثبات یک عامل معنوی و ذهنی چگونه و به چه دستاویزهایی احراز می‌گردد؟

به نظر می‌رسد هیچ یک از رویکردهای نتیجه‌گرا یا انگیزه‌گرا نمی‌تواند به تنهایی راهکار مناسبی برای تشخیص ویژگی‌ها و تعاریف تروریسم سایبری ارائه کند و باید راهکاری ترکیبی از هر دو اندیشهٔ فوق را ملاک عمل قرار داد.

گفتار دوم :ویژگی‌ها و گونه‌های تروریسم سایبری

بند یکم: ویژگی‌ها

تروریسم سایبری به عنوان دسته‌ای از جرائم، دارای ویژگی‌هایی است که ناشی از دو جنبه تروریستی و سایبری بودن آن است. جنبه نخست آن را از جرائم سایبری متمایز می‌نماید و جنبه دوم آن را از تروریسم سنتی جدا می‌کند. نزدیکی تروریسم سایبری به تروریسم بیشتر از جهت انگیزه سیاسی یا عقیدتی یا نژادی است. از حیث اهداف وآثار و شیوهٔ ارتکاب نیز تفاوت اساسی با یکدیگر دارند. این تفاوت‌ها ناشی از ویژگی‌های فضای سایبر است. این فضا گسترده، بدون مرز و بی انتها است، آزاد است، همچون کهکشانی سرشار از اطلاعات و فناوری‌هایی است که توانایی‌های شگرفی به انسان می‌دهد، زوایایی پوشیده و مخفی دارد، فاقد نظام‌های کنترل اجتماعی بر اساس یک سلسله مراتب هرمی است.

الف) از حیث اهداف و آثار

۱. چند گانگی هدف

چندگانگی اهداف ویژگی همه اقدامات تروریستی است." مخاطب یا سبیل مرتکب اقدامات تروریستی حاکمیت و دولت است اما برای دستیابی به آن اهداف شهروندان و

اشخاص بی گناه هدف قرار می‌گیرند."[۳۴] اقدامات تروریستی در فضای سایبر نیز اهداف متفاوت و چندگانه‌ای دارند؛ این اهداف را می‌توان از منظری به اهداف نخستین یا مستقیم و اهداف غایی یا غیر مستقیم و از منظری دیگر به اهداف عینی و اهداف ذهنی تقسیم کرد.اما تفاوت اساسی تروریسم سایبری با تروریسم سنتی این است که اهداف مستقیم در اینجا غیر فیزیکی و غیر ملموس است. یکپارچگی، محرمانگی و دسترس پذیری داده‌ها و سیستم‌های رایانه‌ای هدف مستقیم حمله‌های سایبری هستند که ممکن است به اهداف فیزیکی نیز آسیب وارد نماید و یا حتی مرگ اشخاص را به دنبال داشته باشد. بدیهی است که هدف نخستین تروریست‌ها در فضای سایبر نیز«خرابکاری» است، اما خرابکاری در اهداف غیر فیزیکی. تروریست‌ها با حملاتی که صورت می‌دهند تلاش دارند که بیشترین آسیب را به داده‌ها و سیستم وارد نمایند و یا اینکه از طریق این حملات زیرساخت‌هایی چون انرژی، ارتباطات، بهداشت و درمان و نظایر آن‌ها را تا حد گسترده‌ای تحت تأثیر قرار دهند. به این مفهوم که از طریق ارتکاب جرائمی چون نفوذ غیر مجاز در سیستم‌های رایانه-ای، از بین بردن اطلاعات یا پایگاه‌های اینترنتی، ایجاد اختلال در کارکرد رایانه‌ها و نهایتاً اخلال در شبکه، پراکندن بدافزارها همچون ویروس‌ها و کرم‌های رایانه‌ای جهت تخریب اطلاعات یا کارکرد سیستم‌ها و یا از کار انداختن زیرساخت‌ها به هدف نخستین خود دست یابند.

بنابراین اهداف نخستین تروریست‌ها در فضای سایبر یا خود فضای سایبر است یا زیرساخت‌هایی که با فضای سایبر، یعنی بر اساس شبکه‌های رایانه‌ای کار می‌کنند و برنامه-ریزی یا کنترل می‌شوند. چنین هدفی در تبلیغات و تهدیدات سایبری توسط تروریست‌ها مشاهده نمی‌شود، در این موارد تأکیدی بر اهداف عینی یا آماج نیست، بلکه هدف آن

۳۴ . نجفی ابرند آبادی، استاد علی حسین؛ جرم شناسی تروریسم، تقریرات درس جرم‌شناسی، ۱۳۸۶ دوره دکتری پردیس قم، ص ۲۵۶۲ .

است که تبلیغات یا تهدیدات به لحاظ درونی یا روانی بر مخاطبان اثر بگذارد. بنابراین در چنین مواردی هدف لزوماً فیزیکی نیست.

با این همه اهداف عینی یا تخریب آماج، هدف اصلی تروریست‌ها نیست؛ تروریست‌ها از این اقدامات به دنبال اهدافی ذهنی یا به عبارتی غایی هستند؛ هدف تروریست‌ها همانا فشار بر مقامات سیاسی و دولتمردان و به طور کلی نظام سیاسی است که خود با انگیزه‌های مختلفی به وقوع می‌پیوندد. در واقع در مواردی که حملات سایبری آثار عینی و فیزیکی دارد، همچون تخریب داده‌ها، اختلال در کارکرد سیستم‌ها، قطعی برق، اختلال در سیستم حمل و نقل یا متوقف شدن خدمات پزشکی و نظایر آن، هدف غایی یا ثانوی اساساً تحت تأثیر قرار دادن دولت و قدرت سیاسی است.

