ISSN: 2538-3787
http://www.Joce.ir

مجله علمی فقه، حقوق و علوم جزا (سال سوم)
شماره ۷ / بهار ۱۳۹۷ / ص ۵۸-۴۸

خصیصه‌های حقوقی تروریسم سایبری
(با تاکید بر ویژگی‌های جرم‌شناختی حملات سایبری هسته‌ای)

نجمه احمدی
کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد واحد صفادشت، ایران

نام نویسنده مسئول:
نجمه احمدی

چکیده
اساساً فضای سایبری به مثابه‌ی یکی از مهم‌ترین منابع قدرت در عصر جدید، محیط فناوری اطلاعات و ارتباطات نامیده می‌شود. این فضا با ویژگی‌های منحصر به فرد خود سبب شکل‌گیری رویکردهای متنوع و مختلفی به آن شده است. یکی از ویژگی‌های این فضا، امکانات بالقوه‌ای است که از آن برای اهدافی تروریستی در اختیار تروریست‌ها قرار می‌دهد. برای نمونه حملات سایبری به تاسیسات هسته‌ای کشور از جمله این اقدامات است. از سوی دیگر، اولین تفاوت جنگ سایبری با دیگر انواع جنگ‌ها و بالاخص جنگ فیزیکی و حقیقی، قابلیت طراحی، اجرا و نتیجه‌گیری از راه دور یا اصطلاحاً به شکلی ریموت است. برای حمله سایبری نیازی به حرکت فیزیکی نیست و طبیعی است که این تفاوت از منشأ فضای سایبری و حقیقی ناشی می‌گردد. سربازها و نقاط حمله می‌توانند در دنیا پخش شوند؛ نظیر عملی چنین تجسمی را می‌توان در حملات داس به اثبات رساند. بارزترین نشانه این ویژگی، انواع حملات موسوم به **MTM** یا **MITM**[1] است که توسط تروریست‌ها صورت می‌گیرد. در این حملات، مهاجم مابین دو منبع (معمولاً معتمد) قرارگرفته و اطلاعات ایشان را ربوده یا صحت آن‌ها را مورد مخاطره قرار می‌دهد. اما در عصر حاضر، تروریست‌ها تلاش می‌کنند تا با استفاده از فضای سایبر، به تاسیسات هسته‌ای برخی از کشورها حمله کنند. این حملات، در حقوق بین‌الملل دارای ابعاد جرم‌شناختی شناخته‌شده‌ای است. بنابراین در تحقیق حاضر، تلاش شد ضمن معرفی فضای سایبر و ویژگی‌های اساسی آن برای استفاده تروریست‌ها، به برخی از نمونه‌های حملات سایبری و ابعاد حقوقی و جرم‌شناختی آن از منظر حقوق بین الملل پرداخت.

واژگان کلیدی: فضای سایبر، جرم، تروریسم سایبری، حقوق بین الملل.

[1] . Man in the Middle

فقه، حقوق و علوم جزا ، شماره ۷ ، بهار ۱۳۹۷، ص ۵۸- ۴۸

ISSN: 2538-3787
http://www.Joce.ir

مقدمه

بی‌تردید حملات سایبری گونه‌ای جدید از سلاح‌های مدرن است که شدیداً استعداد ایجاد تغیرات بنیادین در ساحت حملات مدرن را دارد. فناوری رایانه امروزه تا جایی پیش رفته است که در آن نیروهای نظامی توانایی وارد کردن جراحت، کشتن و ایجاد خسارت‌های فیزیکی از طریق فضای مجازی را دارند. دامنهٔ حملات سایبری می‌تواند از خشونت‌های شبکه‌ای بی‌ضرر تا حملات شدید به ساختارهای زیربنایی ملی در نوسان باشد. در این میان، دولت‌ها و سازمان‌های بین المللی باید با اتخاذ تدابیر و راهکارهای مناسب در جهت سالم سازی و مقابله با اجتماعات آلوده به فساد گام بردارند، البته قوانینی را که تا کنون دولتها وضع نموده اند ناظر بر اینگونه اهداف بوده است. و از آنجا که تکنولوژی های کامپیوتر و اینترنت سبب تغییر ماهیت جرایم از شیوه های کلاسیک به نسل جدیدی از آن با عنوان داده ها و اطلاعات می باشد دیگر قوانین کلاسیک در حقوق کشورها کافی نبود و نیاز به وضع قوانین جدید در این خصوص احساس می گردید. قانونگذار ایران نیز در جهت مقابله با اینگونه جرایم و حفاظت از اطلاعات شخصی اشخاص به وضع قوانینی مرتبط با اینگونه جرایم پرداخته است و این نشانگر این است که حقوق جزا وارد مرحله جدید شده است و با گونه جدیدی از جرایم مواجه است که نیاز به حمایت از اطلاعات و داده ها می باشد.

از سوی دیگر، ضربه وارد شدن و حمله به هر کدام از ساختارهای امنیتی در سطوح مختلف ملی و بین المللی، به عنوان تهدیدی نوین و ویرانگر علیه امنیت می باشد که می تواند موجبات فروپاشی و نابودی زیر ساخت های حیاتی و بنیان یک جامعه شود. تروریست‌ها با ساتفاده از ویژگی‌های فضای سایبر امروزه توانسته‌اند ضربات سنگینی به برخی از کشورها وارد کنند.

۱. مفهوم فضای سایبر

سایبر واژه ای است برگرفته از لغت کیبرناتس [1] به معنای سکاندار یا راهنما. این واژه را نخستین بار شخصی به نام ویلیام گیتسون در داستانهای علمی تخیلی خود در کتاب نورومنسر [2] به کار برد. (طارمی، ۱۳۸۷: ۳۷) قبل از اینکه فضای سایبری را تعریف کنیم؛ لازم است مختصری در باره بستر ارتباطات بگوییم؛ این بستر مجموعه ای عظیم از صفر و یک‌هایی است که داده‌های الکترونیکی را تشکیل می‌دهد و آنها نیز در قالب‌های مختلف، مفاهیم را به شکل الکترونیکی منعکس می کنند. فضای سایبری در حقیقت همان بستر مذکور می باشد که داده‌های الکترونیکی در آن، ذخیره، به انحای گوناگون پردازش و در نهایت به شیوه مورد نظر منعکس می شوند. (جلالی فراهانی، ۱۳۸۵: ۱۰۱)