۲. گستردگی آثار

در فضای سایبر معمولاً آثار وقوع بزه گسترده است. انتشار ویروس یا کرم‌های رایانهٔ نمونه‌ای از اقداماتی است که آسیب‌های گسترده‌ای دربر دارد[۳۵]. ویژگی برجسته این اقدامات برای تروریست‌ها این است که بدون وارد آوردن خسارت جانی یا فیزیکی می‌توانند ضررهای اقتصادی وارد نمایند؛ بنابراین کمتر در معرض سرزنش افکار عمومی قرارمی‌گیرند.

گستردگی آثار فرصت دیگری است که روحیه تروریست‌ها در تأثیرگذاری بیشتر را ارضا می‌کند و آنها را به جویندگان نام در سطح جهانی و افشاکنندگان عقاید مقدس خود در گستره اینترنت تبدیل می‌کند. حال آیا می‌توان گفت که اگر حمله‌ای سایبری آثار گسترده‌ای نداشته باشد، صرفاً یک جرم سادهٔ رایانه‌ای است و تروریسم محسوب نمی‌شود؟ اگرچه برخی بر این موضوع تأکید دارند و معتقدند تروریسم سایبری به معنای اختلال

۳۵. برای مثال ویروس I LOVE YOU در سال ۲۰۰۱ منجر به ۸/۷ میلیارد دلار خسارت شد.

شدید سیستم‌های کامپیوتری با انگیزه‌ای سیاسی، مذهبی یا ایدئولوژیکی است؛ و آسیب‌های جزئی فقط جرم سایبری است. البته این عقیده با توجه به اینکه آسیب‌های جزئی قابلیت ایجاد ترس و وحشت را ندارد صحیح است اما نمی‌توان گسترده بودن آثار حملات را برای اینکه حمله‌ای سایبری اقدام تروریستی محسوب شود همواره به عنوان شرط قرار داد، زیرا از سویی با مشکل تعیین ضابطه برای تشخیص آن مواجه هستیم و از سویی همان گونه که در اقدامات تروریستی در عالم واقع با قتل یک نفر یا تیراندازی به سوی ساختمانی ممکن است اقدام تروریستی تحقق یابد، در فضای مجازی نیز چنین شرطی لازم نیست و با حمله به یک سیستم رایانه‌ای نیز حمله تروریستی محقق می‌شود. مهم آن نیست که آثار گسترده باشد، بلکه ممکن است نوع و اهمیت سیستم‌هایی که مورد حمله قرار گرفته‌اند صرف‌نظر از شدت یا گستردگی آثار مورد لحاظ قرار گیرد. همان طور که در قانون جرائم رایانه‌ای ماده ۱۱ این موضوع مورد توجه قرار گرفته است. گستردگی آثار و نتایج در اینکه حمله‌ای را تروریسم سایبر بدانیم یک "ضرورت" و یک "بایستگی" به شمار نمی‌آید، بلکه خصیصهٔ غالب آن است و در مواردی ویژگی مهم بودن سیستم‌ها یا داده‌های هدف حمله جایگزین، گستردگی آن می‌شود.

ب) از حیث شیوه ارتکا ب

۱. شبکه‌ای بودن

فضای سایبر امکان سازمان یافتگی شبکه‌ای را به گروه‌های تروریستی می‌دهد. اعضای یک گروه سازمان‌یافته تروریستی با استفاده از فضای سایبر به راحتی با یکدیگر ارتباط برقرار می‌کنند و دیگر نیازی به مکان فیزیکی و حمایت دولتی ندارند. برنامه‌ریزی و هماهنگی از طریق ارتباطات شبکه، به دلیل افزایش سرعت وکاهش هزینه‌های ارتباطات، افزایش پهنای باند، اتصال گسترده و جهانی آن، آسان شده است.برای مثال از طریق رایانامه (پست الکترونیک) توافقات حاصل می‌شود، بدون اینکه نیازی به گردهمایی فیزیکی باشد. همین مسأله در مورد جذب اعضاء برای سازمان نیز وجود دارد،سازمان

اعضای خود را به راحتی از سراسر جهان جذب می‌نمایند. تحقیقات کارشناسان حاکی از آن است: « تروریست‌ها در مسیر آخرین فناوری‌های شبکه‌بندی سازمانی قرار دارند.آن‌ها با مهار کردن فناوری اطلاعات و رویکرد به ساختارهای شبکه‌ای و دوری از ساختارهای سلسله مراتبی، بر انعطاف‌پذیری، واکنش‌پذیری، و ترمیم‌پذیری خود می‌افزایند.»[۳۶]