بعضی از نویسندگان در تعریف فضای سایبری نوشته اند :« مجموعه ای از ارتباطات درونی انسانها از طریق رایانه و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی است» (صدیق بنای، ۱۳۹۱) بعضی دیگر از نویسندگان در تعریف آن گفته اند: «فضای سایبری یا مجازی، محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص خود؛ در آن، زنده و مستقیم روی می دهد» (طارمی، پیشین، ۳۲)

با این بیان عبارت «واقعی»، مانع از این است که تصور شود مجازی بودن این فضا به معنای غیرواقعی بودن آن است؛ چرا که در این فضا نیز همان ویژگی های تعاملات انسانی در دنیای خارج هم چون مسئولیت وجود دارد.ضمن این که فضای سایبری در واقع یک محیط است که ارتباطات در آن انجام می‌شود؛ نه صرف مجموعه ای از ارتباطات. با توجه به تعریف مذکور، فضای سایبری دارای ویژگی های ذیل می باشد: الف- این فضا جهانی و فرامرزی است: به عبارت دیگر هر فرد در هر نقطه از جهان می تواند از طریق آن به اسانی، به جدیدترین اطلاعات دست یابد. مرزهای جغرافیایی نمی تواند مانع این ارتباطات شود و یا حداقل باید بگوییم که مرزهای جغرافیایی تا اکنون نتوانسته است مانع این ارتباطات شود. به طوری که حتی بعضی از دولتمردان که در صدد فیلتر نمودن قسمتی از این فضا می باشند با مشکل مواجه می شوند. ب- دستیابی آسان به آخرین اطلاعات: فضای مجازی یا سایبری ، امکان دسترسی اسان و سریع را به آخرین اطلاعات دنیا فراهم نموده است. ج- جذابیت و تنوع رسانه ها از فیلم، عکس، متن و یا هر هنر دیگری برای جذاب کردن خویش به کار می گیرند. د- آزادی اطلاعات و ارتباطات : معنای واقعی آزادی اطلاعات، در فضای سایبری محقق شده است. به طوری که شما هر نوع اطلاعاتی را که بخواهید،اعم از فرهنگی، سیاسی و اقتصادی بدون محدودیت‌های حاکم بر دیگر رسانه‌ها، در فضای سایبری قابل دسترسی است. (میلر، ۱۳۹۴: ۷۸)

---

1. Kybernetes
2. Neuromancer

ISSN: 2538-3787
http://www.Joce.ir

۲. جرایم در فضای مجازی

گزارش‌های متعددی در سراسر جهان در مورد انتقال جرائم از فضای فیزیکی به فضای مجازی که پیچیده تر از سابق هستند، منتشر می شود. نقل و انتقالات بانکی، جعل ،جرائم اداری بخشی از جرائم مهم فضای مجازی به شمار می‌روند. اگر قبلاً تروریست‌های افراطی از اسلحه های فیزیکی استفاده می کردند امروز، قدرت نظامی آنها در ساخت یک سیستم اطلاعاتی با توانایی دسترسی به هر نقطه ایی از جهان، تعلیم پیروان جدید در محل سکونت آنها، جذب اعضای جدید و تحت فشار قراردادن عقاید عمومی است. (ملکی، ۱۳۸۸: ۱۱)

آمار جدید کمیسیون تجارت فدرال آمریکا، نشان می دهد که از هفتصد هزار شاکی کلاهبرداری در سال ۲۰۰۵، حدود ۲۷ درصد شاکیان مورد سرقت هویت قرار گرفته بودند که تقریباً برابر با ۲۵۶ هزار نفر شاکی است. این آمار حدود ۲۰ درصد رشد را نسبت به سال ۲۰۰۳ نشان می دهد. (شیتز، ۱۳۸۸: ۹۳)

۳. جرم رایانه ای

نویسندگان ایرانی و غیر ایرانی همه اذعان دارند که تعریف جرم رایانه ای سخت و مشکل می باشد. بنا به دلائل مختلف در باره تعریف جرایم رایانه ای ،اتفاق نظر وجود ندارد؛ و اذعان شده است که ارائه تعریف دقیق ،جامع و مانع از جرایم رایانه‌ای از مشکل ترین مباحث این جرایم می‌باشد. (حیدری، ۱۳۹۰: ۹) اما ارائه تعریف از این جرم در سطح بین‌المللی نیز با چالش مواجه است. در شماره ۴۴ نشریه بین‌المللی سیاست جنایی وابسته به سازمان ملل به این امر اعتراف نموده و بیان داشته است که تعریف مورد توافقی در خصوص جرم رایانه ای وجود ندارد. در همان نشریه جرم رایانه ای را، جرمی می داند که در برگیرنده فعالیت‌های مجرمانه با ماهیت سنتی مانند سرقت وجعل و یا فعالیت های مجرمانه با ماهیت نوین یعنی راه های تازه برای سوء استفاده رایانه ای باشد.(دریانی، ۱۳۸۸: ۲۱) برای نمونه در توصیه نامه ۹ (۸۹) **R** شورای اروپا نیز به این امر اشاره شده و بیان شده که هر کوششی برای تعریف کردن جرم رایانه‌ای با نوعی نارسایی روبرو می شود. انجمن بین المللی حقوق کیفری[1] در نشست ۱۹۹۲ در دانشگاه ورتسبورگ آلمان نیز سرانجام نتوانست تعریفی از جرم رایانه ای ارائه دهد و قرار شد به جای تعریف، فهرست حداقل جرم های مقرر در توصیه نامه مذکور مبنای مشترک قرار گیرد. (خرم آبادی، ۱۳۸۴: ۵۶) در کنوانسیون جرایم محیط سایبر (بوداپست ۲۰۰۱) [2] همانند انجمن بین‌المللی حقوق کیفری فوق الذکر به جای تعریف جرم سایبری؛ طیف وسیعی از اقدامات مرتبط با رایانه جرم‌انگاری شده‌اند. (جلالی فراهانی، ۱۳۸۹: ۹)

(ادوارد ام وایز) استاد دانشگاه میشیگان آمریکا درگزارشی که در مورد جرائم رایانه ای آمریکا برای انجمن بین المللی حقوق جزا تهیه کرده نوشته است: «هیچ تعریفی از جرم رایانه ای وجود ندارد که مورد قبول همه واقع شود. اکنون هر یک از ایالتهای آمریکا یک قانون مخصوص به خود دارند که به ویژه جرائمی را مورد بررسی قرار می‌دهند که متضمن رایانه است. آمریکا یک قانون فدرال هم دارد. جرائم رایانه ای را می توان به عنوان نقض یکی از این قوانین جرائم رایانه ای تعریف کرد، اما شمول این قوانین یکسان نیست. اینکه هر کس یک اصطلاح را چگونه تعریف می کند به این بستگی دارد که هدف وی از تعریف آن چیست. به نظر می‌رسد که هدف از تلاش برای مجزا کردن جرائم رایانه‌ای به عنوان یک پدیده متمایز است که نقاط آسیب پذیر ویژه که در نتیجه وابستگی به تکنولوژی رایانه ای ایجاد شده اند شناسائی شوند. این امر هدفی است که در تعریف سازمان همکاری و توسعه قضائی دیده می‌شوند. حتی تعریف این سازمان گرچه وسیع است ولی در دو جنبه تمام جرائم مربوط به رایانه در بر نمی گیرد.