برخی محققین، پیدایش اشکال جدید سازمان‌های تروریستی هماهنگ با عصر اطلاعات را به نحو دقیقی بررسی نموده‌اند. بر اساس آن تروریست‌ها از قالبی سلسله مراتبی به سوی طراحی‌های شبکه‌ای عصر اطلاعات در حال پیشروی هستند و تلاش‌های بسیاری برای ایجاد گروه‌های شبکه‌ای چندملیتی انجام شده است. این نوع از ساختار سازمانی از نظر کیفی با طراحی‌های سلسله مراتبی سنتی متفاوت است؛ به نحوی که مبتنی بر سازماندهی عملیات تروریستی به شیوه‌های شبکه‌ای، غیرمتمرکز و چند کانالی هستند. هیچ‌گونه رهبری، فرماندهی یا ستاد متمرکز منفردی وجود ندارد و تنها ممکن است بسته به اندازه گروه رهبری‌های چندگانه‌ای وجود داشته باشد. به عبارت دیگر، هیچ نوع رأس یا مرکزیت خاصی که بتوان آن را مورد هدف قرار داد، وجود خارجی ندارد. «برای درک پتانسیل آن باید گفت که چنین شبکه‌ای ضرورتاً جدیدترین و آخرین فناوری‌های اطلاعات و ارتباطات را به کار می‌گیرد. نتیجتاً اینترنت می‌رود تا یک جزء جدایی ناپذیر این گونه سازمان‌ها شود.»[۳۷]

با به کارگیری برنامه‌های سهل‌الاستفاده رمزگذاری که به آسانی از اینترنت قابل انتقال و کپی‌برداری هستند، تروریست‌ها می‌توانند در محیطی امن به برقراری ارتباط بپردازند. با به کارگیری شیوه تعبیه پیام رمزگذاری شده در درون پیامی معمولی[۳۸]،

36. Zanini, M. Opcit, P.42.

37. Arquilla, John, and David Ronfeldt; Cyber war is Coming!, Comparative Strategy, Vol. 12, No. 2, RAND reprint RP-223, 1993, P. 4.

38. Steganography.

دستورالعمل‌ها، طرح‌ها و تصاویر حملاتی را که می‌خواهند انجام دهند در تصاویر دیگر پنهان می‌سازند و با استفاده از چت روم‌ها(گپ گاه) توضیحات لازم را ارسال می‌کنند. این تصاویر و دستورالعمل‌ها با استفاده از کلیدی شخصی یا رمزی که دریافت‌کنندگان در اختیار دارند قابل باز شدن هستند.[۳۹]

۲. فنی بودن

عمده‌ترین خصیصهٔ حملات سایبری استفاده از روش‌ها و امکانات و اهداف فنی است که فضای سایبر برای مرتکبین فراهم می‌کند؛ در این فضا غالباً سلاح‌ها و اهداف غیر فیزیکی است؛ مرتکبین از اسلحه و بمب و نارنجک برای حملات خود استفاده نمی‌کنند، بلکه از ابزارهای حملهٔ غیر مستقیم یا روش‌های مستقیم حمله و از "صفر و یک"ها به عنوان اسلحه‌ای ویرانگر، سود می‌برند که ممکن است آثار بسیار مخرب‌تری نسبت به انفجار یک بمب یا تیراندازی داشته باشد. برای مثال انتشار یک ویروس یا یک کرم رایانه-ای که به صورتی خودکار تکثیر شده و رایانه‌ها را آلوده می‌سازند، به لحاظ اقتصادی می-توانند نتایج بسیار زیان‌بارتری نسبت به انفجار یک بمب داشته باشند، چرا که سیستم‌ها را در سطح جهانی آلوده می‌سازند. همچنین حمله‌های ممانعت از سرویس‌دهی توزیعی (DDOS) که امکان خدمات رسانی را از بین می‌برد و به این وسیله باعث ضررهای اقتصادی هنگفت و ایجاد اغتشاش و بی نظمی می‌شود. در یک تحقیق انجام شده در ۱۹۹۱آمده است: «تروریست‌های آینده ممکن است بتوانند با به کارگیری یک صفحه کلید بیشتر از یک بمب، عملیات ویرانگر خود را به انجام رسانند».[۴۰]

39. A Military Guide to Terrorism in the 21st Century, U.S. Army Training and Doctrine Command-Version 2,2004, p.I3.

40 .National Research Council, Computers at Risk, Washington, dc, National academy Press, 1991.

تحقق اقدامات تروریستی سایبری، در گرو موقعیت فنی است؛ یعنی ارتکاب تروریسم از طریق یا علیه امکانات فنی و پیچیده فضای سایبر. این پیچیدگی‌های فنی فضای سایبر خود گواه آن است که می‌تواند بستر ایجاد تروریسم سایبری را فراهم سازد. گاهی واقعیت فنی تروریسم سایبری مبتنی بر وسیله است که بر اساس آن سیستم‌های رایانه‌ای و ارتباطی می‌توانند در خدمت هر اقدامی از جمله اقدام تروریستی باشند و گاهی ویژگی فنی این پدیده مبتنی بر موضوع که همان اطلاعات و داده است، می‌باشد که بر اساس آن، اطلاعات، هسته و بن‌مایه اقدام تروریستی در فضای سایبر و از یک دید، هدف و سیبل آن خواهد بود. گاهی نیز ویژگی فنی تروریسم سایبری بر پایه رفتارهای فنی و خاص است که در این میان هک و کرک به منظور دسترسی غیر مجاز وحملات ممانعت از سرویس‌دهی توزیعی(DDOS) از همه برجسته‌تر است. این رفتارهای حرفه‌ای و خاص نشان دهنده این است که تروریسم در فضای سایبر چهره‌ای خاص و ممتاز دارد. به این ترتیب ویژگی فنی تروریسم در سه محور وسیله، هدف و رفتار نمایان می‌شود.

به طور کلی در بررسی‌های انجام شده مشخص گردیده تروریست‌ها از فناوری‌های جدید اطلاعاتی و ارتباطی که دو مزیت زیر را داشته باشند؛ استفاده می‌کنند:

الف) فناوری که موجب افزایش توان انجام برخی فعالیت‌ها می شود، مثل تبلیغات، جذب نیرو و آموزش که با تداوم و هدایت دراز مدت عملیات مرتبط هستند.

ب) فناوری که موجب افزایش پیامدهای مستقیم حملات می شوند.[۴۱]

بند دوم: گونه‌ها

از لحاظ گونه‌شناسی اقدامات تروریستی سایبری نگرش‌های متفاوتی وجود دارد. این اختلاف نظرها دلایل متعددی دارد؛ از سویی ورود تروریست‌ها به فضای سایبر و

41 . Bruce W. et all; Network Technologies forNetworked Terrorists Assessing the Value of Information and Communication Technologiesto Modern Terrorist Organizations, RAND, 2007, P:45.

استفاده از اینترنت و فناوری اطلاعات به طور مشخص و هماهنگ و همه جانبه و در زمان یکسان نبوده است، به همین جهت هر روزه ابعاد تازه‌ای از آن کشف شده است. لذا تقسیم بندی‌های اخیر از تروریسم سایبری اشکال متنوع‌تری از این پدیده را در بر می‌گیرد. از سوی دیگر رویکرد فنی یا سیاسی یا حقوقی به موضوع نیز در این امر تأثیرگذار است. در کنار این‌ها عدم اتفاق نظر در مفهوم تروریسم سایبری عامل دیگری در اختلاف نظر در مورد گستره و گونه‌های آن است. زیرا برخی تروریسم سایبری را فقط شامل تروریسم سایبری ناب[۴۲]، در واقع تروریسم سایبری، تنها به رفتار خشونت‌بار یا تهدیدآوری گفته می‌شود که در فضای سایبر رخ می‌دهد یعنی به رفتارهایی اطلاق می‌شود که با انگیزه سیاسی بر ضد داده و سامانه و شبکه ارتکاب می‌یابد. ولی امروزه به قدری دایره تروریسم سایبری گسترده شده که بخش مهمی از مصادیق آن را رفتارهایی دربر می‌گیرند که فضای سایبر تنها نقش وسیله دارد. از این رو حقوق‌دانان جهت تفکیک این دو و تأکید بر تروریسم سایبری به عنوان موضوع بودن فضای سایبر برای اقدامات تروریستی، به ناچار از تروریسم سایبری ناب سخن گفته‌اند. به سخن دیگر در تفکیک مهم میان دو مفهوم استفاده از اینترنت به عنوان یک عامل تبعی در پیشبرد تروریسم و تهاجمات صرف سایبری، گروه بسیاری معتقدند فقط گزینه دوم در مفهوم تروریسم سایبری می‌گنجد؛ مثلاً، همان طور که در تعاریف تروریسم سایبری اشاره شد بسیاری از جمله تحلیل‌گر پیشرو در عرصه تروریسم سایبری، دوروتی دنینگ چنین می‌گوید: تروریسم سایبری عموماً به معنای تهاجم

۴۲ . (Pure cyberterrorism) اصطلاحی است که برخی از نویسندگان برای تفکیک در جایی‌که فضای سایبر هدف اقدامات تروریستی است از تروریسمی که از فضای سایبر به عنوان وسیله استفاده می‌کند، به کار می‌برند. نگاه کنید به:

- Mythri Raghavan, Tara; In fear of Cyberterrorism: an analysis of the congressional response, journal of law, technology and policy, no 1, 2003, p.199

- Gordon ,sara and Ford,Richard; cyberterrorism? ElsevierScienceLtd,2002 www.sciencedirect.com/science?_ob=ArticleURL&_udi#fn4

غیرقانونی و تهدید به تهاجم علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن‌ها است، به منظور ارعاب یا اعمال زور بر دولت یا ملتی جهت پیشبرد هدف‌های سیاسی یا اجتماعی است. به علاوه، از دیدگاه وی در توصیف تروریسم سایبری، تهاجم باید منجر به تعرضی علیه شخص یا اموال شود یا حداقل مسبب صدمه‌ای شود که ایجاد ترس نماید. مانند تهاجماتی که موجب مرگ یا جراحت بدنی، انفجار، سقوط هواپیما، آلودگی آب یا خسارت‌های شدید اقتصادی می‌شوند. و حتی به عقیده برخی « تهاجمات شدید علیه زیرساختارهای حیاتی را، بسته به میزان اثرات آن‌ها، می‌توان در رده اقدامات تروریستی قرار داد و تهاجماتی که خدمات غیر اساسی را مختل می‌سازند یا عمدتاً مزاحمتی پر هزینه هستند در این مقوله قرار نخواهند گرفت.»[۴۳]

اما مفهوم موسع تروریسم سایبری شامل هر گونه اقدام تروریستی در فضای سایبر است که رایانه ابزار یا هدف آن باشد.، با این حال به کارگیری این اصطلاح نشان می‌دهد که در تروریسم سایبری فرقی نمی‌کند که فضای سایبر، وسیله باشد یا هدف. همین که پای تروریست‌ها در میان باشد و یک طرف قضیه نیز فضای سایبر باشد، تروریسم سایبری مطرح می‌شود؛ در حالی که عنوان « تروریسم سایبری ناب» در مقام تفکیک میان وسیله بودن فضای سایبر و هدف بودن آن است و به سخن کوتاه، تروریسم سایبری تنها به حالتی اشاره دارد که فضای سایبر هدف اقدام تروریستی است.