اول: شامل سرقت سخت افزار یا تجهیزات دیگر مانند دیسکت‌های خالی و تخریب آنها نمی شود.

دوم: شامل مواردی که رایانه برای کمک و ارتکاب جرم به کار می رود، نمی‌شود.» (حسنی و پهلوانی فرد، ۱۳۹۳: ۴۶)

اما با وجود مشکل بودن ارائه تعریف از جرم رایانه‌ای، تعاریف متعددی از سوی نویسندگان ایرانی و خارجی همچنین سازمان‌های بین‌المللی مختلف درباره جرم رایانه‌ای ارائه شده است؛ بعضی از نویسندگان با توجه به حیث دامنه شمول جرم، تعاریف مختلف به ترتیب ذیل را از آن ارائه داده اند:

الف- تعریف مضیق: هرجرمی که قانونگذار به صراحت رایانه ای را به منزله موضوع یا وسیله جرم جزء رکن مادی آن اعلام کرده است.

ب- تعریف موسع: هرجرمی که عملاً رایانه به منزله موضوع یا وسیله ارتکاب جرم در آن نقش داشته باشد.

ج- تعریف بسیار موسع: هرجرمی که رایانه به منزله موضوع یا ابزار آن نقش داشته باشد یا دلایل و اطلاعات مربوط به آن در رایانه ذخیره یا پردازش یا منتقل شده باشد. (خرم آبادی، ۱۳۸۴: ۷۴)

---

2. Association Internationale de droit Pénal (AIDP)
1. Budapest convention on cyber crime

ISSN: 2538-3787
http://www.Joce.ir

جرم رایانه‌ای هم در مجامع و سازمان‌های بین المللی تعریف شده است:

الف- سازمان ملل متحد: از بین مجامع و سازمانهای بین المللی؛ سازمان ملل متحد، اولین سازمانی است که اقدام به تعریف و طبقه‌بندی جرایم رایانه ای کرد. انواع مشترک و عمومی جرایم رایانه‌ای از دید سازمان ملل عبارتند از :۱- کلاهبرداری رایانه ای .۲- جعل رایانه ای. ۳- تخریب یا تغییر داده ها و برنامه‌های رایانه ای. ۴- دستیابی غیر مجاز به سیستم‌ها و خدمات رایانه ای . ۵- تکثیر غیر مجاز برنامه‌های رایانه ای حمایت شده. (حسنی و پهلوانی‌فرد، ۱۳۹۳: ۴۶)

ب- تعریف شورای اروپا: کمیته اروپایی مسائل جنایی در شورای اروپا در سال ۱۹۸۹ براساس یک گزارش تعریف زیر را از جرم رایانه ای ارائه داده است؛ هر فعل مثبت غیر قانونی که کامپیوتر، ابزار یا موضوع جرم باشد، یعنی به عبارت دیگر هر جرمی که ابزار یا هدف آن تاثیر گذاری بر عملکرد کامپیوتر باشد. (خداقلی، ۱۳۸۴: ۳۰)

ج- سازمان همکاری و توسعه اقتصادی: گروه متخصصان جرم رایانه ای سازمان همکاری و توسعه اقتصادی [1] در گزارش «جرم کامپیوتری- تحلیل سیاست‌های قانونی» در تعریف آن در سال ۱۹۸۶ بیان داشته‌اند که سوء استفاده از کامپیوتر ها شامل هر رفتار غیر قانونی، غیر اخلاقی یا غیر مجاز مربوط به پردازش خود کار انتقال داده هاست همچنانکه می بینیم در تعریف فوق به جای جرم رایانه ای ،عبارت سوء استفاده از کامپیوتر به کار رفته است.

د- وزارت دادگستری آمریکا؛ وزارت دادگستری آمریکا نیز تعریف ذیل را درباره جرم رایانه ای ارائه داده است: «جرم رایانه‌ای عبارت است هر اقدامی غیرقانونی که برای ارتکاب، پی جویی یا پیگرد قضائی آن، بهره برداری از دانش فن آوری رایانه ای ضروری است.» (پرویزی، ۱۳۹۲: ۶)

ه- پلیس جنایی فدرال آلمان: این پلیس جرم کامپیوتری را به ترتیب ذیل تعریف نموده است: جرم کامپیوتری در برگیرنده همه اوضاع و احوال و کیفیاتی است که در آن شکلهای پردازش الکترونیک داده‌ها، وسیله ارتکاب و یا هدف یک جرم قرار گرفته است و مبنایی برای نشان دادن این ظن است که جرمی ارتکاب یافته است.» (باستانی، ۱۳۸۳: ۲۲)

و- پلیس ژاپن: پلیس ژاپن نیز جرم کامپیوتری را به ترتیب ذیل تعریف نموده است: «جرائم متضمن اعمال توام با بی‌مبالاتی یا حوادثی که موجب تخریب عملکرد سیستم کامپیوتر یا استفاده غیر قانونی از آن باشد، جرم کامپیوتری است.» (باستانی، پیشین، ۲۳)

۴. حقوق سایبر و ویژگی‌های جرایم سایبر

در رابطه با حقوق و جهان مجازی دو حالت قابل تصور و فرض می‌باشد؛

الف- حقوق برای جهان مجازی.

ب- حقوق در جهان مجازی.

الف- منظور از حقوق برای جهان مجازی کلیه قوانینی است که مبنای وقوع آنها جهان واقعی است و لوازم وقوع جرم در جهان مجازی فراهم می‌شود. این دسته از قوانین حالتی کلی‌تر داشته و شامل، جرم رایانه ای، اینترنتی و الکترونیک می شود.