در یکی از نخستین تقسیم بندی‌ها در ۱۹۹۸ [۴۴] توسط متخصصان جرائم سایبری اقدامات تروریستی سایبری در سه شکل عمده توصیف شدند که صرفاً ناظر به تروریسم سایبری ناب می‌باشد: انهدام فایل‌ها، ممانعت از قابلیت دسترسی به فایل‌های داده‌ای از طریق رمزگذاری آن‌ها، و سربارگذاری سیستم به نحوی که موجب تخریب قابلیت‌های

43. Walker, Clive; Cyber-Terrorism: Legal Principle and Law in the United Kingdom, Penn State Law Review, Vol. 110:3,2006,P.633.

44. Grabosky.

سیستم شود.اما متعاقباً تروریسم سایبری در مفهوم گسترده مورد توجه محققین و نیز قانون-گذاران قرار گرفت.

به طوری که در رده‌بندی دیگری تحت عنوان "عملیات اطلاعات"، توسط زنینی و ادواردز[۴۵] از متخصصین جنگ شبکه‌ای؛ اقدامات تهاجمی توسط تروریست‌ها را به سه دسته تقسیم نموده‌اند: یک: استفاده تروریست‌ها از فناوری‌های اطلاعات مثل اینترنت برای مدیریت افکار و تبلیغات، دو: حملات مختل‌کننده با استفاده از اینترنت و دیگر شبکه‌های رایانهٔ، سه: حملات ویرانگر با استفاده از این فناوری‌ها. توضیح اینکه؛ مدیریت افکار و تبلیغات هم حاوی اثرگذاری بر افکار عمومی و هم دربردارنده امکان استخدام اعضاء جدید است.آخرین گونه تعدی، حمله ویرانگر است که موجب تخریب واقعی سیستم‌های مجازی و فیزیکی شامل سیستم‌های انرژی، منبع آب، و کنترل ترافیک می‌شود.

گونه‌شناسی جامع‌تری از تروریسم سایبری تحت عنوان " گونه‌شناسی وقایع سایبری"ارائه شده است،[۴۶] که شامل: حملات اطلاعاتی، حملات زیرساختاری، تسهیلات فنی و تأمین مالی می‌باشد.

کلیو والکر حقوق‌دان انگلیسی در گونه‌شناسی انوا ع تروریسم سایبری با رویکرد موسع هم تهاجمات وهم مساعدت‌ها را مورد توجه قرار داده است و آن‌ها را در پنج گروه قرار داده است که شامل موارد زیر می گردد:

۱. جنگ اطلاعات (در این نوع از اعمال، فناوری اطلاعات هم ابزار و هم هدف تهاجم است)۲. ارتباطات ۳. حمایت لجستیکی و پرسنلی۴. جمع‌آوری اطلاعات جاسوسی ۵. تبلیغات[۴۷].

45. Zanini, Op.cit,p:41.

46 . Ballard, J. D. Hornik , J. G., & McKenzie, D.; Technological facilitation of terrorism: Definitional, legal and policy issues, American Behavioral Scientist, vol. 45, 2002, p.1009.

47 . Walker, Clive. Op.Cit, p:36.

برخی از نویسندگان بر این عقیده‌اند که « رایانه سه زمینه اصلی برای فعالیت‌های تروریستی در اینترنت گشوده است: یکم: حملات مخرب به وسیله اینترنت. دوم: انتشار مجموعه اطلاعات با محتوای غیر قانونی. سوم: استفاده از اینترنت برای ارتباط شخصی و ارتکاب اشکال سنتی جرائم تروریستی.»[۴۸] و برخی دیگر از نویسندگان در مباحث ماهوی تروریسم، به نوع اقدامات فنی یا شیوه عملکرد تروریست‌ها در فضای سایبر پرداخته‌اند و از این رو معیار را بر پایه نوع حمله قرار داده‌اند. سوزان برنر، یکی از طراحان اصلی مباحث تروریسم سایبری ابتدا با تردید به دنبال آن است که نشان دهد اینترنت یا فناوری اطلاعات می‌تواند به سه طریق به خدمت تروریست‌ها درآید: « به عنوان سلاح کشتار جمعی همگانی[۴۹]، به عنوان سلاح‌های تشویش همگانی[۵۰]، به عنوان سلاح‌های اخلالگر همگانی»،[۵۱] هرچند وی نسبت به تحقق کشتار جمعی از طریق فضای سایبر دست کم در مقطع زمانی کنونی ابراز تردید می‌کند[۵۲] ولی در یک تقسیم‌بندی دیگر حملات به داده‌ها و سامانه‌ها را به حملات فیزیکی، ساختاری و معنایی[۵۳] تقسیم می‌نماید و در کنار این‌ها سه نوع دیگر اقدامات تروریستی را نیز تحت عنوان حملات مختلط (تقویت‌کننده خشونت)، مکانیزم پشتیبانی و حملات به هم پیوسته سایبری/ شیمیایی، زیستی، انفجاری، تشعشعی و هسته‌ای (CBERN)[۵۴] بررسی می‌نمایند.[۵۵]

48. Sieber, Ulrich; Op.cit.p.50.
49. weapon of mass destruction.
50. weapon of mass distraction.
51. weapon of mass disruption.
52. Brenner, Susan W; Cybercrime, Cyberterrorism And Cyber Warfare, Op.cit , p.456.
53. physical Attacks , Syntactic Attacks and Semantic Attacks
Brenner, S. W., & Goodman, M. D; In defense of cyber terrorism: An argument for anticipating cyber-attacks, University of Illinois Journal of Law, Technology &Policy,2002,P. 28-31.
54 . CBERN terrorism: Chemical, Biological, Explosive, Radiological, Nuclear Terrorism.
55. Brenner, S. W., & Goodman, M. D;Ibid , 2002,pp27-33.