حقوق در جهان مجازی به طور مستقیم با افراد انسانی سروکار دارد و مکان و زمان در آن جاری است. از این جمله قوانین می‌توان، به سرقت اینترنتی، حمله هکری، جاسوسی اینترنتی اشاره نمود. این نوع جرایم به واسطه کلی بودن، عمومی تر بوده و موارد بیشتری را شامل می‌شوند.

حقوق در جهان مجازی قوانین و مقرراتی را شامل می شود که جهان مجازی مبنای وقوع آن است و همه چیز در آن مجازی است. این نوع قوانین را می‌توان با شهرهای زندگی دوم مرتبط دانست. در این شهرها فرد به صورت مستقیم وارد نمی‌شود و این کاراکتر آنلاین و مجازی کاربر است که به نمایندگی از او در محیط مجازی حضور می‌یابد و فرد می‌تواند خود را به جای او قرار داده و خود را در جهان مجازی حس کند. قوانین در جهان مجازی اگر چه ممکن است با قوانین جهان و واقعیت مشابهت‌هایی داشته باشند اما دارای تفاوت‌های اساسی با آن هستند و نمی‌توان رفتاری یکسان در برابر آنها داشت.

این ویژگی به ماهیت جهان مجازی بر می‌گردد. چرا که جهان مجازی اگر چه به میزان بسیار زیادی شبیه جهان واقعی است و هر روزه سعی می کند میزان مشابهت خود را با این جهان بیشتر کند اما رفتار ها، کارکردها و عملکردهای خاص خود را دارد که انجام آنها در جهان واقعی غیرممکن است. (قاجارقیونلو، ۱۳۹۱: ۶۱) بعضی از نویسندگان بیان داشته‌اند؛ امروزه معادل حقوق فن‌آوری اطلاعات را با مسامحه می‌توان «حقوق سایبر» یاد کرد که شاخص و بیانگر تحولات علمی است. (زندی، ۱۳۹۳: ۱۸) در هر حال جهان در عرصه اطلاعات و پیدایش و حاکمیت جامعه اطلاعاتی طبعاً قوانین و مقررات باید در بستر حقوق لازم در قالب حقوق انفورماتیک وحقوق اطلاعات طرح

[1]. The organisation for economic co-operation and development (OECD)

ISSN: 2538-3787
http://www.Joce.ir

شوند. امروزه حقوق فناوری اطلاعات تلفیقی از حقوق صنعتی و حقوق اطلاعات است در باب واژه شناسی حقوق فناوری اطلاعات، باید گفت ابتدا حقوق رایانه و حقوق فناوری اطلاعات به طور معادل و یکسان به کار می‌رفت. حقوق فناوری اطلاعات ناظر به تمامی شاخه‌های پیدایش یافته است. شاخه‌های حقوق مدنی مانند مسئوولیت، قراردادها ،حقوق تجارت، حقوق عمومی مانند بحث جریان آزاد اطلاعات، حقوق کیفری و بحث جرایم رایانه ای است. (زندی، پیشین، ۱۷)

۵. ویژگی‌های جرایم سایبری

می‌توان گفت که یکی از ممیزات جرایم رایانه ای با انواع جرایم سنتی، بالا بودن رقم سیاه این جرایم است که این مسئله نیز خود ناشی از ویژگی های منحصر بفرد آنها می‌باشد. برای مثال مرتکب جرایم سایبر دیگر نیازی به حضور فیزیکی در صحنه جرم ندارد و براحتی می تواند هویت خود را در فضای مجازی پنهان نماید. همچنین بسیاری از بزه دیدگان تمایل چندانی به افشای بزه صورت گرفته ندارند. نتیجه اینکه یکی دیگر از ویژگی‌های جرایم سایبری این است که پی بردن به آمار واقعی این جرایم امر ساده ای نیست. لذا تحقیقات نشان می‌دهد صرفاً ده الی پانزده درصد از جرایم رایانه ای قابل کشف می‌باشند چرا که قربانیان اغلب تمایلی ندارند اطلاعاتی ارائه دهند که به عقیده آنها می‌تواند به وجهه‌شان لطمه وارد کند یا آنکه باعث تکرار جرایم شود. (دریانی، ۱۳۸۸: ۲۸۳)

۶. حملات سایبری

اصطلاح جنگ اطلاعاتی [1] برای اولین بار توسط دکتر توماس رونا [2] در سال ۱۹۷۶ به کار گرفته شد. جنگ اطلاعاتی عبارت است از: اقداماتی که شامل استفاده از حملات سایبری به وسیلهٔ کشورها یا گروه‌های برانگیخته سیاسی، که به منظور دستیابی به اهداف سیاسی انجام می‌شود.(Andrew Lewis, 2010: 1).

جنگ سایبری را به سه گونه تقسیم بندی کرده‌اند، جنگ اطلاعاتی علیه داده‌های افراد، جنگ اطلاعاتی علیه داده‌های شرکت‌ها یا 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 کره جنوبی [3] در ژوئیهٔ ۲۰۱۱ اشاره نمود که در طی آن، اطلاعات شمارهٔ 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 حملهٔ سایبری از سوی ایران از دست داده است. در سال ۲۰۱۲ هم، اطلاعات کمیسیون دوجانبهٔ اقتصادی، بین چین و آمریکا توسط نفوذگران هندی، هک شد که در طی آن، دسترسی به اطلاعاتی، شامل تبادلات پست‌های الکترونیک بین اعضای کمیسیون دوجانبه بوده است. جدا از این، حملات سایبری [4] نیز به فعالیت‌های مجرمانه ی انجام شده از طریق اینترنت گفته می‌شود که به صورت تهاجمی و به وسیلهٔ اشخاص حرفه‌ایی، مانند نفوذگران یا بدافزارهایی ساخته شده، به منظور صدمه رساندن و ایجاد خسارت در اهداف مشخص صورت می‌گیرد. این حملات می‌تواند شامل سرقت مالکیت فکری یک سازمان، ضبط حساب‌های بانکی آنلاین، ایجاد و توزیع ویروس‌ها بر روی رایانه‌ها و سیستم‌های مخابراتی، ارسال اطلاعات کسب و کار محرمانه بر روی اینترنت و اخلال در زیرساخت‌های ملّی و حیاتی کشور باشد.

۶-۱. تروریسم سایبری

تروریسم سایبری، حاصل تلاقی تروریسم و فضای مجازی یا سایبر است. ریشه‌های مفهوم تروریسم سایبری را می‌توان در دههٔ ۱۹۹۰ میلادی جستجو کرد؛ یعنی زمانی که استفاده از اینترنت رشد فزاینده‌ای یافت و مباحثی نو ظهور تحت عنوان جامعهٔ اطلاعاتی را به وجود آورد. اوایل ۱۹۹۰ بود که آکادمی ملّی علوم آمریکا گزارش خود را در مورد امنیت سیستم‌های رایانه‌ای این گونه آغاز کرد:

«ما در معرض خطر هستیم و آمریکا روز به روز به رایانه وابسته می‌شود این امکان برای تروریست‌ها وجود دارد که با یک صفحه کلید خسارت بیشتری در مقایسه با بمب اتمی به بار آورند» (Curran, 2008: 2).

بری کالین، یکی از متخصصان حوزهٔ سایبر، تروریسم سایبری را این گونه تعریف نموده است: «سوءاستفادهٔ عمدی از سیستم، شبکه یا دستگاه‌های اطلاعاتی رایانه‌ای برای تحقق هدفی که مؤید یا تسهیل کنندهٔ مبارزه یا اقدام تروریستی است» (فلمینگ و استول، ۱۳۸۴: ۳۵).

---

1. Information Warfare
2. Thomas Rona
3. SK
4. Cyber Attacks

ISSN: 2538-3787
http://www.Joce.ir

بالاخره در تعریف این پدیده می‌توان گفت: تخریب شدید داده‌ها و سیستم‌های رایانه‌ای و مخابراتی به وسیلهٔ افعالی چون حملات سایبری یا تهدید به حمله، توسط اشخاص غیردولتی، برای ارعاب و یا اجبار دولت‌ها یا جوامع در دستیابی به اهداف سیاسی، اقتصادی، فرهنگی یا اجتماعی. در تروریسم سایبری به جای اعمال خشونت مستقیم علیه اشخاص و یا اموال فیزیکی، عملیات مرتکب باعث تخریب داده‌های دیجیتال می‌شود (Denning, 2007: 2).

بنابراین (تروریسم سایبری) را می‌توان چهره ی جدید تروریسم دانست، که گسترش تکنولوژی و خلق فضای مجازی آن را ایجاد کرده است. (فلمینگ و استول، ۱۳۸۴: ۱۴۹) به واقع تکنولوژی ابزار جدیدی را در اختیار تروریست‌ها قرارداده است که با استفاده از آن و بدون آنکه سایر اقسام تروریسم را برای آن ها در پی داشته باشد، می توانند اهداف وحشت بار خود را پی بگیرند. گسترش استفاده از این فضای مجازی که از دهه‌ی ۱۹۹۰ شدت گرفته است، امکان رسیدن تروریست‌ها به اهدافشان را بیشتر کرده است. حضور میلیون‌ها کاربر در دنیای مجازی، همراه با شرکت‌ها، کارخانجات و صنایع عمده‌ی بسیار که در بسیاری از موارد از قابلیت آسیب‌پذیری بالایی نیز برخوردار می باشند، خطر استفاده‌ی سوء از فضای مجازی را بیشتر کرده و جذابیت آن را نیز افزایش داده است. برخی سایبر تروریسم را به عنوان حملات ازقبل طراحی شده و با انگیزه های سیاسی تعریف می کنند که علیه سیستم‌های کامپیوتری، برنامه‌های کامپیوتری و اطلاعات ذخیره شده در فضای مجازی صورت می‌گیرد، با این شرط که این اقدامات منجر به خشونت علیه اهداف غیرنظامی توسط عاملان مخفی یا گروه‌های ملی گردد. (Curran, 2008: 10)

این تعریف که تعریفی نتیجه گراست، نمی تواند درست باشد، زیرا آن چیزی که سایبری بودن یک اقدام تروریستی را تعریف می‌کند، ابزار بزه تروریستی است نه نتیجه‌ی آن. بدون تردید تخریب مادی یک را یا نه، انفجار یک مرکز رایانه ای یا اقداماتی از این دست، گرچه در عمل نتیجه‌ی خود را به صورت اختلال در سیستم رایانه ای برجای می‌گذارند، اما نمی‌توانند بزه سایبری باشند. در سوی دیگر برخی معتقدند که تروریسم سایبری عبارت است از استفاده از شبکه‌ی کامپیوتر به عنوان ابزاری برای از کار انداختن زیربناهای اساسی به منظور تحت تأثیر قراردادن یا اجبار دولت یا جمعیت غیرنظامی. مراد از زیربناهای اساسی نیز سیستم‌های تأسیساتی هستند که درصورت تخریب، بر امنیت فیزیکی، امنیت اقتصادی و یا سلامتی عمومی تأثیر بگذارد، که خود شامل صنایع یا فعالیت‌های غذایی، انرژی، حمل ونقل، بانک داری، ارتباطات، دولت و یا خود فضای مجازی می‌شود. (Owen, 2008: 36)

در کنار این دو تعریف برخی تروریسم سایبری را براساس ابزار و نتیجه تعریف کرده اند. بر اساس این تعریف تروریسم سایبری عبارت است از اقدامی که با استفاده از کامپیوتر برای انجام حملات غیرقانونی و تهدید به حمل حمله کامپیوترها، شبکه ها و اطلاعات ذخیره شده‌ی الکترونیکی صورت می گیرد و منظور از آنها ایجاد رعب و وحشت در قربانی و یا وارد آوردن صدمه به او است. (جلالی، ۲۰۰۱: ۵۱) برخی دیگر نیز تروریسم سایبری یا تروریسم مجازی را عبارت می دانند از «بهره‌گیری از اینترنت و شبکه‌های رایانه‌ای و امکاناتی که این شبکه‌ها پدید می‌آورند، با هدف نابود ساختن ساختارهای زیربنایی یک جامعه مانند انرژی، حمل و نقل، فعالیت‌های دولتی و تأثیر گذاشتن بر یک دولت، شهروندان، گروهها.» (عباسی، ۱۳۸۳: ۳)