حمله‌های فیزیکی؛ حمله به شیوه‌های فیزیکی به سیستم‌های رایانه‌ای است که باید تحت عنوان تروریسم بررسی گردد. حمله‌های ساختاری، «در بردارنده تغییر منطق سیستم عامل کامپیوتر به منظور ایجاد وقفه یا غیر قابل پیش‌بینی کردن عملکرد سیستم هستند. اکثرحمله‌ها در سال‌های اخیر جزء حمله‌های ساختاری بوده‌اند. مانند حمله‌های ممانعت از سرویس‌دهی، کرم‌ها، ویروس‌ها، اسب‌های تروجان.»[۵۶] ولی بر خلاف حملات ساختاری که سیستم عامل کامپیوتر را مورد هدف قرار می‌دهند، حملات معنایی « اعتماد کاربر را درباره صحت اطلاعات قابل دستیابی مورد هدف قرار می‌دهد.»[۵۷] «یک حمله معنایی، بدون این که کاربر متوجه شود، به منظور القاء اشتباهات شامل تغییر دادن اطلاعاتی است که وارد سیستم می‌شوند»[۵۸]. سیستم تحت حمله معنایی ظاهراً عملکرد خود را به طور صحیح ادامه می‌دهد، اما واقعیت را به طور منقلب شده نشان خواهد داد.[۵۹]

بعضی دیگر معتقدند تروریسم سایبری دارای دو مؤلفه است که عبارتند از: «اول، استفادهٔ تروریست‌ها از رایانه برای انجام فعالیت‌های غیر خشونت‌آمیزی که اگرچه با تروریسم فاصله دارند ولی آن را تسهیل می‌نمایند؛ و دوم، فعالیت‌های تروریستی که در آن‌ها فناوری رایانه یکی از اجزای مشخص حملهٔ تروریستی (خواه به عنوان سلاح مورد

56. Brenner, Susan, Toward a Criminal Law for Cyberspace: Distributed Security, University of Dayton, School of Law, 2005. P.27, httP. //law.bepress.com/expresso/eps /.

57. Libicki, Martin; The Mesh and the Net: Speculations on Armed Conflict in an Age of Free Silicon, McNair Paper 28, March 1994, httP. //www.ndu.edu/ inss/ macnair/ mcnair 28 /m028cont.html.

58. Galley, Patrick; Computer Terrorism: What Are the Risks?, Swiss Federal Institute of Technology (May 30, 1996). Supra note 78, httP. //homer.span.ch/-spaw1165/infosec /st-en/ index.html.

59. Libido, Martin; What Is Information Warfare? – Cyber warfare, Acis Paper 3, Aug. 1995, httP. //www.ndu.edulinss/actpubs/act003/aOO3ch09.html.

استفاده یا هدف مورد حمله) است.»[۶۰] و نهایتاً اقدامات تروریستی سایبری را در دو دسته جای می‌دهند. شامل دسته اول: فناوری رایانه‌ای به عنوان عامل تسهیل‌کننده تروریسم و دسته دوم فناوری رایانه‌ای به عنوان جزء مشخصی از سلاح‌ها یا آماج‌های تروریستی.

به نظر می‌رسد برای تقسیم‌بندی اقدامات تروریستی سایبری که همگی در مفهوم موسع تروریسم سایبری قرار گیرند، بهتر است ابتدا اقدامات تروریستی ابزار محور و هدف محور را جدا کرد. که در نتیجه دو گروه عمده ایجاد می‌شود و سپس اقدامات هر گروه را ذیل آن بررسی نمود. البته در جرم انگاری تروریسم سایبری باید گروه سومی را نیز در نظر داشت که در واقع اقدامات مقدماتی برای ترویسم سایبری محسوب می‌شوند ولی از آنجا که عموماً تروریست‌ها از طریق این رفتارها به اعمال تروریستی خود نزدیک می‌شوند در جرم انگاری اقدامات تروریستی سایبری باید لحاظ شوند و در واقع این رفتارها هرچند فی-نفسه جرم هستند، حکم جرم بازدارنده را نسبت به تروریسم سایبری پیدا می‌کنند. این تقسیم‌بندی در راستای جرم انگاری اقدامات تروریستی سایبری که باید متضمن همه اشکال آن باشد مفید به نظر می‌رسد.

بنابراین اقدامات تروریستی سایبری را می‌توان در سه دسته قرار داد:

یکم: جرائم مقدماتی: شامل جرائمی مانند دسترسی غیر مجاز، شنود و جاسوسی رایانه‌ای است که مستقلاً نیز جرم می‌باشند.

دوم: تروریسم سایبری ابزارمحور یا به عبارتی پشتیبانی از تروریسم در فضای سایبر: انواع استفاده‌هایی که تروریست‌ها از اینترنت برای تسهیل اقدامات تروریستی خود انجام می‌دهند در این گروه قرار می‌گیرد. اقداماتی نظیر: ارائه و انتشار و جمع‌آوری اطلاعات،

۶۰ . فلمینگ پیتر واستول مایکل؛سایبر تروریسم: پندارها و واقعیت‌ها، برگردان اسماعیل بقایی‌هامانه وعباس باقر پور اردکانی،در مجموعه تروریسم، گردآوری و ویرایش علیرضا طیب، نشر نی، چاپ دوم،۱۳۸۴، ص ۱۵۹.

تبلیغات، عضوگیری، تأمین مالی و افزایش سرمایه، برنامه‌ریزی، شبکه‌سازی، ارتباطات و پنهان سازی.[۶۱] که می‌توان آنها را در سه دسته کلی: تبلیغ تروریسم (شامل هرگونه ارائه و انتشار اطلاعات است که معمولاً در راستای آموزش، ارتباط دهی و پیام رسانی انجام می-شود) تأمین تروریسم (اعم از تأمین مالی، انسانی و اطلاعاتی) و تهدید می‌باشد.

سوم: تروریسم سایبری هدف محور یا به عبارتی تروریسم سایبری ناب که حملات و یورش‌هایی است که برضد داده‌ها و سامانه‌ها انجام می‌شود. در مجموع می‌توان گفت حملات بر ضد فضای سایبر را می‌توان در قالب سه رفتار دید که در بیشتر حالات نیز در طول هم قرار دارند. رفتار نخست انتشار نرم افزارهای زیان‌آور به ویژه ویروس است که با توجه به ویژگی پخش سریع و ناگهانی نرم افزارهای مضر (بدافزارها) می‌توان از آنها به انفجار سایبری یاد نمود. رفتار دوم تخریب سایبری است که عمدتاً اشاره به از بین بردن یا از کار انداختن اطلاعات و داده‌ها دارد و رفتار سوم اخلال سایبری که بیشتر ناظر به مختل کردن یا از کار انداختن سامانه‌ها و شبکه‌های رایانه‌ای است. البته این اخلال ممکن است منهی به نتایج بیرونی مانند خسارات فیزیکی یا حتی مرگ اشخاص نیز بشود. بدیهی است که تخریب و اخلال می‌تواند نتیجه انتشار نرم‌افزارهای مضر باشد، نظر به اهمیت انتشار نرم افزارهای مضر،صرف انتشار چنین نرم افزارهایی با انگیزه سیاسی باید جرم تلقی شود.[۶۲]

61. Conway, Maura; Reality Bytes, cyber terrorism and terrorists 'use'of the internet: first Monday-–vol:7, No:11, o4/11/2002, P:12.

۶۲ . برای مطالعه بیشتر نگاه کنید به رساله دکتری نگارنده؛ تروریسم سایبری، رساله دکتری حقوق کیفری و جرم‌شناسی، دانشکده حقوق دانشگاه شهید بهشتی، زمستان ۱۳۸۸.

نتیجه‌گیری

تروریسم سایبری به علت ویژگی‌ها و قابلیت‌های منحصر به فرد فضای سایبر که بستر ارتکاب، موضوع و هدف آن می‌باشد، تفاوت‌هایی اساسی با سایر اشکال تروریسم دارد. ویژگی‌های تروریسم سایبری نشان از ماهیت جدیدآن دارد. از سویی از تروریسم جدا است و از سوی دیگر با جرائم سایبری کاملاً همخوانی ندارد بنابراین تعریف آن باید به گونه‌ای باشد که از جرائم رایانه‌ای و تروریسم تفکیک شود.

تروریسم سایبری با ماهیت خاص خود واقعیت عینی و حقوقی نیز یافته است و مصادیق متعدد و متنوع آن جوامع را متأثر نموده‌اند. اگر چه سطح فناوری اطلاعات و ارتباطات در همه کشورها یکسان نیست و آسیب‌پذیری از تروریسم سایبری نیز یکسان نمی‌باشد، اما به جهت ماهیت فرامرزی و جهانی بودن فضای سایبر امکان ارتکاب آن از هر نقطه جهان می‌رود.

برای مبارزه مؤثر با تروریسم سایبری با توجه به تنوع و گوناگونی اقدامات تروریستی سایبری نیاز به شناخت دقیق اشکال آن وجود دارد. در گونه‌شناسی اقدامات تروریستی سایبری،بیشتر رویکرد موسع مد نظر بوده است تا همه خطرات ناشی از این اقدامات را دربر گیرد. بنابراین تروریسم سایبری شامل همه اقداماتی است که فضای سایبر افزار یا هدف آنها است. مواردی که از فضای سایبر به عنوان وسیله برای ارتکاب اقدامات تروریستی استفاده می‌شود، در واقع این اقدامات نزدیک به تروریسم سنتی هستند و می‌توانند مشمول قوانین مربوط به تروریسم سنتی قرار گیرند. اما اقداماتی که ضد فضای سایبر انجام می‌شوند به عبارتی تروریسم سایبری ناب به جرائم سایبری نزدیک می‌باشند و نیاز به جرم انگاری خاص دارند. بدیهی است در خلأ چنین مقرراتی، صرف‌نظر از انگیزه ارتکاب، این گروه از اقدامات تروریستی سایبری قابل مجازات بر اساس قوانین مربوط به جرائم رایانه‌ای یا سایبری می‌باشند.

فهرست منابع

الف) فارسی

۱. آزمایش،دکتر سید علی؛ **نگرشی نو به مفهوم تروریسم بین‌المللی**؛ مجله پژوهش، حقوق و سیاست، دانشگاه علامه طباطبایی، دانشکده حقوق علوم سیاسی، شماره ۴، بهار و تابستان ۱۳۸۰.