۶-۲. تروریسم سایبری و حمله به تاسیسات هسته‌ای

تروریسم سایبری نسبت به سایر اقسام تروریسم بر پایه‌ی ابزار بزه وحشت عمومی کمتری را موجب گردیده است و هر چند که همچنان یکی از دغدغه‌های مهم و اساسی متخصصان است، در میان افراد عادی کمتر خطری از ناحیه آن احساس می‌شود. راحتی استفاده از این نوع تروریسم همراه با ناشناختگی مرتکب در دنیای مجازی دو عاملی هستند که مرتکبین را نسبت به استفاده از رایانه برای اهداف تروریستی ترغیب می‌کند. سختی نشستن بر روی یک صندلی راحت و ارسال ویروس و برنامه‌های مخرب و یا هک و دستکاری در سیستم‌های رایانه ای گرچه نیاز به تخصص دارد، اما به هیچ عنوان سختی و خطر یک حمله‌ی مسلحانه به یک بانک را ندارد. «اینترنت ماهیتاً قلمروی ایده آل برای فعالیت‌های سازمان‌های تروریستی است و مزیت‌های برجسته ای را ارائه می‌کند، از جمله؛ دسترسی آسان، نبودن یا حداقل بودن مقررات سانسور یا دیگر کنترل‌های حاکم، خیل عظیم و بالقوه‌ای از مخاطبین در سرتاسر جهان، ابهام هویت در ارتباطات، جریان سریع اطلاعات، ارتباطات تعاملی، کم هزینه بودن ایجاد و نگهداری حضور شبکه ای و محیط چندرسانه ای.»

از سوی دیگر، خسارات ناشی از چنین حملاتی بسیار زیاد است. در دنیایی که اقتصاد به سیستم های رایانه‌ای وابسته است، دستکاری دراین سیستم ها و یا ارسال برنامه‌های مخرب به آنهابه سادگی می‌تواند خسارات اقتصادی فراوانی را به دولت‌ها تحمیل کند.

امروزه ابزار و روش‌های ورود غیرمجاز به سیستم‌های رایانه‌ای به صورت آنلاین در دسترس قرار دارد و علاوه بر آن کتاب‌های فراوانی در این‌باره در بازار کتاب موجود است. این اطلاعات امکان ورود غیرمجاز را برای افراد کنجکاو یا ماجراجو فراهم می‌کند. علاوه بر این اگر شخصاً از این دانش‌ها نتوان بهره برد، می‌توان به سادگی آن‌ها را با قیمت مناسب خریداری نمود. در دسترس بودن این امکانات در کنار استفاده‌ی شخصی ازدانش موجود، این امکان را برای گروه‌های ثروتمندی چون القاعده فراهم می‌کند تا با صرف هزینه‌ی نه چندان زیاد به

ISSN: 2538-3787
http://www.Joce.ir

سادگی به اهداف مورد نظرخود دست یابند. استفاده از این روش این امکان را به افراد می‌دهد تا بدون خطر باقی گذاشتن ردپایی از خود، اطلاعات لازم را از محیط‌های امنیتی بربایند و یا سیستم‌های اطلاعاتی را به سادگی از کار بیندازند.

این ویژگی خاص اینترنت که طرح ها و برنامه های بسیاری رابه صورت قابل دسترس در خود دارد، آن را آسیب‌پذیر کرده و محتویات آن را مستعد حمله قرارداده است. در کنار این حساسیت، همبستگی میلیون‌ها رایانه در فضای مجازی سایبر، این امکان را ایجاد نموده است تا در صورت ایجاد خطر، تهدیدی عمومی به وقوع بپیوندد و اثرات گسترده ای را در پی داشته باشد. تهدیدات تروریستی سایبری می‌تواند شامل موارد زیادی باشد که از جمله آن است؛ انتقال سریع تهدیدها به طیف گسترده‌ای از خاطبان یا مخاطبان خاص، تهدید تأسیسات آب و برق و...، و سیستم حمل ونقل عمومی، تهدید نهادهای تجاری و شرکت‌های فراملی، تهدید سازمان‌های بین المللی دولتی و سازمان‌های بین‌المللی غیردولتی، تهدید افراد، تهدید گروه‌های سیاسی یا دیگر واحدهای نژادی، مذهبی، یا ملیت گرا که دشمن شناخته می‌شوند، تهدید نیروهای امنیتی و تهدید دولت‌های ملی. (پاکزاد، ۱۳۸۸: ۱۶۳)

۶-۳. تروریسم هسته‌ای و رادیولوژیک

ترور و رعب و وحشت هسته‌ای زمانی ایجاد می‌شود که افراد یا گروه‌های تروریستی از مواد، ادوات و تجهیزات هسته‌ای و رادیواکتیو به عنوان وسیله‌ای برای ایجاد رعب و وحشت استفاده کنند. (رضایی، ۱۳۸۱: ۵۶) تروریسم هسته‌ای می‌تواند خطر دوگانه‌ای ایجاد نماید. از یک سو انفجار یک بمب هسته‌ای می‌تواند باعث مرگ و تخریب گسترده‌ای گردد و از سوی دیگر تهدید به استفاده از مواد رادیواکتیو قرار دارد که می‌تواند با طرح احتمال استفاده از این مواد، هراس گسترده‌ای را در جامعه رقم بزند. در حال حاضر هزاران رآکتور هسته‌ای در کشورهای پیشرفته وجود دارد که لزوماً تمامی آن‌ها از امکانات لازم برای غیرقابل دستیابی کردن و حفظ ایمنی خود برخوردار نیستند. دستیابی به این مواد ازسوی تروریست‌ها، تهدیدی است که درصورت عملی شدن می‌تواند زندگی هزاران نفر را به خطر اندازد و باعث اخلال در ساختارها و خدمات عمومی جامعه گردد. علاوه بر این، آلودگی محیطی ناشی از این مواد نیز قابل توجه است که محیط زیست رادر معرض خطر جدی آلودگی قرار می‌دهد. خطر دستیابی تروریست‌ها به ابزارهای رادیولوژیک ومواد هسته‌ای با فروپاشی شوروی وکاهش امنیت رآکتوارهای هسته‌ای آن بیش‌تر شده است. از سوی دیگر انفجار تأسیسات هسته‌ای چرنوبیل و خسارات ناشی از آن، خطرات ناشی از این مواد را به خوبی نشان داد. این مورد همراه با مورد نخست که دستیابی تروریست‌ها به مواد هسته‌ای و رادیواکتیو را در بازار سیاه موجب می‌گردد، خود غدغه‌ای را در این باره موجب گردیده است که وحشت از تروریسم هسته‌ای را برای بشر زنده نگه‌داشته است.

خطرات استفاده از این مواد هسته‌ای نسبت به تروریسم شیمیایی و بیولوژیک به مراتب بیشتر است (همان: ۶۷)، اما ازآن‌جایی که این خطر خود تروریست‌ها را نیز در برخواهد گرفت، گونه‌ای امیدواری را برای عدم استفاده از این مواد ایجاد می‌کند. در کنار هراس تروریست‌ها از استفاده از این ابزارها، با توجه به غیرقابل کنترل بودن پیامدهای آن نیز نبود دانش کافی برای به‌کارگیری مواد هسته‌ای، می‌توان مورد سومی را نیز اضافه کرد و آن اینکه تروریست‌ها انسان هستند. این انسان‌ها گرچه در بسیاری از موارد قواعد اخلاقی را نقض کرده و می‌کنند، اما بی‌تردید همچنان بقایایی از اصول اخلاقی را می‌توان در وجود آن‌ها دید و این عنصر مانع از اجام هر رفتار خشونت بار و ویرانگری توسط آن‌ها می‌گردد. خواه اینکه تروریست‌ها همچنان از یک بقایای تعهد اخلاقی بهره ببرند، یا اینکه به واقع دسترسی به وسایل هسته‌ای و رادیولوژیک نداشته باشند، تاکنون نمونه‌ای از تروریسم هسته‌ای مشاهده نشده است. وحشت ناشی از احتمال استفاده از این مواد نیز به تجربه جهانی استفده آمریکا از مواد هسته‌ای در جنگ جهانی دوم بر می‌گردد که خسارات انسانی بسیاری را ایجاد کرد. از سوی دیگر، اصطلاح تروریسم هسته‌ای در حال حاضر برای تروریست‌ها امتیاز آور و برای مردم وحشت‌زا است. گرچه گزارشات مربوط به اقدامات تروریستی و تلاش گروه‌های مختلف برای انجام چنین اقداماتی برای رسانه‌ها امری عادی و معمولی در طول شبانه روز است، با این حال تروریسم هسته‌ای کابوسی است که گرچه تاکنون تنها به شکل تهدید بوده است، اما ترس ناشی از آن به اندازه‌ای است که سناریوی وحشتناکی را در ذهن شهروندان شکل داده است. این تهدید گرچه تاکنون به اجرا در نیامده است و به دشواری بتوان ظهور آن را در زمانی کوتاه در عالم خارج دید، با این حال سخن گفتن از آن و بررسی ابعاد مختلف آن می‌تواند ما را در مواجهه با آن آماده‌تر سازد. سابقه توجه به ضرورت و پیشگیری از تروریسم هسته‌ای درعرصه بین‌المللی به سال‌های پایانی دهه‌ی ۱۹۶۰ برمی‌گردد و از آن پس به اندازه‌ای گسترش یافته است که در حال حاضر به بحث مهمی در عرصه‌ی مبارزه با تروریسم تبدیل گردیده است. (رضایی، ۱۳۸۱: ۵۷)

اما بررسی تعاریف ارائه شده از تروریسم توسط حقوق‌دانان بیانگر این مطلب است که این تعاریف به طور کلی بر اساس یک دیدگاه سنتی از تروریسم که همان به کارگیری ابزار خشونت آمیز برای رسیدن به اهداف سیاسی است، شکل گرفته‌اند و حال آن که تروریسم هسته‌ای به عنوان یکی از اشکال نوین تروریسم صرفاً ارتکاب خشونت هسته‌ای یا تهدید به آن علیه دولت‌ها یا افراد ملت نیست و به مراحل قبل از آن نیز اشاره دارد، زیرا با توسل به جرم انگاری این اعمال مقدماتی تلاش می‌شود تا تروریست‌ها از دستیابی به مواد رادیو اکتیو و تسلیحات هسته‌ای ناکام بمانند و امنیت هسته‌ای مخدوش نگردد. (غنی‌کله‌گو، ۲۰۰۵: ۱۷)

فقه، حقوق و علوم جزا ، شماره ۷ ، بهار ۱۳۹۷، ص ۵۸- ۴۸

ISSN: 2538-3787
http://www.Joce.ir

گرچه جرم انگاری تروریسم هسته‌ای در معنای خاص آن را می‌توان نوعی جرم انگاری پیش دستانه دانست که تاکنون فرصت و مجالی برای ظهور از سوی گروه‌های تروریستی نیافته است، با این حال خطرات گسترده ناشی ازاستفاده‌ی احتمالی ازآن، دولت‌ها را بر آن داشته است تا به مقوله‌های پیشینی آن نیز توجه کنند. استفاده از سلاح‌های هسته‌ای متضمن دستیابی و دسترسی به آن‌هاست و دسترسی نیز به عنوان یک عمل پیشینی، در بردارنده‌ی تملک، خرید و فروش است. بدین ترتیب در ضمن یک جرم انگاری پیش دستانه، مقوله‌های دیگری نیز به عنوان عوامل پیشینی با مانع قانونی مواجه شده‌اند.

ISSN: 2538-3787
http://www.Joce.ir

نتیجه‌گیری

اساساً گسترش حملات سایبری فرامرزی، امنیت سایبری را به یکی از نگرانی‌های عمده جهانی در قرن بیست و یکم تبدیل کرده است و به همین دلیل، تدوین یک سند حقوقی بین‌المللی برای مقابله با این حملات، تبدیل به یک نیاز و خواسته جهانی گردیده است. در واقع، این موضوع تبدیل به یک دغدغه مشترک بشری شده است؛ صرف نظر از این‌که کجا زندگی می‌کنیم و یا چگونه فکر می‌کنیم. در واقع حملات سایبری، پدیده‌ای نوظهور در میان جنگ افزارهای مدرن محسوب می‌شوند. این حملات، صلح و امنیت جهانی را تهدید می‌کنند و نیاز به تعریف قواعد جدید و منطبق با اصول حقوق بین‌الملل و منشور سازمان ملل متحد را گوشزد می‌نماید. از سوی دیگر، به لحاظ حقوق بین الملل، اقدامات متقابل دولت‌ها در قبال حملات سایبری یک گروه و یا یک کشور، در رویه قضایی مورد پذیرش قرار گرفته است. اما با وجود این پذیرش، هنوز توافق زیادی در رابطه با نقش و جایگاه اقدامات متقابل صورت نگرفته است. در واقع با توجه به ماهیت ویژه حملات سایبری در فضای سایبر از جمله بدون مرز بودن فضای سایبر، کاهش هزینه جرم، امکان وارد آوردن خسارت مالی بدون آسیب‌های جسمی، تامین راحت امکانات و عوامل مورد نیاز، امکان هماهنگی لحظه‌ای در سراسر جهان با ضریب اطمینان بالا، امکان جذب حامیان از سراسر جهان و اینکه اثر عمل نقض در دنیای واقعی قابل رویت در دنیای خارج است پیدا کردن ریشه و مبنای نقض در اثر حملات سایبری و عامل آن در شبکه عنکبوتی اینترنت به سختی قابل ردیابی است و از این رو، تشخیص دولت واقعی مسئول حمله سایبری به ندرت امکان پذیر است. بنابراین باید تاکید کنیم که کشور زیان دیده‌ای که مورد حمله سایبری قرار گرفته است، ابتدا باید حقوق بنیادین بشر را مورد ملاحظه قرار دهد. دیگر اینکه در هر اقدام تلافی جویانه‌ای بایستی حقوق بشر دوستانه و قواعد آن مورد لحاظ قرار گیرد.