۲. اردبیلی، محمد علی؛ **حقوق بین‌الملل کیفری**، گزیده مقالات ۱، تهران، نشر میزان، ۱۳۸۳.

۳. پاکزاد، بتول؛ **تروریسم سایبری**، رساله دکتری حقوق کیفری و جرم‌شناسی، دانشکده حقوق دانشگاه شهید بهشتی، زمستان ۱۳۸۸.

۴. عالی پور، حسن؛ **توازن میان امنیت ملی و آزادی فردی در مقابله با جرائم تروریستی**، رساله دکترای حقوق جزا و جرم‌شناسی، دانشکده حقوق دانشگاه شهید بهشتی، بهمن۱۳۸۷.

۵. فلمینگ پیتر و استول مایکل؛ **سایبر تروریسم: پندارها و واقعیت‌ها**، ترجمه اسماعیل بقایی‌هامانه و عباس باقر پور اردکانی، در مجموعه تروریسم، گردآوری و ویرایش علیرضا طیب، نشر نی، چاپ دوم، ۱۳۸۴.

۶. میرمحمد صادقی، حسین؛ «**تروریسم رسانه‌ای**»، مجموعه مقالات همایش تروریسم و دفاع مشروع از منظر اسلام و حقوق بین‌الملل، روزنامه رسمی،۱۳۸۱.

۷. علی حسین نجفی ابرندآبادی و حمید هاشم بیگی؛ **دانشنامه جرم‌شناسی**، انتشارات دانشگاه شهید بهشتی وکتابخانه گنج دانش، چاپ اول، ۱۳۷۷.

ب) لاتین

8. Arquilla, John, and David Ronfeldt; **The Advent of Net war** ,Santa Monica ,Calif.: RAND, MR-789-OSD, 1996.

9. Arquilla, John, and Theodore Karasik,Chechnya; A **Glimpse of Future Conflict?,** Studies in Conflict and Terrorism, Vol. 22, No. 3, July–September 1999
10. Alex P. Schmid & Albert J. Jongman; P**olitical Terrorism: A New Guide To Actors, Authors, Concepts**, Data Bases, Theories, And Literature28 ,North-Holland, Amsterdam, 1988.
11. A Military Guide to Terrorism in the 21st Century, U.S. Army Training and Doctrine Command,Version 2, 12 October 2004.
12. Bruce W. Don, David R. Frelinger, Scott Gerwehr,Eric Landree, Brian A. Jackso**; Network Technologies forNetworked Terrorists Assessing the Value of Information and Communication Technologiesto Modern Terrorist Organizations**, Prepared for the Department of Homeland Security (pbk.) Published by the RAND Corporation, 2007.
13. Barry Collin;**The Future of Cyberterrorism**, Crime and Justice International, March 1997
14. Brenner, Susan. W. and Goodman, Mark D; **In defense of Cyber terrorism: An argument for anticipating cyber-attacks**, Journal of law, technology and policy, 2002.
15. Sieber, Ulrish, Cyber terrorism –The use of the Internet for terrorist purposes ,Council of Europe, December, 2007.
16. Conway, Maura ;**Reality Bytes, cyber terrorism and terrorists 'use'of the internet**: first Monday-–vol:7, No:11, o4/11/2002.
17. Cramer, Rachel; **Internet use by terrorists and Analysis of terrorist websites**, university college london, 2002-2003

18. Dorothy Denning**;Cyber terrorism**.2000. http://www.cs.georgetown.edu/-den ing/ infosec/ cyberterror.html.
19. Denning, Dorothy**; Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool for Influencing Foreign Policy,** Sponsored by Nautilus Institute,1999. http://www. nautilus. org/info policy/workshop /papers/ denning. html.
20. Harvey W.Kushner; **Encyclopedia of Terrorism**, sage publication,Inc, 2003.
21. Kerr,Kathryn; **Putting Cyberterrorism Into Context**,24 October 2003: http://www.auscert.org. au/render.html? cid=2997&it=3552
22. Libicki, Martin; **The Mesh and the Net: Speculations on Armed Conflict in an Age of Free Silicon**, McNair Paper 28, March 1994, http://www.ndu.edu/ inss/macnair/mcnair28/m028cont.html.
23. National Research Council,**Computers at Risk**,Washington,dc,National academy Press, 1991
24. Ozeren ,Suleyman **; Global Response To Cyber terrorism And Cyber crime** :A Matrix For International Cooperation And Vulnerability Assessment, Dissertation Prepared For The Degree Of Doctor Of Philosophy; University Of North Texas; August 2005, Pro Quest Information and Learning Company, August 2005.
25. Oots,K. **Barganing with Terrorist**: **Organizational Consideeration,** Terrorism, vol. 13,1988
26. Sieber. Ulrich; **Cyber terrorism –the use of the Internet for terrorist purposes**, Council of Europe Publishing, 2008.

27. Walker, Clive; **Cyber-Terrorism: Legal Principle and Law in the United Kingdom**, Penn State Law Review, Vol. 110:3, 2006.
28. **Webster's Third New International dictionary**, Massachusetts Martin – Webster inc. 1986
29. Zanini, Michele and Edwards, Sean J.A.;**The Networking Of Terror In The information Ages**, Sponsore by Nautilus Institute, 1999. http://www.nautilus. Org/info policy/workshop /papers/denning.html.