ISSN: 2538-3787
http://www.Joce.ir

منابع و مراجع

[۱] باستانی، برومند (۱۳۸۳)؛ جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، تهران: انتشارات بهنامی.

[۲] جلالی فراهانی، امیرحسین (۱۳۸۹)؛ کنوانسیون جرایم سایبر و پروتکل الحاقی آن، تهران: انتشارات خرسندی.

[۳] جلالی، محمود (۲۰۰۱)، تروریسم از دیدگاه حقوق بین‌الملل با تاکید بر حادثه ۱۱ سپتامبر ۲۰۰۱.

[۴] حسنی، علیرضا و پهلوانی فرد، احسان (۱۳۹۳)؛ قانون جرایم رایانه ای در حقوق ایران و حقوق بین الملل؛ تهران: مجمع علمی و فرهنگی مجد.

[۵] خداقلی، زهرا (۱۳۸۴)، جرائم کامپیوتری، تهران: انتشارات آریان.

[۶] خرم آبادی، عبدالحمد (۱۳۸۴)؛ جرائم فناوری اطلاعات، تهران: انتشارات دانشگاه تهران.

[۷] دریانی، محمد حسن (۱۳۸۸)؛ گزیده‌های اخبار جرایم سایبری، ترجمه احمد رحیمی مقدم، تهران، نشر روزنامه رسمی جمهوری اسلامی.

[۸] زندی، محمدرضا (۱۳۹۳)، تحقیقات مقدماتی در جرائم سایبری، تهران: انتشارات جنگل، چاپ اول.

[۹] شیتز، میشل (۱۳۸۸) ، جرائم رایانه ای، مترجم، تراب زاده، تهران: انتشار کارآگاه.

[۱۰]فلمینگ، پیتر. و استول، مایکل (۱۳۸۴)، سایبر تروریسم: پندارها و واقعیت‌ها، ترجمه: بقایی هامانه، اسماعیل. و پور اردکانی، عباس باقر چاپ دوم. تهران: نشر نی.

[۱۱]قاجارقیونلو، سیامک (۱۳۹۱)، مقدمه حقوق سایبر؛ تهران: انتشارات میزان.

[۱۲]ملکی، عقیل (۱۳۸۸)، جرائم مرتبط با فناوری‌های برتر، ترجمه مهدی اعلانی، تهران: انتشارات پلیس بین‌الملل ناجا.

[۱۳]میلر؛ لورا (۱۳۹۴)، فضای سایبری، ترجمه فاطمه قره باقی، تهران: انتشارات سبزان.

[۱۴]پرویزی، رضا (۱۳۹۲)؛ «جرم‌های رایانه‌ای»، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فن آوری اطلاعات، قوه قضائیه، معاونت حقوقی و توسعه قضائی، سلسبیل ۱۳۹۲.

[۱۵]جلالی فراهانی، امیرحسین (۱۳۸۵)؛ «تروریسم سایبری»، نشریه حقوق اسلامی، ۱۳۸۵،سال سوم، شماره ۱۰ زمستان ۱۳۸۵.

[۱۶]حیدری، علی مرادی (۱۳۹۰)؛ «شناخت جرایم رایانه ای از منظر اسناد بین المللی و قوانین داخلی»، مجله فقه و حقوق ارتباطات، پاییز و زمستان ۱۳۹۰، شماره ۱.

[۱۷]رضایی، صالح (۱۳۸۱)، «حقوق بین‌الملل و مبارزه با تروریسم هسته‌ای»، مجله نگاه، سال سوم، شماره ۳۱،بهمن ماه ۱۳۸۱.

[۱۸]طارمی، محمد حسین (۱۳۸۷)، «فضای سایبر: آسیب‌ها و مخاطرات»، مجله راه آورد نور، بهار ۱۳۸۷، شماره ۲۲.

[۱۹]عباسی، مهدی (۱۳۸۳)، «اینترنت؛ ابزار سیاست (تروریسم مجازی؛ تهدیدی برای آینده)»، نشریه فرهنگی و فناوری، سال اول ، شماره سوم، دی و بهمن ۱۳۸۳.

[۲۰]غنی کله‌کو، کیوان (۲۰۰۵)، «بررسی تروریسم هسته‌ای با تاکید بر کنوانسیون بین‌المللی سرکوب اعمال هسته‌ای مصوب ۲۰۰۵»، فصلنامه رویکرد. شماره ۵.

[۲۱]پاکزاد، بتول (۱۳۷۵)، «جرایم کامپیوتری»، پایان نامه کارشناسی ارشد دانشگاه شهید بهشتی، دی ماه ۱۳۷۵.

[۲۲]صدیق بنای ،هلن ؛ سایبراسپیس، پایگاه اینترنتی آفتاب www.aftab.ir مورخ ۱۳۹۱/۲/۲۳

[23] Curran, Kevin, Concanon, Kevin, McKeever, Sean, Cyberterrorism Attacks, in Jonczewski, Lech, J and Colardik, Adrew. M (Eds), CyberWarfare and Cyber terrorism, New York: Information Science Reference, 2008.

[24] Denning, Dorothy E, A View of Cyberterrorism Five Years Later, Chapter 7 in Internet Security: Hacking, Counterhacking, and Society (K. Himma ed.), Boston: Jones and Bartlett Pub, 2007,

[25] Owen, Robert. S, Infrastructure of Cyberwarfare, in Jonczewski, Lech, J and Colardik, Adrew, M(eds), CyberWarfare and Cyberterrorism, New York: Information Science Refernce, 2008.

[26] Andrew Lewis. J., 2010, The Cyber War Has Not Begun, Center for Strategic and International Studies. 1-4. Available at:

ISSN: 2538-3787
http://www.Joce.ir

http://csis.org/files/publication/100311_TheCyber WarHasNotBegun.pdf.retrievedat: 9/2/2013.